UNIVERSIDAD NACIONAL DE LOJA

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

INGENIERÍA EN SISTEMAS

TEMA

"ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPv6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE."

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS.

AUTORES:

JHON ALEXANDER CALDERÓN SANMARTÍN
RUBI RAFAEL CABRERA ERREYES

DIRECTOR:

ING. RENE ROLANDO ELIZALDE SOLANO

Loja - Ecuador

2011

ING. RENE ROLANDO ELIZALDE SOLANO, DOCENTE DEL ÁREA DE ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES Y DIRECTOR DE TESIS.

CERTIFICA:

Haber dirigido, orientado y discutido en todas sus partes el desarrollo del presente tema de tesis: **"ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPv6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE."** el cual se ajusta a los requerimientos de la Universidad Nacional de Loja y reúne a satisfacción los requisitos de fondo y forma exigidos para una investigación de éste nivel, por lo que autorizo su presentación.

Loja, Julio de 2011

ING. RENE ROLANDO ELIZALDE SOLANO.
DIRECTOR DE TESIS

AUTORÍA

Todas las opiniones, conceptos, análisis e interpretación del presente desarrollo de la tesis son de absoluta responsabilidad de los autores, quienes firmamos para su constancia.

Jhon Alexander Calderón Sanmartín. Rubi Rafael Cabrera Erreyes.

LICENCIA DE LA TESIS

AGRADECIMIENTO

Dejamos constancia de nuestro agradecimiento a la Universidad Nacional de Loja, a la Unidad de Telecomunicaciones e Información, que nos brindaron información y nos dieron las facilidades para la implementación del proyecto de tesis, al Ing. Rene Rolando Elizalde Solano, director de la tesis quien, con su experiencia y conocimiento fue nuestro guía en la elaboración y desarrollo de la tesis, para que sirva como medio de consulta en posteriores investigaciones y sea el reflejo de una ardua labor por las experiencias adquiridas.

LOS AUTORES

DEDICATORIA

Al cumplir una de las metas más importantes de mi vida, quiero dedicar la presente investigación a mis padres Gilberto y Aura Flor por su cariño, apoyo incondicional y confianza que depositaron en mí, a mis hermanos Hennry, Nilder, Carlos y Ronar por su compresión y brindarme su ayuda en los momentos que los necesite, finalmente a mis familiares y amigos que de una u otra manera me han apoyado desinteresadamente.

Jhon Alexander Calderón Sanmartín.

A mis Padres y abuelita por su cariño y abnegación, a mi hija Ayelen Carolina Cabrera Calva que es la razón y mi inspiración para seguir adelante, a mis hermanas y hermanos por su comprensión y apoyo incondicional y finalmente a amigos que de una u otra manera me han apoyado desinteresadamente.

Rubi Rafael Cabrera Erreyes.

1. TEMA

"ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPv6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE."

2. RESUMEN

2.1.RESUMEN (español)

En la Universidad Nacional de Loja, creemos que la implementación del Protocolo de Internet versión 6 (IPv6) en la red de datos Ethernet IEEE 802.3 es esencial para la apertura de Internet, sea por resultado de una investigación o por actualizaciones constantes.

El presente proyecto describe las características del nuevo protocolo de Internet IPv6, se realizó el análisis de la red de datos y mecanismos de transición a IPv6. Seguido del diseño del direccionamiento IPv6, procedimiento de instalación y configuración de los servicios de Internet en un entorno de desarrollo. Se llevo a cabo la fase de implementación en los servidores de producción, y finalmente se realizó las pruebas de validación de IPv6 en todo el campus universitario.

IPv6, está en auge, la cual permitirá la innovación y el crecimiento continuo de Internet, por tal motivo este proyecto propone un proceso para la implementación usando el mecanismo de transición doble pila (IPv4 e IPv6) para los servicios de Internet que se encuentran en un estado de producción en la institución.

La ejecución del presente proyecto de tesis se realizó con herramientas Software Libre y Open Source, como sistema base en los servidores se utilizó la distribución Gnu / Linux Centos. El uso de estas herramientas libre no involucra el pago de licencias para su utilización, también permiten adaptabilidad al entorno universitario y sobre todo independencia tecnológica.

2.2. SUMMARY

At the National University of Loja, we believe that the implementation of Internet Protocol version 6 (IPv6) data network in the IEEE 802.3 Ethernet is essential for the openness of the Internet, either by the result of an investigation or updates.

This project describes the characteristics of the new IPv6 Internet protocol, we performed the analysis and data network to IPv6 transition mechanisms. Following the design of IPv6 addressing, installation procedure and configuration of Internet services in a development environment. He carried out the implementation phase in production servers, and finally to the validation tests of IPv6 throughout the campus.

IPv6 is growing, which will allow innovation and continued growth of the Internet, for that reason this project proposes a process for implementing the transitional mechanism using double - stack (IPv4 and IPv6) for Internet services that are production in a state of the institution.

