Universidad Nacional Autónoma de Nicaragua
UNAN – León

Facultad de Ciencias

Departamento de Computación

Tema:

IMPLEMENTACION DE UNA RED AVANZADA SOBRE IPV6 EN LAS UNIVERSIDADES PERTENECIENTES A RENIA

Monografía para optar al Titulo de Ingeniero en Sistemas de Información

Autores:

- **Br. CLAUDIA ELIZABETH MARTINEZ DARCE**
- **Br. BENITA DEL SOCORRO MAYORGA MAYORGA**
- **Br. ARGEO ALEXANDER ZAVALA PAREDES**

Tutor:

Ing. Marcos Antonio Carcamo Narváez

León, Nicaragua
Viernes 26 de Mayo de 2006

DEDICATORIA

A Jesús el Hijo de Dios por ser mi sentido de vida.

A quienes me enseñaron a nadar contra la corriente, mis amados padres, Maria de Lourdes Darce Balmaceda y Andrés Martínez, por sembrar en mí la semilla de la sensibilidad y la comprensión, por tu cariño, amor y por enseñarme a que debemos tener la fortaleza de continuar hacia adelante no importa las circunstancias que la vida nos presenta.

A mis hermanos por todos los juegos, conversaciones y momentos vividos, juntos, aún en la distancia. A mis compañeras que siempre han estado junto a mí en esta carrera.

A todas las personas que han creído en mí

Muchas gracias…

Claudia Elizabeth Martínez Darce

A Dios mi padre celestial que siempre esta conmigo cuando lo necesito, a mi madre Magali Mayorga que me apoyado incondicionalmente, a una persona que considero mi padre Juan Prado, a mi esposo Michael Treminio que me ha dado su apoyo, y lo mas lindo de mi vida, a mi hermana y a mi suegra, que con su ayuda me ha permitido culminar mi carrera y sobre todo ha mi Hija: Maykeling Xiomara Treminio Mayorga que ha sido lo mas lindo que Dios me ha dado.

Quiero agradecer a mis compañeros de monografía (Claudia Elizabeth Martínez Darce, Argeo Alexander Zavala Paredes), por su comprensión, a todos los que me apoyaron en esta universidad y creyeron en mi capacidad (Msc. Octavio Guevara, Ing Marcos Carcamo).

Benita del Socorro Mayorga Mayorga.

A mis padres Maria Auxiliadora paredes y Argeo Zavala por su inmenso amor, comprensión, apoyo durante toda mi vida y por creer en mí siempre. A la mona de mi hermana Maria Esther Zavala por su cariño incondicional, por sus conversaciones y compañía desde pequeños.

A todos mis amigos que me han entregado su amor, estando siempre junto a mi en los momentos difíciles, gracias por su apoyo siempre.

A todas las personas que han creído en mí…

Argeo Alexander Zavala Paredes

AGRADECIMIENTO

Estamos profundamente agradecidos con nuestro querido Tutor guía, Marcos Antonio Carcamo Narváez, por su paciencia, apoyo, confianza, dirección y entrega durante todo el tiempo que tenemos de conocernos.

Al Ing. Peter Pettersson de la UNA, por su gran paciencia y apoyo brindado durante nuestra labor monográfica, tanto en el área teórica como en la parte práctica, por su comprensión y tolerancia.
Gracias……

Al Lic. Derman Zepeda de UNAN-Managua por su apoyo en el área técnica, especialmente a Juan Navaz, Edison Cuevas quienes como colegas han tenido la gran voluntad y disposición de ayudarnos a pesar de la distancia.

Y a cada uno de nuestros profesores que ayudaron en nuestra formación superior, especialmente a Máximo Guido, Álvaro Altamirano, Santiago Molina, Néstor Castro y Rina Arauz.

A las autoridades facultativas de Ciencias, especialmente al Msc. Octavio Guevara, que con su respaldo y comprensión nos brindo su ayuda en los momentos más difíciles de nuestra vida universitaria.
Infinitamente **Gracias.**

A todas la directiva del Proyecto TIC de UNAN-León por su apoyo y colaboración para la realización de esta investigación.

A nuestros amigos, que por medio de las discusiones y preguntas, nos hacen crecer en conocimiento, especialmente al grupo de Educación a Distancia y al grupo de Chat Multiusuario.

Y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de esta investigación, hacemos extensivo nuestros más sinceros agradecimientos. A Doña Mariana de la Hemeroteca, Al personal de Seguridad (Don Cesar, Don Ernesto) y a Doña Fran.

Por último queremos dar las gracias a todos aquellos que nos devolvieron una sonrisa, a todos aquellos que nos ofrecieron un pan en tiempos difíciles, a todos aquellos que han puesto de su parte para que el trajín diario sea más llevadero y muy en especial a la vida que, como dijera Violeta Parra, me ha dado tanto....

CONTENIDO

1. INTRODUCCION 1
2. ANTECEDENTES 3
3. JUSTIFICACION 4
4. OBJETIVOS 5
4.1 Objetivo General 5
4.2 Objetivos Específicos 6
5. MARCO TEORICO 7
5.1 WAN 7
5.2 ROUTER 8
5.3 INTERNET 9
5.4 INTERNET 2 9
5.5 INTERNET E INTERNET 2 10
5.6 DEFINICIÓN DE DIRECCIONES IP 12
5.7 IPV4 12
5.8 NAT "NETWORK ADDRESS TRANSLATION" 14
5.9 ENRUTAMIENTO SOBRE IPV4 15
5.9.1 Protocolos de enrutamiento 15
5.9.2 Configuración Básica de Ruteadores CISCO 16
5.10 IPV6 21
5.10.1 ¿Por qué IPv6 y no IPv5? 22
5.10.2 Diferencias entre IPv4 e IPv6 22
5.10.3 Ventajas de IPv6 23
5.10.4 Desventajas de IPv6 24
5.10.5 Direcciones IPv4 y sus equivalentes en IPv6 24
5.10.6 Principales características del nuevo IPV6 25
5.10.7 Funcionalidades de IPv6 27
5.10.8 Notación para las direcciones IPv6 28
5.10.9 Tipos de Direcciones 30
5.10.10 Identificación de los tipos de Direcciones 31
5.10.11 Número de direcciones disponibles en Ipv6 32
5.10.12 Asignación de las nuevas direcciones IPv6 a los usuarios 33
5.10.13 Estructura de un paquete IPv6 34
5.11 TRANSICIÓN DE IPV4 A IPV6 37
5.11.1 Mecanismos empleados 37
5.11.2 Formas en las cuales pueden ser usados los Túneles 38
5.11.3 Diferencias entre las dos técnicas de Tunneling 38
5.12 INSTALACIÓN Y CONFIGURACIÓN DE UN ROUTER CON SOPORTE IPV6 SOBRE LINUX 39
5.12.1 Cisco IOS recomendados para integrar IPV6 en la red 40
5.12.2 Pasos a seguirse en la configuración del router 3660 41
5.12.3 Pasos para verificar la configuración de Router 41
5.13 APLICACIONES DE IPV6 43
6. METODOLOGÍA DE IMPLEMENTACIÓN 44
6.1 SITUACION TECNICA ACTUAL DE GEANT Y CLARA 44
6.2 ANÁLISIS DE LA SITUACION ACTUAL DE RENIA 48

6.2.1 Entrevistas con los principales impulsores de la red 49
6.2.2 Informe Reuniones RENIA 51
6.2.3 Topologías Analizadas en RENIA 55
6.3 ESPECIFICACIÓN DE REQUISITOS DE LA RED 58
6.3.1 Introducción 58
6.3.2 Descripción General 60
6.4 DISEÑO 61
6.4.1 Diseño de la Red 61
6.4.1.1 Diseño Lógico 61
6.4.1.1.1Diseño Lógico General 61
6.4.1.1.2Diseño Lógico de la conexión entre RENIA y CLARA 61
6.4.1.1.3Diseño Lógico del Backbone Nacional de RENIA 62
6.4.1.2 Diseño Físico 63
6.4.2 Diseño de Direcciones 65
6.5 CONFIGURACIÓN DE ENRUTAMIENTO DE RENIA A RED CLARA 66
6.6 CONFIGURACIÓN BÁSICA DE LOS PUNTOS CONECTADOS A RENIA 73
6.6.1 Guía para realizar actualización de IOS en equipos Cisco 73
6.6.2 Configuración de routers RENIA para el enlace Ipv6 a UNAN-Managua ... 74
6.6.3 Pruebas de verificación del túnel Ipv6 entre UNAN-Managua-RENIA. 75
6.6.4 Configuración de un Router Linux con Suse10 en Ipv6 77
6.6.5 Creación y Configuración del túnel 6to4 para transmitir paquetes IPv6 en Servidor de UNAN-León 86
6.6.6 Configuración del túnel en el Router de Renia hacia el túnel en el servidor Router de León 93
6.6.7 Pruebas de verificación del túnel Ipv6 entre UNAN-León-RENIA. 93
7. CONCLUSIONES 95
8. RECOMENDACIONES 96
9. ANEXOS 86
9.1 Anexo 1: Noticia 86
9.2 Anexo 2: Topología idónea 87
9.3 Anexo 3: Configuración del switch 3750 88
9.4 Anexo 4: Característica de Router Cisco 3660 93
9.5 Anexo 5: Fotos 94
9.6 Anexo 6: Glosario 98
10. BIBLIOGRAFIA 102
10.1 FUENTES BIBLIOGRAFICAS: 102
10.2 FUENTES DE INTERNET: 102
10.3 OTRAS FUENTES 102

1. INTRODUCCION

Entre los años 70 y 90, los equipos informáticos estaban conectados a alguna de las múltiples redes independientes que existían entonces. Estas redes estaban separadas y formaban islas incomunicadas entre sí. IP conecta todas estas redes aisladas en una gran red unificada, que hoy conocemos como Internet. IP son las siglas de "Internet Protocol" (protocolo entre-redes). El protocolo fue diseñado en los años 70 con el fin de interconectar redes entre sí.

Actualmente esta red utiliza mayoritariamente la versión 4 del protocolo de Internet. Sin embargo, el gran número de usuarios, dispositivos, aplicaciones, servicios, y en general el éxito de Internet en si misma, esta llevando la versión 4 a sus limites (Se habla de escasez de direcciones). Por ello se comenzó, en los años 90, la búsqueda de un sustituto, el cual permitirá la continua evolución de Internet, y así surgió IPv6, la versión 6 del protocolo de Internet.

Hoy IPv6 esta empezando a ser una realidad. Todas las redes de Investigación y Educación del mundo soportan IPv6, e incluso algunos grandes operadores.
Recientemente, en Nicaragua se ha incrementado la demanda de la comunidad universitaria de servicios avanzados. En repuesta a este reto las universidades del país se han propuesto asociarse con la meta de lograr tener mejores servicios costo-efectivos, aprovechar economías de escala y el costo de oportunidad.

Las cuatro universidades públicas (UNAN León y Managua, UNA, UNI), conformaron hace tres años la Red Nicaragüense de Internet Avanzada (Renia), de la que hasta hoy se ven sus beneficios, uniéndose últimamente la UPOLI y la UCA.

La Red Nicaragüense de Internet Avanzada (RENIA), representa los intereses comunes de la comunidad académica y de investigación, en el desarrollo de la siguiente generación de servicios de comunicación, utilizando las tecnologías de Internet, más robustas y de alta calidad, conocidas como Internet de segunda generación.

RENIA forma parte de la RedCLARA (Cooperación Latinoamericana de Redes Avanzadas), a través de un enlace a dicha Red y RedCLARA a su vez nos conecta con las Redes Académicas del mundo mediante la red paneuropea GÉANT, utilizando un enlace dedicado de alta velocidad: 600 universidades e institutos de investigación en América Latina están ahora conectados a más de 3.500 instituciones en Europa y a muchas más en todo el mundo.

La conexión de las redes paneuropea y latinoamericana forma parte de un proyecto de la Unión Europea denominado ALICE (América Latina Interconectada Con Europa), que está coordinado por DANTE, una asociación que integra varias redes de investigación europea.

El pertenecer a la nueva RedCLARA permite que por primera vez los investigadores del país y de la región puedan trabajar en-línea en iniciativas conjuntas, promoviendo un espíritu de colaboración entre las distintas naciones.

RENIA es el esfuerzo de las universidades nicaragüenses por mantener el liderazgo en el desarrollo de las TIC en nuestro país, es el prototipo de red de investigación y educación del futuro, es vital para promover el desarrollo, la inclusión de nuestro país y la reducción de la brecha digital.

2. ANTECEDENTES

El protocolo de IPng representa la evolución de muchas propuestas de IETF diferentes y grupos activos enfocada en desarrollar un IPng. Representa encima de tres años de esfuerzo enfocados en este tema. Una historia breve sigue:

Por el invierno de 1992 la comunidad de Internet había desarrollado cuatro propuestas separadas para IPng. Éstos eran "CNAT", "IP Encaps", "Nimrod", y "CLNP Simple". En diciembre de 1992 tres nuevas propuestas surgieron; "El P Internet Protocolo" (PIP), "El Protocolo de Internet Simple" (SIP) y "TP/IX". En la Primavera de 1992 el "CLNP Simple" evolucionó en "TCP y UDP con las Direcciones más Grandes" (TUBA) e "IP Encaps" evolucionó en "la Dirección de IP Encapsulation" (IPAE).

Por el otoño de 1993, IPAE se unió con SIP todavía manteniendo el nombre SIP. Este grupo después unido con el PIP y el grupo activo resultante se llamó "Internet Protocolo Ventaja Simple" (SIPP). Aproximadamente al mismo tiempo el TP/IX el Grupo Activo cambió su nombre a "Arquitectura Común para el Internet" (CATNIP).

El área de directores de IPng hizo una recomendación para un IPng en julio de 1994.
Se adopta SIPP, se cambia el tamaño de direccionamiento a 128 bits y se renombra como Ipv6.

Como fase adicional, podemos añadir la constitución oficial en julio de 1999, del “Ipv6 forum” o foro Ipv6, que ha implicado en un plazo de tan solo 6 meses un importante crecimiento respecto al fomento, promoción, uso y aplicación del protocolo con adopciones tan importantes como las realizadas por OTAN, ETSI, UMTS, 3GPP, o la comunidad europea.

Entre el 13 y 16 de Marzo del 2000, en Telluride (colorado-U.S), se celebro el primer congreso internacional de Ipv6 en Norte América (Global Ipv6 Summit), organizado por el Foro Ipv6.

En el 2004 se llevaron a cabo dos eventos Transcendentes:

1. Lanzamiento del Servicio Global de Ipv6. (Brucelas, Bélgica).
2. Futuro de la sociedad del conocimiento (Haya, Holanda)

En Latinoamérica, en marzo y octubre del 2004 se formalizo el trabajo que llevan a cabo varias universidades e instituciones, con la integración del grupo de trabajo Ipv6 para Latinoamérica y el caribe con siglas en Ingles “LAC Ipv6 TF”, respaldado por LACNIC (Registro de direcciones de Internet para América Latina y el caribe), y varios NICs (Centros de Información de la Red) nacionales e institucionales.

Es importante mencionar que en el 2006 Ipv6 marca un paso fundamental ya que las redes experimentales pasan necesariamente a ser redes de producción, con la ayuda de acciones que se están realizando.

3. JUSTIFICACION

- Por el poco rendimiento que ofrece IPV4 en cuanto al agotamiento de las direcciones, nos vemos en la necesidad de implementar el nuevo protocolo de Internet (IPV6) por tener mayor calidad de servicios.

- A nivel mundial se ha utilizado IPV4, pero IPV6 por ser una nueva tecnología, solo en la mayoría de las Universidades de los países industrializados se ha implementado.

- Implementar IPV6 para que los usuarios dispongan de la mejor tecnología en sus accesos privados y públicos.

- Es importante utilizar protocolo sobre IPV6, por ser una tecnología con mayor velocidad en redes y así nuestra universidad avanzaría en tecnología de punta para el desarrollo de la educación a distancia.

- La Universidad cuenta con la infraestructura para facilitar la conexión a Internet.

- Es necesario para los docentes, estudiantes y trabajadores de la Universidades contar con herramientas para intercambio de información más rápida y efectiva con fines de investigaciones académicas.

- La Internet actual no es un medio apto para dar el salto tecnológico que se necesita.

4. OBJETIVOS

4.1 Objetivo General

- Implementar una Red Avanzada sobre IPv6 de tal forma que interconecte a todas las Universidades pertenecientes a RENIA

4.2 Objetivos Específicos

- Generar documentación que sirva a las instituciones integradas al proyecto RENIA.
- Investigar y probar las implementaciones de IPv6.
- Tener experiencia en la configuración de router utilizado en IPv6.
- Ayudar en la transición de IPv4 a IPv6.
- Impulsar el uso y desarrollo de IPv6 y sus aplicaciones en UNAN-León.
- Buscar ser un ámbito de integración, comunicación y discusión, al servicio de los objetivos de la educación, la investigación y las transformaciones de la sociedad.
- Comprender las principales razones para cambiar IPv4.
- Presentar las principales funcionalidades de IPv6.
- Presentar el formato de los datagramas IPv6.
- Proponer la implementación de otros servicios avanzados sobre IPV6.

5. MARCO TEORICO

5.1 WAN

Las WAN es un acrónimo de Wide Área Network que en inglés significa (red de área amplia). Un ejemplo de este tipo de redes sería Red IRIS, el mismo Internet o cualquier red en que no esté en un mismo edificio todos sus miembros. Opera en la capa física y de enlace del modelo de referencia OSI. Son entornos complejos que incorporan múltiples medios, múltiples protocolos, e interconexión con otras redes, como Internet.
El crecimiento y la facilidad de administración de estos entornos de red se logran mediante la compleja interacción de protocolos y funciones.

Cuando una estación final local desea comunicarse con una estación final remota, la información se debe enviar a través de uno o más enlaces WAN.

La comunicación WAN a veces se denomina servicio, porque el proveedor de la red a menudo les cobra a los usuarios por los servicios WAN que proporciona.

Modelo jerárquico de diseño WAN

Las ventajas del uso de un modelo jerárquico incluyen las siguientes:

- Escalabilidad
- Facilidad de implementación
- Facilidad para el diagnóstico de fallas
- Capacidad de predicción
- Soporte de protocolo
- Facilidad de administración

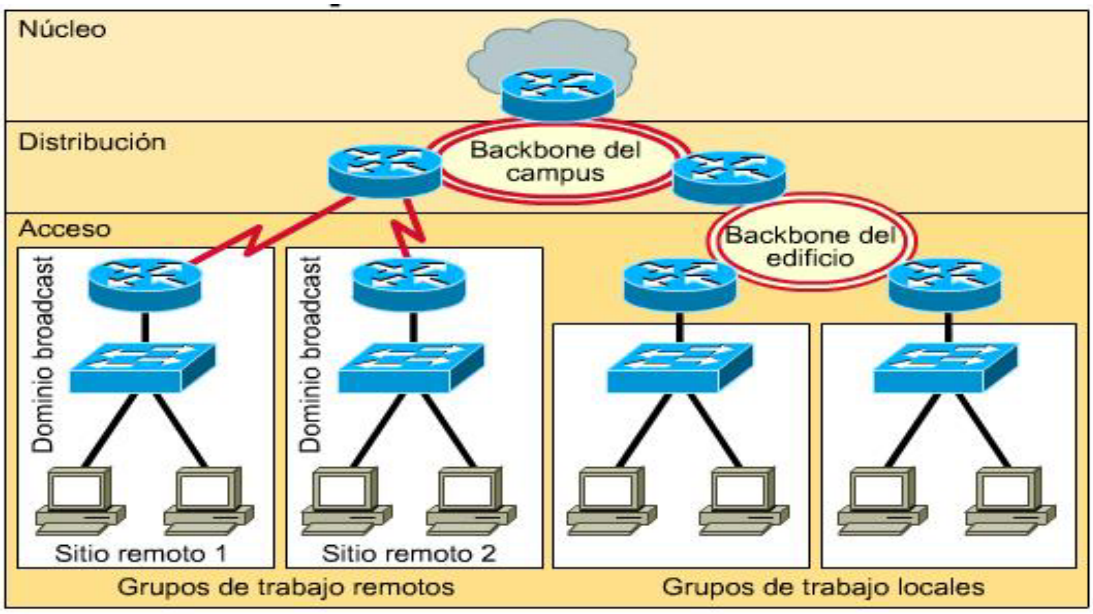
Tres capas de diseño jerárquico WAN

Un diseño de red jerárquico incluye las siguientes tres capas:

1. La **capa núcleo,** proporciona transporte óptimo entre sitios. Proporciona conexiones rápidas de área amplia entre sitios separados por grandes distancias geográficas, uniendo varias redes de campus en una WAN corporativa o empresarial. Los enlaces núcleo normalmente son punto a punto y rara vez hay hosts en la capa núcleo. Sus funciones son: Rutas redundantes, compartir la carga, convergencia rápida y uso eficiente del ancho de banda.

2. La **capa de distribución**, que brinda conectividad basada en políticas. Ofrece servicios de red a múltiples LAN dentro de un entorno WAN. Esta capa es donde se encuentra la red backbone de la WAN, y normalmente se basa en Fast Ethernet. Esta capa se implementa en grandes sitios y se usa para interconectar edificios. Sus funciones son: Control de acceso a los servicios, definir las métricas de ruta y control de publicaciones de red.

3. La **capa de acceso**, que proporciona acceso para los usuarios y grupos de trabajo a la red. Normalmente es una LAN o grupo de LANs, Ethernet o Token Ring, que ofrece a los usuarios acceso frontal a los servicios de red. La capa de acceso es donde casi todos los hosts se conectan a la red, incluyendo servidores de todo tipo y estaciones de trabajo de usuario. Sus funciones son: Control de acceso a los servicios, definir las métricas de ruta y control de publicaciones de red.



Para conectar redes WAN de relativa baja velocidad, como ISDN, una línea T1, Frame Relay, etc se utilizan los llamados Routers.

5.2 ROUTER

Un router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de ordenadores/computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Los routers son más ``inteligentes" que los switches, pues operan a un nivel mayor lo que los hace ser capaces de procesar una mayor cantidad de información. Esta mayor inteligencia, sin embargo, requiere más procesador, lo que también los hará más caros. A diferencia de los switches y bridges, que sólo leen la dirección MAC, los routers analizan la información contenida en un paquete de red leyendo la dirección de red.

Los routers leen cada paquete y lo envían a través del camino más eficiente posible al destino apropiado, según una serie de reglas recogidas en sus tablas. Un router también sabe cuándo mantener el tráfico de la red local dentro de ésta y cuándo conectarlo con otras LANs, es decir, permite filtrar los broadcasts de nivel de enlace. Un router dispondrá de

una o más interfases de red local, las que le servirán para conectar múltiples redes locales usando protocolos de nivel de red. Eventualmente, también podrá tener una o más interfases para soportar cualquier conexión WAN.

5.3 INTERNET

Es una red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.

Cuando se dice red de redes se hace referencia a que es una red formada por la interconexión de otras redes menores.

Algunos de los servicios disponibles en Internet aparte de la Web son el acceso remoto a otras máquinas (SSH y telnet), transferencia de archivos (FTP), correo electrónico (SMTP), boletines electrónicos (news o grupos de noticias), conversaciones en línea (IRC y chats), mensajería instantánea (MSN Messenger, ICQ, YIM, AOL, Jabber), transmisión de archivos (P2P, P2M, Descarga Directa), etcétera.

5.4 INTERNET 2

Internet 2 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.

Actualmente, es común que el término Internet 2 se asocie como nombre genérico para identificar las redes nacionales avanzadas educativas y de investigación, National Research and Education Network (NREN, por sus siglas en inglés) que tuvieron su origen en los Estados Unidos, cuando se creó una red alternativa a la Internet comercial, para permitir el intercambio y colaboración de investigación y educación entre diversas instituciones educativas.

En ese sentido, el término Internet 2 es, en realidad, el nombre del consorcio de las 206 universidades, empresas y organismos gubernamentales asociados para el desarrollo, operación y utilización de esta red académica en Estados Unidos; no obstante, por el rico intercambio existente en la colaboración de proyectos, el concepto de las redes académicas y de investigación rebasa la frontera americana y diversos países alrededor del mundo que inician la construcción de este tipo de redes.

Su desarrollo abre las puertas a aplicaciones que usan transferencia masiva de datos, video en tiempo real, investigación y colaboración remota; de igual forma, permite impulsar la creación de nuevas herramientas para la educación superior y la investigación.

Desde ya se observan iniciativas en Internet2 que nos señalan la vía a un mundo de herramientas que en la Internet de hoy son improbables por no decir imposibles. La tele-inmersión a través de cubículos virtuales y cuevas de realidad virtual, los laboratorios virtuales, la computación distribuida que permitirá el acceso en tiempo real a instrumentos remotos son aplicaciones que están en desarrollo. El mundo de las artes también se ha beneficiado de esta novedosa red en expansión y ya cuenta con la primera orquesta asociada a esta iniciativa. La sinfónica New World utiliza Internet2 para realizar practicas a distancia, enseñar a través de esta red y hasta realizar audiciones de un extremo a otro de los EE UU en tiempo real. La medicina es una de las áreas que más se beneficiará de esta herramienta del futuro cuando un medico pueda manipular datos de un paciente remotamente o visualizar en tercera dimensión una estructura anatómica compleja.

REDES ACADÉMICAS Y DE INVESTIGACIÓN

CUDI	Corporación Universitaria para el Desarrollo de Internet	México
REUNA	Red Universitaria Nacional	Chile
RETINA	Red Teleinformática Académica	Argentina
RNP	Red Nacional de Enseñanza e Investigación	Brasil
UCAID	University Corporation for the Advanced Internet Development	Estados Unidos
Abilene, Internet 2		Estados Unidos
CANARIE	Canadian Network for the Advancement of Research Industry and Education	Canada
RedIRIS		España
DANTE	Delivery of Advanced Network Technology to Europe	Europe
CLARA	Cooperación Latinoamericana de Redes Avanzadas	Latinoamérica
RENIA	Red Nicaragüense de Internet avanzada	Nicaragua

Entre las aplicaciones de nueva generación producidas para su transporte en Internet 2 se encuentran los laboratorios virtuales y remotos, los cálculos complejos y en tiempo real, la educación a distancia, las bibliotecas digitales, la medicina a distancia, la tele inmersión y las creaciones artísticas, por mencionar las más importantes.

5.5 INTERNET E INTERNET 2

El funcionamiento de la red Internet 2 en comparación con Internet es muy similar, inclusive, pueden compartir los mismos medios de comunicación (fibras, ruteadores, etcétera). La diferencia primordial entre la red Internet e Internet 2 es el uso que se les da; mientras la primera tiene, fundamentalmente, un uso comercial, informativo y de entretenimiento; la segunda es una red de usos educativos, de colaboración científica y de investigación, por este motivo, la divulgación del conocimiento y el aprendizaje constituyen sus principales objetivos.

Otra diferencia importante es que las redes de Internet 2, muchas de ellas son administradas por universidades, lo que permite que sea la misma comunidad de Internet 2 la que defina la forma de operación y los protocolos que deberán ser soportados en ellas, sin tener que esperar a que éstos sean soportados y requeridos por un gran número de usuarios, ejemplo de estos protocolos son Multicast e IPv6, donde el primero ha servido para la creación de Access-grid (transmisión de hasta 100 sitios de videoconferencia, transmisión de video de alta calidad, grids de súper computo, etcétera).

Además de que las redes que serán usadas por Internet2 serán más rápidas, las aplicaciones desarrolladas utilizaran un completo conjunto de herramientas que no existen en la actualidad. Por ejemplo, una de estas herramientas es comúnmente conocida como la garantía "Calidad de servicio". Actualmente, toda información en Internet viene dada con la misma prioridad como si ésta pasara a través de toda la red de un ordenador a otro. "Calidad de servicio" permitirá a las aplicaciones requerir una especifica cantidad de ancho de banda o prioridad para ella. Esto permitirá a dos ordenadores hacer funcionar una aplicación como la tele-inmersión comunicarse a las altas velocidades necesarias para una interacción en tiempo real. Al mismo tiempo, una aplicación con unas necesidades de comunicación como la World Wide Web sólo necesita usar la velocidad de transmisión necesaria para funcionar adecuadamente.

Es importante resaltar la diferencia en velocidad que tendrá, mucho más que una rápida WWW. Se piensa que una red de 100 a 1000 veces más permitirá a las aplicaciones cambiar el modo de trabajar e interactuar con los ordenadores. Aplicaciones como la tele-inmersión y las bibliotecas digitales cambiaran el modo que tiene la gente de usar los ordenadores para aprender, comunicarse y colaborar. Quizás las más excitantes posibilidades son aquellas que todavía no se han imaginado y serán desarrolladas junto con Internet2.

Adicionalmente, los proveedores de servicios sobre Internet "sobre venden" 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.

Debido al gran éxito que Internet 2 ha tenido en algunos países, ellos han ido más lejos y han decidido adquirir sus propias fibras ópticas (dark fibers), lo cual les permite que sean ellos quienes definan los anchos de banda de sus redes, pudiendo crear redes con grandes anchos de banda de 1 a 10 giga bits o, incluso, superiores usando técnicas como DWDM, en la cual, se hace uso de varios láser de diferentes longitudes de onda; con esta última tecnología, no sólo se está limitando a la creación de redes IP. DWDM permite crear redes con cualquier tecnología óptica, como ejemplo fiber-channel, con la cual, se pueden crear redes de almacenamiento masivo (SAN, Store Área Network), que al tener sus propias fibras, puede crear una red de almacenamiento masivo distribuida geográficamente, uniendo varias SAN y con ello sumando las capacidades existente de todas. En Estados Unidos de Norteamérica existe el proyecto llamado HOPI.

En cuanto a la infraestructura física de las redes, Internet 2 fue creado para ser una red de alto desempeño con la finalidad de satisfacer las demandantes aplicaciones que serán transportadas por ella.

5.6 DEFINICIÓN DE DIRECCIONES IP

Dirección del proveedor de acceso a Internet (**I**nternet Access **P**rovider). Es un número que identifica de forma única a un ordenador o red local dentro de Internet, y que un usuario recibe de su proveedor. Puede ser constante o variable.

La dirección IP es un identificador único que se aplica a cada dispositivo que esté conectado a una red IP. De esa forma los distintos elementos participantes de la red (servidores, routers, ordenadores de usuarios, etc.) se comunican entre si utilizando su dirección IP como identificación.

IP son las siglas de “Internet Protocol”. El nombre Internet para designar el protocolo, y posteriormente la red mundial de información, significa justamente “inter red”, es decir, conexión entre redes. Al principio el protocolo tuvo un uso exclusivamente militar pero rápidamente se fueron añadiendo ordenadores de universidades y posteriormente usuarios particulares y empresas.

La Internet como red mundial de información es el resultado de la aplicación práctica del protocolo IP, es decir, el resultado de la interconexión de todas las redes de información que existen en el mundo.

En la versión 4 del protocolo IP (la usada actualmente) las direcciones están formadas por 4 números de 8 bits (un número de 8 bits puede valer desde 0 hasta 255) que se suelen representar separados por puntos, por ejemplo: 217.76.128.63

En total, una dirección IP versión 4 tiene 32 bits, lo que equivale a 232 direcciones IP diferentes.

5.7 IPV4

Cuando IPv4 fue estandarizado, hace unos quince años, nadie podía imaginar que se convertiría en lo que es hoy: una arquitectura de amplitud mundial, con un número de usuarios superior al centenar de millones y que crece de forma exponencial. Aquella primera "Internet" fundada, sobre todo, con fines experimentales, científico-técnicos y, por supuesto, con objetivos militares, no se parece en nada a la actual. Cada día se advierte una mayor tendencia hacia su comercialización, ya sea por el propio acceso en sí a la red (empresas proveedoras) o por servicios accesibles desde ella.

No hay una fecha concreta de cuando se agotaran las direcciones en IPv4, pero se estima que con el crecimiento actual el número de direcciones IP versión 4 disponibles se agotará antes de que termine la presente década.

Teniendo en cuenta que se necesitan varios años de coexistencia entre ambas versiones para preparar la migración, no es difícil imaginar que el paso a la nueva generación de Internet se realizará muy pronto.

Estos cambios de escala y orientación suponen varios problemas para IPv4:

- Escala: Cada máquina presente en la red dispone de una dirección IP de 32 bits. Ello supone más de cuatro mil millones de máquinas diferentes. Esa cifra, no obstante, es muy engañosa. El número asignado a un ordenador no es arbitrario, sino que depende de una estructura más o menos jerárquica (en especial, pertenece a una red), lo cual ocasiona que se desperdicie una enorme cantidad de direcciones. La cuestión es que en 1993 fue claro que con el ritmo de crecimiento sostenido de Internet hasta aquel momento (exponencial), el agotamiento del espacio de direcciones era casi inminente.

- Enrutado: Otro de los grandes problemas del crecimiento de Internet es la capacidad de almacenamiento necesaria en las pasarelas (routers) y el tráfico de gestión preciso para mantener sus tablas de encaminamiento. Existe un límite tecnológico al número de rutas que un nodo puede manejar, y como dado que Internet crece mucho más rápidamente que la tecnología que la mantiene, se vio que las pasarelas pronto alcanzarían su capacidad máxima y empezarían a desechar rutas, con lo que la red comenzaría a fragmentarse en subredes sin acceso entre sí.

  Dado lo grave de la situación se definió el CIDR (Classless Inter-Domain Routing) con el que las pasarelas reducían el tamaño de sus tablas colapsando juntas varias subredes con el mismo prefijo. Gracias a ello se ha ganado un tiempo muy valioso, pero tan sólo se ha postergado lo inevitable.

- Multiprotocolo: Cada vez resulta más necesaria la convivencia de diversas familias de protocolos: IP, OSI, IPX... Se necesitan mecanismos que permitan abstraer al usuario de la tecnología subyacente para permitir que concentre su atención en los aspectos realmente importantes de su trabajo. Se tiende, pues, hacia una red orientada a aplicaciones, que es con lo que el usuario interacciona, más que a una red orientada a protocolos (como hasta el momento).

- Seguridad: El mundo IPv4 es el mundo académico, científico, técnico y de investigación. Un ambiente, en general, que podría calificarse como "amigable", desde el punto de vista de la gestión y la seguridad en la red. Con la aparición de servicios comerciales y la conexión de numerosísimas empresas, el enorme incremento en el número de usuarios y su distribución por todo el planeta, y la cantidad, cada vez mayor, de sistemas que necesitan de Internet para su correcto funcionamiento, etc., es urgente definir unos mecanismos de seguridad a nivel de red. Son necesarios esquemas de autentificación y privacidad, tanto para proteger a los usuarios en sí como la misma integridad de la red ante ataques malintencionados o errores.

- Tiempo Real: IPv4 define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. A pesar de que en la cabecera IP hay un campo destinado a fijar, entre otras cosas, la prioridad del datagrama, en la práctica ello no supone ninguna garantía. Se necesita una extensión que posibilite el envío de tráfico de tiempo real, y así poder hacer frente a las nuevas demandas en este campo.

- Tarificación: Con una red cada día más orientada hacia el mundo comercial hace falta dotar al sistema de mecanismos que posibiliten el análisis detallado del tráfico, tanto por motivos de facturación como para poder dimensionar los recursos de forma apropiada.

- Comunicaciones Móviles: El campo de las comunicaciones móviles está en auge, y aún lo estará más en un futuro inmediato. Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios. La seguridad de las comunicaciones, en este tipo de sistemas, se ve, además, especialmente comprometida.

- Facilidad de Gestión: Con el volumen actual de usuarios y su crecimiento estimado, resulta más que obvio que la gestión de la red va a ser una tarea ardua. Es preciso que la nueva arquitectura facilite al máximo esta tarea. Un ejemplo de ello sería la autoconfiguración de los equipos al conectarlos a la red.

- Política de enrutado: Tradicionalmente los datagramas se han encaminado atendiendo a criterios técnicos tales como el minimizar el número de saltos a efectuar, el tiempo de permanencia en la red, etc. Cuando la red pertenece a una única organización eso es lo ideal, pero en el nuevo entorno económico en el que diferentes proveedores compiten por el mercado las cosas no son tan simples. Es imprescindible que la fuente pueda definir por qué redes desea que pasen sus datagramas, atendiendo a criterios de fiabilidad, coste, retardo, privacidad, etc.

5.8 NAT "NETWORK ADDRESS TRANSLATION"

No es suficiente para luchar con los problemas de espacio de direcciones, NAT es un sistema que permite que una red local se pueda conectar a Internet teniendo una única dirección IP real, por ejemplo la dirección IP asignada a una conexión ADSL o cable.

Casi todas las redes locales actuales se implementan asignando a cada ordenador direcciones IP privadas del rango 192.168.X.X. Estas direcciones se pueden asignar libremente dentro de una red local, pero a cambio no pueden utilizarse en la red Internet.

Para conectarse a Internet, las redes locales con direccionamiento interno privado, utilizan una única dirección IP "real". Cuando cualquier ordenador de la red local sale a Internet, lo hace utilizando dicha IP real, por tanto, todos los ordenadores de la red local salen a

Internet con la misma dirección IP. El NAT se encarga de gestionar todas estas conversiones entre IPs privadas internas y la IP real.

La existencia del NAT ha sido un auténtico salvavidas para el protocolo IP actual (versión 4). Sin el NAT hace mucho tiempo que las direcciones IP se hubieran agotado, pues no hay suficientes como para asignar una dirección única para cada equipo susceptible de conectarse a Internet. Entonces cabría preguntarse, ¿no sería posible seguir aguantando con el esquema de direccionamiento IP actual a base de utilizar más y más NAT?

La respuesta es que las direcciones IP versión 4 se están agotando incluso contando con un uso masivo del NAT. Si además tenemos en cuenta que en un futuro cercano multitud de dispositivos como teléfonos móviles UMTS o electrodomésticos estarán conectados a Internet de forma permanente (con dirección IP fija), queda claro que el uso del NAT sería insuficiente para satisfacer tal demanda de conectividad.

Además NAT añade complejidad de mantenimiento y uso de recursos de computación en los routers. Los routers que realizan NAT tienen que reasignar las direcciones IP de cada uno de los paquetes entrantes o salientes a la red, lo cual es una sobrecarga grande de CPU respecto a su misión original, que es simplemente enrutar los paquetes.

Además hemos de tener en cuenta que IPv6 no solamente incrementa el espacio de direcciones. Es más que eso. IPv4 se ha utilizado durante más de veinte años y existen agujeros y limitaciones en sus especificaciones para el uso actual. IPv6 intenta incluir tecnologías que están utilizándose hoy en día e intenta ser un protocolo preparado para el siglo XXI.

5.9 ENRUTAMIENTO SOBRE IPV4

5.9.1 Protocolos de enrutamiento

Son aquellos protocolos que utilizan los routers o encaminadores para comunicarse entre sí y compartir información que les permita tomar la decisión de cual es la ruta más adecuada en cada momento para enviar un paquete.

Los protocolos mas usados son RIP (v1 y v2), OSPF (v1, v2 y v3), y BGP (v4), que se encargan de gestionar las rutas de una forma dinámica. Aunque no es estrictamente necesario que un router haga uso de estos protocolos, pudiéndosele indicar de forma estática las rutas (caminos a seguir) para las distintas subredes que estén conectadas al dispositivo.

- **RIP** (Routing information protocolo, protocolo de información de enrutado). Es un protocolo de enrutado interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a Internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

- **OSPF** (Open shortest path first, El camino más corto primero). Se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a que distancia (medida en routers) está cada router. Así cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos.

- **BGP** (Border gateway protocol, protocolo de la pasarela externa). Es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de Internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc., para enviar un paquete por una ruta o por otra. Un router BGP da a conocer sus direcciones IP a los routers BGP y esta información se difunde por los routers BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre routers, no utiliza RIP.

Existe la posibilidad de no utilizar equipos dedicados, opción que puede ser la más adecuada para redes locales o redes con un tráfico limitado, y usar software que implemente los protocolos de red antes mencionados. Para dar funcionalidad de router a un PC con los sistemas operativos GNU/Linux o BSD es suficiente con añadirle al menos dos interfaces de red y activar el soporte de enrutamiento en el kernel. Si se desea proporcionarle la funcionalidad de un router completo, y que soporte diversos protocolos de red, se pueden utilizar paquetes como: Quagga, Zebra, ZebOs.

Otra forma de adquirir un router es ya contactando con fabricantes que se dedican a desarrollar su propio software no libre y con su hardware especialmente hecho para tal fin, este es el caso de fabricantes como: Cisco Systems, Juniper Networks.

Cisco Systems es líder mundial en redes para Internet. Las soluciones de conectividad de Cisco son la base de Internet así como de las demás redes corporativas, educativas y de gobierno en todo el mundo. Hoy, Internet es un componente esencial de los negocios, la educación, las comunicaciones personales y el entretenimiento. Los equipos de Cisco aseguran que todos los mensajes o transacciones virtuales que pasan por Internet sean llevados en forma rápida y segura a su destino.

5.9.2 Configuración Básica de Ruteadores CISCO

Componentes de un enrutador Cisco

***Tipos de Memoria*:** RAM, ROM, Flash, NVRAM (RAM No-Volátil)
Software: POST, Bootstrap, ROM Monitor, IOS, Config-Register.

Configuración: La configuración del enrutador afecta:

- Las direcciones IP y las máscaras de cada interfaz
- Información de ruteo (estático, dinámico o por defecto)

- Información de inicio
- Seguridad (contraseñas).

El enrutador siempre tiene dos configuraciones:

- "Running" (actual): en RAM, indica con qué parámetros el enrutador está operando actualmente. Se modifica con el comando configure y para verla: show running-config.
- "Startup" (de inicio): en NVRAM, determina cómo va a operar el enrutador cuando sea reiniciado, se modifica usando el comando copy y para verla: show startup-config

Modos de Acceso:

Modo de ejecución de usuario (User EXEC): Examinar el enrutador de forma limitada

Router>

Modo de ejecución privilegiado (Privileged EXEC): Examen detallado, resolución de problemas, pruebas, manipulación de ficheros

Router#

ROM Monitor: Útil para recuperación de contraseñas y para instalar IOS

Modo Setup – Disponible cuando no existe el fichero

Startup-config

Los comandos de configuración se pueden ejecutar de forma interactiva. Los cambios se activan (casi) inmediatamente en la configuración corriente. Puede usar una conexión directa vía puerto serie, o hacer Telnet/SSH a las vty's ("virtual terminals"), o una conexión vía módem al puerto auxiliar, o escribir los comandos en un fichero de texto y cargarlo, luego en el enrutador vía TFTP copy tftp start o config net

Entrar al enrutador (Login)

Conectarse al puerto consola o hacer Telnet

router>

router>enable

Password

router#

router#?

Configurar el enrutador

Terminal (Entrar los comandos directamente)

router# configure terminal

router(config)#

USER MODE, PROMPT, PRIVILEDGED, MODE PROMPT

Configuración de un enrutador nuevo

- ***Cargar los parámetros de configuración en la RAM***

  Router#configure terminal
- ***Dar al enrutador una identificación***

  Router#(config) hostname RouterA
- ***Asignar contraseñas de acceso***

  RouterA#(config)line console 0
  RouterA#(config-line) password cisco
  RouterA#(config-line)login
- ***Configurar interfaces***

  RouterA#(config) interface ethernet 0/0
  RouterA#(config-if)ip address n.n.n.n m.m.m.m
  RouterA#(config-if)no shutdown
- ***Configurar protocolos ruteados y de ruteo***

  Guardar la configuración en NVRAM
  RouterA#copy running-config startup-config o write memory

Indicadores

Puede saber en qué área de la configuración se encuentra sólo mirando los indicadores

Router>	- modo USER
Router#	- modo PRVILEDGED EXEC
Router(config)	– modo configuración global
Router(config-if)	– modo configuración interfaz
Router(config-subif)	– modo configuración sub-interfaz
Router(config-route-map)	– modo configuración route-map
Router(config-router)	– modo configuración enrutamiento
Router(config-line)	– modo configuración de línea

Configuración Global

Configure la contraseña "enable secret":

La clave aparecerá en texto en claro. Ejecute el comando siguiente para hacer más segura: router(config)# enable secret <clave>

Otro método es usar el comando 'enable password'. Este no es seguro (débil y texto en claro) y NO ES RECOMENDADO: router(config)# service password-encryption.

Comandos globales relacionados con IP:

ip classless
ip name-server n.n.n.n

Creación de rutas estáticas

ip route <n.n.n.n> <m.m.m.m> <g.g.g.g>
n.n.n.n = bloque IP
m.m.m.m = máscara de red (tamaño del bloque)
g.g.g.g = enrutador del próximo salto por omisión

El comando 'no': Utilizado para desactivar o invertir un comando

ip domain-lookup
no ip domain-lookup
router ospf 1
no router ospf 1
ip address 1.1.1.1 255.255.255.0
no ip address

Configuración de Interfaces

Su nombre tiene el formato Tipo/Ranura/[Número].ej.:
ethernet0, ethernet1,... Ethernet5/1
Serial0/0, serial1 ... Serial3

Y se pueden abreviar:
ethernet0 o eth0 or e0
Serial0/0 o ser0/0 or s0/0

Configuración de la dirección IP y máscara

```
router#configure terminal
router(config)#interface e0/0
router(config-if)#ip address n.n.n.n m.m.m.m
router(config-if)#no shutdown
router(config-if)#^Z
router#
```

Activar/Desactivar la interfaz con carácter administrativo

```
router(config-if)#no shutdown
router(config-if)#shutdown
```

Descripción

router(config-if)#description enlace ethernet al edificio de administración.

Mostrar la configuración

Use "show running-configuration" para ver la configuración corriente
Use "show startup-configuration" para ver la configuración guardada en NVRAM

Guardar la configuración en un servidor

Requiere tftpd en una máquina unix. El fichero destino debe existir en el directorio antes de ser copiado y debe tener permiso de escritura

```
Router#copy run tftp
Address or name of remote host []? 192.168.1.5
Destination filename [Router-confg]? y
```

!!!!!
15693 bytes copied in 0.792 secs (19814 bytes/sec)

Recuperar la Configuración desde el servidor

Use 'tftp' para cargar la configuración desde el servidor TFTP, copiándola en running-config o startup-config
Router#copy tftp start
Address of remote host [255.255.255.255]? 192.168.1.5
Name of configuration file [Router-confg]?
Configure using Router-confg from 192.168.1.5? [confirm]
Loading Router-confg from 192.168.1.5(via Ethernet0/0): !
[OK - 1005/128975 bytes]
[OK]
Router# reload

Borrar la configuración

Para borrar la configuración completamente

Router#erase startup-config

ó

Router#write erase

Y luego

Router#reload

El enrutador se reiniciará en modo "setup", porque no encontrará el archivo de configuración.

Ayuda de cómo obtener comandos

La IOS tiene una utilidad integrada para ayuda use "?" para obtener una lista de posibles comandos, o "<comando incompleto> ?" Lista todos los posibles sub-comandos que empiezan con la cadena, Ej.:

router#con?
configure connect

Esto es diferente que

router#conf ?

memory	Configure from NVRAM
network	Configure from a TFTP network host
overwrite-network	Overwrite NV memory from TFTP network host
terminal	Configure from the terminal
<cr>	

También funciona en modo de configuración:

router(config)#ip a?
accounting-list accounting-threshold accounting-transits
address-pool alias as-path

"Explorar" un comando para determinar su sintaxis:

router(config-if)#ip addr ?

A.B.C.D IP address

La tecla TAB puede completar una cadena incompleta

```
router(config)#int<TAB>
router(config)#interface et<TAB>
router(config)#interface ethernet 0
```

Aunque no es necesario. También se aceptan comandos incompletos:

```
router#conf t
router(config)#int e0/0
router(config-if)#ip addr n.n.n.n
```

5.10 IPV6

IPv6 es la nomenclatura abreviada de “Internet Protocol Versión 6”. IPv6 es el protocolo de la próxima generación de Internet, por lo que a veces también se denomina IPng que viene de “Internet Protocol Next Generation”.

IPv6 es por tanto la actualización del protocolo de red de datos en el que se fundamenta Internet. El IETF (Internet Enginering Task Force) desarrolló las especificaciones básicas durante los 90 para sustituir la versión actual del protocolo de Internet, IP versión 4 (IPv4), que vio la luz a finales de los 70.

IPv4 ha demostrado por su duración un diseño flexible y poderoso, pero está empezando a tener problemas, siendo el más importante el crecimiento en poco tiempo de la necesidad de direcciones IP.

Nuevos usuarios en países tan poblados como China o la India, nuevas tecnologías con dispositivos conectados de forma permanente (xDSL, cable, PDA, teléfonos móviles UMTS, etc) están provocando la rápida desaparición de las direcciones IP disponibles en la versión 4.

IPv6 resuelve este problema creando un nuevo formato de dirección IP con muchísimas más variaciones, de forma que el número de direcciones IP no se agote incluso contando con que cada dispositivo que podamos imaginar (incluyendo electrodomésticos) se termine conectando a la red Internet.

IPv6 añade también muchas mejoras en áreas como el routing y auto configuración de red. Los nuevos dispositivos que se incorporen a la red serán plug and play. Adiós a configurar las IP del DNS, el gateway predeterminado, la máscara de subred y demás parámetros. Simplemente habrá que enchufar el equipo a la red y éste obtendrá de la misma todos los datos de configuración que necesita.

Se espera que IPv6 reemplace gradualmente a IPv4, coexistiendo las dos un determinado número de años durante la transición. arsys.es siguiendo con su filosofía de vanguardia

tecnológica ofrece ya a los clientes que lo requieran servicios de hosting y conectividad con soporte para el protocolo IPv6.

No hay que confundir los términos IPV6 e Internet2, Internet2 es el nombre utilizado para designar a la red académica de investigación de los Estados Unidos e IPV6 es un protocolo de red diseñado para el sucesor del actual protocolo Ipv4, de hecho Ipv6 es una de las nuevas tecnologías utilizadas por Internet2

5.10.1 ¿Por qué IPv6 y no IPv5?

La información que circula por una red IP como Internet está distribuida en paquetes. Cada paquete incluye no sólo los datos a transmitir sino también un "envoltorio" que, entre otras cosas, tiene el número de versión del protocolo IP que se está utilizando.

IANA decidió asignar el número de versión 5 para un protocolo experimental que nunca llegó a utilizarse en la práctica llamado ST-II "Stream Protocol versión 2". La idea era identificar los paquetes de ST mirando el número de versión del protocolo IP: Si el número es 4 entonces se trata de un paquete normal, si es 5 entonces es un paquete del Stream Protocol.

Por ese motivo el número 5 no se puede utilizar para designar a la versión del protocolo IP que sigue a la 4. Por tanto no hay un salto de versión, simplemente la versión 6 es la que sigue a la 4 porque el número 5 se reservó para otro protocolo.

5.10.2 Diferencias 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).
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.
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	El Protocolo de resolución de	Los marcos de solicitud ARP se

solicitud ARP	dir.(ARP) utiliza marcos de solicitud ARP de difusión para resolver una dir. IPv4 como una dirección de capa de vínculo.	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.	El Descubrimiento de enrutadores 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 de ámbito local del vínculo.
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, mientras se desarrolla A6.
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 de 576 bytes (posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (sin fragmentación).

5.10.3 Ventajas de IPv6

Escalabilidad: IPv6 tiene direcciones de 128 bits frente a las direcciones de 32 bits de IPv4. Por tanto el número de direcciones IP disponibles se multiplica por 7,9 * 1028

Seguridad: IPv6 incluye seguridad en sus especificaciones como es la encriptación de la información y la autentificación del remitente de dicha información.

Aplicaciones en tiempo real: Para dar mejor soporte a tráfico en tiempo real (videoconferencia), IPv6 incluye etiquetado de flujos en sus especificaciones. Con

este mecanismo los routers pueden reconocer a qué flujo extremo a extremo pertenecen los paquetes que se transmiten.

Plug and Play: IPv6 incluye en su estándar el mecanismo "plug and play", lo cual facilita a los usuarios la conexión de sus equipos a la red. La configuración se realizará automáticamente en los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.

Especificaciones más claras y optimizadas: IPv6 seguirá las buenas prácticas de IPv4 y eliminará las características no utilizadas u obsoletas de IPv4, con lo que se conseguirá una optimización del protocolo de Internet. La idea es quedarse con lo bueno y eliminar lo malo del protocolo actual.

Convivencia con IPv4, que hará posible una migración suave.

Formato de cabecera: más flexible que en IPv4 para agilizar el encaminamiento.

La fragmentación y reensamblado: se realiza en los nodos finales, y no en los routers como en IPv4.

5.10.4 Desventajas de IPv6

- La necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella.

- Para estar enlazada al universo IPv4 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT (compartición de direcciones IP) en los routers pasarela (IPv6<-->IPv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.

- Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de IPv6 multihoming.

5.10.5 Direcciones IPv4 y sus equivalentes en IPv6

Asignación actual del espacio de direcciones de IPv6

Dirección IPv4	**Dirección IPv6**
Clases de direcciones de Internet	No se ha implementado en IPv6
Direcciones de multidifusión (224.0.0.0/4)	Direcciones de multidifusión IPv6 (FF00::/8)
Direcciones de difusión	No se ha implementado en IPv6
La dirección no especificada es 0.0.0.0	La dirección no especificada es ::
La dirección de bucle de retroceso es 127.0.0.1	La dirección de bucle de retroceso es ::1
Direcciones IP públicas	Direcciones de unidifusión global agregables
Direcciones IP privadas (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16)	Direcciones locales de sitio (FEC0::/48)

Direcciones configuradas automáticamente (169.254.0.0/16)	Direcciones locales de vínculo (FE80::/64)
Representación de texto: notación decimal con puntos	Representación de texto: formato hexadecimal con signos de dos puntos, supresión de 0's a la izquierda y compresión de ceros. Las direcciones compatibles con IPv4 se expresan en notación decimal con puntos.
Representación de bits de red: máscara de subred en notación decimal o longitud de prefijo.	Representación de bits de red: sólo longitud de prefijo.
Resolución de nombres DNS: registro de recursos de direcciones de host IPv4 (A)	Resolución de nombres DNS: registro de recursos de direcciones de host IPv6 (AAAA)
Resolución de DNS inversa: dominio IN-ADDR.ARPA	Resolución de DNS inversa: dominio IP6.INT

arsys.es suministra servicios de hosting sobre servidores Windows Server 2003 y Linux con soporte IPv6 a todos los clientes que lo deseen. Los webmasters, desarrolladores de aplicaciones Web, administradores de sistemas, etc., podrán probar ya sus desarrollos para la nueva generación de Internet en un servidor real en producción.

Así mismo, se suministra conectividad IPv6 tunelizada sobre IPv4. Para utilizar este tipo de conectividad, el usuario debe instalar en su equipo el software IPv6 y arsys.es suministrará un túnel que conecte el ordenador del usuario con la red nativa IPv6 a la que arsys.es está conectado.

De esta forma el usuario dispondrá de una completa conexión nativa sobre IPv6 que le permitirá navegar por todos los servidores con soporte para la versión 6 y en modo compatibilidad con aquellos (la mayoría de momento) que están sobre la versión 4.

El túnel se utiliza para atravesar el segmento IPv4 que todavía existe entre el ordenador del usuario y el router de arsys.es (el segmento de red gestionada por el operador de conectividad).

5.10.6 Principales características del nuevo IPV6

A continuación se enumeran las características del nuevo protocolo IPv6:

- Nuevo formato de encabezado
- Gran espacio de direcciones
- Direccionamiento jerárquico e infraestructura de enrutamiento eficientes
- Configuración de direcciones sin estado y con estado
- Seguridad integrada
- Mayor compatibilidad con QoS

- Nuevo protocolo para la interacción de nodos vecinos
- Capacidad de ampliación

Nuevo formato de encabezado: El encabezado de IPv6 presenta un nuevo formato diseñado para que la carga de trabajo del encabezado sea mínima. Para ello, se mueven los campos de opciones y los que no son esenciales a encabezados de extensión que se colocan tras el encabezado de IPv6. El encabezado optimizado de IPv6 proporciona un procesamiento más eficiente en los enrutadores intermedios.

Los encabezados de IPv4 no pueden funcionar conjuntamente con los encabezados de IPv6. Un host o un enrutador deben utilizar una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado de IPv6 es sólo el doble de grande que el de IPv4, aunque las direcciones de IPv6 son cuatro veces mayores que las de IPv4.

Gran espacio de direcciones: IPv6 tiene direcciones IP de origen y destino de 128 bits (16 bytes). Aunque con 128 bits se pueden expresar más de $3{,}4x10^{38}$ combinaciones posibles, el gran espacio de direcciones de IPv6 se ha diseñado para permitir varios niveles de subredes y asignaciones de redes de la red troncal de Internet a las subredes individuales de una organización.

Aunque actualmente sólo se asigna un pequeño número de las direcciones posibles para los hosts, hay muchas direcciones disponibles para su uso en el futuro. Con un número de direcciones disponibles mucho mayor, dejan de ser necesarias las técnicas de conservación de direcciones, como la distribución de NAT.

Direccionamiento jerárquico e infraestructura de enrutamiento eficientes: La direcciones globales de IPv6 utilizadas en la parte IPv6 de Internet están diseñadas para crear una infraestructura de enrutamiento jerárquica eficiente que se puede resumir, basada en la aparición de múltiples niveles de proveedores de servicios Internet. En Internet IPv6, los enrutadores troncales tienen tablas de enrutamiento mucho más pequeñas, que corresponden a la infraestructura de enrutamiento de Agregadores de nivel superior.

Configuración de direcciones sin estado y con estado: Para simplificar la configuración de hosts, IPv6 permite la configuración de direcciones con estado, como la configuración de direcciones en presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones en ausencia de un servidor DHCP). Con una configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (que se denominan direcciones locales de vínculo) y con direcciones derivadas de prefijos anunciados por enrutadores locales. Incluso en ausencia de un enrutador, los hosts del mismo vínculo pueden configurarse automáticamente con direcciones locales de vínculo y se comunican sin configuración manual.

Seguridad integrada: La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares en

respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6.

Mayor compatibilidad con QoS: Los nuevos campos del encabezado de IPv6 definen cómo se identifica y se controla el tráfico. La identificación del tráfico mediante un

campo Flow Label (Etiqueta de flujo) en el encabezado de IPv6 permite a los enrutadores identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo, un conjunto de paquetes que viaja entre un origen y un destino. Como el tráfico se identifica en el encabezado de IPv6, se puede proporcionar compatibilidad con QoS incluso si la carga de paquetes está cifrada mediante IPSec.

Nuevo protocolo para la interacción de nodos vecinos: El protocolo Neighbor Discovery (Descubrimiento de vecino) para IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6, *Internet Control Message Protocol for IPv6*) que administran la interacción de nodos vecinos (nodos que se encuentran en el mismo vínculo). Neighbor Discovery reemplaza al Protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*) basado en difusión, al protocolo de descubrimiento de enrutadores de ICMPv4 y a los mensajes Redirect (Redirección) de ICMPv4 con mensajes Neighbor Discovery de unidifusión y multidifusión.

Capacidad de ampliación: IPv6 se puede ampliar fácilmente con nuevas características si se agregan encabezados de extensión tras el encabezado de IPv6. A diferencia de las opciones del encabezado de IPv4, que sólo permite 40 bytes de opciones, el tamaño de los encabezados de extensión de IPv6 sólo está limitado por el tamaño del paquete de IPv6.

5.10.7 Funcionalidades de IPv6

- Mayor número de direcciones. Pasa de 32 bits en IPv4 a 128 bits en IPv6.
- Encabezado con formato flexible. IPv6 utiliza un nuevo e incompatible formato de datagrama; utiliza un conjunto de encabezados opcionales.
- Opciones mejoradas. Como IPv4, IPv6 permite incluir en un datagrama información de control opcional. IPv6 incluye nuevas opciones.
- Soporte para la reservación de recursos. IPv6 reemplaza la especificación del tipo de servicio en IPv4 con un mecanismo que permite la reservación anticipada de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones como video en tiempo real que requiere garantías en ancho de banda y retardo.
- Previsión de extensiones en el protocolo.

  La capacidad de extensión permitirá a la IETF adaptar el protocolo a nuevas tecnologías en redes o a nuevas aplicaciones.

5.10.8 Notación para las direcciones IPv6

La dirección está formada por 128 bits, frente a los 32 de las actuales. Se representa en 8 grupos de 16 bits cada uno, separados por el carácter “:”, Cada grupo de 16 bits se representa a su vez mediante 4 cifras hexadecimales, es decir, que cada cifra va del 0 al 15 (0, 1,2,... a, b, c, d, e, f siendo a=10, b=11, etc hasta f=15).

Por ejemplo,

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

Es una dirección IPv6 válida.