The implementation of this thesis project was carried out with tools Free and Open Source Software as server-based system was used GNU / Linux Centos. The free use of these tools does not involve licensing fees for use, they also allow adaptability to the university environment and especially technological independence.

3. ÍNDICE

3.1. INDICE GENERAL

3.2. INDICE DE FIGURAS

Página

3.3. INDICE DE TABLAS

Página

4. INTRODUCCIÓN

La Universidad Nacional de Loja es una institución de Educación Superior que desde sus inicios viene realizando investigación científico-técnica sobre los problemas del entorno, con el fin de coadyuvar al desarrollo sustentable de la región y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales con responsabilidad social, reconociendo y promoviendo la diversidad cultural y étnica, apoyándose en el avance científico y tecnológico en procura de mejorar la calidad de vida de nuestro país.

La evolución de Internet ha supuesto una revolución en el desarrollo de las comunicaciones y de la información, prueba inequívoca de ello es la inmensidad de información que existe en Internet. Cuando IPv4 fue estandarizado, 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.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades.

Con las consideraciones mencionadas anteriormente, surgió el protocolo IPv6 cuya finalidad es cubrir el déficit de direcciones IPv4 mediante la inclusión de direcciones de 128 bits, además de incluir nuevas funcionalidades que hacen que IPv6 sea un protocolo robusto y seguro. Aún con todas las mejoras en IPv6 se tiene que seguir utilizando IPv4. Se debe tomar en cuenta si se desea realizar una migración completa hacia IPv6, la infraestructura tendría un cambio vertiginoso; lo cual no es posible hacerlo de forma directa ya que la infraestructura con la que se cuenta actualmente se maneja bajo el protocolo IPv4, por ello debe realizarse una transición a IPv6 y la migración darse de forma paulatina.

Los objetivos específicos que se plantearon para el desarrollo del proyecto investigativo son los siguientes:

- Describir la situación actual de la infraestructura en la red de datos Ethernet 802.3 de la Universidad Nacional de Loja para la implementación del Protocolo Internet versión 6.
- Describir el Protocolo de Internet versión 6, que permita determinar el método de transición de IPv4 a IPv6 más eficiente.
- Diseñar el mecanismo de transición de IPv4 a IPv6, acorde al direccionamiento IP actual de la Universidad Nacional de Loja para su aplicabilidad.
- Instalar y configurar el hardware y software necesario para la red de datos Ethernet IEEE 802.3 de la Universidad Nacional de Loja que soporten IPv6.
- Desarrollar e implementar los servicios de Internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.

La investigación desarrollada se encuentra estructurada de acuerdo a los lineamientos establecidos por la Universidad Nacional de Loja y el Área de la Energía de la siguiente manera: RESUMEN que es una síntesis general del contenido del trabajo de tesis; ÍNDICE donde se detalla cada tema, figura y tabla con su página respectiva, en la INTRODUCCIÓN, se destaca la importancia del tema, el aporte para el desarrollo tecnológico de la Universidad Nacional de Loja referente al tema de estudio; la METODOLOGÍA se exponen los diversos métodos, técnicas y procedimientos utilizados en el desarrollo de éste trabajo investigativo; seguidamente se presenta la FUNDAMENTACIÓN TEÓRICA, donde se encuentra los conceptos IPv6 en sus diferentes ámbitos de interacción; EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN, donde se detalla cada uno de los equipos y herramientas utilizadas para la ejecución del proyecto planteado, DESARROLLO DE LA PROPUESTA ALTERNATIVA, luego del análisis y diseño realizado se construye la propuesta alternativa que permita la implementación de IPv6 dentro del la Universidad Nacional de Loja, se realiza una VALORACIÓN TÉCNICO. ECONÓMICA-AMBIENTAL sobre la implementación del proyecto investigado.

En la parte final se presenta las conclusiones y recomendaciones para dar solución y dejar constancia de nuestro trabajo en la Universidad Nacional de Loja, y diferentes herramientas que permitan un mejor aprovechamiento del Internet con fines académicos. Se da por finalizado con la bibliografía, y anexos correspondientes que sirvieron de base para el desarrollo de la investigación.

5. METODOLOGÍA

5.1. Materiales.

Los materiales que se utilizaron en éste proceso investigativo: "ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPV6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE.", están clasificados de forma general en los siguientes grupos:

- Materiales de oficina.
- Equipos de cómputo.
- Software libre y Open Source.
- Hardware destinado a servidores.
- Herramientas libres de diseño.

5.2. Métodos.

Los métodos utilizados en esta investigación los detallamos a continuación:

- **Método Científico**: Compuesto de principios, reglas y procedimientos, nos permitió orientar la investigación a fin de alcanzar un conocimiento objetivo de los procesos internos y externos de la red de datos de la Universidad Nacional de Loja.
- **Método Deductivo:** Permitió la recolección de la información relacionada a las actividades, problemas, causas y posibles alternativas en la implementación del protocolo IPv6 en la Universidad Nacional de Loja.

- **Método Inductivo**: Con la aplicación de este método se obtuvo todos los requerimientos necesarios para poder iniciar el diseño de la implementación de IPV6; mediante la entrevista, observación directa de la red de datos de la Universidad Nacional de Loja.