Si un grupo de cuatro dígitos es nulo (es decir, toma el valor "0000"), puede ser comprimido. Por ejemplo,

```
2001:0db8:85a3:0000:1319:8a2e:0370:7344
```

Es la misma dirección que

```
2001:0db8:85a3::1319:8a2e:0370:7344
```

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión solo en uno de ellos. Así,

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000:1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab
```

Son todas válidas y significan lo mismo, pero

```
2001::25de::cade
```

es inválido porque no queda claro cuantos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo pueden ser omitidos. Así,

```
2001:0DB8:02de::0e13
```

Es lo mismo que

```
2001:DB8:2de::e13
```

Si la dirección es una dirección IPv4 camuflada, los últimos 32 bits pueden escribirse en base decimal; así,

`::ffff:192.168.89.9` es lo mismo que
`::ffff:c0a8:5909,` pero no lo mismo que
`::192.168.89.9` o
`::c0a8:5909.`

El formato ::ffff:1.2.3.4 se denomina *dirección IPv4 mapeada*, y el formato ::1.2.3.4 *dirección IPv4 compatible*.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 ó ::874B:2B34.

Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser ::135.75.43.52. Este tipo de dirección *IPv4 compatible* casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

También existe un método para designar grupos de direcciones IP o subredes que consiste en especificar el número de bits que designan la subred, empezando de izquierda a derecha, siendo los bits restantes para designar equipos individuales dentro de la subred.

Por ejemplo la notación:

2001:0ba0:01a0::/48

Indica que la parte de la dirección IP utilizada para representar la subred tiene 48 bits. Como cada cifra hexadecimal son 4 bits, esto indica que la parte utilizada para representar la subred está formada por 12 cifras, es decir: “2001:0ba0:01a0”. El resto de las cifras de la dirección IP (las que estén a su derecha cuando se escriba completa) se utilizarían para representar objetos dentro de la subred.

La red IP versión 6 de arsys.es se designa mediante los dos primeros grupos de cifras y se utilizan todas las variaciones posibles de los 6 grupos restantes para designar subredes y equipos.

RIPE recomienda a los ISP y operadores que asignen a cada cliente una subred del tipo /48 con el fin de que el cliente pueda gestionar sus propias subredes sin tener que utilizar NAT (el NAT desaparece en IPv6).

Así, un cliente de conectividad en IPv6 de arsys.es podría tener una subclase como la siguiente:

2001:0ba0:1c01::/48

A su vez, este cliente podría crear sus propias subredes en sus instalaciones haciendo variar el siguiente grupo de 16 bits. Por ejemplo, una de sus subredes podría ser esta:

2001:0ba0:1c01:5c23::/64

Los 64 bits restantes hasta completar la dirección IPv6 se utilizarán exclusivamente para designar el equipo dentro de la subred. Las tarjetas de red ethernet llevan incorporado un identificador único asignado por el fabricante llamado MAC (Media Access Control). El MAC está formado por 48 bits por lo que "cabe" dentro de los 64 bits de la dirección IP que corresponden al dispositivo.

Esta es la base del sistema de auto configuración de IPv6: Los equipos podrán conectarse a la red y autoconfigurarse generando automáticamente su propia dirección IP. Ésta se formaría tomando la parte de red de dispositivos como los routers e incorporando su propia MAC a la dirección IP, lo cual garantizaría que ésta sea única.

En definitiva, las nuevas direcciones IP versión 6 tienen 128 bits de los cuales 64 se utilizan para representar la parte de red y los otros 64 el equipo conectado a la misma. Esto se puede representar esquemáticamente como sigue:

<table>
<tr><td>2001</td><td>0ba0</td><td>1c01</td><td>5c23</td><td>00001a56f3bd0153</td></tr>
<tr><td>RIPE</td><td>Red de arsys.es</td><td>Red para uso del cliente</td><td>Subred del cliente</td><td rowspan="2">Interface del equipo. Formada a partir de la MAC de la tarjeta de red</td></tr>
<tr><td>16 bits</td><td>16 bits</td><td>16 bits</td><td>16 bits</td></tr>
<tr><td colspan="4">64 bits para designar subred</td><td>64 bits para dispositivo</td></tr>
</table>

5.10.9 Tipos de Direcciones

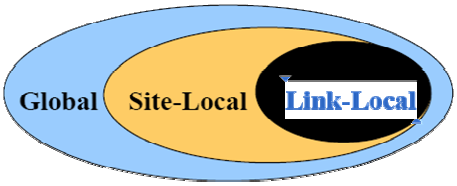
Los tipos de direcciones de IPv6 son los siguientes:

- **UNICAST:** son direcciones bien conocidas. Un paquete que se envía a una dirección unicast deberían llegar a la interfaz identificada por dicha dirección. es el tipo general de direcciones. RIPE ha asignado a RedIRIS un rango de direcciones Unicast.

- **MULTICAST**: identifican un grupo de interfaces. Un paquete destinado a una dirección multicast llega a todos los interfaces que se encuentran agrupados bajo dicha dirección. análogas a las direcciones multicast de IPv4

- **ANYCAST**: son sintácticamente indistinguibles de las direcciones unicast pero sirven para identificar a un conjunto de interfaces. Un paquete destinado a una dirección anycast llega a la interfaz "más cercana" (en términos de métrica de "routers"). Las direcciones anycast sólo se pueden utilizar en "routers". tipo de direcciones aplicables a un grupo. Al contrario que con las direcciones Multicast, el paquete sólo se envía a un miembro del grupo que se determina mediante algún protocolo de routing.

En función del prefijo podemos distinguir varios tipos de direcciones en Ipv6



Direcciones tipo "Link Local" todos los interfaces de red de un sistema con soporte Ipv6 tendrán de forma automática asignada una dirección ip de este tipo. Su función es únicamente para comunicaciones administrativas, autoconfiguración etc. Los prefijos reservados para este tipo de direcciones son fe8x:, fe9x:, feax:, febx:, aunque en la actualidad solo se usa fe8x:.

Direcciones tipo "Site Local" son aquellas direcciones de ámbito local, lo que normalmente llamamos direcciones privadas. Los prefijos reservados para este tipo de direcciones son fecx:, fedx:, feex:, fefx:, aunque el mas usado es fecx:.

Direcciones tipo "Global" son aquellos de ámbito global lo que conocemos como direcciones publicas que nos permitirán salir a Internet. Los prefijos reservados para direcciones de este tipo son: 2xxx:, 3xxx:, aunque dentro de estas hay mas subdirecciones (3ffe:,2002:, etc) para distintos propósitos.

5.10.10 Identificación de los tipos de Direcciones

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

- ::/128 – la dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.
- ::1/128 – la dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.
- ::/96 – La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6.
- ::ffff:0:0/96 – La dirección IPv4 mapeada es usada como un mecanismo de transición en terminales duales.
- fe80::/10 – El prefijo de *enlace local* (< inglés *link local*) específica que la dirección sólo es válida en el enlace físico local.
- fec0::/10 – El *prefijo de emplazamiento local* (< inglés *site-local prefix*) específica que la dirección sólo es válida dentro de una organización local. LA RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial.
- ff00::/8 – El prefijo de multicast es usado para las direcciones multicast.

Tabla. Direcciones IPv6 reservadas

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
`::`	128 bits	sin especificar	como `0.0.0.0` en Pv4
`::1`	128 bits	dirección de bucle local (loopback)	como las `127.0.0.1` en IPv4
`::00:xx:xx:xx:xx`	96 bits	direcciones IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones "empotradas."
`::ff:xx:xx:xx:xx`	96 bits	direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
`fe80::` - `feb::`	10 bits	direcciones link-local	equivalentes a la dirección de loopback de IPv4
`fec0::` - `fef::`	10 bits	direcciones site-local	Equivalentes al direccionamiento privado de IPv4
`ff::`	8 bits	multicast	
`001` (base 2)	3 bits	direcciones unicast globales	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son "001".

Hay que resaltar que las direcciones de difusión (< inglés *broadcast*) no existen en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1, denominada *todos los nodos* (< inglés *all nodes*)

5.10.11 Número de direcciones disponibles en Ipv6

El número de direcciones IP disponibles en IPv6 es igual al número máximo que se puede representar con 128 bits, es decir:

$$2^{128} = 3.4 * 10^{38}$$

La cifra que representa este número es tan increíblemente grande que resulta difícil de imaginar.

Para hacernos una idea de su magnitud podemos compararla con el número de estrellas de la Vía Láctea, que es unos cien mil millones. Necesitaríamos 100 mil billones de galaxias iguales a nuestra Vía Láctea para juntar tantas estrellas como direcciones IP tendrá la nueva Internet. Aunque es sabido que existen miles de millones de galaxias, seguramente no nos

arriesgamos demasiado si decimos que la nueva Internet tendrá más direcciones IP disponibles que estrellas existen en el Universo.

Otra comparación posible es con el número de átomos de la materia. Necesitaríamos 67.000 toneladas de hierro para juntar tantos átomos de dicho metal como direcciones IPv6 existen. Si en lugar de hierro nos fijamos en la atmósfera, necesitaríamos un cubo de unos 23 Km. de lado para que el aire encerrado en él tuviese tantas moléculas como direcciones IP en la Internet de nueva generación.

5.10.12 Asignación de las nuevas direcciones IPv6 a los usuarios

Los proveedores e ISP europeos que están ya en el proceso de implantación de la nueva versión del protocolo IP siguen las instrucciones del RIPE respecto a cómo repartir el enorme espacio de direccionamiento IP versión 6 entre sus clientes.

Existe una diferencia muy grande entre las recomendaciones para la asignación de las direcciones IP versión 4, que busca ante todo la economía de direcciones, pues como es sabido falta muy poco tiempo para que se agoten, y las de la versión 6 que busca la flexibilidad.

RIPE recomienda a los ISP y operadores que asignen a cada cliente de IPv6 una subred del tipo /48 con el fin de que el cliente pueda gestionar sus propias subredes sin tener que utilizar NAT.

Con el protocolo IP versión 4 un cliente de conectividad (por ejemplo con una conexión RDSI Red Digital de Servicios Integrados) de arsys.es podría tener como mucho una única dirección IP fija para su red. Las direcciones IP de los equipos de su red local deberían ser privadas (192.168.X.X) y utilizar NAT para dar salida a Internet a su red local.

Sin embargo, con IPv6 el cliente recibiría una subclase como la siguiente:

2001:0ba0:1c01::/48

Dicho cliente puede a su vez crear en sus instalaciones 65.535 subredes diferentes, que son las combinaciones creadas variando w,x,y,z en el grupo:

2001:0ba0:01b0:wxyz::/64

Cada una de esas 65.535 subredes que nuestro cliente puede crear, puede a su vez tener más de 18 trillones de direcciones IP diferentes, que pueden ser de asignación automática (plug and play) o manual por el cliente.

Para utilizar IPv6 en su ordenador necesita tener instalado como protocolo de red el software IP versión 6, el cual está disponible para prácticamente todos los sistemas operativos. En el caso de Windows XP y Windows 2003, el software viene incorporado con

el sistema operativo, aunque es necesario instalarlo ya que no viene instalado como protocolo de red por defecto.

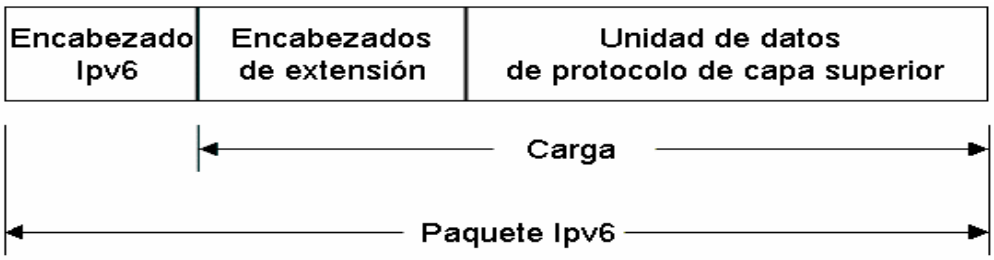
Para los restantes sistemas operativos deberá descargar el software correspondiente para la pila TCP/IP en versión 6 e instalarlo en su equipo.

5.10.13 Estructura de un paquete IPv6

Un paquete en IPv6 está compuesto principalmente de dos partes: la cabecera y los datos.

La cabecera está en los primeros 40 bytes del paquete y contiene las direcciones de origen y destino (128 bits cada una), la versión de IP (4 bits), la clase de tráfico (8 bits, Prioridad del Paquete), etiqueta de flujo (20 bits, manejo de la Calidad de Servicio), longitud del campo de datos (16 bits), cabecera siguiente (8 bits), y límite de saltos (8 bits, Tiempo de Vida). Después viene el campo de datos, con los datos que transporta el paquete, que puede llegar a 64k de tamaño en el modo normal.

En Ipv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en Ipv4 en donde los routers pueden fragmentar un paquete. En IPv6, las opciones también se salen de la cabecera estándar y son especificadas por el campo "Cabecera Siguiente" (*Next Header*), similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción "ruta fijada desde origen" (*Strict Source and Record Routing*) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo "Cabecera Siguiente" indicando que una cabecera de encaminamiento es la siguiente en venir. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e indicar que, por ejemplo, la cabecera TCP será la siguiente.



- *Encabezado de IPv6***:** El encabezado de IPv6 siempre está presente y tiene un tamaño fijo de 40 bytes. Los campos del encabezado de IPv6 se describen detalladamente más adelante en este mismo documento.

- *Encabezados de extensión*: Puede no haber ninguno o que haya varios encabezados de extensión con distintas longitudes. Un campo Next Header (Encabezado siguiente) en el encabezado de IPv6 indica el siguiente encabezado de extensión. En

cada encabezado de extensión hay otro campo Next Header que indica el siguiente encabezado de extensión. El último encabezado de extensión indica el protocolo de

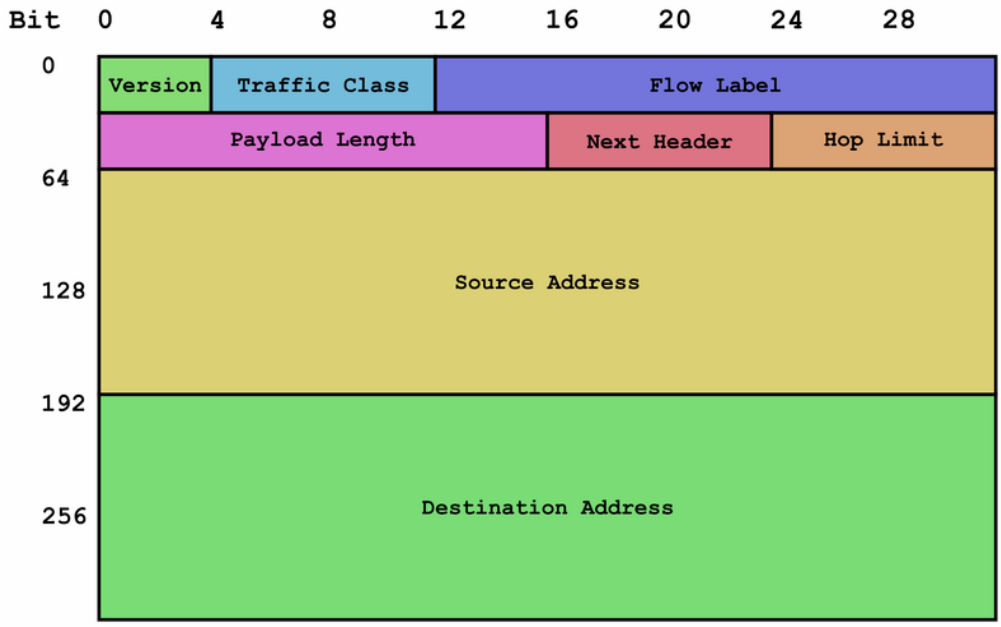
nivel superior (como TCP, UDP o ICMPv6) contenido en la unidad de datos del protocolo de nivel superior.

El encabezado de IPv6 y los encabezados de extensión reemplazan al encabezado de IPv4 con opciones. El formato del nuevo encabezado de extensión permite ampliar IPv6 para que pueda responder a futuras necesidades y ofrezca más capacidades. A diferencia de las opciones del encabezado de IPv4, los encabezados de extensión de IPv6 no tienen un tamaño máximo y pueden ampliarse para aceptar todos los datos de extensión necesarios para la comunicación con IPv6.

- *Unidad de datos del protocolo de nivel superior*: La unidad de datos de protocolo (PDU, Protocol Data Unit) de nivel superior suele constar de un encabezado de protocolo de nivel superior y su carga (por ejemplo, un mensaje ICMPv6, un mensaje UDP o un segmento TCP).

  La carga del paquete IPv6 es la combinación de los encabezados de extensión de IPv6 y la unidad PDU de nivel superior. Normalmente, puede tener hasta 65.535 bytes. Las cargas con una longitud superior a los 65.535 bytes se pueden enviar mediante la opción de carga Jumbo en el encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto).

Estructura de la cabecera de un paquete IPv6



-Versión: Es un campo de 4 bits que designa que el paquete es de IPv6 (0110).Todo el software IP debe verificar este campo antes de procesar el datagrama, para ver si el formato coincide con las especificaciones y la versión esperada.

-Clase de tráfico: Este es un campo de 8 bits donde se puede dar especificar un identificador de diferenciación de tráfico. Actualmente varios grupos de la IETF están trabajando en la forma que mejor se pueda usar este campo.

-Etiqueta de flujo: Este campo de 20 bits es usado cuando se necesita un manejo especial de un paquete. Este contiene información que los enrutadores usan para asociar ciertos datagramas con un flujo y prioridad especifica. Por ejemplo se quiere establecer una videoconferencia, por lo tanto se fija un flujo que garantice un retardo mínimo entre el audio y el video. También un ISP podría contratar con sus clientes un flujo de datos específico, o distribuido de acuerdo a servicios o sitios que visita (QoS).

-Longitud de la carga útil: Es un entero de 16 bits usado para designar la longitud de la carga útil del datagrama IP (información), sin el encabezado base, la cual esta dada en octetos. Esto da 2^16 posibilidades, alrededor de 64000 octetos. Teniendo la posibilidad de transmitir paquetes tan grandes, en ciertas circunstancias puede significar un gran aumento en eficiencia. Cuando los paquetes son grandes, el numero de paquetes necesarios para enviar cierta información es menor, y cuando hay menos paquetes para enrutar, entonces el enrutador tiene mas tiempo para enrutar otros paquetes, o realizar otras tareas (manejo de cache, mantenimiento de tablas, etc).
Los encabezados extendidos si se incluyen en la longitud de la carga útil.

-Próximo encabezado: Este campo es designado para que los enrutadores sepan si hay más encabezados consecuentes que deben ser analizados en el datagrama. Este campo de 8 bits permite 255 posibilidades, de las cuales actualmente se tienen definidas unas cuantas.

1. Hop-by-hop Header: Son las propiedades que cada nodo por el que pase un paquete debe analizar.
2. Destination Options Header I: Son las opciones que el destino tiene para el manejo del paquete, este con el uso del encabezado hop by hop, puede denotar que el destino es el siguiente router.
3. Routing Header: Define una lista de nodos intermedios por el cual un paquete debe pasar para llegar a su destino.
4. Fragment Header: Es usado por el origen para enviar paquetes que son más grandes que el MTU definido. Contrariamente a IPv4, IPv6 no permite fragmentar un paquete durante el transito. Para esto descubre en la ruta por medio de ICMPv6 y el Hop-by-hop header el MTU mínimo de la ruta. Entonces este encabezado se usa cuando se requiere mandar un paquete más grande que el MTU descubierto.
5. Authentication Header: Permite garantizar que un paquete si pertenece al origen.

6. Encrypted Security Payload Header: Ahora que se puede garantizar que un paquete pertenece al origen, se debe garantizar que la carga útil pueda ser leída solo por el host destino. El encabezado de autenticación y este proveen lo que se conoce como IPsec.
7. Destination Options Header II: A diferencia del encabezado de destino I, este solo posee opciones para el destino, como las opciones de seguridad se encuentran antes, estas opciones se consideran seguras de extremo a extremo.

-Límite de saltos: Cumple una funcionalidad similar al TTL en IPv4. Especifica el número de saltos que un paquete, a nivel de la capa de red, puede tener. Un límite de estos es de mucha importancia para que no se den ciclos infinitos cuando haya problemas de enrutamiento. Al igual que en IPv4 este campo es de 8 bits y es inicializado en 255, decrementandose en 1 cuando pasa por un enrutador.

-Dirección origen: Es la dirección de la máquina que origina el paquete.

-Dirección destino: A diferencia de IPv4, esta no es necesariamente la dirección del destino, puede ser una dirección intermedia al destino, de acuerdo a los encabezados extendidos que se use (NEXT HEADER).

5.11 TRANSICIÓN DE IPV4 A IPV6

Hoy en día existen mecanismos que pueden ser implementados por hosts y routers IPv6 para mantener la compatibilidad con IPv4 los cuales agilizan la expansión de IPv6 en Internet y facilitan la transición. La clave para una transición exitosa a IPv6 es la compatibilidad con IPv4.
Los mecanismos están diseñados para ser empleados por hosts y routers IPv6 que necesitan interactuar con hosts IPv4 y que utilizan la infraestructura de enrutamiento de IPv4.

5.11.1 Mecanismos empleados

• **Dual IP layer (doble capa IP):** Consiste en proveer en hosts y routers un soporte completo tanto para IPv6 como para IPv4.

• **IPv6−over−IPv4 tunneling (IPv6 sobre IPv4):** Consiste en encapsular los paquetes de IPv6 dentro de los headers de IPv4 para transportarlos sobre las estructuras de enrutamiento actuales. Los dos tipos de túneles que se emplean son: configurados y automáticos.

La infraestructura IPv6 esta en una constante evolución. Mientras esta infraestructura se desarrolla y se expande, la infraestructura de enrutamiento existente (IPv4) puede seguir funcionando y ser utilizada para transportar trafico IPv6. Tunneling provee un camino para lograr esto.
Los hosts y routers IPv6/IPv4 pueden pasar datagramas IPv6 sobre regiones de topología de enrutamiento IPv4 encapsulándolos dentro de paquetes IPv4.

5.11.2 Formas en las cuales pueden ser usados los Túneles

• **Router-to-Router**: Los routers IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse entre sí paquetes IPv6. En este caso el túnel abarca un segmento del trayecto que toma el paquete IPv6.

• **Host-to-Router:** Los host IPv6/IPv4 pueden pasar paquetes IPv6 por un router IPv6/IPv4 intermediario que sea alcanzable por la infraestructura IPv4. Este tipo de túnel abarca el primer segmento del trayecto del paquete.

• **Host-to-Host:** Los hosts IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse paquetes IPv6 entre sí. En este caso el túnel abarca el recorrido completo que toman los paquetes.

• **Router-to-Host**: Los routers IPv6/IPv4 pueden pasar paquetes IPv6 hasta su host IPv6/IPv4 destinatario (final). Este túnel abarca el último segmento del recorrido.

Las técnicas de tunneling se clasifican según el mecanismo por el cual el nodo de encapsulamiento determina la dirección del nodo al final del túnel. En los primeros dos casos (Router-to-Router y Host-to-Router) el paquete IPv6 es pasado (tunneled) a un router. El endpoint de este tipo de túneles es un router intermediario el cual debe desencapsular el paquete IPv6 y reenviarlo a su destino final. Cuando se envían paquetes a un router, el endpoint del túnel es distinto del destino final del paquete que se esta enviando. Así, la dirección del paquete IPv6 que se envía no provee la dirección IPv4 del endpoint del túnel. Por esto, dicha dirección deberá obtenerse de la información de configuración en el nodo que ejecuta el tunneling. Por lo tanto se usa el termino tuneling configurado (configurate tunneling) para describir el tipo de túneles donde el endpoint esta explícitamente configurado.

En los últimos dos casos (Host-to-Host y Router-to-Host) el endpoint del túnel es el nodo al cual el paquete IPv6 esta direccionado. Por lo tanto el endpoint puede ser determinado por la dirección IPv6 de destino del paquete. Si dicha dirección es una dirección IPv6 compatible con IPv4 entonces los últimos 32 bits especifican la dirección del nodo de destino y se puede usar como dirección del endpoint del túnel. De esta forma se evita configurar explícitamente de la dirección del endpoint. Esta técnica es llamada tuneling automático.

5.11.3 Diferencias entre las dos técnicas de Tunneling

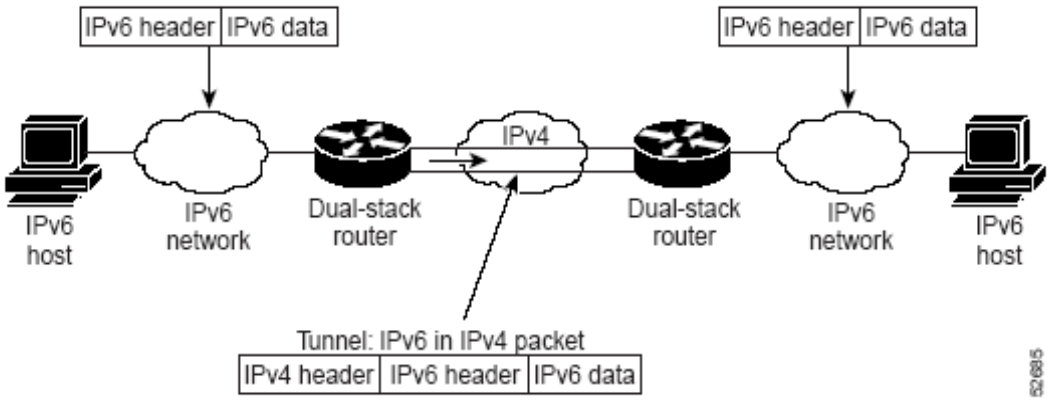
Las dos técnicas de tunneling se diferencian principalmente en como se valen para determinar la dirección del endpoint del túnel. La mayor parte de estos mecanismos son lo mismo:

• El nodo de entrada del túnel (nodo de encapsulamiento) crea un paquete IPv4 en el que encapsula el paquete IPv6, y lo transmite encapsulado. El header IPv4 contiene las direcciones fuente y destino y el cuerpo del paquete contiene el header IPv6 seguido inmediatamente por los datos.

• El nodo de salida del túnel (nodo de desencapsulamiento) recibe el paquete encapsulado, elimina el header IPv4, actualiza el header IPv6 y procesa el paquete IPv6 recibido.

		Cabecera IPV4
Cabecera IPV6		Cabecera IPV6
Cabecera de capa de transporte		Cabecera de capa de transporte
Datos		Datos

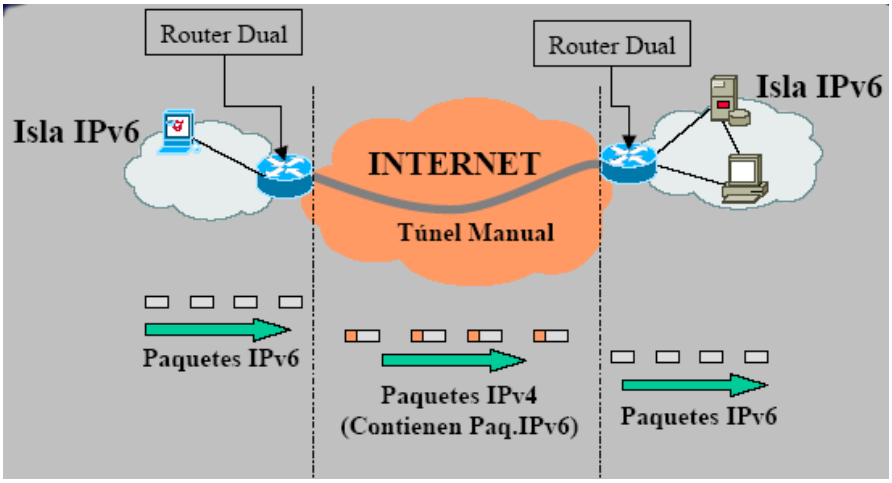
En un futuro probablemente se desarrollen mecanismos alternativos



5.12 INSTALACIÓN Y CONFIGURACIÓN DE UN ROUTER CON SOPORTE IPV6 SOBRE LINUX

Funcionalidad: interconectar islas IPv6 a través de océanos IPv4.

• Cada extremo es un nodo dual y en ellos se configura direcciones IPv6 e IPv4 tanto local como remotas.



5.12.1 Cisco IOS recomendados para integrar IPV6 en la red

Cisco ha ofrecido soporte para IPV6 desde mayo de 2001 cuando estuvo disponible Cisco IOS 12.2T, para permitir a los clientes comenzar a experimentar con IPv6. Hoy, IPv6 está disponible en muchas versiones de Cisco IOS. Nuestras recomendaciones sobre las versiones de Cisco IOS para los clientes que están buscando soporte para IPv6, son:

- Producción General: Cisco IOS 12.3M
- Core ISP y NREN: Cisco 12.0S en los routers de Cisco de las series 12000 y 10720
- Infraestructura empresarial e ISP: Cisco IOS 12.2S
- Acceso de Banda Ancha: Cisco IOS 12.2B
- Nuevo despliegue tecnológico IPv6: Cisco IOS 12.3T y 12.2S

Con esto queremos decir que prácticamente todos los modelos de cisco soportan ipv6 por lo menos los mas actuales y aquellos que cumplen un mínimo de por lo menos 256 de RAN y 64 M de FLASH lo único que se tiene que hacer es actualizar el IOS del router como lo explicaremos mas adelante y listo tenemos un router con soporte ipv6 claro esta que esto solo es para las universidades o cualquier otro institución que quiera conectarse a RENIA.

En el caso del panorama RENIA-CLARA es necesario como mínimo un Cisco 2800 Integrated Services Routers La serie Cisco 2800 ha sido diseñada para cubrir los requisitos de las pequeñas y medianas empresas, también es ideal para comunicar pequeñas sedes con la red de la empresa. Permite transmitir de forma segura datos, voz y vídeo con una gran eficiencia.

Se trata de la evolución de la serie 2600 y esta formada por los siguientes modelos:

- Cisco 2801

- Cisco 2811
- Cisco 2821
- Cisco 2851

En nuestro caso se utilizara un cisco 3660 mas adelante se explicara con detalle.

5.12.2 Pasos a seguirse en la configuración del router 3660

1. enable
2. configure {**terminal** | **memory** | **network**}
3. interface tunnel *tunnel-number*
4. ipv6 address *ipv6-prefix*/*prefix-length* [**eui-64**]
5. tunnel source {*ip-address* | *type number*}
6. tunnel destination *ip-address*
7. tunnel mode ipv6ip

Ejemplo de comando	Detalles
Router> enable	Permite modo privilegiado de EXEC. Incorpore su contraseña si está incitado.

Router# configure terminal Entra en modo global de la configuración.

Router(config)# interface tunnel 0 Especifica un interfaz y un número del túnel, y entra en modo de la configuración del interfaz.

Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127 Especifica la red IPv6 asignada al interfaz y permite IPv6 que procesa en el interfaz. La nota refiere a la conectividad básica de configuración para el módulo IPv6 para más información sobre la configuración de las direcciones IPv6.

tunnel source {ip-address | type number}
Router(config-if)# tunnel source ethernet 0 Especifica la dirección de la fuente IPv4 o la fuente interconecte el tipo y el número para el interfaz del túnel. ¿? Si se especifica un interfaz, el interfaz se debe configurar con una dirección IPv4.

Router(config-if)# tunnel destination 192.168.30.1 Especifica la dirección de la destinación IPv4 o el nombre de anfitrión para el interfaz del túnel

Router(config-if)# tunnel mode ipv6ip Especifica un túnel manual IPv6. nota: El comando del modo ipv6ip del túnel especifica IPv6 como el protocolo del pasajero e IPv4 como la encapsulación y transporte protocolan para el túnel manual IPv6.

5.12.3 Pasos para verificar la configuración de Router

Pasos

1. enable
2. show interfaces tunnel *number* [**accounting**]
3. ping [*protocol*] *destination*
4. show ip route [*address* [*mask*]]

Router> enable: Permite niveles más altos del privilegio, tales como modo privilegiado de EXEC. ¿? Incorpore su contraseña si está incitado.

Router# show interfaces tunnel 0 información (opcional) del interfaz del túnel de las exhibiciones. ¿? Utilice la discusión del número a la información de exhibición para un túnel especificado.

Router# ping 10.0.0.1 conectividad básica de la red de las diagnosis (opcionales).

Router# show ip route 10.0.0.2 (opcional) exhibe el estado actual de la tabla de encaminamiento. Se demuestra la nota solamente la sintaxis relevante para esta tarea.

5.13 APLICACIONES DE IPV6

- **Chat**
  - IRC: cliente BitchX
  - RAT y SDR

- **Correo**
  - Exim
  - Qmail
  - Public Sendmail
  - WIDE Sendmail

- **DNS**
  - BIND 9 Beta 2
  - Totd

- **Firewall**
  - ipfilter
  - IPFW

- **FTP**
  - LFTP
  - NcFTP (Windows)
  - NcFTP (BSD)

- **Java**
  - Ipv6 Java (Windows)

- **Herramientas de Monitoreo**
  - ASPath-tree
  - Link View
- **Noticias**
  - INN v2.2.2
  - Mnews

- **Parches**
  - Linux
  - KAME
  - WIDE

- **Software para Sockets**
- IPV6 socket 1.1
- Trumpet winsock

- **Traductores IPV6/IPV4**
- Toolnet6
- Traductor IPV6/IPV4 (Windows)

- **Para Tuneles**
- BT Ultima Ipv6 Access
- CSELT Tunnel Broker
- V6tun

- **Juegos**
- Quakeforge

- **Analizador de protocolos**
- Link View (Reconoce paquetes de IPV6.

- **Videoconferencia**
- 6UMS
- GnomeMeeting
- ISABEL
- MPEG-4IP
- Vic y Rat
- VOCAL
- Access Grid

6. METODOLOGÍA DE IMPLEMENTACIÓN

6.1 SITUACION TECNICA ACTUAL DE GEANT Y CLARA

LA RED GEANT

La red paneuropea de investigación a alta velocidad GÉANT entró en funcionamiento en noviembre de 2001 por un periodo de cuatro años. Está interconectada con 28 redes nacionales y regionales de investigación y de educación (NREN) de unos treinta países y ofrece servicios a más de 3.000 instituciones.

Financiada por la Comisión Europea y administrada por el consorcio DANTE, la red GÉANT sustituye a la red TEN-155 que utilizaba la tecnología ATM de 155 Mbit/s sobre una infraestructura de unos 22.000 km. En el momento en el que se inauguró GÉANT, había nueve enlaces de núcleo de 10 Gbit/s y otros once enlaces de núcleo de 2,5 Gbit/s. Durante el proyecto se actualizarán varios enlaces de menor capacidad.

GÉANT soporta tráfico de producción dentro de programas de investigación informática distribuida (GRID), aplicaciones nativas y multicast, VPN y el protocolo IPv6. Se conecta mediante tres circuitos dedicados de 2,5 Gbit/s con la red de investigación estadounidense Abilene, lo que le permite ser un par de la red de base Abilene de Nueva York y participar en el servicio International Transit Network (ITN) de los pares de Abilene fuera de Estados Unidos, junto a CA*net.

Compararla con la americana Internet2 permite comprender lo importante de la apuesta. Gèant une más de 3.000 centros de investigación de 32 países, frente a los poco más de 180 centros de Internet2. Su velocidad en muchos tramos es de 10 Gigabits por segundo, cuatro veces más que la estadounidense. Y cuando ésta alcance la capacidad europea actual, en unos dos años, Gèant estará en los 40 Gigabits.

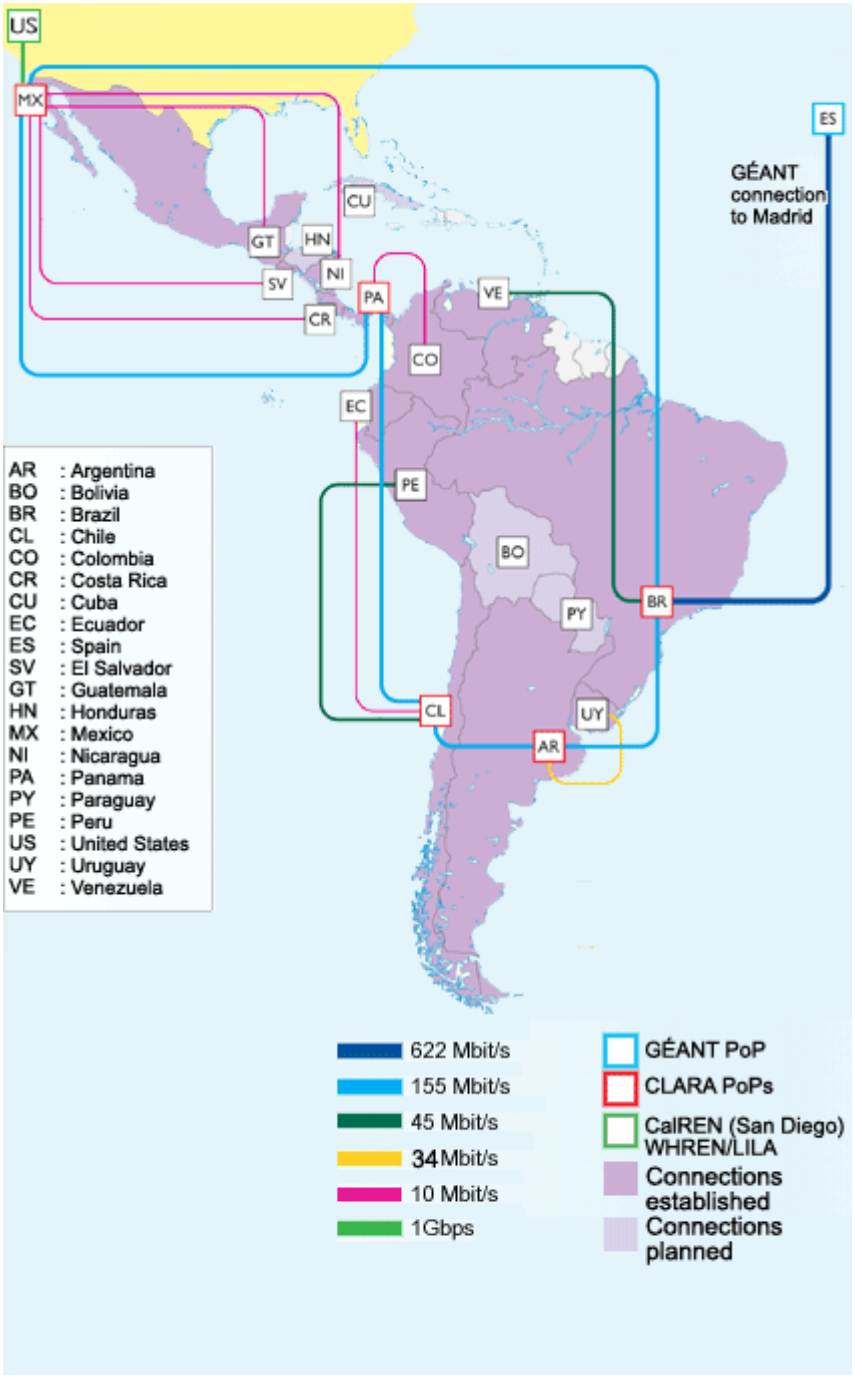
RedCLARA se conecta con las Redes Académicas del mundo mediante la red paneuropea GÉANT.

RED GEANT:

INTERNET2
Tijuana / México
CU
HN
GT
SV
CR
PN
Venezuela / Caracas
Colombia / Bogotá
Ecuador / Quito
CU Cuba / Habana
HN Honduras /Tegucigalpa
GT Guatemala /Ciudad de Guatemala
SV El Salvador/ San Salvador
NI Nicaragua / Managua
CR Costa Rica / San José
PN Panamá / Ciudad de Panamá
Perú / Lima
Bolivia / La Paz
Brasil / Brasilia
Paraguay / Asunción
Uruguay / Montevideo
Chile / Santiago
Argentina / Buenos Aires
GEANT
RED CLARA

SITUACION TÉCNICA ACTUAL DE CLARA

Mapa de la Topología de RedCLARA Abril 2006



Descripción Técnica

CLARA es responsable de la implementación y manejo de una infraestructura de red que interconectará a las redes académicas nacionales (NREN) de América Latina.

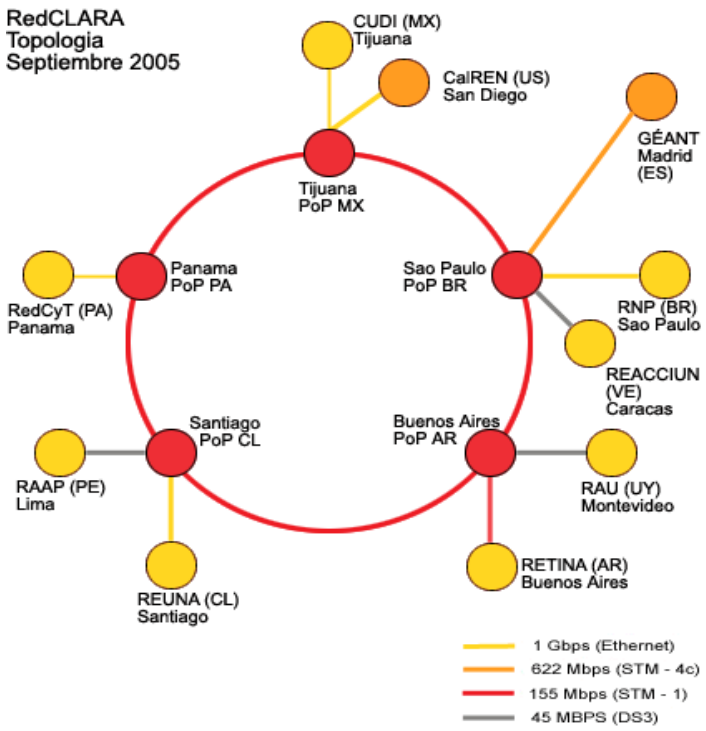
Con un gran número de universidades y centros de investigación conectados a RedCLARA, muchos proyectos que carecían de una infraestructura adecuada para sustentar los procesos de comunicación y colaboración, hoy están en posición de avanzar.

La troncal (backbone) de RedCLARA está compuesta por cinco nodos enrutadores principales, conectados en una topología de anillo. Cada nodo principal representa a un PoP para RedCLARA, y cada uno de ellos está ubicado en un país de América Latina.

Los cinco principales nodos IP de RedCLARA están ubicados en São Paulo (Brasil - BR), Buenos Aires (Argentina - AR), Santiago (Chile - CL), Panamá (PA) y Tijuana (México - MX). Todas las conexiones de las redes nacionales latinoamericanas (NREN) a RedCLARA serán a través de uno de estos cinco nodos. La troncal de CLARA está interconectada con la red paneuropea GÉANT a través del enlace del PoP de CLARA en São Paulo con el punto de acceso de GÉANT en Madrid (España - ES).

Cuando una NREN latinoamericana hace conexión con RedCLARA, lo hace a través de uno de los cinco nodos principales de la troncal de CLARA; esta conexión le brinda a estas NREN y sus miembros (clientes) acceso a RedCLARA, otorgándoles un Punto de Intercambio.

Troncal de RedCLARA y actuales NREN latinoamericanas conectadas



Entre sus múltiples tareas:

- Videoconferencia
- Voz sobre IP
- Seguridad
- Multicast
- Ipv6
- Enrutamiento Avanzado
- Mediciones

Entre las redes Latinoamericanas que conforman la Red Clara se encuentran:

Ecuador	CEDIA
El Salvador	RAICES
Guatemala	RAGIE
Honduras	UNITEC
México	CUDI
Nicaragua	RENIA
Panamá	REDCyT
Paraguay0.	Arandu
Peru	RAAP
Estados Unidos	UCAID
Uruguay	RAU
Venezuela	REACCIUN
Canadá	CANARIE
Argentina	RETINA
Bolivia	BolNet
Brasil	RNP
Chile	REUNA
Costa Rica	CRNET
Cuba	RedUniv.

6.2 ANÁLISIS DE LA SITUACION ACTUAL DE RENIA

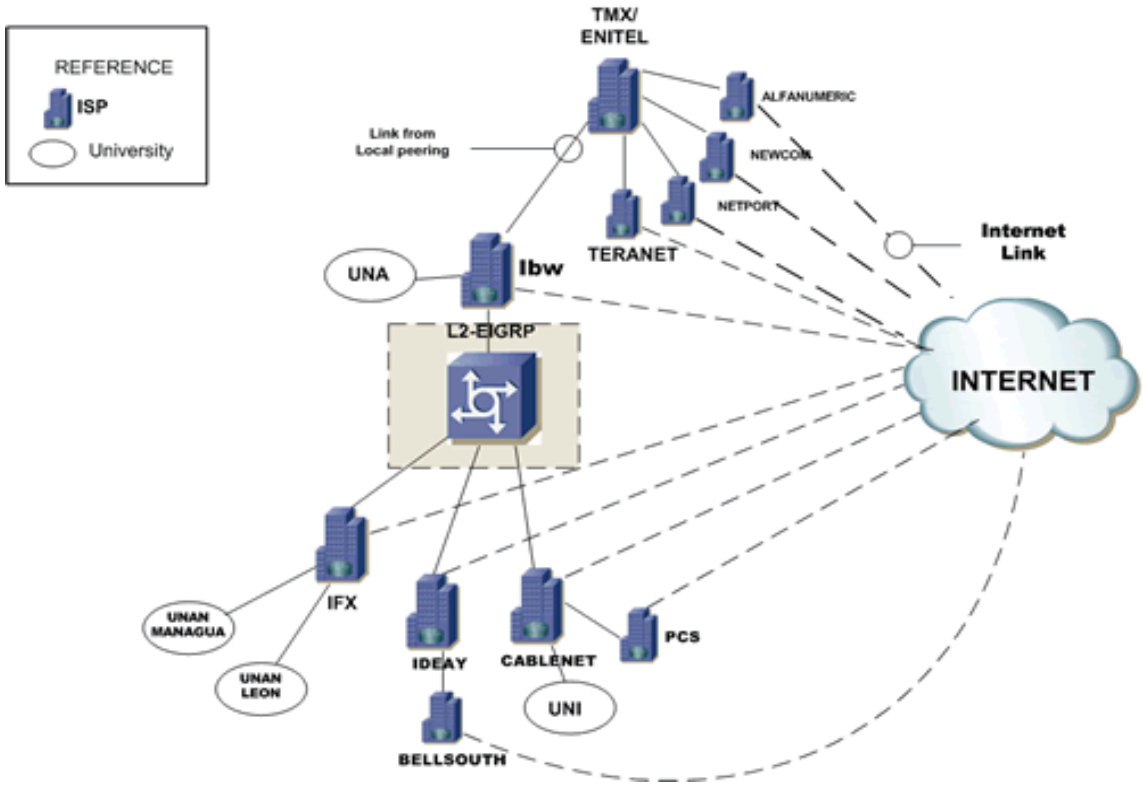
RENIA (Red Nicaragüense de Internet Avanzada)

Es un organismo de cooperación técnica, constituido por las redes universitarias de Internet afiliadas, que promueve elevar la capacidad y calidad de los servicios de Internet Avanzada de sus miembros, la inclusión de nuestro país, el acceso a la red mundial de Internet2/GEANT2 y la reducción de la brecha digital.

El pasado 20 de marzo RENIA, la red nicaragüense de Internet Avanzada, se conectó por primera vez a RedCLARA. Con esto Nicaragua fue la red número 13 de las conectadas a esta gran red en Latinoamérica.

Con esta conexión, RedCLARA ya cuenta con 13 países conectados, haciendo cada vez más cercano el éxito de este proyecto.

Diagrama actual de conexión a Internet de las Universidades pertenecientes a RENIA



6.2.1 Entrevistas con los principales impulsores de la red

En muchas ocasiones tuvimos la oportunidad de visitar la UNAN-MANAGUA e IBW teniendo la oportunidad de entrevistar de manera informal a las personas mayormente involucradas en el Proyecto de IPV6 entre ellos encontramos:

Director ejecutivo de RENIA: Ing. Roberto Blandino (**UNA**)
Coordinador Técnico: Ing Marcos Cárcamo Narváez (**UNAN-León**)

Comité Técnico:

- Marvin Castañeda. UNI
- Juan Navas. UNAN-Managua
- Derman Zepeda. UNAN-Managua
- Peter Pettersson. UNA
- Oscar Delgado Cuadra. UNAN-León
- Cesar Real Lechado. UNAN-León

- Ángela Chow IBW
- Marvin Bonilla IBW

Con el Ing Roberto Blandino nos planteo los distintos proyectos a desarrollar una vez Implementado y Desarrollado Ipv6 en Nicaragua (RENIA).

El Ing. Marcos Cárcamo nos ha brindado información acerca de la topología de la Red, días de reuniones, sobre los avances que se han tenido en cuanto al proyecto de IPV6 y las nuevas configuraciones y conexiones. Además de facilitarnos todos los recursos para llevar a cabo nuestro trabajo monográfico.

Derman Zepeda de la UNAN-Managua nos ha facilitado información acerca de la configuración del túnel en el Routers de RENIA. Así como también nos informa de los avances que se van desarrollando los cambios que se han ido realizando, las nuevas configuraciones y algunas pruebas fuera de las reuniones.

Peter Pettersson de la UNA nos ha ayudado en la configuración de nuestro servidor en cuanto a router y túnel para realizar pruebas en IPV6.

Ángela Chow de IBW se tomo la tarea de explicarnos detalladamente algunos puntos abordados en las reuniones. Demostración de la configuración de cliente en las pruebas de las conexiones de IPV6.

Juan Navas de la UNAN-Managua nos ha facilitado recursos en la UNAN-Managua (computadora, ip pública), para realizar las pruebas de IPV6.

6.2.2 Informe Reuniones RENIA

En las reuniones realizadas por encuentros en UNAN-Managua. En las que estuvieron presente los miembros de:

Director ejecutivo de RENIA: Ing. Roberto Blandino (**UNA**)
Coordinador Técnico: Ing Marcos Carcamo Narváez (**UNAN-León**)

- Ángela Chow IBW
- Oscar Delgado Cuadra. UNAN-León
- Derman Zepeda. UNAN-Managua
- Peter Pettersson. UNA
- Marvin Bonilla IBW
- Cesar Real Lechado. UNAN-León
- Marvin Castañeda. UNI
- Bayardo Silva

En la primera reunión a la que asistió el grupo de IPV6, la cual fue expuesta por el Lic. Derman Zepeda en agosto en la UNAN-MANAGUA, se abordaron temas sobre modelos y tipo de direccionamiento de IPV6, así como una Introducción general acerca de que es IPV6 y como funciona.

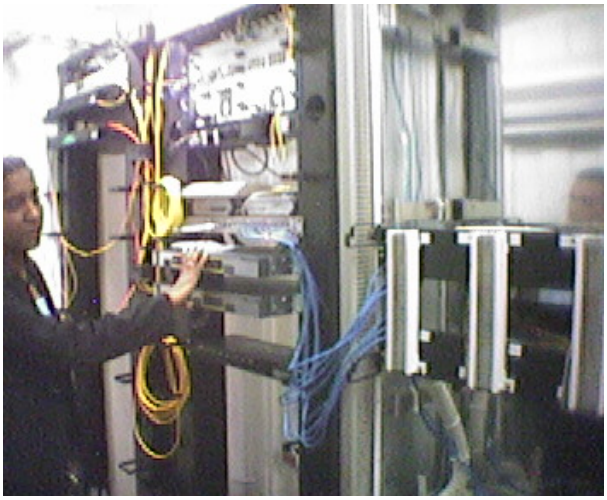
La segunda reunión fue expuesta en septiembre en la UNAN- Managua por Eugenio Icaza de ENTRESA (Sistema de Transporte de Energía Eléctrica) en la que se expuso todos y cada uno de los puntos en las que se ha implementado la conexión por fibra

óptica en el territorio Nacional, haciendo énfasis en los tipo y modelos de equipos utilizados en esta gran Red.

En una de las visitas a IBW realizada en octubre, conocimos el lugar donde está ubicado el Router de RENIA, la encontramos con la siguiente situación en la que fuimos guiados por Ángela Chow de IBW:

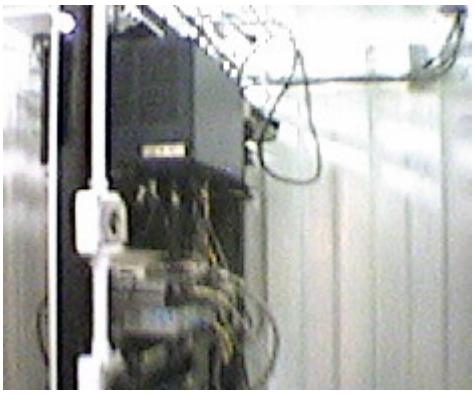
Este es el cuarto en el que se encuentran los switch y los router que dan conexión a cada Universidad. En este cuarto no se puede entrar con zapatos por problemas de contaminación a los equipos y se encuentra las 24 horas hermético.

Desde esta máquina se accedían a cada uno de los router y para mantener un control de ellos. Esta máquina está encendida todo el tiempo.



En uno de estos paneles se ubica el Router de Renia que dará conexión por fibra óptica a cada una de las Universidades

Este es el cable de fibra óptica por donde da conexión del Router a cada Universidad perteneciente a Renia.



Aquí va la salida del cable de fibra óptica

En otra de las reuniones realizadas en octubre en la UNAN-MANAGUA, expuesta por Ing. Peter Pettersson en la que se realizaron pruebas sobre la configuración manual de un túnel 6to4 y la configuración de enrutamiento cuyos resultados fueron exitosos.

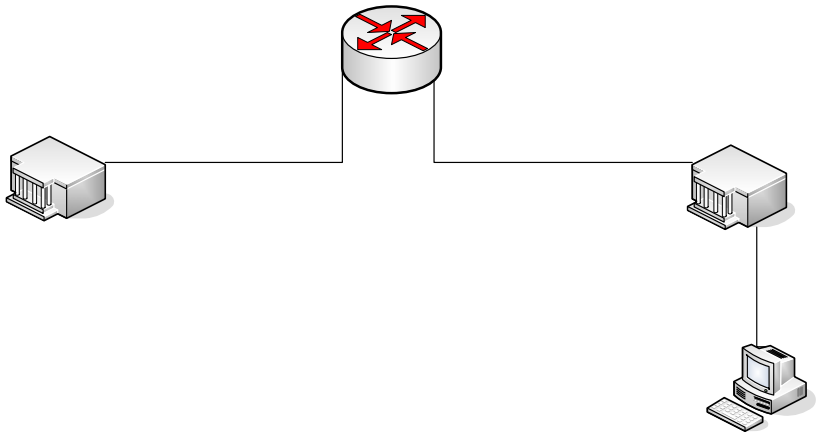
En noviembre asistimos a otras de las reuniones llevadas a cabo en IBW, la cual fue expuesta por el Ing. Marvin Bonilla en la que se trataron los métodos a utilizar para

integrarse a la RedCLARA y se llevo cabo una pequeña demostración de la configuración de Dual- Stack.

En otra de las reuniones en diciembre en la UNAN- MANAGUA

Teniendo disponibles los recursos: 2 servidores, 1 clientes y acceso al Router de RENIA.

Siendo estas pruebas precedidas por: Peter Pettersson. (UNA).Se planteo el siguiente diagrama para realizar algunas prácticas sobre el mecanismo de conexión Ipv6:



Se configuro el router RENIA, se asignaron direcciones a cada uno de los puntos (Universidad 1, Universidad2, cliente) registradas en el Router de Renia y se realizaron ping6 entre ambos servidores, luego se instalo el protocolo en el cliente (Windows) asignamos su dirección de Ipv6, desactivamos el Firewall y desde ahí se hizo ping6 y tracert6 hacia los diferentes puntos de la conexión. Obteniendo resultados exitosos en cuanto a la conexión entre los equipos Ipv6.

En febrero del 2006 asistimos a UNAN-Managua, en esta ocasión trasladamos nuestro servidor para realizar algunas pruebas del túnel 6to4, teniendo resultados exitosos, en esta ocasión tuvimos el apoyo del Lic. Derman Zepeda (UNAN-Managua) y el Ing. Peter Pettersson (UNA).

En marzo realizamos una visita a UNAN-Managua trasladando de nuevo nuestro servidor esta vez con el propósito de realizar pruebas de ping en Ipv6 (ping6), una vez ya configurado nuestro túnel, y configurado el radvd en nuestro servidor. Estas pruebas se llevaron a cabo de forma exitosa. Esta vez teniendo el apoyo del Ing. Juan Navas (UNAN-Managua), el Ing. Peter Pettersson (UNA) y Lic Derman Zepeda. En esta reunion los tecnicos acordaron cambiar de switch 3750 a Router Cisco 3660 por lo que el switch con capacidad de Ruteo presentaba algunos

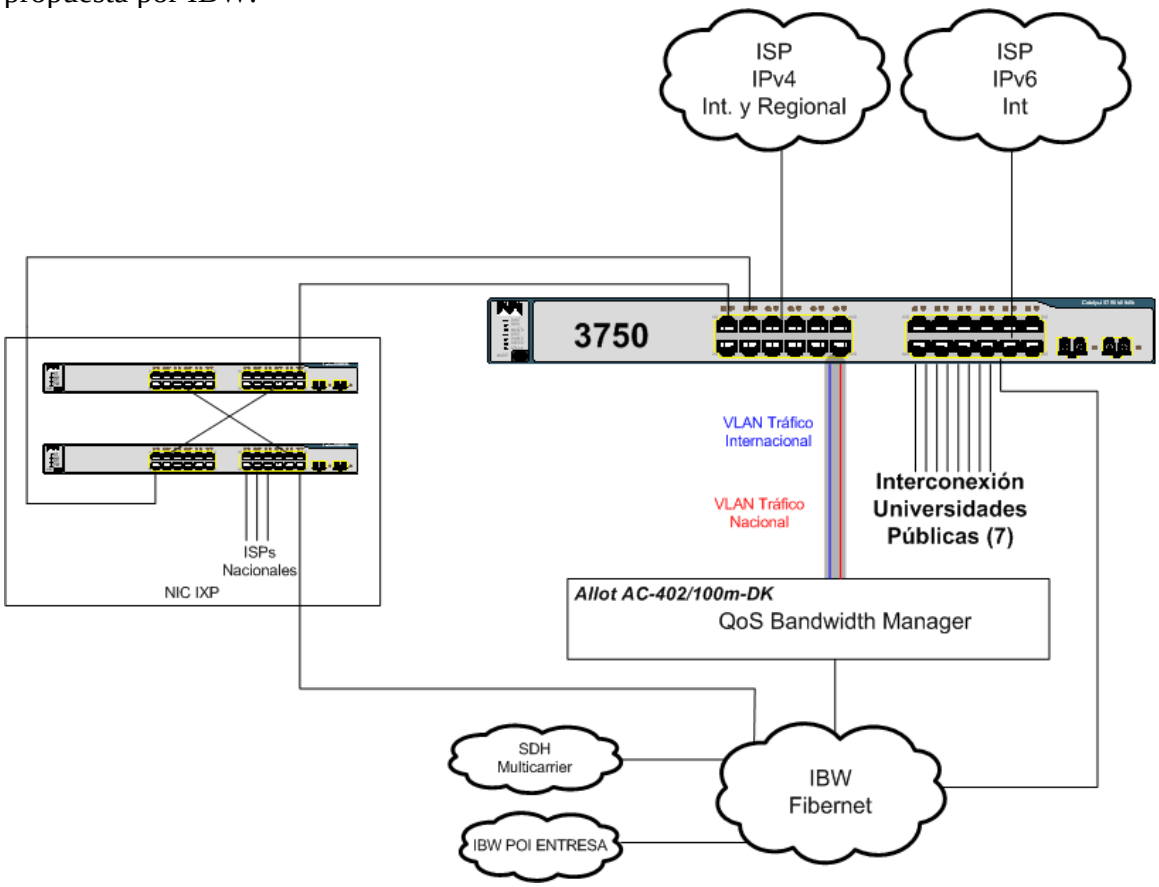
problemas al almacenar gran cantidad de direcciones. Presentamos la configuración del 3750 en el anexo 4

El 25 de Abril se realizo una reunión en UNA Managua de los técnicos donde conocimos la topología interna de la UNA expuesta por Ing. Peter Pettersson informando acerca de los avances ha experimentado, en esta reunión se dio diferentes opiniones de la topología de Renia, también se informo de las características de los equipos con el que cuenta cada Universidad para la conexión de RENIA, se trato acerca de la actualización de la pagina de Renia www.unanleon.edu.ni/renia con nuevos documentos y se acordaron fechas para las próximas reuniones.

6.2.3 Topologías Analizadas en RENIA

El Router de Renia se encuentra ubicado en el edificio de AIN en Managua.

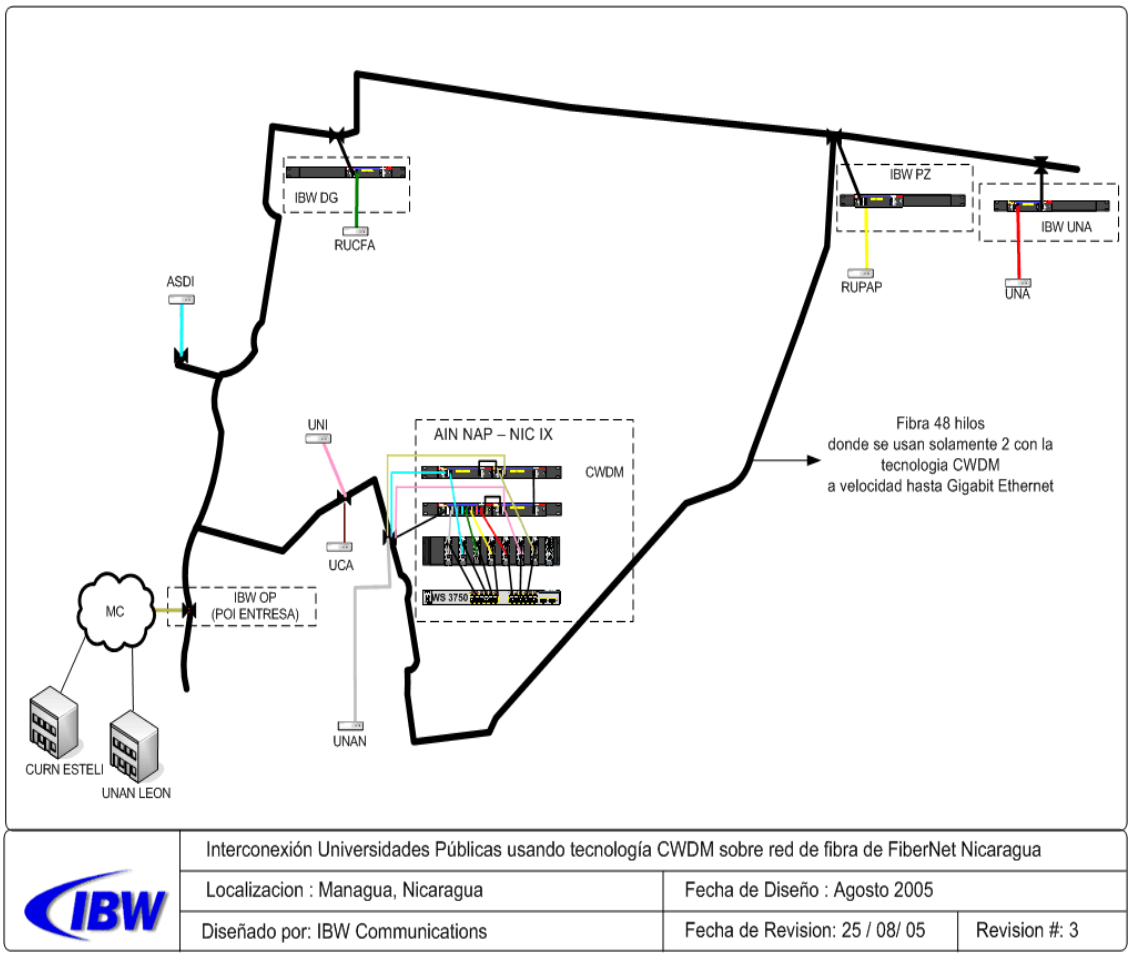
Escenario 1: Esta es la topología que se tenía en un principio en agosto 2005 propuesta por IBW.



Esta es una de las primeras propuestas echa por IBW en colaboración para impulsar lo que es RENIA, se tiene swith 3750 apila hasta nueve switches como una única unidad

lógica para obtener un total de 468 puertos Ethernet 10/100 o 252 puertos Ethernet 10/100/1000 al cual se conectaran las entidades pertenecientes a RENIA de forma directa a través de fibra óptica y creara redundancia conectándose al NIC IXP nacional y además proporcionara conexión a ISP, este 3750 proporcionando SMI que da lugar a funciones avanzadas de calidad de servicios (QoS) , limitación de velocidad de transferencia, listas de control de acceso (ACL) y enrutamiento de protocolo de información enrutada (RIP) y básico estático.
La EMI incomparada ofrece un conjunto más completo de funciones de clase empresarial, incluido el enrutamiento avanzado de uní difusión y multidifusión de IP basado en hardware.

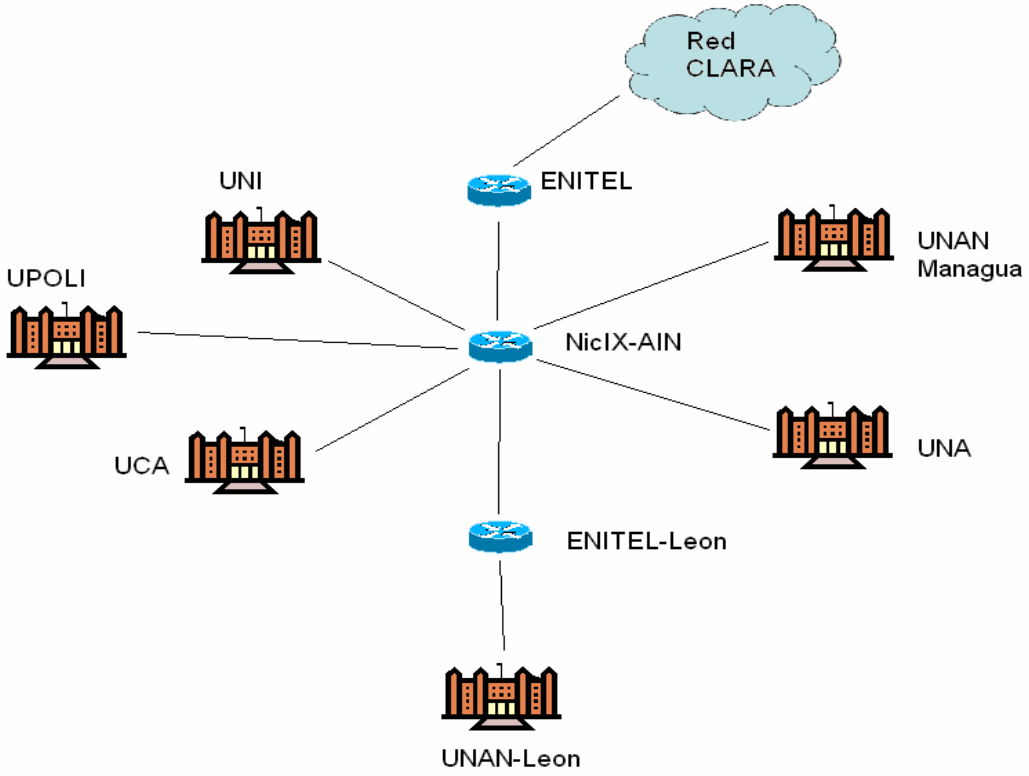
Escenario 2: Esta es la segunda propuesta por medio de fibra óptica



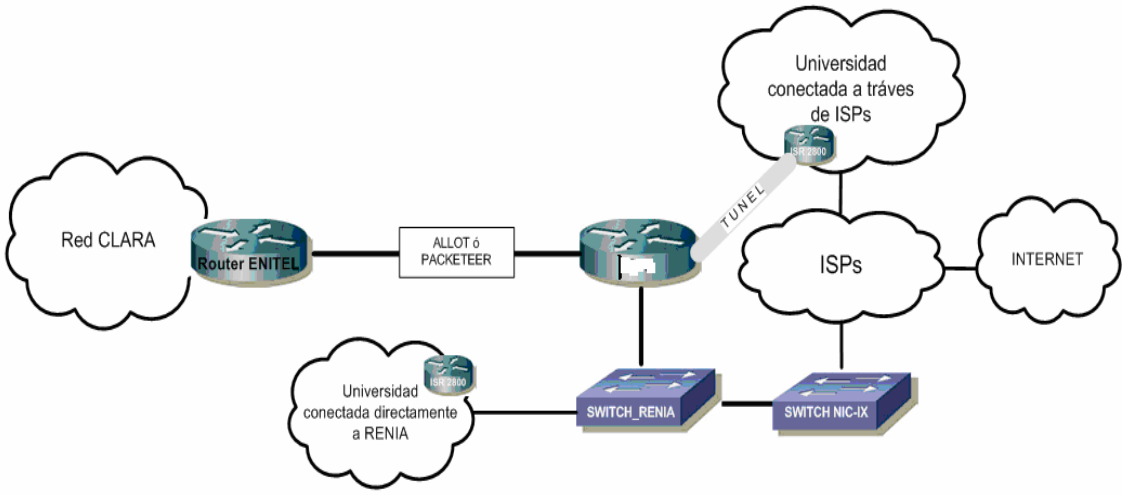
Esta es la segunda propuesta en la cual se puede ver que el panorama de conexión directa ofrecida en el primer escenario no va a ser posible por causas económicas la conexión se realizara a través de ISP en los cuales tenemos a IBW, telered y AMNET claro esta que el medio de conexión será proporcionado por ENTRESA la cual nos

brindara el medio de conexión a través de fibra óptica de 48 hilos con velocidades hasta de giga bit ethernet de los cuales 2 hilos serán utilizados con velocidades hasta de giga bit ethernet .

Escenario 3: Esta es la tercera topología propuesta:
Red Nicaragüense de Internet Avanzada



Escenario 4: Esta es la última propuesta de la interconexión de RENIA consensuada por el comité técnico de RENIA en Abril 2006:



6.3 ESPECIFICACIÓN DE REQUISITOS DE LA RED

6.3.1 Introducción

6.3.1.1 Propósito

Renia es un organismo de cooperación técnica formado por las redes universitarias cuyo propósito es promover una red de telecomunicaciones con capacidades avanzadas, contribuir a mejorar la calidad de los servicios, fomentar proyectos de investigación de tecnología avanzada, contribuir al desarrollo de recursos humanos de las redes en el uso de tecnología avanzada de telecomunicaciones.

6.3.1.2 Alcance

La interconexión de las Universidades Nicaragüenses (UNAN-León, UNAN-Managua, UCA, UNI, UNA, UPOLI) hacia red CLARA permitiendo de este modo la comunicación con Internet 2

6.4.1.3 Funciones y Políticas

1. ***Servicio a proveer***
   Se brindará servicio de conectividad a la Internet Avanzada, tales como multicasting, IPv6 y de manejo de QoS
   La velocidad de conexión será: E1 (2.048 Mbps),1 Mbps, 512 Kbps.

2. ***Solicitud de Conexión***

Toda solicitud al Responsable Administrativo de RENIA.

3. Resolución de problemas

Los problemas deberán ser resueltos por el Ingeniero de Red asignado y el técnico designado por ENITEL, que da conectividad a I2.

4. ***La parte de soporte técnico a las universidades,*** será atendido por un Ingeniero de RedRENIA y tendrá conocimiento de cómo acceder a los servicios de soporte. El mismo auditará el enlace para detectar intrusos, tráfico comercial, entre otros.

5. ***El monitoreo, administración y la aplicación*** de las políticas de enrutamiento las aplicará el Ingeniero de RedRENIA.

6. ***El Responsable Técnico de RedRENIA*** estará a cargo de la recepción de solicitudes y asignación del número IPv6 de los miembros, así mismo, solicitara el Bloque IPv6 al LACNIC y lo administrará, de acuerdo a la política de la Asociación.

7. ***Políticas de asignación de ancho de banda disponible*:**

a) En caso de que un miembro necesite ancho de banda extra al disponible, hará una solicitud al Director de RedRENIA, especificando justificación, ancho, día, horas que lo requiere. Sin exceder el tiempo de 4 horas

b) Si entrara un nuevo miembro, se definirá en reunión general de asociados qué organización cederá determinado ancho de banda y bajo que criterios (se definirá una vez se tengan costos reales).

8. Se elaborará un manual en detalle del procedimiento de operación del nodo de RENIA, el cual se elaborará en conjunto con los técnicos designados por cada una de las universidades miembros.

6.4.1.4 Referencias

Información proporcionada por el Director ejecutivo de RENIA (Ing. Roberto Blandino), Coordinador Técnico (Ing. Marcos Carcamo) y el Comité Técnico de la misma.

6.4.1.5 Visión General

Se cuenta con un Router Cisco 12006 ubicado en Tijuana/México perteneciente a la RedCLARA, teniendo esta un enlace con una de las redes latinoamericana en Nicaragua por medio del Router de Enitel 7600 ubicado en Managua, desde este

router se dará la conexión a RENIA utilizando un router CISCO 3660 ubicado en AIN, este a la vez se conecta con un switch 3750 y desde aquí se interconecta cada universidad a través de su ISP comercial. El punto de entrega de la conexión sigue siendo el NicIX-AIN.
El enlace entre el Switch de RENIA a cada universidad, se pretende óptimamente sea de Fibra Óptica.

6.3.2 Descripción General

Renia (Red Nicaragüense de Internet Avanzada) a la que pueden unirse toda Universidad o centro de Investigación y Educación que cumplan con ciertas restricciones.

6.3.2.1 Características de los usuarios

Las Instituciones que se incorporen a RENIA serán personas con conocimientos básicos en la manipulación de cualquier visualizador de Internet.

6.3.2.2 Restricciones Generales

- Contar con acceso a Internet.
- Conexión por medio de Fibra Óptica o Wifi.
- Contar con equipos que tengan compatibilidad con Ipv6
- Aplicaciones que usen, corran sobre Ipv6.

La conexión de nuevos miembros será autorizada, previa solicitud, por la JD de RENIA y su ejecución estará a cargo de los Responsables administrativo y Técnico de la Red únicamente.

6.3.2.3 Requisito Específico

El requisito mas importante que debe cumplir toda institución que desee pertenecer a RENIA es que su medio de interconexión sea Fibra Óptica o Wifi.

Se requiere

- 2 switches 3750 (L2)
- 1 Router 3660 (ML)
- 2 Server HP

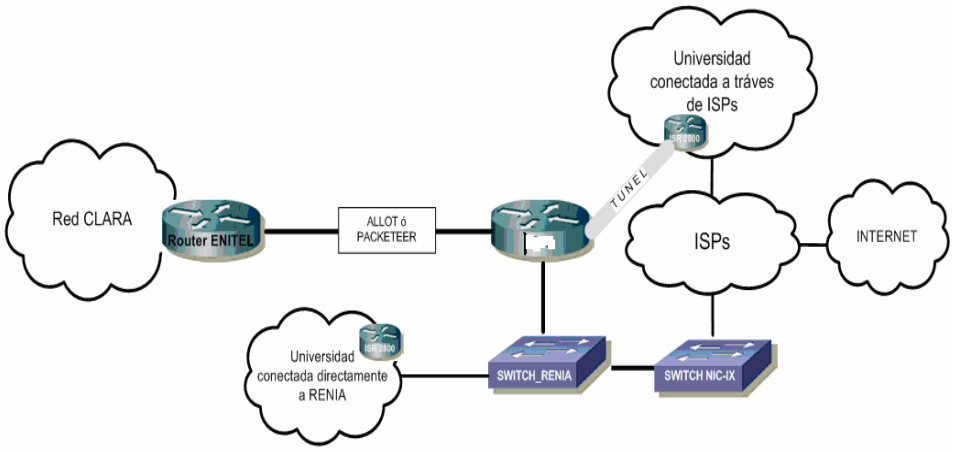
6.4 DISEÑO

6.4.1 Diseño de la Red

6.4.1.1 Diseño Lógico

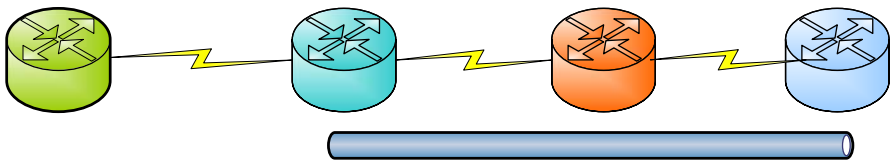
6.4.1.1.1 Diseño Lógico General

DIAGRAMA DE INTERCONEXION A RENIA MEDIANTE ROUTERS CISCO



Este es el escenario mas recientes elaborado por los técnicos en el cual entre esta la red RENIA y CLARA se ha colocado un router 3660 el cual nos brindara la conexión y este se conectara al swith 3750 y esta a su vez a algún ISP que proporciones conexión a las diferentes entidades a través de túneles a excepción de la UNI que se conectara director por razones de posición geográfica por ser este una de las mejores propuestas y la que mejor se adapta a lo que tenemos a sido la mas acertada y se esta llevando a la practica.

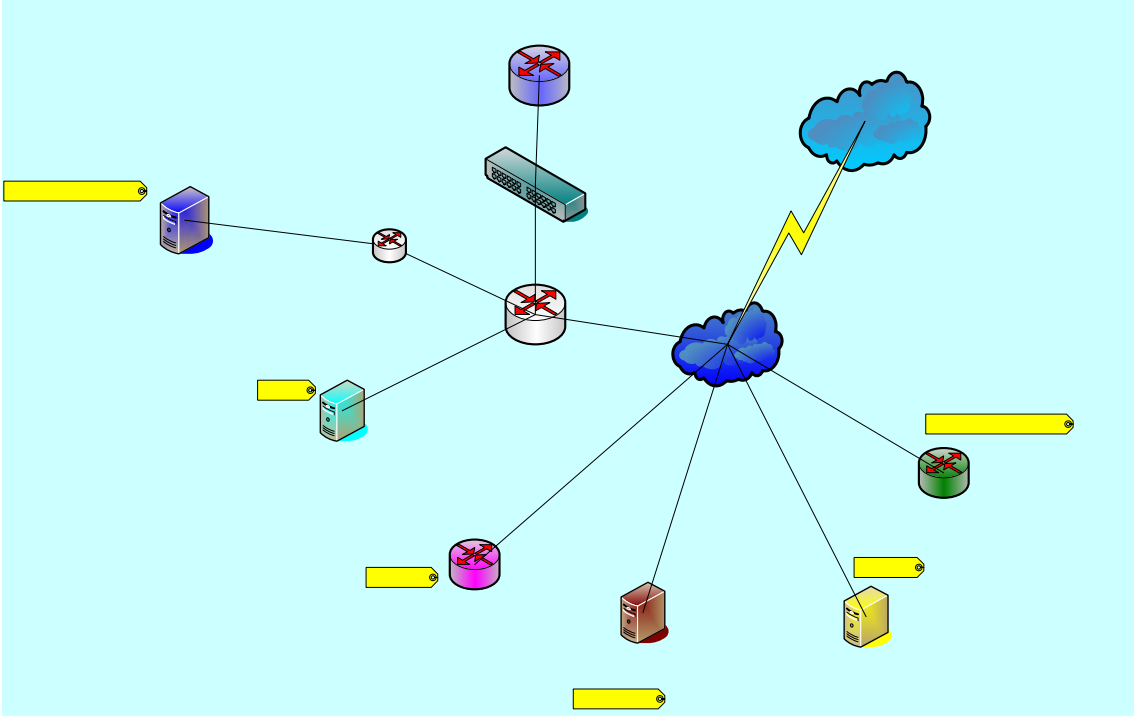
6.4.1.1.2 Diseño Lógico de la conexión entre RENIA y CLARA



Es un ejemplo grafico, de la conexión de Renia a RedCLARA donde se representa el router 3660 Cisco que combina el acceso telefónico,

enrutamiento y servicios entre redes de área local (LAN) y el multiservicio integrado de voz, video y datos en el mismo aparato, una de las ventajas clave de la plataforma Cisco 3660 es que en ella se ejecuta el software Cisco IOS, el sistema operativo que se distribuye en la mayoría de los equipos de backbone de Internet en el mundo. El 3660 se conectará a través de la infraestructura de cableado que nos proporcionara Enitel mediante un router 7600 conectándose con Telecom a través del router 12006 ubicado en Tijuana/México uno de los nodos de RedCLARA.

6.4.1.1.3 Diseño Lógico del Backbone Nacional de RENIA



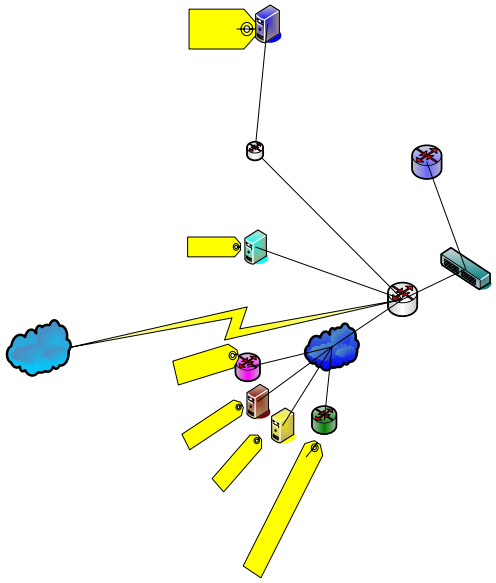
La topología seleccionada para este tipo de red de acuerdo a la tecnología IEEE 802.3 es de estrella, porque ofrece un mejor rendimiento, ya que los datos no van pasando de un ordenador a otro hasta llegar al destinatario, sino que directamente van desde el ordenador de origen al de destino, sin pasar por intermediarios (excepto por el concentrador). Como se esta utilizando fibra óptica, es obligatorio utilizar una topología en estrella.

2800:10:13::/48
165.98.36.0
UNAN-Leon
Router Linux
Suse 10
NICIX
Regional

UNI
UNAN - LEON
165.98.39.0
2800:10:10::/48
Router

6.4.1.2 Diseño Físico

Debido a que esta red es muy extensa no de detalla específicamente su diseño Físico, por lo que se da un aproximado a través de esta figura:



Las universidades que se conectan a RENIA cuentan con:

Recursos con lo que cuentan los puntos que se conectaran a RENIA

Universidad o Entidad	ISP	Tecnología	Ancho de Banda	No. de usuarios	Tecnología para conectarse a I2	Contacto
Punto de Encuentro	IBW	Fibra Óptica	100 Mbps Local 256 Mbps Inter.	43	Astaro IBM PC Compatible	Bayardo Rivas
UNAN-Managua	AMNET	Fibra Óptica	100 Mbps Local 1 Mbps Inter.	400	Cisco Router 2811	Derman Zepeda
UNAN-León	IBW Telered	Fibra Óptica Wifi	3 Mbps Local	500	Linux Router clon	Marcos Carcamo
UNA	IBW	Wifi	2 Mbps 512 Kbps Inter.	300	Router Linux Suse Compaq Proliant	Peter Pettersson
UNI	IBW	Wifi	18 Mbps Local 2 Mbps Inter.	400	Linux Debian Router	Marvin Castañeda
UPOLI	AMNET	Wifi	1 Mbps Inter.	250	Linux Suse Router Cisco Router 2600	Bayardo Silva
UCA	IBW	Fibra Óptica	100 Mbps Local 2 Mbps Inter.	1200	Cisco 3845	Félix Sobalvarro

El Router Renia se encuentra en el edificio AIN el cual se conecta con el switch 3750 entregando éste conexión al NICIX que es el punto de intercambio en Internet en la cual los proveedores de servicios (IBW, Telered, AMNET), entregarán la conexión a cada Universidad.

La UNAN-Managua se conecta con un Router Cisco 2811 de la serie 2800 requiere un circuito de entre 120v-15ª con una conexión a la puerta de energía de 5-15p admiten un módulo de red mejorado (NME) simple, cuatro tarjetas de interfaz WAN de alta velocidad simples o dos dobles (HWIC), dos AIM, dos módulos de datos de voz en paquete (PVDM), dos conexiones Fast Ethernet y 24 puertos de salida de alimentación telefónica IP, su proveedor AMNET utilizando Fibra óptica con una velocidad de 100Mbps Local y 1 Mbps internacional. Interconectándose con router RENIA a una distancia de 3 Km.

La UNAN-León se conectara a un Router Linux clon equipo Intel(R) Pentium(R) 4 CPU 2.80ghz 496 MB de RAM, su proveedor Telered con wifi a una velocidad de 3Mbps Local. Con una distancia de 110 Km. del Router de Renia (Edificio AIN).

La UNA se conectara por medio de un Linux Suse 10 Compaq Proliant su proveedor es IBW por medio de fibra óptica a una velocidad de 2Mbps Local y 512 Mbps Internacional. Esta a una distancia de 30 Km. del Router de Renia (Edificio AIN).

La UNI su conexión será a través de un Router Linux Debian su proveedor es IBW utilizando fibra óptica a velocidad de 18 Mbps Local y 2 Mbps Internacional. Este se conectara directamente al router RENIA por ser uno de los miembros de AIN.

La UPOLI se conectara desde un Router Linux Suse 10 aunque también cuenta con Cisco 2600 su proveedor es AMNET con wifi a una velocidad de 1Mbps Internacional. Este esta a una distancia de 12 Km. del router de RENIA.

La UCA se interconectara por medio de un Router Cisco 3845 disponen de cuatro ranuras de módulo de red, etiquetadas como 1, 2, 3 y 4. Cada ranura admite cualquiera de los siguientes módulos: módulo de red de ancho simple, módulo de red de ancho simple mejorado o módulo de red de ancho simple mejorado y ampliado. Las ranuras 1 y 2 se combinan para admitir módulos de red de ancho doble o módulos de red de ancho doble ampliados. Del mismo modo, las ranuras 3 y 4 se combinan para admitir módulos de red de ancho doble o módulos de red de ancho doble ampliados. Los routers Cisco 3845 también admiten una ranura SFP opcional, dos puertos Gigabit Ethernet LAN incorporados, dos puertos USB incorporados para uso futuro, cuatro HWIC de ancho simple o dos de ancho doble, dos AIM, cuatro PVDM, 48 puertos de salida de alimentación telefónica IP y aceleración de cifrado VPN basada en hardware, su proveedor es IBW por medio de fibra óptica a una velocidad de 100Mbps Local y 2 Mbps Internacional. Su conexión se da a una distancia de 2 Km. del router de RENIA.

6.4.2 Diseño de Direcciones

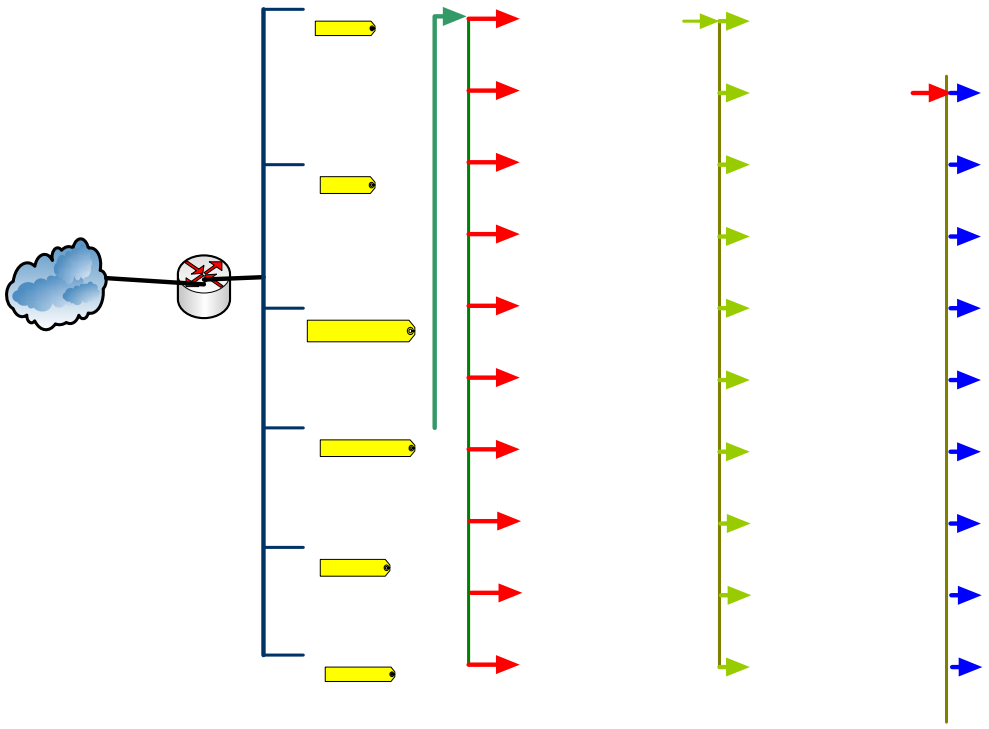
En Nicaragua, se han asignado varios segmentos IPV4 a las Universidades que estarán en RENIA estos son:

UNAN-MANAGUA	165.98.35.0/24
UNAN-LEON	165.98.36.0/24
UNA	165.98.37.0/24
UPOLI	165.98.38.0/24
UNI	165.98.39.0/24

De igual modo se han asignado la siguiente numeración IPV6 segmentos /48 para las Universidades:

2800:10:10::/48	Universidad Nacional de Ingeniería (UNI)
2800:10:11::/48	Universidad Nacional Agraria (UNA)
2800:10:12::/48	Universidad Nacional Autónoma de Nic (UNAN)
2800:10:13::/48	Universidad Nacional Autónoma de León (UNAN-León)
2800:10:14::/48	Universidad Politécnica de Nic (UPOLI)
2800:10:15::/48	Universidad Centroamericana (UCA)
2800:10:16::/48	IBW

Propuesta de Direccionamiento para Nicaragua:



El Direccionamiento de la Red en UNAN-León seria:
A esta Universidad le han asignado este rango

2800:10:13::/48

Podría establecer la siguiente jerarquía:

Podrían repartirse distintas direcciones regionales en todo el departamento de León ofreciendo conexión hasta 16 redes regionales tomando 4 bits de los 16 bit consecutivos de la dirección asignada a León. (2800:10:13::/48).

Dispone así de 2^8=256 facultades. Las cuales a su vez pueden tener 16 redes LAN. A cada una de ellas pueden conectar 2^{64} host, aproximadamente 18446744073709551616. La Facultad puede considerar reservar un bloque de redes para sus propios proyectos.

Los valores anteriores se pueden variar, según las necesidades.

Así la Universidad podria empezar a asignar de la siguiente manera:

2800:10:13:00::/56 Rango para las interfaces de los routers
2800:10:13:01::/56 Reservado.

6.5 CONFIGURACIÓN DE ENRUTAMIENTO DE RENIA A RED CLARA

Este es el Router de RENIA al cual tienen permiso de acceder solo los técnicos una vez introducido el usuario y su correspondiente contraseña pasamos a la configuración de 4 de abril del 2006.

```
RENIA_C3660#sh run
Building configuration...                    //cargando la configuracion

Current configuration : 7159 bytes           //configuración actual
!
version 12.4                                 //version del Router
service timestamps debug uptime              //servicio elimina errore
service timestamps log uptime                //mantienen los registros
service password-encryption                  //contraseña encriptada
!
hostname RENIA_C3660                         //nombre del Router
!
boot-start-marker                            //carga inicio
boot-end-marker                              //carga el fin
!
```

Nota: Hasta aquí se carga la configuración actual, la versión y los servicios activos como la eliminación de errores, mantenimiento de los registros y la contraseña encriptada. El nombre de Router que es RENIA_C3660, marcadores de inicio y fin.

```
no logging monitor
```

```
enable secret 5 $1$Z7j/$DpSPMX9hvoqe1ls1htYtm.
!
no aaa new-model                                    //ningun modelo nuevo
!
resource policy                                     //politicas de recurso
!
!
!
ip cef
!
!
ipv6 unicast-routing                                //encaminamiento unicast ipv6

!
!
!
!
username renia password 7                           //nombres de los usuarios
username enitel secret 5
!
!
!
!
```

Nota: están activo secret, detecta que no hay un modelo nuevo aaaa la política de recurso y las ip; encaminamiento unicast IPv6, a como podemos observar hay dos cuentas de usuarios RENIA y ENITEL con sus contraseñas.

```
                                        //tunel Ipv6 creado de Renia hacia UNI

interface Tunnel10
description "Tunnel de IPv6 hacia la UNI"
 no ip address
 ipv6 address 2800:10:10:100::1/64
 tunnel source 200.85.172.109
 tunnel destination 165.98.119.93
 tunnel mode ipv6ip
!
                                        //tunel Ipv6 creado desde Renia hacia UNA
interface Tunnel11
 description "Tunnel de IPv6 hacia la UNA"
 no ip address
 ipv6 address 2800:10:11:100::1/64
 tunnel source 200.85.172.109
 tunnel destination 165.98.116.115
 tunnel mode ipv6ip
!
                                        //tunel Ipv6 creado desde Renia hacia Unan-Leon
interface Tunnel20
description << Tunnel de Ipv6 a la UNAN-Leon >>
 no ip address
 ipv6 address 2800:10:13:1::1/64
 tunnel source 200.85.172.109
 tunnel destination 192.107.104.26
 tunnel mode ipv6ip
```

```
!
                                        //tunel Ipv4 creado desde Renia hacia UNA
interface Tunnel37
 description "Tunnel de IPv4 hacia la UNA"
 ip address 165.98.37.17 255.255.255.252
 ip tcp adjust-mss 1400
 tunnel source 200.85.172.109
 tunnel destination 165.98.116.115
!
                                        //tunel Ipv4 creado desde Renia hacia UNI
interface Tunnel39
 description Tunnel de IPv4 a la UNI
 ip address 165.98.39.1 255.255.255.252
 ip mtu 1476
 tunnel source 200.85.172.109
 tunnel destination 165.98.119.93
!
                                    //tunel Ipv4 creado desde Renia hacia UNAN-Managua
interface Tunnel40
description UNAN_MANAGUA
 ip address 10.40.0.1 255.255.255.252
 ip mtu 1000
 ip tcp adjust-mss 1436
 tunnel source 200.85.172.109
 tunnel destination 165.98.8.90
!

interface Tunnel42              //tunnel ipv6 creado de Renia hacia UNAN-Managua
 no ip address
 ipv6 address 2800:10:12:40::2/64
 tunnel source 165.98.8.90
 tunnel destination 200.85.172.109
 tunnel mode ipv6ip
!
```

Podemos observar ya que están configurados cuatro túneles de Ipv6 desde RENIA hacia UNI, UNA, UNAN-LEON, UNAN-Managua y tres tuneles de Ipv4 hacia UNA, UNI, UNAN-Managua. Los pasos de esta configuración la explicamos en la sección 10.1 del marco teórico.

```
interface Loopback3                                  //Interfaz de Loopback3
 ip address 200.9.187.101 255.255.255.252
!
```

Esta es la interfaz que se conecta hacia el Router 7600 de Enitel

```
interface FastEthernet0/0
 description "Trunk contra Router en Enitel"
 no ip address
 duplex auto
 speed auto
!

interface FastEthernet0/0.1
```

```
 description PACKETEER
 encapsulation dot1Q 1 native
 ip address 165.98.41.37 255.255.255.252
 no snmp trap link-status
!
```

Esta es la interface en la que se hace el enlace hacia el Router Cisco 12006 ubicado en Tijuana/México.

```
interface FastEthernet0/0.102
 description VLAN102 ENLACE HACIA MEXICO
 encapsulation dot1Q 102
 ip address 200.0.204.166 255.255.255.252
 ip mtu 1470
 no snmp trap link-status
 ipv6 address 2001:1348:1:A::2/64
!
```

Esta interfaz se conecta con IBW la que dara conectividad a las Universidad a las que brinda sus servicios. Como es el caso de UNI, UNA, UCA y Puntos de Encuentro.

```
interface FastEthernet0/1
 description "Trunk contra Router en IBW para Clientes de IBW-RENIA"
 no ip address
 duplex auto
 speed auto
!
```

Esta interfaz se conecta con el Switch 3750

```
interface FastEthernet0/1.100
 description MONITORE_SWITCH_3750
 encapsulation dot1Q 100
 ip address 165.98.41.33 255.255.255.252
 no snmp trap link-status
!

interface FastEthernet0/1.300
 description Internet-Access-x-IBW
 encapsulation dot1Q 300
 ip address 200.85.172.109 255.255.255.248 secondary
 ip address 165.98.41.1 255.255.255.224
 no snmp trap link-status
!
```

Interfaz en la se conecta Puntos de Encuentro

```
interface FastEthernet0/1.301
 description "Puntos de Encuentro Streaming"
 encapsulation dot1Q 301
 ip address 165.98.191.1 255.255.255.248
 ip mtu 1470
 no snmp trap link-status
 ipv6 address 2800:10:16::1/64
!
```

Esta es la interfaz en donde se conecta directamente la UCA

```
interface FastEthernet0/1.302
 description UCA-RENIA
 encapsulation dot1Q 302
 no snmp trap link-status
!
interface FastEthernet1/0                    //Interfaces no asignadas
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0.301
 ip mtu 1470
!
```

Esta interfaz es hacia la direccion asignada a UNAN-Managua

```
interface FastEthernet1/1
 ip address 165.98.35.4 255.255.255.0
 duplex auto
 speed auto
!
```

El router con protocolo BGP 65102 donde se especifican los cambios en los registros de las subredes Ipv4. Estas son las redes a las que dará conectividad el Router

```
router bgp 65102
 no synchronization
 bgp log-neighbor-changes
 network 165.98.33.0 mask 255.255.255.0
 network 165.98.35.0 mask 255.255.255.0
 network 165.98.37.0 mask 255.255.255.0
 network 165.98.39.0 mask 255.255.255.0
 network 165.98.116.120 mask 255.255.255.248
 neighbor 10.10.0.2 remote-as 64939
 neighbor 10.10.0.2 ebgp-multihop 255
 neighbor 10.10.0.2 soft-reconfiguration inbound
 neighbor 10.37.0.2 remote-as 64937
 neighbor 10.37.0.2 ebgp-multihop 255
 neighbor 10.37.0.2 soft-reconfiguration inbound
 neighbor 10.40.0.2 remote-as 64940
 neighbor 10.40.0.2 ebgp-multihop 255
 neighbor 10.40.0.2 soft-reconfiguration inbound
 neighbor 2001:1348:1:A::1 remote-as 27750
 neighbor 2001:1348:1:A::1 password 7 097E1D274825014448
 neighbor 2001:1348:1:A::1 route-map filtro-ipv6-out out
 neighbor 165.98.37.18 remote-as 64937
 neighbor 165.98.37.18 ebgp-multihop 255
 neighbor 165.98.37.18 soft-reconfiguration inbound
 neighbor 165.98.39.2 remote-as 64939
 neighbor 165.98.39.2 ebgp-multihop 255
 neighbor 165.98.39.2 soft-reconfiguration inbound
 neighbor 165.98.41.5 remote-as 64601
 neighbor 200.0.204.165 remote-as 27750
 neighbor 200.0.204.165 password 7 12511744075A2C4D61
 neighbor 200.0.204.165 soft-reconfiguration inbound
 neighbor 200.0.204.165 route-map filtro-saliente-bgp out
```

```
 neighbor 200.9.187.73 remote-as 64601
 neighbor 200.9.187.73 ebgp-multihop 255
 neighbor 200.9.187.73 update-source Loopback3
 neighbor 200.9.187.73 soft-reconfiguration inbound
 no auto-summary
 !
```

Las direcciones de la familia de Ipv6 asignadas a las Universidades (UNI, UNA UNAN-Managua, UNAN-Leon e IBW)

```
 address-family ipv6
 neighbor 2001:1348:1:A::1 activate
 neighbor 2001:1348:1:A::1 send-community
 neighbor 2001:1348:1:A::1 soft-reconfiguration inbound
 network 2800:10:10::/48
 network 2800:10:11::/48
 network 2800:10:12::/64
 network 2800:10:13::/64
 network 2800:10:16::/48
 exit-address-family
!
no ip http server
!
```

Estas son las ip de los router que se conectas a RENIA

```
ip route 0.0.0.0 0.0.0.0 165.98.41.5
ip route 165.98.8.90 255.255.255.255 200.85.172.105
ip route 165.98.35.0 255.255.255.0 10.40.0.2              //UNAN-MANAGUA
ip route 165.98.37.0 255.255.255.0 165.98.37.18           //UNA
ip route 165.98.39.0 255.255.255.0 165.98.39.2            //UNI
ip route 165.98.36.0 255.255.255.0 165.98.36.2            //UNAN-Leon
ip route 165.98.116.120 255.255.255.248 165.98.37.18
ip route 165.98.191.16 255.255.255.248 Tunnel40
!
!
```

Esta es la lista de las direcciones ipv4 permitidas para que se conecten a RENIA

```
access-list 5 permit 165.98.33.0 0.0.0.255
access-list 5 permit 165.98.34.0 0.0.0.255
access-list 5 permit 165.98.35.0 0.0.0.255
access-list 5 permit 165.98.36.0 0.0.0.255
access-list 5 permit 165.98.37.0 0.0.0.255
access-list 5 permit 165.98.39.0 0.0.0.255
access-list 5 permit 165.98.191.0 0.0.0.255
access-list 5 permit 165.98.116.120 0.0.0.7
access-list 5 deny   any log
access-list 6 deny   165.98.191.0 0.0.0.255
access-list 6 deny   165.98.116.120 0.0.0.7
access-list 6 permit any
snmp-server community ReNia RO
```

Esta es la lista de las direcciones ipv6 que se conectan a RENIA.

```
ipv6 route 2800:10:10::/48 2800:10:10:100::2              //UNI
ipv6 route 2800:10:11:2::/64 2800:10:11:100::2            //UNA
ipv6 route 2800:10:11:3::/64 2800:10:11:100::2
ipv6 route 2800:10:11:5::/64 2800:10:11:100::2
ipv6 route 2800:10:11:6::/64 2800:10:11:100::2
ipv6 route 2800:10:11:7::/64 2800:10:11:100::2
```

```
ipv6 route 2800:10:11:8::/64 2800:10:11:100::2
ipv6 route 2800:10:11:9::/64 2800:10:11:100::2
ipv6 route 2800:10:11:10::/64 2800:10:11:100::2
ipv6 route 2800:10:11::/48 2800:10:11:100::2
ipv6 route 2800:10:12:2::/64 2800:10:12:40::2          //UNAN-MANAGUA
ipv6 route 2800:10:13::/64 2800:10:13:1::2             //UNAN-LEON
ipv6 route 2800:10:13::/64 Null0
ipv6 route 2800:10:16::/48 Null0                       //IBW
!
route-map filtro-saliente-bgp-ibw permit 5
 match ip address 6
 set metric 5
!
route-map filtro-ipv6-out permit 5
 match ipv6 address FilterInternet2
 set metric 5
!
route-map filtro-saliente-bgp permit 5
 match ip address 5
 set metric 5
!
!
!
```

Esta es la lista de direcciones Ipv6 registradas en el Filtro de Internet2

```
ipv6 access-list FilterInternet2
 permit ipv6 2800:10:11::/48 any
 permit ipv6 2800:10:12::/48 any
 permit ipv6 2800:10:13::/48 any
 permit ipv6 2800:10:14::/48 any
 permit ipv6 2800:10:15::/48 any
 permit ipv6 2800:10:16::/48 any
 permit ipv6 2800:10:10::/48 any
!
control-plane
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 password 7 0254540B5E140A2F454F
 login local
line vty 5 15
 password 7 15405B5C51382E2A2132
 no login
!
!
end                         //Fin de la configuración
```

6.6 CONFIGURACIÓN BÁSICA DE LOS PUNTOS CONECTADOS A RENIA

Los distintos puntos que se conectaran a RENIA realizaran distintas configuraciones dependiendo de los equipos con los que se cuentan. La UNAN-León, UNA, UNI y UPOLI configuraron Linux Router y UNAN-Managua y UCA Cisco Router de diferentes versiones.

6.6.1 Guía para realizar actualización de IOS en equipos Cisco

Antes de iniciar a describir los pasos para realizar una actualización de un sistema IOS para un equipo cisco, le recomiendo que realice esta actividad solamente si es necesario.

1. Descargue una versión de IOS que necesita o que cumpla con los requerimientos de su Sistema.
2. Instale un servidor FTP o TFTP (recomiendo trabajar con el tftp Server de solard wind) aunque otro puede servir.
3. Verifique que el enrutador tiene habilitada la opción ftp-server enable.
4. Realice los siguientes pasos:

- Router#***copy tftp: flash:***
- Address or name of remote host []? ***10.1.10.21***
- Source filename []? ***c2800nm-spservicesk9-mz.124-4.T.bin***
- Destination filename [c2800nm-spservicesk9-mz.124-4.T.bin]?
- Accessing tftp://10.1.10.21/c2800nm-spservicesk9-mz.124-4.T.bin...
- Loading c2800nm-spservicesk9-mz.124-4.T.bin from 10.1.120.21 (via FastEthernet0/1):

!!
!!

Una vez copiada la nueva IOS

5. Router(config)#***boot system flash:c2800nm-spservicesk9-mz.124-4.T.bin*** *(nueva IOS)*
6. Router(config)#***boot system flash:c2800nm-ipbase-mz.123-8.T8.bin*** *(Antigua IOS)*

Realizados estos cambios puede verificar si realmente se esta haciendo uso de la nueva IOS con el comando:

7. Router#***sh version***

Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.3(8)T8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 06-Apr-05 16:46 by yiyan
ROM: System Bootstrap, Version 12.3(8r)T7, RELEASE SOFTWARE (fc1)
Ipv6_UNAN uptime is 2 hours, 4 minutes
System returned to ROM by power-on

System image file is "flash:*c2800nm-spservicesk9-mz.124-4.T.bin*"

6.6.2 Configuración de routers RENIA para el enlace Ipv6 a UNAN-Managua

Ipv6_UNAN#sh run

```
version 12.4
service timestamps debug datetime msec

hostname Ipv6_UNAN

username xxxx

interface Tunnel40
 no ip address
 ipv6 address 2800:10:12:40::2/64
 tunnel source 165.98.8.90
 tunnel destination 200.85.172.109
 tunnel mode ipv6ip

interface Loopback0
 no ip address
!
interface FastEthernet0/0
 ip address 165.98.8.90 255.255.255.128
 duplex full
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 ip address 10.1.120.200 255.255.255.0
 duplex full
 speed auto
 no cdp enable
```

RENIA_C3660#sh run

```
hostname RENIA_C3660
ip cef
ipv6 unicast-routing
username yyyyy
!
interface Tunnel11
 description "Tunnel de IPv6 hacia la UNA"
 no ip address
```

ipv6 address 2800:10:11:100::1/64
tunnel source 200.85.172.109
tunnel destination 165.98.116.115
tunnel mode ipv6ip
!
interface Tunnel20
description << Tunnel de Ipv6 a la UNAN-Leon >>
no ip address
ipv6 address 2800:10:13:1::1/64
tunnel source 200.85.172.109
tunnel destination 192.107.104.26
tunnel mode ipv6ip

interface Tunnel40
description << Tunnel de Ipv6 a la UNAN-Managua >>
no ip address
ipv6 address 2800:10:12:40::1/64
tunnel source 200.85.172.109
tunnel destination 165.98.8.90
tunnel mode ipv6ip
!

6.6.3 Pruebas de verificación del túnel Ipv6 entre UNAN-Managua-RENIA.

Ipv6_UNAN#ping ipv6 2800:10:12:40::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:10:12:40::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Ipv6_UNAN#

Ipv6_UNAN#ping ipv6
Target IPv6 address: **2800:10:12:40::1**
Repeat count [5]: **1000**
Datagram size [100]: **2048**
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 1000, 2048-byte ICMP Echos to 2800:10:12:40::1, timeout is 2 seconds:
!!!
!!!
!!!
!!!
!!!
!!!

!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/9/116 ms

RENIA_C3660#ping ipv6 2800:10:12:40::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:10:12:40::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/5 ms
RENIA_C3660#

RENIA_C3660#ping ipv6
Target IPv6 address: **2800:10:12:40::2**
Repeat count [5]: **1000**
Datagram size [100]: **5000**
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 1000, 5000-byte ICMP Echos to 2800:10:12:40::2, timeout is 2 seconds:
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 8/9/76 ms

6.6.4 Configuración de un Router Linux con Suse10 en Ipv6

Contamos con un equipo al que llamaremos servidor (Router) y dos maquinas que servirán de clientes donde se anunciara el router en el cual tendremos en el Servidor el sistema operativo Suse 10, el cual contiene 2 interfaces de red, y en las dos maquinas clientes que tienen el sistema operativo Windows 2000, office 2003.

En el servidor :

6.6.4.1 Cargar modulo Ipv6 (el soporte de Ipv6): por medio del comando modprobe a como se muestra en la Figura 1

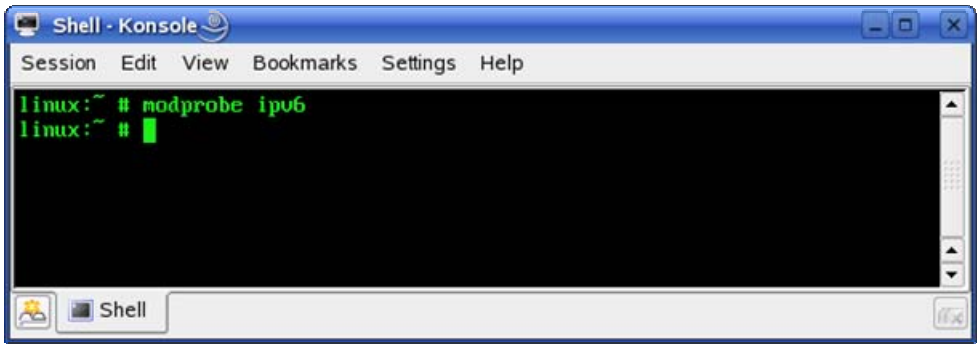


Figura 1

Después de activar el módulo, entramos al centro de control Yast (se mostrará un resumen de la configuración de red). En la parte superior del diálogo se muestra una lista de todas las tarjetas de red configuradas (Figura 2). Si su tarjeta ha sido detectada correctamente al arrancar el sistema, aparecerá mencionada aquí. Los dispositivos no reconocidos aparecen como ‘Otros (no

detectados)'. En la parte inferior de la vista se mencionan dispositivos ya configurados junto con el tipo y la dirección de red. Ahora puede configurar nuevas tarjetas de red o cambiar una configuración ya existente.

6.6.4.2 Configuración de la interfaz:

La interfaz que le proveerá los servicios al cliente, esta configuración la hacemos con la herramienta Yast de Linux:

Yast ->Dispositivos de red -> Tarjeta de red -> ASRock In (Rhine -II) -> Editar (Figura 2).

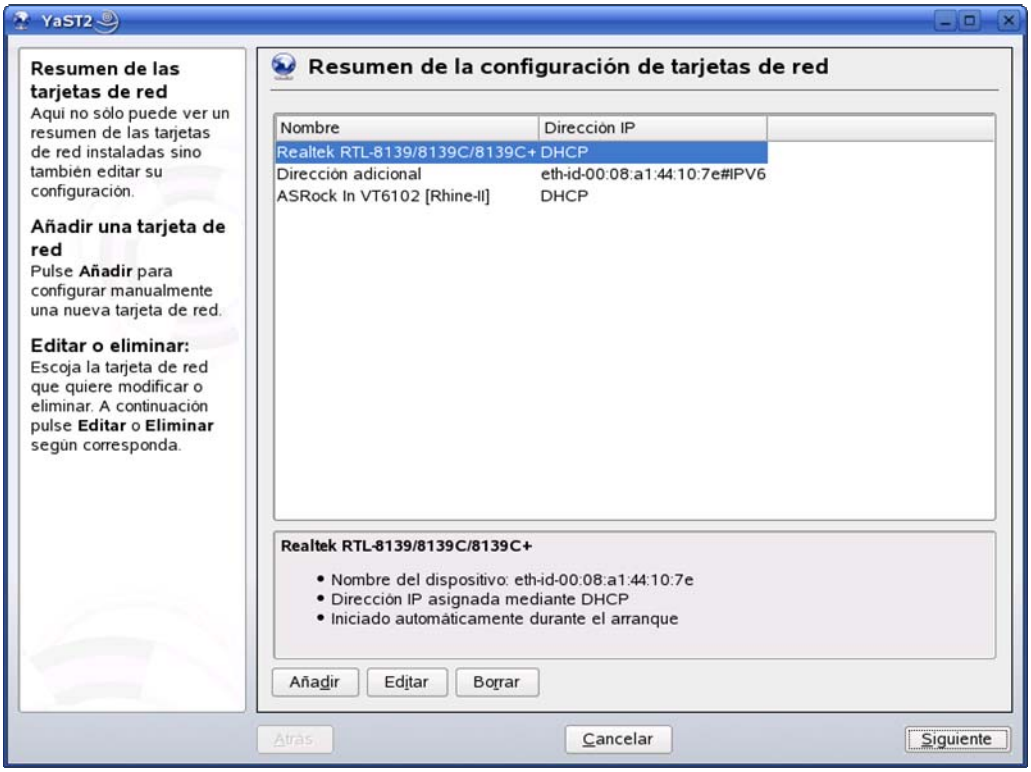


Figura 2

Seleccionamos ->Configuración automática de direcciones (por DHCP), a como se muestra en la Figura 3.

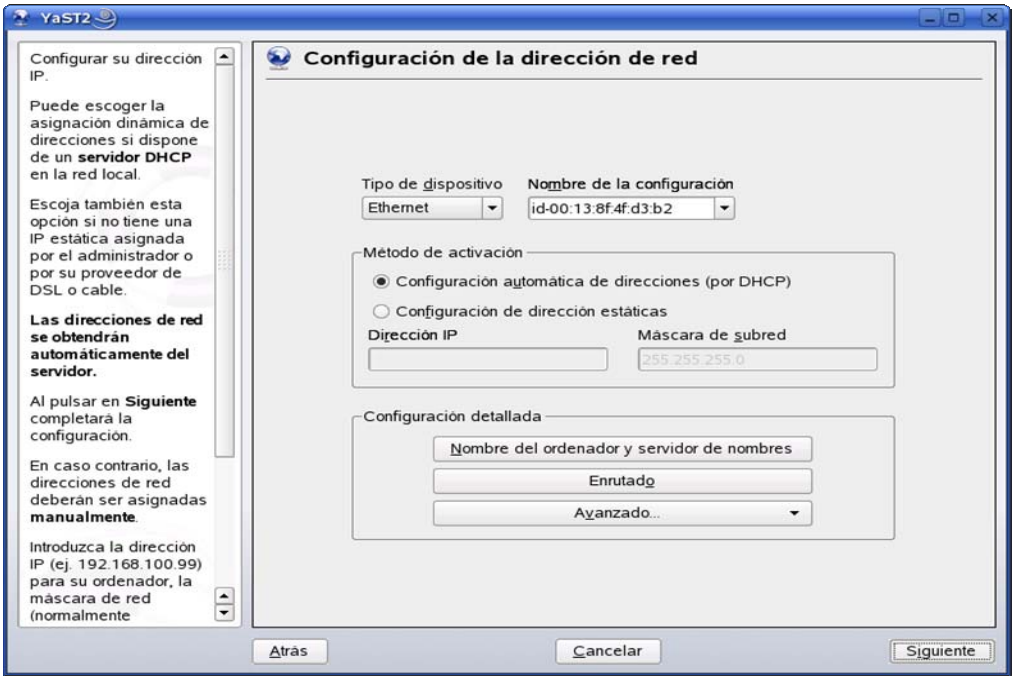


Figura 3

->clic en Enrutado y en “Pasarela predeterminada” ponemos la ip de la pasarela y clic en Aceptar (Figura 4).

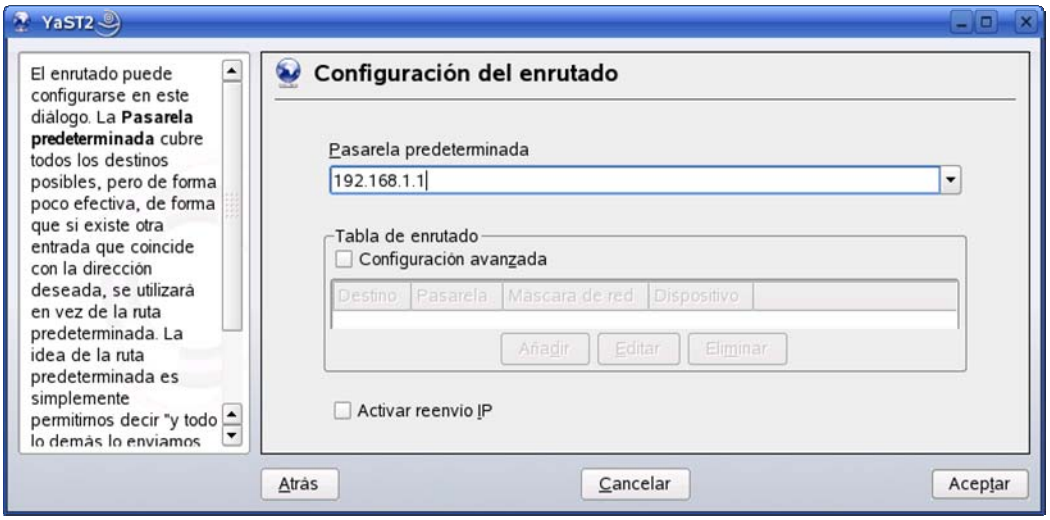


Figura4

Luego damos clic en siguiente y así se guarda la configuración de la interfaz (Figura 5).

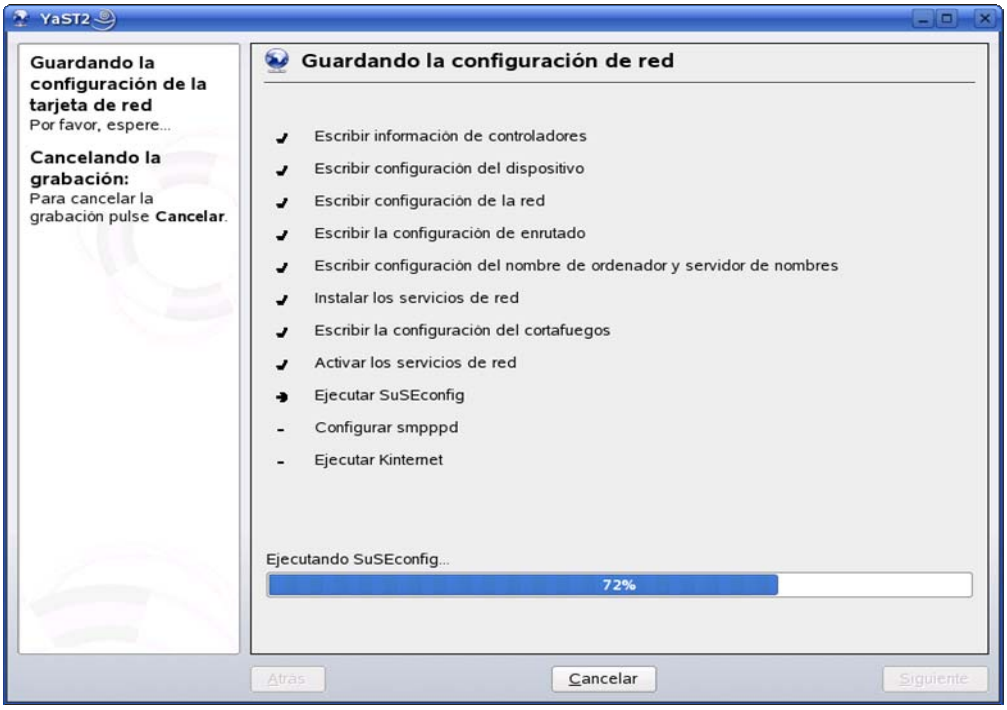


Figura 5

6.6.4.3 Instalación del Router Advertisement Protocol (radvd).

Este programa indica a los clientes el prefijo utilizado para las direcciones IPv6 y el/los enrutador(es) en la red, el radvd realiza la asignación de las direcciones IPv6 de forma totalmente automática desde el Yast-> Software -> Instalar/desinstalar software (Figura 6).

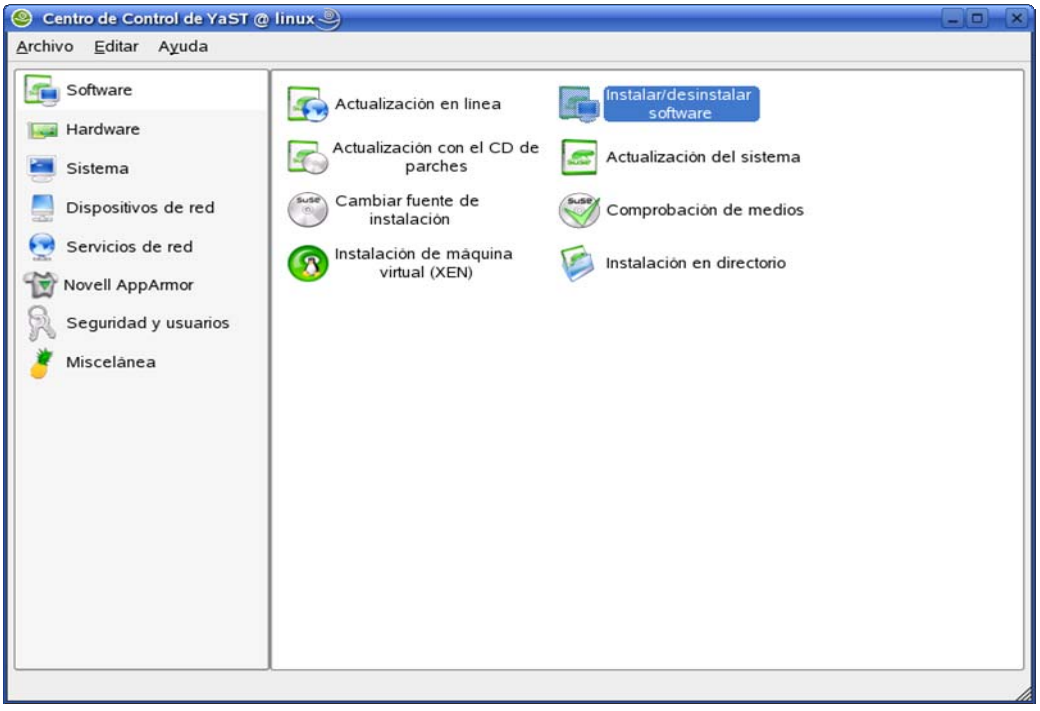


Figura 6

En Filtro seleccionamos Buscar y ahí editamos radvd y clic en buscar, lo seleccionamos y damos Aceptar (Figura 7); nos pedirá el disco de instalación y un vez introducido nuestra fuente de instalación le damos aceptar.

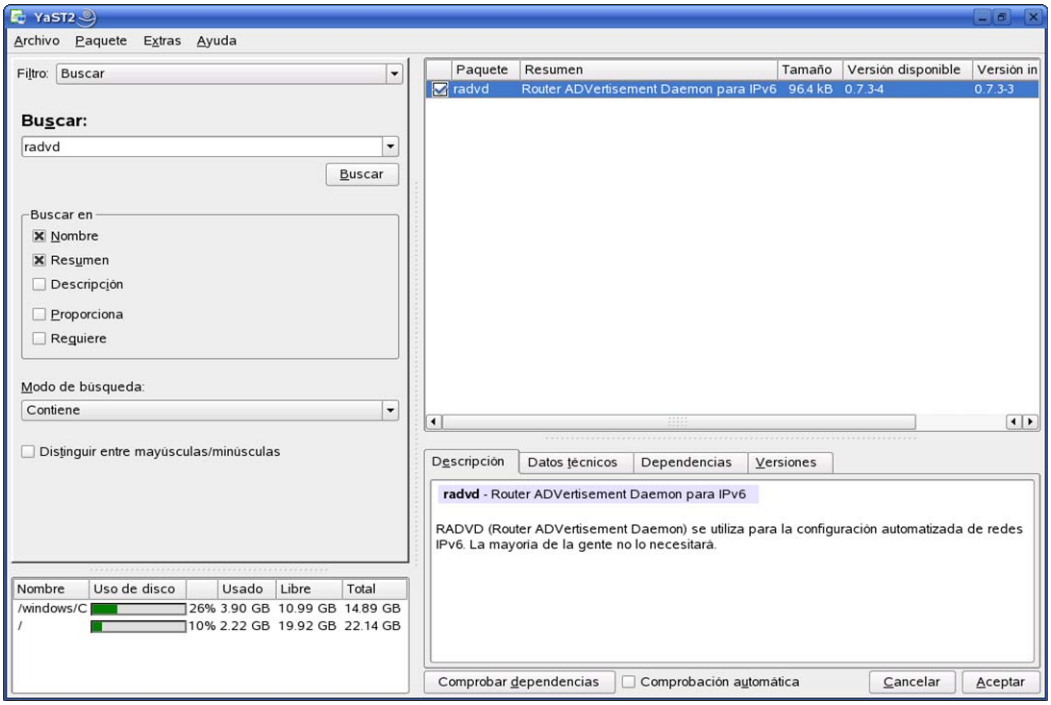
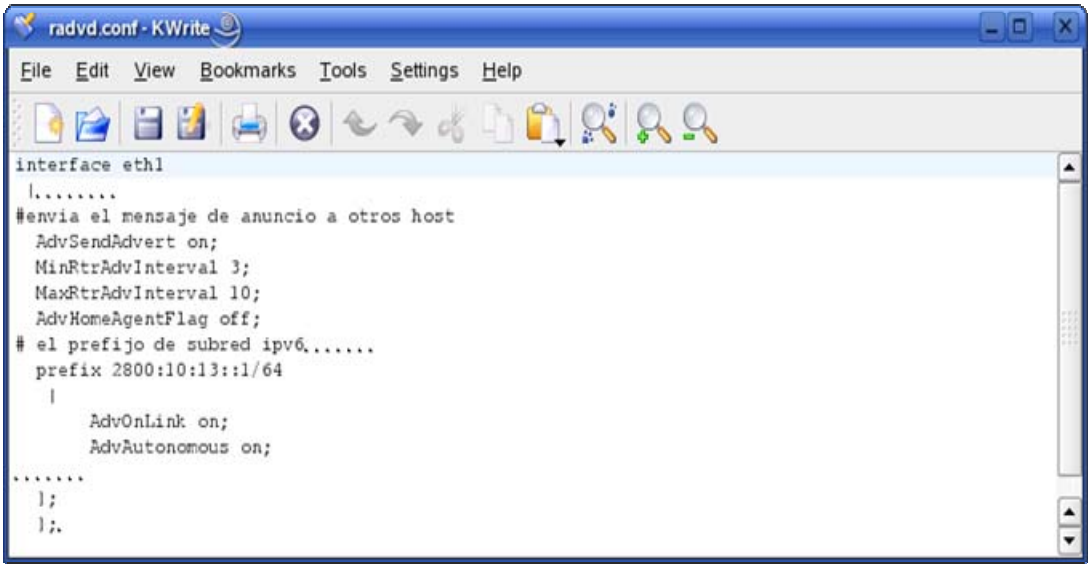


Figura 7

ahora una vez instalado el paquete radvd, ya se ha creado de forma automática el archivo /etc/radvd.conf, que contiene lo siguiente (Figura 8):

```
interface eth1
 {
#envía el mensaje de anuncio a otros host
            AdvSendAdvert on;
            MinRtrAdvInterval 3;
           MaxRtrAdvInterval 10;
           AdvHomeAgentFlag off;
          # el prefijo de subred ipv6
            prefix 2800:10:13::1/64
             {
                AdvOnLink on;
                AdvAutonomous on;
            };
 };
```

A como lo demostramos en la figura siguiente:



Figúra 8

Después de esto tenemos que activar el enrutamiento para esto añadimos la siguiente línea al script /etc/init.d/radvd que abrimos con KWrite

echo 1 >/proc/sys/net/ipv6/conf/all/forwarding a como se muestra en la Figura 9.

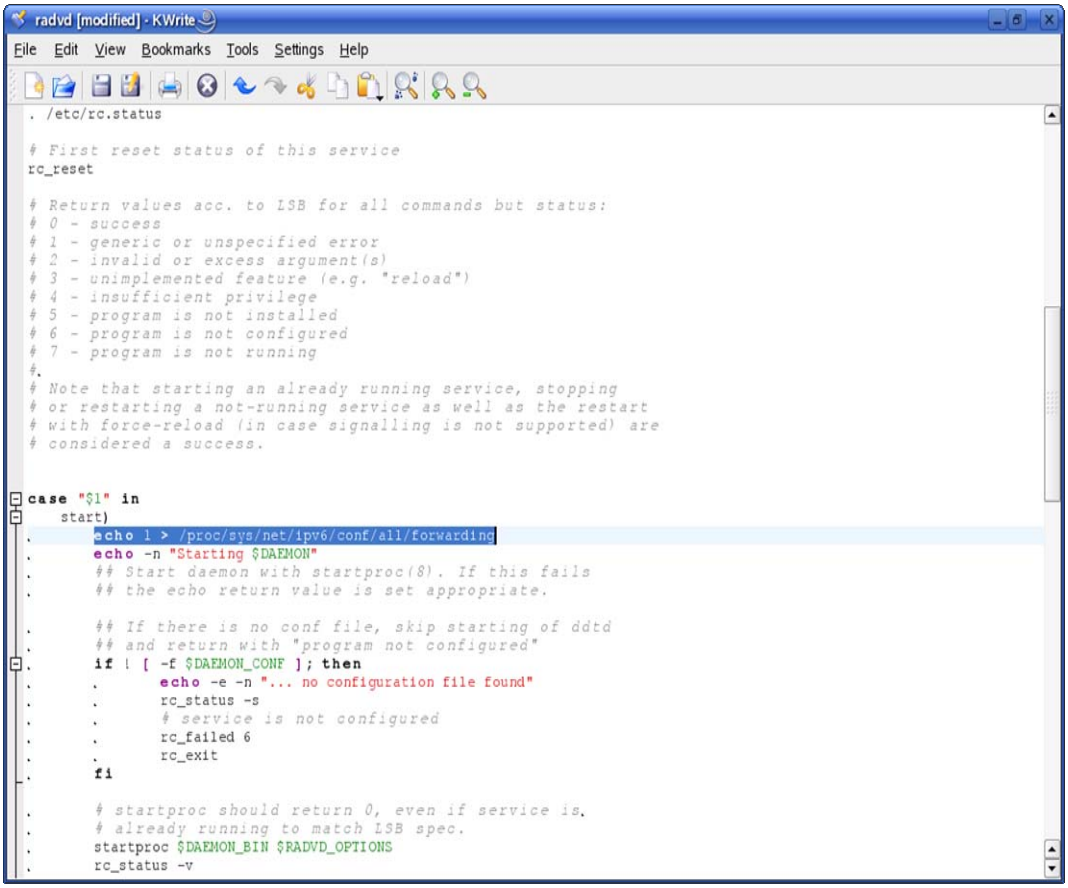


Figura 9

Ahora pasamos a realizar las comprobaciones de que el radvd esta funcionando de manera correcta y se puede verificar con el comando "radvdump". El resultado se detalla en la Figura 10

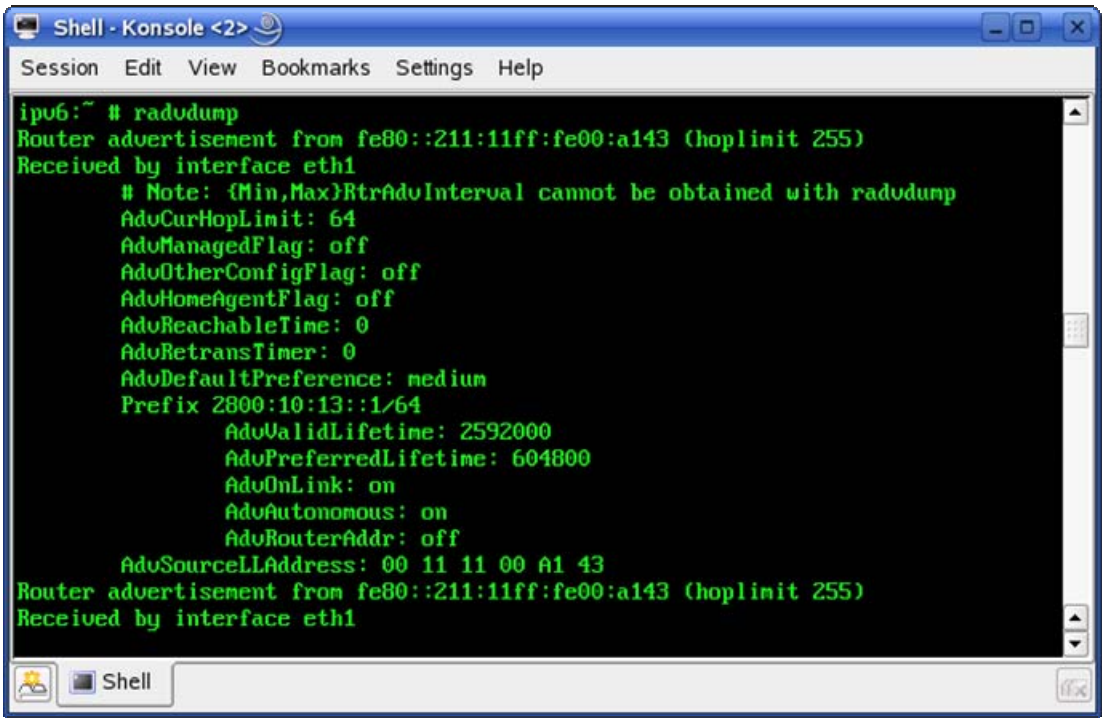


Figura 10

Otra herramienta para comprobar del "radvd" es, con el comando **tcpdump** se pueden ver todos los paquetes enviados a las subredes.

Ponemos a correr nuestro router con el comando **rcradvd start** y vemos que si esta funcionando Figura 11

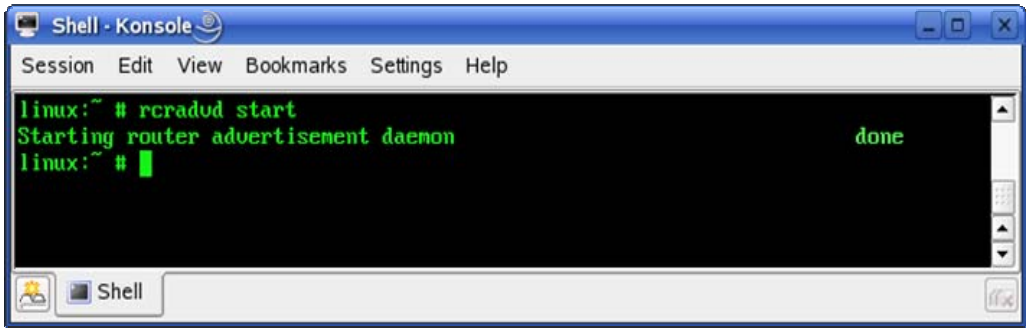


Figura 11

y también desde el Yast-> Sistemas-> Niveles de ejecución, podemos comprobar que el radvd este corriendo en los niveles 3 y 5 al seleccionarlo y dar clic en Iniciar/Parar/Refrescar y seleccionamos Iniciar a como se muestra en la Figura 12.

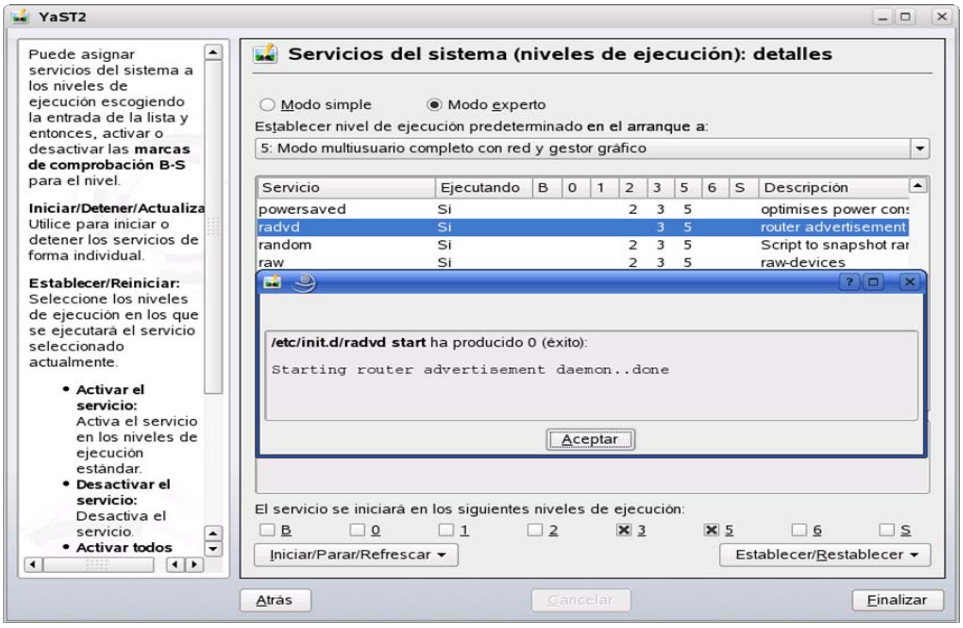


Figura 12

Hasta ver algo como la Figura12 para que la próxima vez que reiniciamos nuestro servidor router ya se este anunciando en las maquinas Clientes.

En una maquina cliente al dar un **ifconfig** desde consola podemos observar que se ha agregado automáticamente una nueva dirección ipv6 global en eth0, si esto no es así tendremos que bajar y levantar la interfaz con los comandos: **ifdown eth0** y luego **ifup eth0** para poder observar la dirección que esta anunciando nuestro router (Figura 13).

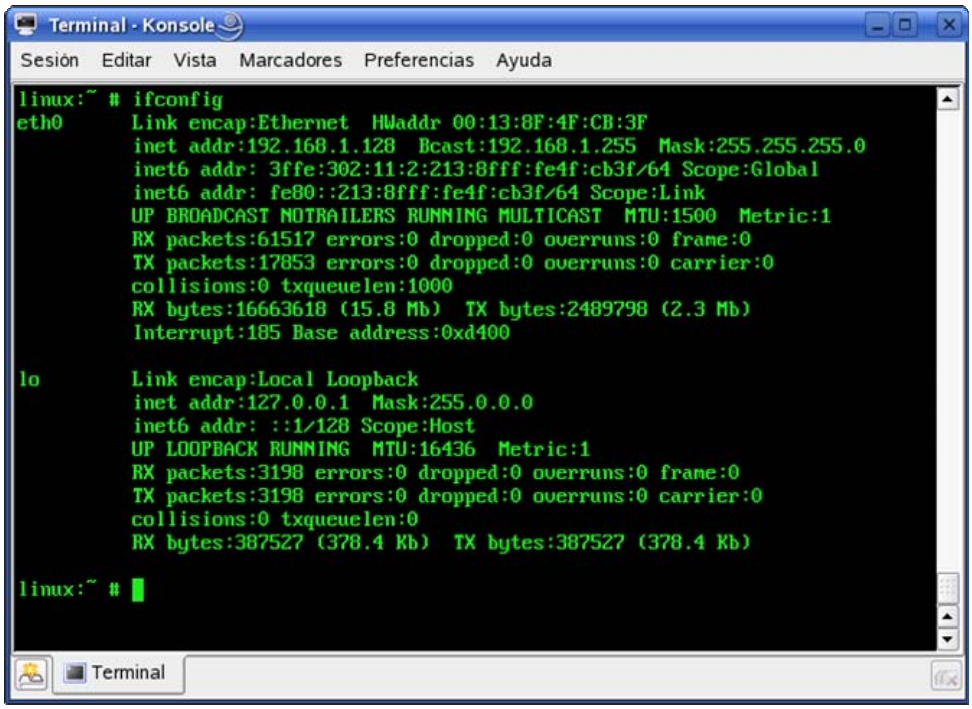


Figura 13

Ahora vamos a comprobar que existe comunicación ipv6 ente ambas maquinas para lo cual usaremos el comando **ping6**, pero antes tendremos que asignar una dirección ipv6 local a nuestra maquina cliente esta es la primera línea de la Figura 14.

A la cual asignamos la dirección **fec0:0:0:f101::2/64** como prueba, y después hacemos ping6 hacia el router al cual le asignamos la dirección **fec0:0:0:f101::1/64** (Figura 15) y vemos que si funciona el ping6 (Figura 14).

Este es el cliente haciendo ping6 al router Linux.

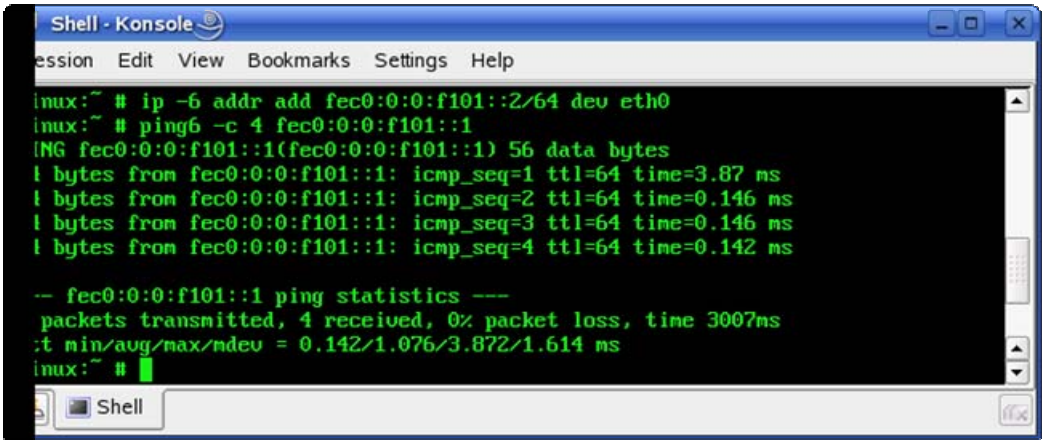


Figura 14

Ahora en el router, asignamos una dirección local y hacemos un **ping6** al cliente al cual le asignamos la dirección **fec0:0:0:f101::2/64** a como se muestra en la Figura 15.

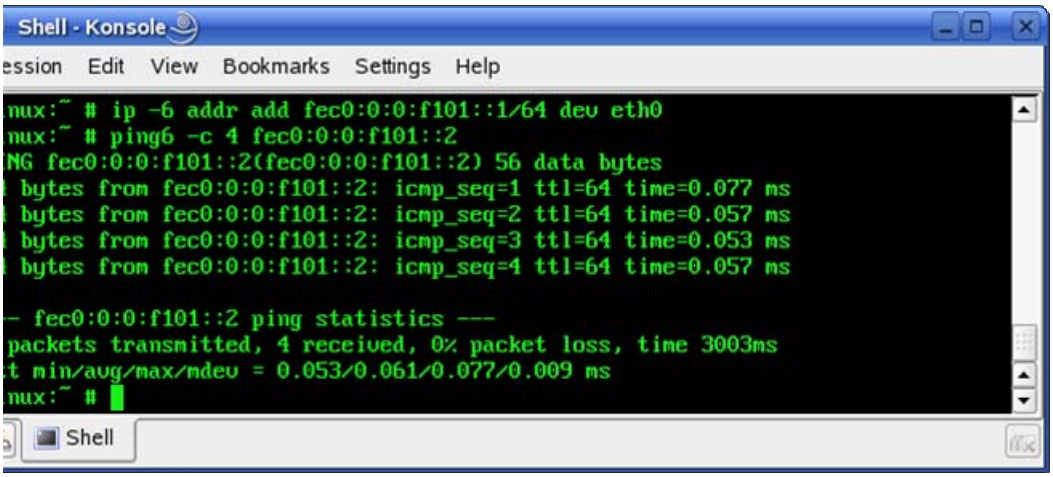


Figura 15

Una vez que todo esto funciona y comprobamos que existe la comunicación entre las maquinas clientes, a través de nuestro router.

6.6.5 Creación y Configuración del túnel 6to4 para transmitir paquetes IPv6 en Servidor de UNAN-León

Se nos ha asignado una ip publica que es la 192.107.104.26, la pagina http://6to4.version6.net/ da el servicio de calcular a partir de la ip publica que tenga la maquina desde donde se esta cargando la pagina, los pasos para crear el túnel 6to4.

.

De la cual tomamos las tres siguientes líneas de comandos:

ifconfig sit1 up

Con esta orden subimos la interfaz sit1

ifconfig sit1 add 2002:c0a8:6624::1921:0710:4026/48

Aquí agregamos la dirección de ipv6 a la interfaz sit1.

route –A inet6 add 2000::/3 gw ::192.88.99.1 dev sit1

Con esta ultima enrutamos todo el trafico de direcciones ipv6 a través de nuestro dispositivo túnel sit1.

Ahora desde consola editamos el comando **ifconfig** para ver las interfaces donde podemos apreciar el túnel llamado sit1 mostrado en la Figura 16.

```
sit1      Link encap:IPv6-in-IPv4
          inet6 addr: 2800:10:13:1::1/64 Scope:Global
          inet6 addr: fe80::c06b:681a/128 Scope:Link
          UP POINTOPOINT RUNNING NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Figura 16

Ahora realizamos una prueba de **ping6** y nos resulta lo que mostramos en la Figura 17

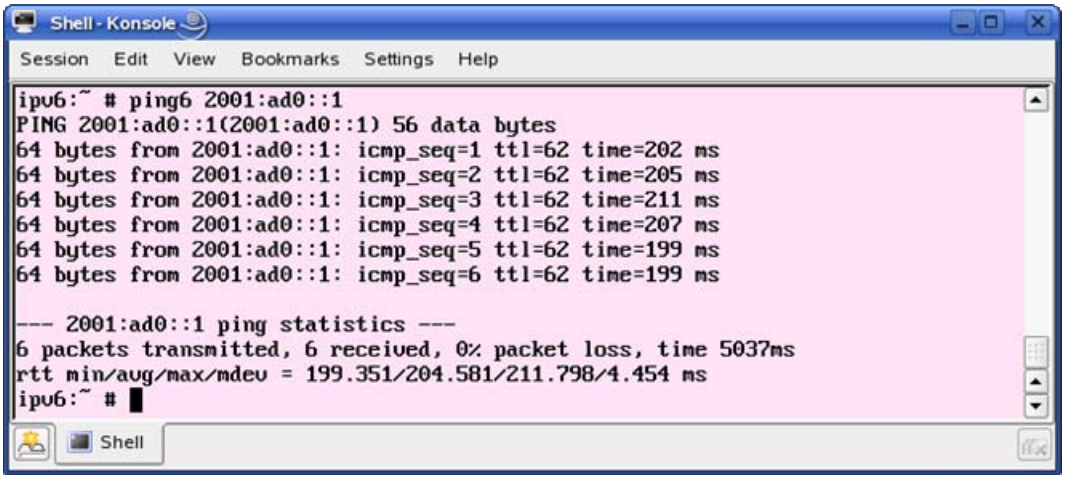


Figura 17

Ahora agregamos una dirección de ipv6 en el archivo de configuración de eth1 que es la que tiene asignada la ip pública y lo hacemos de esta forma:

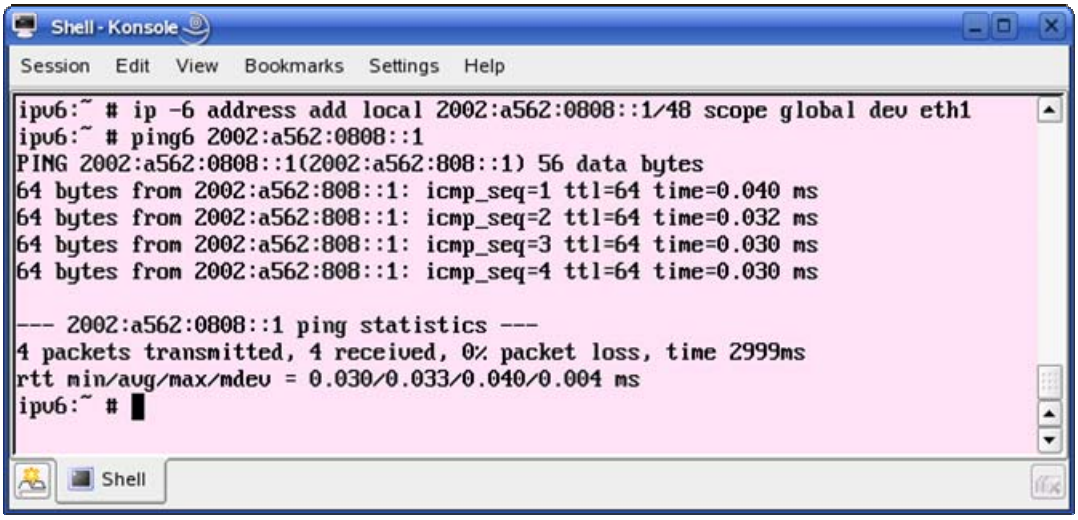


Figura 18

Realizamos la prueba de ping6 hacia esa dirección y nos resulta lo que podemos observar en la Figura 18.

Después de esto si recargamos las interfaces (con el comando /etc/init.d/network restart), esta dirección desaparece de la tarjeta eth1, por lo tanto para que no se elimine debemos añadir esta dirección en el archivo de configuración de la tarjeta, esta la encontramos en la dirección /etc/sysconfig/network/ifcfg-eth-id-00:13:8f:4f:d3:b2 en donde añadimos la siguiente línea (Figura 19):
IPADDR_IPV6='2800:10:13:1::2'

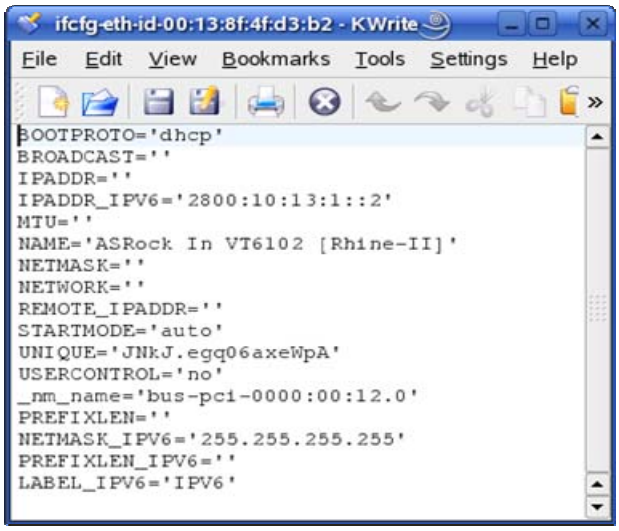


Figura 19

Una vez realizado este cambio podemos dar un ifconfig y observar que la dirección añadido en el archivo de configuración se esta mostrando y aunque recarguemos las interfaces de red (/etc/init.d/network restart) esta no desaparece, la podemos observar en la línea 3 del eth1 (Figura 20).

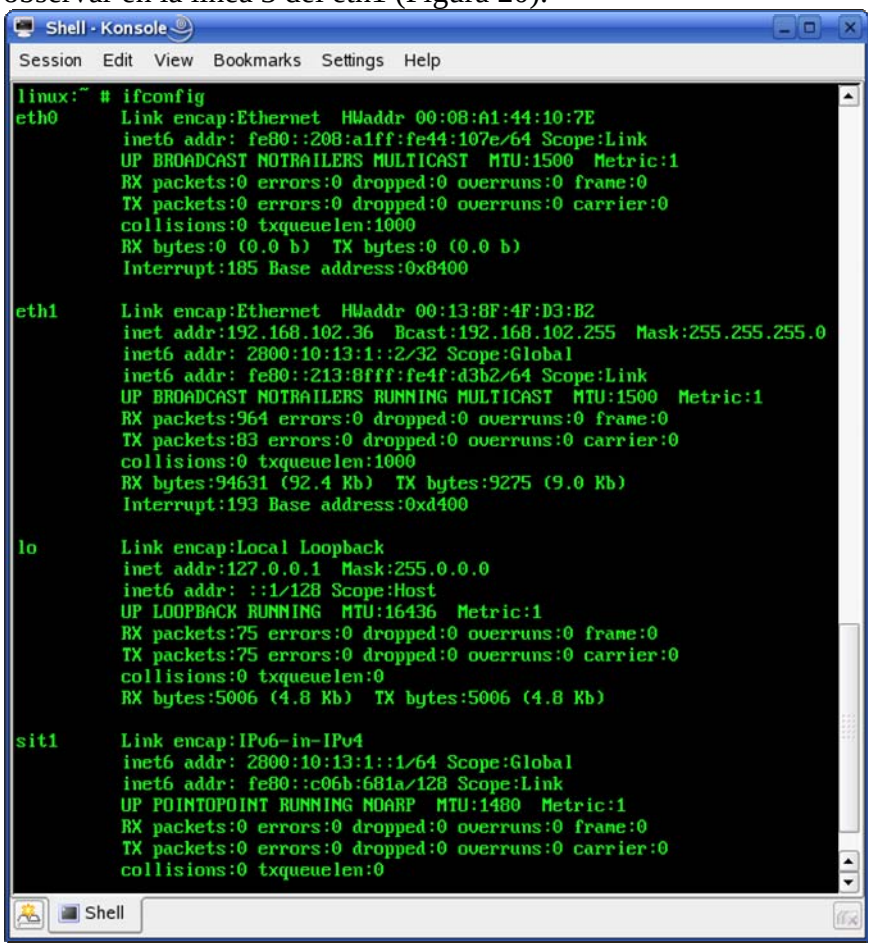


Figura 20

Como ya se dijo anteriormente el demonio radvd permite a los clientes obtener una ip y una ruta predeterminada simplemente levantando el dispositivo de red en el cliente. Ahora podemos iniciar el radvd con start y vemos que funciona correctamente.

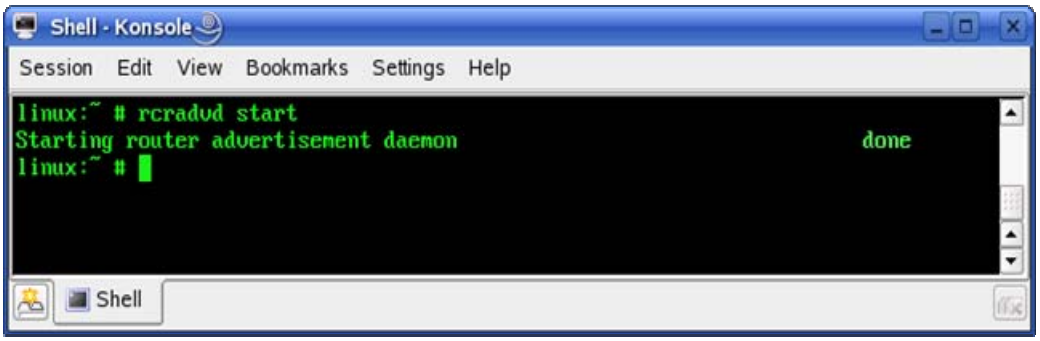


Figura 21

En un cliente que tiene el Sistema Operativo Debian se anuncia una dirección **2800:10:13:1:213:8fff:fe4f:dbb1** que es de nuestro router Linux. (Figura 22)

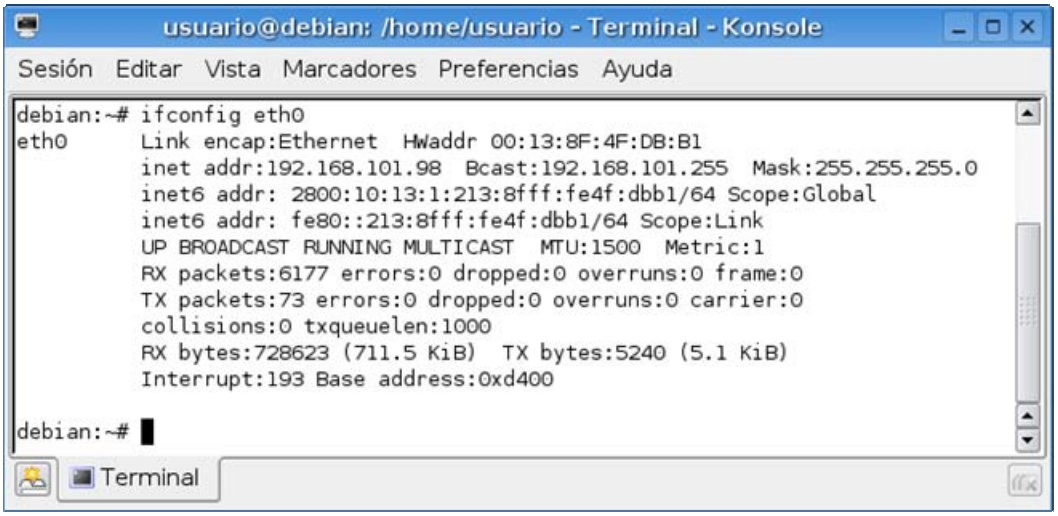


Figura 22

Si reiniciamos nuestra maquina no se guardarían los cambios por lo tanto el túnel desaparece y tendríamos que volver a realizar una a una las sentencias de configuración. Es para esto que debemos crear un archivo en /etc/sysconfig/network/ifcfg-sit1 con el siguiente contenido:

```
STARTMODE='onboot'
BOOTPROTO='static'
TUNNEL='sit'
TUNNEL_LOCAL_IPADDR='192.107.104.26'
TUNNEL_REMOTE_IPADDR='200.85.172.109'
IPADDR='2800:10:13::1/64'
TTL='64'
```

También crearíamos el archivo /etc/sysconfig/network/ifroute-sit1 y editamos lo siguiente:

```
2000::/3 ::192.168.1.1 metric 1
```

Una vez hecho esto reiniciamos nuestra maquina y la configuración del túnel será la misma y al dar un ifconfig.

A como podemos observar se encuentran las 2 interfaces eth0 (Internet), eth1(nuestra red LAN), lo (loopback) y nuestro túnel sit1 y esta vez de manera permanente debido a los archivos de configuración que creamos anteriormente.

A como podemos observar en la parte de la interfaz **eth1** se encuentran las direcciones de **ipv6** la que añadimos nosotros **2002:a562:808::1/64** y la dirección de tipo "Link Local" que tienen todos los interfaces de red de un sistema con soporte IPV6 de forma automática, su función es única para comunicaciones administrativas, auto configuración, etc (parte superior de la Figura 22.

Pruebas del túnel

- ping6 2001:ad0::10 (Figura 23)

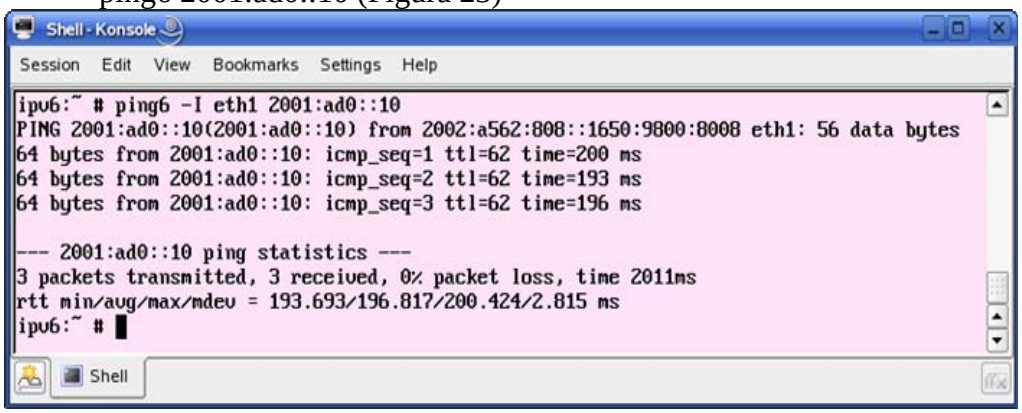
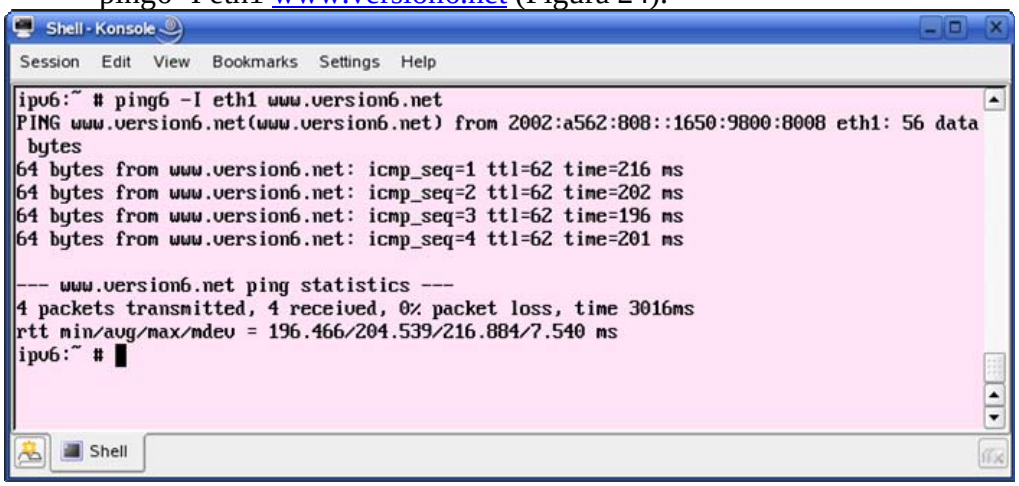


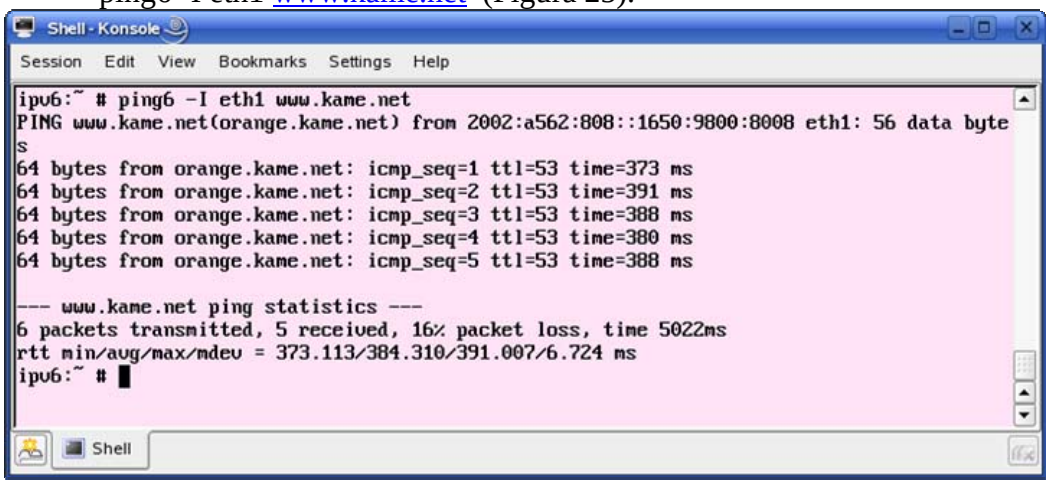
Figura 23

- ping6 -I eth1 www.version6.net (Figúra 24).



Figúra 24

- ping6 -I eth1 www.kame.net (Figúra 25).



Figúra 25

- dig aaaa www.version6.net (Figura 26).

El **comando dig** (**Domain information Groper**) constituye una herramienta para realizar consultas de diverso tipo a un servidor de **DNS**. Este muestra las respuestas recibidas de acuerdo a su solicitud. Es muy útil para detectar problemas en la configuración de los servidores de **DNS** debido a su flexibilidad, facilidad de uso y claridad en su salida. En este caso lo hacemos al servidor DNS cuyo dominio es www.version6.net y el resultado lo observamos en la Figura 26.

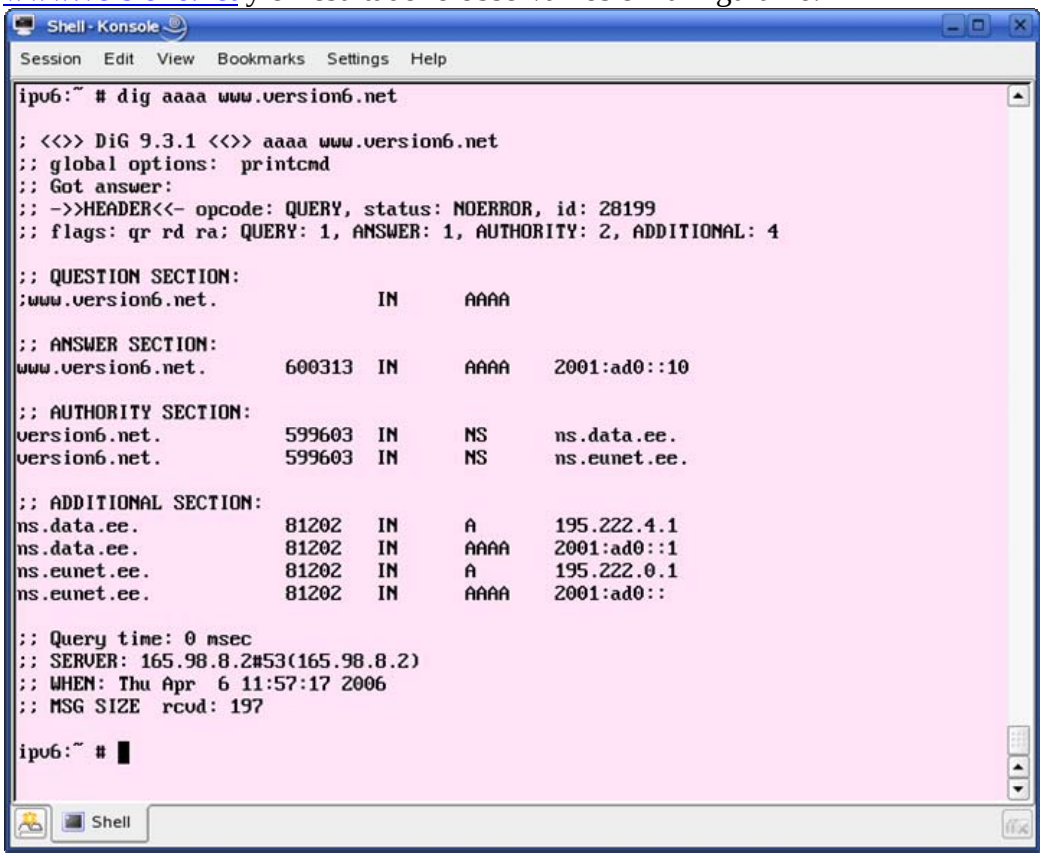


Figura 26

Explicamos el resultado de este comando:

;; QUESTION SECTION:

;www.version6.net		IN	AAAA	

La pregunta enviada al servidor DNS

;; ANSWER SECTION:

www.version6.net	600313	IN	AAAA	2001:ad0::10

La respuesta del servidor DNS contenido en el campo el cual es posible lograr el nombre del servidor de correo.

;; AUTHORITY SECTION:

version6.net.	599603	IN	NS	ns.data.ee.
version6.net.	599603	IN	NS	ns.eunet.ee.

;; ADDITIONAL SECTION:

ns.data.ee	81202	IN	A	195.222.4.1
ns.data.ee	81202	IN	AAAA	2001:ad0::1
ns.eunet.ee	81202	IN	A	195.222.0.1
ns.eunet.ee	81202	IN	AAAA	2001.ad0::

;; Query time: 0 msec
;; SERVER: 165.98.8.2#53(165.98.8.2)
;; WHEN: Thu Apr 6 11:57:17 2006
;; MSG SIZE rcvd: 197

- traceroute 2001:ad0::10 (Figúra 27).

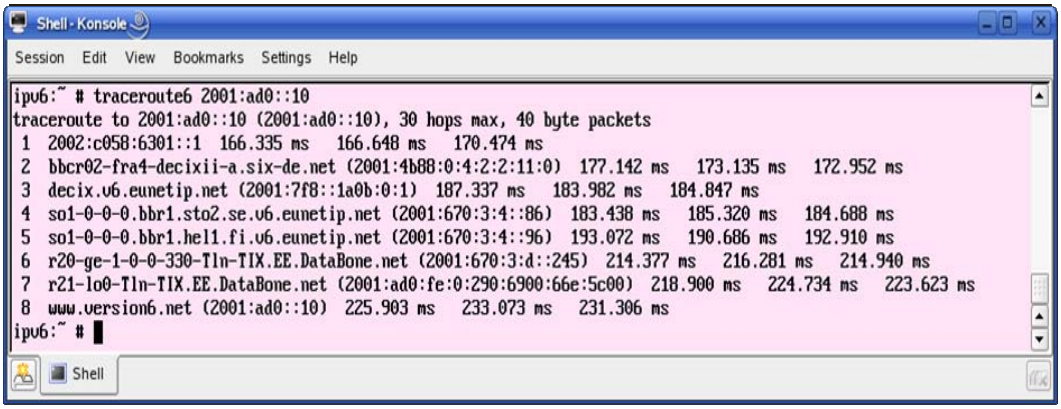


Figura 27

Una vez terminada la configuración del Servidor de nuestra Intranet pasamos a lo que seria la configuración del túnel en el Router de Renia.

6.6.6 *Configuración del túnel en el Router de Renia hacia el túnel en el servidor Router de León*

```
conf t= con este comando entramos de una vez a configurar el tunnel
```

Pasos para la configuración del túnel

```
interface tunnel#       (#= colocamos el numero del tunnel)
ipv6 address ipv6       (ipv6= dirección ipv6 asignada a la
interfaz)
tunnel source ip        (ip= dirección ipv4 origen del
tunnel(Router))
tunnel destination ip   (ip= dirección ipv4 destino del
tunnel(Servidor))
tunnel mode ipv6ip
```

Una vez que sabemos como realizar la configuration del tunnel en el Router pasemos a realizarlo:

```
RENIA_C3660#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RENIA_C3660(config)#int tunnel 20
RENIA_C3660(config-if)#ipv6 address 2800:10:13:1::1/64
RENIA_C3660(config-if)#tunnel source 200.85.172.109
RENIA_C3660(config-if)#tunnel destination 165.98.8.110
RENIA_C3660(config-if)#tunnel mode ipv6ip
RENIA_C3660(config-if)#description <<Tunnel de IPV6 de la UNAN-
León>>
RENIA_C3660(config-if)#exit   (Para salir de la configuración)
RENIA_C3660#
```

Después de la configuración del túnel podemos dar de nuevo la orden

```
RENIA_C3660(config)#do sh run
```

Yaqui ya podemos apreciar la parte del tunnel20 de la UNAN-León configurado en el Router RENIA.

```
interface Tunnel20
 description << Tunnel de Ipv6 a la UNAN-Leon >>
 no ip address
 ipv6 address 2800:10:13:1::1/64
 tunnel source 200.85.172.109
 tunnel destination 192.107.104.26
 tunnel mode ipv6ip
RENIA_C3660(config-if)#exit
```

6.6.7 *Pruebas de verificación del túnel Ipv6 entre UNAN-León-RENIA.*

```
linux:/etc/sysconfig/network # ping6 2800:10:13:1::2
PING 2800:10:13:1::2(2800:10:13:1::2) 56 data bytes
64 bytes from 2800:10:13:1::2: icmp_seq=1 ttl=64 time=0.067 ms
```

64 bytes from 2800:10:13:1::2: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 2800:10:13:1::2: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 2800:10:13:1::2: icmp_seq=4 ttl=64 time=0.049 ms
^X64 bytes from 2800:10:13:1::2: icmp_seq=5 ttl=64 time=0.049 ms

--- 2800:10:13:1::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.047/0.052/0.067/0.007 ms

```
linux:/etc/sysconfig/network # ping6 2800:10:13:1::1
```
PING 2800:10:13:1::2(2800:10:13:1::2) 56 data bytes
64 bytes from 2800:10:13:1::1: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 2800:10:13:1::1: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 2800:10:13:1::1: icmp_seq=3 ttl=64 time=0.048 ms

--- 2800:10:13:1::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.047/0.052/0.067/0.007 ms

RENIA_C3660#ping6 2800:10:13::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:10:13::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/5 ms
RENIA_C3660#ping6
Target IPv6 address: **2800:10:13::1**
Repeat count [5]: **1000**
Datagram size [100]: **5000**
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 1000, 5000-byte ICMP Echos to 2800:10:13::1, timeout is 2 seconds:
!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (90/90), round-trip min/avg/max = 8/9/76 ms

7. CONCLUSIONES

La principal conclusión de este trabajo monográfico es que técnicamente, ya se puede implantar IPv6 en Nicaragua con el proyecto RENIA. En principio es costoso, pero las ventajas que aporta el nuevo protocolo permitirán amortizar la inversión en poco tiempo. En la actualidad tenemos en UNAN-León un router Linux Ipv6 funcionando y entregando conectividad a clientes por cada una de sus interfaces de red.

Mediante la experiencia adquirida y la evolución de los sistemas operativos logramos realizar la configuración sencilla de herramientas necesarias (router Linux) para crear redes locales, así como en router hardware (Cisco), que fueron utilizados en las distintas Universidades permitiendo la interacción y transferencia de información para Internet de segunda generación.

El camino de IPv4 a IPv6 no es una cuestión de transición ni de migración, sino de evolución, integración, pero se trata de una fuerte integración que al mismo tiempo es necesaria.

Logramos que la comunidad Universitaria se diera cuenta del uso y desarrollo que IPV6 y sus aplicaciones presentan en la actualidad. Impulsando de esta manera su implementación.

IPv6 está diseñado para resolver muchos de los problemas de la versión actual de IP (conocida como IPv4) como son los relativos a la escasez de direcciones, seguridad, autoconfiguración, capacidad de ampliación y otros más. Su uso en el futuro permitirá también aumentar las posibilidades de Internet, haciendo posibles una serie de escenarios nuevos y sumamente atractivos, como las aplicaciones punto-a-punto y para dispositivos móviles.

En el presente trabajo se trataron temas y conceptos básicos de comunicaciones de suma importancia, como lo son las redes en el área de la informática. Se conoce detalladamente la conexión entre la Red Nicaragüense de Internet Avanzada (RENIA) y las Universidades de Nicaragua: UNAN-León, UNAN-Managua, UNI, UNA, UCA, UPOLI. Logrando de esta manera ser un ámbito de integración, comunicación y discusión al servicio de los objetivos de la educación y la investigación.

8. RECOMENDACIONES

A los grupos que desean tener conectividad en Ipv6 a través de RENIA, contar con equipo actualizados que soporten IPv6, hablamos de un Router Cisco con 256 de RAM, y 64 de Flash al cual le es necesario solo actualizar la IOS dependiendo de la versión del Cisco. O bien contar con un Router Linux que tenga las características…

No deben perder la oportunidad de conectarse a la Internet de segunda generación la cual ofrecerá un mejor intercambio de información fácil, confiable y muy pronto IPv6 cambiará por completo su medio ambiente ofreciendo nuevos servicio avanzados.

Se recomienda a las diferentes universidades que fomenten en las diferentes facultades algún trabajo en el cual los estudiantes se vean involucrados con este tipo de tecnología para contribuir así al desarrollo de la información explotando así al máximo ipv6.

También es importante que los diferentes departamentos de computación en este caso los técnicos y docentes, sean capacitados y proporcionarles las herramientas suficientes para contribuir así al desarrollo de ipv6.

Promover entre los estudiantes de informática el aportar o desarrollar equipos de trabajos para que así contribuyan en el desarrollo de nuevas aplicaciones en ipv6.

Hacer conciencia que esta es una red de nicaragua sin fines de lucro que permitirá compartir información con todas las redes de Investigación y educación en las que se pueden integrar cualquier otra institución o entidad con fines educativos.

A las TIC que contribuyan generando proyectos para lograr así una mejor organización del trabajo y de la dirección que ipv6 tomara en el futuro para las diferentes instituciones.

Es importante que ipv6 corra sobre su propia infraestructura, esto es que deje de compartir medios con otras versiones de ip, puesto que esto contribuiría a la explotación de los verdaderos recursos que ofrece ipv6. Claro está que esta transición evolucionara con el tiempo.

Invitar a más instituciones a pertenecer a la Red Nicaragüense de Internet Avanzada.

ANEXOS

9. ANEXOS

9.1 Anexo 1: Noticia

(27/03/2006)

RENIA ya es parte de RedCLARA

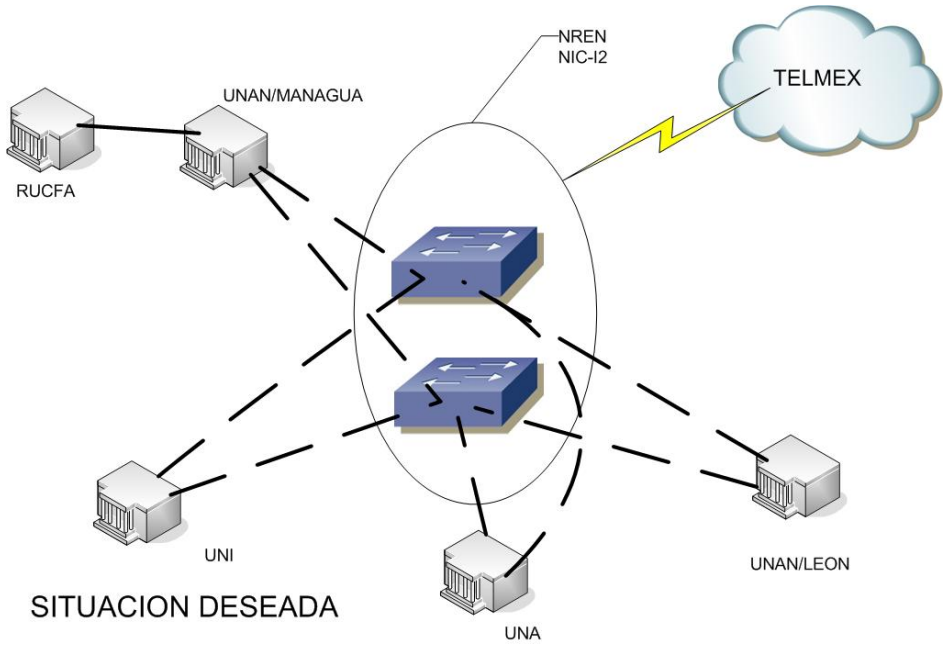
Con esta conexión, RedCLARA ya cuenta con 13 países conectados, haciendo cada vez más cercano el éxito de este proyecto.

El pasado 20 de marzo RENIA, la red nicaragüense de Internet Avanzada, se conectó por primera vez a RedCLARA. Con esto ya suman 13 las redes conectadas a esta gran red en Latinoamérica.
La noticia fue comunicada por Roberto Blandino Obando, el director ejecutivo de RENIA, quien agradeció el apoyo de los países miembros de CLARA y reconoció el trabajo de los técnicos de RedCLARA y los de RENIA. "Gracias al trabajo de todos, RENIA esta conectada. Ha sido toda una gran experiencia y ciertamente se tuvo una buena recompensa. Ahora esta el reto de como utilizar, de la mejor manera, esta conexión", expresó Blandino.
Los directores ejecutivos de varios países miembros de CLARA han manifestado su alegría y han enviado sus felicitaciones a RENIA.

Este comunicado fue encontrado en el mes de Marzo en: http://www.redclara.net/07/02/03_04.htm cuando RENIA estableció por primera ves conexión con Red Clara. Recalcamos que con esto Nicaragua fue la décima tercera red conectada a la Red de Cooperación Latino Americana de Redes Avanzadas.

9.2 Anexo 2: Topología idónea

En principio se pensó que lo idóneo de la topología de RENIA sería:



De este modo observamos 2 switches que generarían redundancia entre las conexiones a las Universidades de manera que si se cayera la conexión en uno de ellos, no se perdería la comunicación puesto que existe otro switch.

La red Clara cuenta con un Cisco 12006 Router, presentando un chasis 6-ranuras configurado con una tarjeta de línea 4-port OC3 POS (Packet Over Sonet) en la ranura 1, y una tarjeta de línea 4-port GE (Gigabit Ethernet) en la ranura 2 esta interconectada con la Red Renia en un Router Cisco 3660 Cisco 3660 6-slot Modular Router-AC with IP SW S366CP-12105YB Cisco 3660 Series IOS IP PLUS este a la vez se interconecta con un switch 3750 apila hasta nueve switches como una única unidad lógica para obtener un total de 468 puertos Ethernet 10/100 o 252 puertos Ethernet 10/100/1000 al cual se conecta el Nic-IX de este parte la conexión a cada Universidad por medio de fibra óptica.

9.3 Anexo 3: Configuración del switch 3750

Este es el Router de RENIA al cual tienen permiso de acceder solo los técnicos una vez introducido el usuario y su correspondiente contraseña pasamos a la configuración:

```
RENIA_C3750(config)#do sh run
Building configuration...
Current configuration : 5041 bytes       //configuracion actual
!
versión 12.4
service timestamps debug uptime          //elimina errores
service timestamps log uptime            //mantienen los registros
service password-encryption              //contraseña encriptada
!
hostname RENIA_C3750                     //nombre
!
boot-start-marker                        //carga el inicio
boot-end-marker                          //carga el fin
!
```

Nota: Hasta aquí se carga la configuración, y se muestra la actual, la versión y los servicios activos como la eliminación de errores, mantenimiento de los registros y la contraseña encriptada. El nombre de Router que es RENIA_C3750, marcadores de inicio y fin.

```
enable secret 5 $1$Z7j/$DpSPMX9hvoqe1ls1htYtm. //permite secreto
!
no aaa new-model                         //ningún modelo Nuevo
resource policy                          //política de recurso
ip cef                                   //cef ip

ipv6 unicast-routing                     //encaminamiento unicast ipv6
username renia password 7 025454490E0806201C1B
username enitel secret 5 $1$zlYa$1LBoIQpNMl1NMsbpKT9mq1
```

Nota: notamos que esta activo secret, detecta que no hay un modelo nuevo aaaa la política de recurso y las ip; encaminamiento unicast IPv6, a como podemos observar hay dos cuentas de usuarios RENIA y ENITEL con sus contraseñas.

```
interface Tunnel11
 description "Tunnel de IPv6 hacia la UNA"
 no ip address
 ipv6 address 2800:10:11:100::1/64
 tunnel source 200.85.172.109
 tunnel destination 165.98.116.115
 tunnel mode ipv6ip
!
interface Tunnel37
 description "Tunnel de IPv4 hacia la UNA"
 ip address 10.37.0.1 255.255.255.0
 ip mtu 1476
 tunnel source 200.85.172.109
 tunnel destination 165.98.116.115
!
```

Hasta la fecha están configurados dos túneles hacia UNA uno de Ipv6 y otra de Ipv4 los pasos de esta configuración la explicamos en la sección 10.1 del marco teórico.

```
interface Loopback3
 ip address 200.9.187.101 255.255.255.252
!
interface FastEthernet0/0
 description "Trunk contra Router en Enitel"
 no ip address
 duplex auto
 speed auto
!
```

La interfaz Loopback3 con su dirección ipv4 y su mascara, también tenemos la Fastethernet0/0 que es la que se conecta a Enitel

```
interface FastEthernet0/0.102
 description Vlan102
 encapsulation dot1Q 102
 ip address 200.0.204.166 255.255.255.252
 ip mtu 1470
 no snmp trap link-status
 ipv6 address 2001:1348:1:A::2/64
!
```

La interfaz FastEthernet0/0.102 que es hacia Vlan102 con su dirección ipv4, la mascara, su dirección de Ipv6.

```
interface FastEthernet0/1
 description "Trunk contra Router en IBW para Clientes de IBW-RENIA"
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.300
 description Internet-Access-x-IBW
 encapsulation dot1Q 300
 ip address 200.85.169.82 255.255.255.252 secondary
 ip address 200.85.172.109 255.255.255.248
 no snmp trap link-status
!
```

La interfaz FastEthernet0/1 esta dirigida al ISP de IBW para las Universidades clientes de IBW. La interfaz FastEthernet0/1.300 que es para el acceso a Internet de IBW con dos direcciones de ipv4 y sus mascara.

```
interface FastEthernet0/1.301
 description "Puntos de Encuentro Streaming"
 encapsulation dot1Q 301
 ip address 165.98.33.1 255.255.255.0
 no snmp trap link-status
 ipv6 address 2800:10:16::1/64
!
```

La interfaz FastEthernet0/1.301 esta ira hacia Puntos de Encuentros que es una entidad esta

```
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface FastEthernet1/1
 ip address 165.98.35.4 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2800:10:10::1/64
 ipv6 address 2800:10:12::1/64
 ipv6 address 2800:10:13::1/64
!
```

Esta interfaz FastEthernet 1/1 esta asignada a la red 165.98.35 de UNAN-Managua tiene asignada tres direcciones de ipv6 pertenecientes a UNI, UNAN-Managua y UNAN-León.

```
router rip
 version 2
 redistribute connected
 redistribute bgp 65102 metric transparent
 passive-interface default
 no passive-interface Tunnel37
 network 10.0.0.0
 no auto-summary
!
router bgp 65102
 no synchronization
 bgp log-neighbor-changes
 network 165.98.33.0 mask 255.255.255.0
 network 165.98.35.0 mask 255.255.255.0
 network 165.98.37.0 mask 255.255.255.0
 neighbor 2001:1348:1:A::1 remote-as 27750
 neighbor 2001:1348:1:A::1 password 7 097E1D274825014448
 neighbor 2001:1348:1:A::1 route-map filtro-ipv6-out out
 neighbor 200.0.204.165 remote-as 27750
 neighbor 200.0.204.165 password 7 145F005819550A626F
 neighbor 200.0.204.165 soft-reconfiguration inbound
 neighbor 200.0.204.165 route-map filtro-saliente-bgp out
 neighbor 200.9.187.73 remote-as 64601
 neighbor 200.9.187.73 ebgp-multihop 255
 neighbor 200.9.187.73 update-source Loopback3
 neighbor 200.9.187.73 soft-reconfiguration inbound
 neighbor 200.9.187.73 route-map filtro-saliente-bgp out
 no auto-summary
 !2800:10:13::/48    ---> Universidad Nacional Autónoma León(UNAN-LEON
 address-family ipv6
 neighbor 2001:1348:1:A::1 activate
 neighbor 2001:1348:1:A::1 send-community
 neighbor 2001:1348:1:A::1 soft-reconfiguration inbound
 network 2800:10:10::/64
 network 2800:10:11:2::/64
 network 2800:10:11:3::/64
 network 2800:10:11:5::/64
 network 2800:10:11:6::/64
 network 2800:10:11:7::/64
 network 2800:10:11:8::/64
 network 2800:10:11:9::/64
 network 2800:10:11:10::/64
 network 2800:10:11:100::/64
 network 2800:10:12::/64
 network 2800:10:13::/64
 network 2800:10:16::/48
```

```
 exit-address-family
!
```

El router BGP 65102 donde se especifican los cambios en los registros de las subredes Ipv4 y las direcciones de la familia de Ipv6 (UNI, UNA UNAN-Managua, UNAN-Leone IBW)

```
no ip http server
!
ip route 0.0.0.0 0.0.0.0 200.85.172.105
ip route 165.98.33.0 255.255.255.0 Null0
ip route 165.98.35.0 255.255.255.0 Null0
ip route 165.98.37.0 255.255.255.0 10.37.0.2
!
!
access-list 5 permit 165.98.33.0 0.0.0.255
access-list 5 permit 165.98.34.0 0.0.0.255
access-list 5 permit 165.98.35.0 0.0.0.255
access-list 5 permit 165.98.36.0 0.0.0.255
access-list 5 permit 165.98.37.0 0.0.0.255
access-list 5 deny   any log
snmp-server community ReNia RO
ipv6 route 2800:10:10::/64 Null0
ipv6 route 2800:10:11:2::/64 2800:10:11:100::2
ipv6 route 2800:10:11:3::/64 2800:10:11:100::2
ipv6 route 2800:10:11:5::/64 2800:10:11:100::2
ipv6 route 2800:10:11:6::/64 2800:10:11:100::2
ipv6 route 2800:10:11:7::/64 2800:10:11:100::2
ipv6 route 2800:10:11:8::/64 2800:10:11:100::2
ipv6 route 2800:10:11:9::/64 2800:10:11:100::2
ipv6 route 2800:10:11:10::/64 2800:10:11:100::2
ipv6 route 2800:10:12::/64 Null0
ipv6 route 2800:10:13::/64 Null0
ipv6 route 2800:10:16::/48 Null0
!
route-map filtro-ipv6-out permit 5
 match ipv6 address FilterInternet2
 set metric 5
!
route-map filtro-saliente-bgp permit 5
 match ip address 5
 set metric 5
!
ipv6 access-list FilterInternet2
 permit ipv6 2800:10:11::/48 any
 permit ipv6 2800:10:12::/48 any
 permit ipv6 2800:10:13::/48 any
 permit ipv6 2800:10:14::/48 any
 permit ipv6 2800:10:15::/48 any
 permit ipv6 2800:10:16::/48 any
!
```

Esta es la lista de direcciones Ipv6 permitidas en el Filtro de Internet2

```
control-plane
!
line con 0
line aux 0
line vty 0 4
```

```
 password 7 0254540B5E140A2F454F
 login local
line vty 5 15
 password 7 15405B5C51382E2A2132
 no login
!
end
```

Este switch con capacidad de Ruteo presento problemas por lo que se pretendió almacenar 9000 direcciones y el buffer no lo soportaba. Fue por esta razón que se cambio al Router 3660.

9.4 Anexo 4: Característica de Router Cisco 3660

El producto, conocido como "PLATAFORMA MULTIFUNCIONAL CISCO SERIE 3660", se utiliza para redes multiservicio de grandes sucursales o para los servicios que gestionan las compañías telefónicas, como el equipamiento en la instalación del cliente. Tiene la versatilidad para admitir los requisitos actuales de datos, voz, video y las aplicaciones híbridas de acceso telefónico de las sucursales y empresas, y la conectividad de alta velocidad para soportar las crecientes necesidades de ancho de banda de las aplicaciones multiservicio.

La plataforma multifuncional Cisco combina el acceso telefónico, enrutamiento y servicios entre redes de área local (LAN) y el multiservicio integrado de voz, video y datos en el mismo aparato. Sus especificaciones son las siguientes:

Cisco IOS Software, 3600 Software (C3660-IS-M), Version 12.4(7), RELEASE SOFTWARE (fc6)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 28-Feb-06 21:28 by alnguyen

ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)

RENIA_C3660 uptime is 9 weeks, 5 days, 21 hours, 58 minutes
System returned to ROM by power-on
System image file is "flash:c3660-is-mz.124-7.bin"

Cisco 3660 (R527x) processor (revision 1.0) with 250880K/11264K bytes of memory.
Processor board ID JAB043281FN
R527x CPU at 225MHz, Implementation 40, Rev 10.0, 2048KB L2 Cache

3660 Chassis type: ENTERPRISE
4 FastEthernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of NVRAM.
32768K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)
16384K bytes of processor board PCMCIA Slot1 flash (Read/Write)

Una de las ventajas clave de la plataforma Cisco 3660 es que en ella se ejecuta el software Cisco IOS, el sistema operativo que se distribuye en la mayoría de los equipos de backbone de Internet en el mundo. La compatibilidad con el software Cisco IOS permite a los clientes instalar muchas características en una gran variedad de aplicaciones.

9.5 Anexo 5: Fotos

Estas imágenes muestran la representación de las redes.

Foto tomada en IBW cuando se realizo una reunión técnica de la configuración del Router de Renia en donde están presentes los técnicos de RENIA.

Las siguientes fotografías muestran la primera aplicación corriendo en Ipv6 sobre Ipv4 (Isabel) presentada en una de las reuniones en la que se presenciaba una videoconferencia entre México y Madrid (España). Fue realizada en UNA. Y a esta asistieron todos los técnicos de RENIA.

Grupo de trabajo de Ipv6

9.6 Anexo 6: Glosario

Este glosario pretende tener una rápida referencia de los términos pocos familiares.

- **ADSL:** (Línea de Abonado Digital Asimétrica). Consiste en una línea digital de alta velocidad apoyada en el par trenzado de cobre que lleva la línea telefónica convencional o línea de abonado

- **arsys.es:** es el nº 1 en registro de dominios con más de 250.000 dominios registrados. Arsys lidera el mercado español de nuevas tecnologías y más especialmente el que se relaciona con el alojamiento de páginas web, con el registro de dominios, acceso a Internet. También propone otros servicios como cuentas SMS, servidores dedicados, y servidores de aplicación.

- **BGP**: El BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un router que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca. Se trata del protocolo más utilizado para redes con intención de configurar un EGP (external gateway protocol).

- **Broadcast**: Tipo de comunicación en la que un solo emisor llega a múltiples receptores. se producen cuando una fuente envía datos a todos los dispositivos de una red.

- **Conexión RDSI:** Una conexión RDSI es una conexión a Internet con un módem a través de una línea de teléfono especial instalada por la compañía de teléfonos.

- **DANTE**: (Delivery of Advanced Network Technology to Europe o Distribución de Tecnología Avanzada de Redes a Europa) Organización sin ánimo de lucro creada en 1993 con el objetivo de mejorar las redes de comunicación de los organismos de investigación europeos.

- **Dirección IPV4 compatible:** La dirección IPv4 compatible con direcciones IPv6 constituye una clase especial de dirección IPv6. Es una dirección de IPv6 cuyos primeros 96 bits son ceros, mientras que los últimos 32 bits representan una dirección IPv4.

- **Dirección IPV4 mapeada**: El formato ::ffff:1.2.3.4 se denomina dirección IPv4 mapeada, La dirección IPv4 mapeada es usada como un mecanismo de transición en terminales duales.

- **DWDM:** es el acrónimo, en inglés, de *Dense wavelength División Multiplexing*, que significa *Multiplexación por división en longitudes de onda densas*. DWDM es una técnica de transmisión de señales a través de fibra óptica.

- **E1**: es un formato europeo de transmisión digital ideado por el ITU-TS; su nombre fue dado por la administración de la Conferencia Europea de Correos y Telecomunicaciones (CEPT). El formato de la señal E1 lleva datos en una tasa de 2,048 millones de bits por segundo y puede llevar 32 canales de 64 Kbps * cada uno, de los cuales treinta son canales activos simultáneos para voz o datos. E1 lleva en una tasa de datos algo más alta que el T-1 (que lleva 1,544 millones de bits por segundo) porque, a diferencia del T-1, no hace el bit-robbing y los ocho bits por canal se utilizan para cifrar la señal. E1 y el T-1 se pueden interconectar para uso internacional.

- **GEANT:** La red paneuropea de investigación a alta velocidad GÉANT entró en funcionamiento en noviembre de 2001 por un periodo de cuatro años. Está interconectada con 28 redes nacionales y regionales de investigación y de educación (NREN) de unos treinta países y ofrece servicios a más de 3.000 instituciones

- **IANA: El Internet Assigned Numbers Authority** (IANA) es una organización que supervisa la asignación del IP ADDRESS , la gerencia de la zona de la raíz del DNS , y otras asignaciones del Internet Protocol. El IANA es ampliamente responsable de la asignación de los nombres y de los números global-únicos que se utilizan en los protocolos del Internet.

- **IETF**: (**I**nternet **E**ngineering **T**ask **F**orce, en castellano Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986.

- **IN-ADDR.ARPA**: El dominio in-addr.arpa se usa en todas las redes TCP/IP que se basan en el direccionamiento del Protocolo Internet versión 4 (IPv4). El Asistente para crear zona nueva supone de forma automática que se utiliza este dominio cuando se crea una zona de búsqueda inversa nueva.

- **Infovia**: Red de transmisión de datos de Telefónica que permitía el acceso a Internet desde cualquier punto de nuestro país a precio de llamada local. Esta red, que supuso un avance importante en el desarrollo de Internet en España, ha sido sustituida a mediados de enero por "Infovía Plus".

- **Interfaz**: Una interfaz es la parte de un programa informático que permite a éste comunicarse con el usuario o con otras aplicaciones permitiendo el flujo de información.

- **IPsec:** (la abreviatura de Internet Protocol security) es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente fue desarrollado para usarse con el nuevo estándar IPv6, aunque posteriormente se adaptó a IPv4.

- **ISABEL**: es un software configurable de audio/video/data conferencia, que permite crear escenarios de colaboración adaptados a las necesidades de usuarios. El elemento central es el gestor programable de escenarios de colaboración que permite crear escenarios a la medida del usuario, con el que se han construido plataformas de tele-educación de ámbito universitario, de tele-reunión y tele formación corporativa o de realización de congresos y talleres distribuidos.

- **LACNIC**: es el Internet Registry regional para América latina y el Caribe. Administra direcciones del IP, números del Autonomous System, la resolución inversa, y otros recursos de la red para esa región.

- **Loopback**: Sistema de trabajo en red en modo local. Con este sistema podemos trabajar en red con nuestro propio ordenador, su utilidad radica en probar programas de seguridad, leer las noticias o el correo de los servidores instalados en nuestro ordenador o simplemente poder ejecutar Xwindow.

- **NICIX:** es el punto de intercambio en Internet en la cual los proveedores de servicios convergen a fin de mantener local el trafico nacional, ofreciendo de esta manera mayor velocidad y mejor calidad de servicios a sus clientes.

- **non-IPv6:** hardware que no cumple con los requisitos del IPv6.

- **NREN:** Red Nacional de Investigación y Educación. Proyecto impulsado por el vicepresidente de los EE.UU, Al Gore, con el fin de interconectar todos los componentes de investigación y docencia americana, con la ayuda de redes de alta velocidad**.**

- **OSI**: El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

- **Protocolo UDP**: El protocolo UDP (User Datagram Protocol, protocolo de datagrama de usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. UDP utiliza el protocolo IP para transportar sus mensajes, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.

- **QoS:** Quality of Service: Calidad de servicio. En Internet y otras redes, designa la posibilidad de medir, mejorar y, en alguna medida, garantizar por adelantado los índices de transmisión y error. Es importante para la transmisión fluida de información multimedia: por ejemplo, para los usos académicos de Internet2.

- **RedIRIS:** Red académica española destinada a la interconexión de recursos informáticos de las universidades y centros de investigación.

- **RFC 3879:** ingles de Request For Comments. Conjunto de notas técnicas y organizativas donde se describen los estándar es o recomendaciones de Internet.

- **RIPE**: **Réseaux IP Européens (RIPE)** es un foro colaborativo para los grupos interesados en redes IP. El objetivo de RIPE es asegurar la coordinación administrativa y técnica necesaria para que funcione Internet dentro de la región de RIPE

- **RNP:** Red Nacional de Ensino e Pesquisa (RNP) (red de la educación nacional y de la investigación) es espina dorsal de Internet académica del Brasil. Fue creada el 1989 y la red comenzó a ser construida en 1991.

- **TCP/IP**: es un protocolo de comunicaciones, el TCP/IP se compone de capas:
  - **IP** - es responsable de mover el paquete de datos desde nodo al nodo. El IP remite cada paquete basado en una dirección de destinación de cuatro octetos (el IP Number). Las autoridades del Internet asignan gamas de números a diversas organizaciones. Las organizaciones asignan los grupos de sus números a los departamentos. El IP funciona encendido las máquinas de la entrada que mueven datos desde el departamento a la organización a la región y entonces alrededor del mundo.
  - **TCP** - es responsable de verificar la entrega correcta de datos del cliente al servidor. Los datos se pueden perder en la red intermedia. El TCP agrega la ayuda para detectar errores o datos perdidos y para accionar la retransmisión hasta que los datos se reciben correctamente y totalmente.

10. BIBLIOGRAFIA

10.1 FUENTES BIBLIOGRAFICAS:

- Libro IPv6 "IPV6 Network Administration"
  Nial Richard Murphy & David Malone
  O'REILY

10.2 FUENTES DE INTERNET:

- http://www.ripe.net/perl/whois?-r%20-T%20inet6num%202001:0ba0::/32/
- http://www.ipv6.unam.mx/
- http://www.rau.edu.uy/ipv6/queesipv6.htm/
- www.unanleon.edu.ni/renia/proyectos.htm
- http://www.redclara.net
- http://www.6sos.org/que_es_ipv6.php/
- http://www.6sos.org/
- http://imasd.elmundo.es/imasd/ipv6/cfg/router-freebsd.html
- http://www.dante.net/
- http://www.consulintel.es/Html/ForoIPv6/ Documentos/IPv6%20-0La%20Nueva%20Generación.pdf
- http://www.inf.uach.cl/apuntes/Propuesta%20IPv6%20nativo%20para%20Chile%20Dic-2002.pdf.
- http://www.unanleon.edu.ni/renia/documentos.htm
- http://www.lacnic.net/ipv6tour/docs/a-fernandez-cudi-ipv6.pdf
- http://people.fluidsignal.com/~luferbu/docs/Direccionamiento-IPv6.txt
- http://ws.edu.isoc.org/workshops/2004/CEDIA2/material/Configuracion_Basica_Cisco.pdf
- http://alfa.noc.redclara.net/nocredclara/redclara/contenidos/topologia.php
- http://www.lac.ipv6tf.org/

10.3 OTRAS FUENTES

- Reportaje de EL NUEVO DIARIO Domingo, 10 de julio de 2005.
- Entrevistas con técnico y personal involucrado en el proyecto de RENIA.