- **Método descriptivo**: Se utilizó para caracterizar, registrar, analizar e interpretar el manejo de la información existente y de los procesos que se efectúan actualmente.

Además los métodos utilizados en esta investigación son del orden teórico y práctico.

5.3. Técnicas de trabajo.

- **Observación.** La observación fue un elemento fundamental de este proceso investigativo, permitió observar hechos, para obtener el mayor número de datos. Entre las clases de observación que realizamos tenemos:

- **Observación directa.** La cual nos permitió identificar la estructura de la red de datos y todos sus componentes; y, el funcionamiento y los servicios que presta a los estudiantes, docentes y servidores universitarios.

- **Entrevista.** Se la realizó con el fin de obtener información, al director de la Unidad de Telecomunicaciones e Información, responsables de la secciones de Redes y Equipos Informáticos, Mantenimiento y Electrónico, Software; y, Telecomunicaciones, y a los técnicos encargados del manejo de la red de datos.

5.4. Desarrollo de Proyecto

Con la aplicación de los diferentes métodos y técnicas, se desarrolló el proyecto simplificado en comparación con otros procesos más tradicionales, se unificó un conjunto de métodos con el objetivo de abarcar todo el proyecto en su conjunto.

El presente proyecto investigativo se lo realizó en las siguientes fases, las cuales comprenden varias actividades que se deben realizar para asegurar el éxito del proyecto. Las cuales mencionamos a continuación:

- Análisis
- Diseño
- Implementación y,
- Pruebas

Cada una de las fases está relacionada con los objetivos planteados en el presente proyecto investigativo, lo que permitió ir desarrollando paso a paso para obtener un rendimiento óptimo en los diferentes servicios de Internet implementados.

6. FUNDAMENTACIÓN TEÓRICA

PROTOCOLO INTERNET VERSIÓN 6 (IPV6).

6.1. Introducción

El Protocolo Internet versión 6 (IPv6) es a veces llamado la siguiente generación de Internet Protocolo, o IPng. Es una nueva versión de IP (Protocolo Internet), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, que actualmente esta implementado en la gran mayoría de dispositivos que acceden a Internet.

Aún cuando el protocolo existente, IPv4, proporciona un espacio de direcciones de 32 bits, que teóricamente son 232 direcciones globales únicas (aproximadamente 4.000 millones), en la práctica, el número de direcciones globales IPv4 que pueden ser utilizadas es bastante inferior, debido a las ineficiencias en la asignación y uso de las direcciones. IPv4 tiene una capacidad limitada inherente para permitir la expansión de Internet y por tanto no permite conectar miles de millones de dispositivos cuando sea apropiado. La traducción de direcciones de red (Network Address Translation, NAT), conjuntamente con direcciones IPv4 privadas, ha permitido la prolongación de la vida útil de IPv4. Sin embargo, NAT añade complejidad al despliegue de nuevos modelos extremo a extremo, inhibiendo el crecimiento de Internet y la innovación, incluyendo aquellos servicios como "siempre-conectado" y "peer-to-peer", que requieren acceso seguro y constante a dispositivos como por ejemplo en redes domésticas. IPv6 ha sido concebido para facilitar estos dos objetivos, proporcionando una capacidad de direccionamiento virtualmente ilimitada que puede direccionar hasta 2128 dispositivos (hasta340.282.366.920.938.463.463.374.607.431.768.211.456).

6.2. Historia[1].

El esfuerzo para desarrollar un sucesor del protocolo IPv4 se inició en la década de 1990 por la Internet Engineering Task Force (IETF). Varios esfuerzos paralelos comenzó al mismo tiempo, todos tratando de resolver la limitación de espacio de direcciones previstas, así como proporcionar una funcionalidad adicional. El IETF empezó la zona de IPng en 1993 para investigar las diferentes propuestas y hacer recomendaciones para los procedimientos.

Los directores de área IPng de la IETF recomienda la creación de IPv6 en la reunión de la IETF Toronto en 1994. Su recomendación se especifica en el RFC 1752, "La recomendación

[1] HAGAN, Silvia. 2002. IPv6 Essentials, United States of America

para la próxima generación del protocolo IP." Los directores formaron la Address Lifetime Expectation (ALE) grupo de trabajo, cuyo trabajo fue determinar si la duración prevista para el IPv4, que permitiría el desarrollo de un protocolo con la nueva funcionalidad, o si el resto del tiempo sólo permitiría el desarrollo de una solución de espacio de direcciones. En 1994, el grupo de trabajo ALE prevee el agotamiento de direcciones IPv4 que puede ocurrir en algún momento entre 2005 y 2011, basado en las estadísticas de que se disponía en ese momento.

Para aquellos de ustedes que están interesados en las diferentes propuestas, aquí hay más información al respecto (de RFC 1752). Había cuatro principales propuestas que se CNAT, IP Encaps, Nimrod, y Aimple CLNP. Hay más propuestas son el fruto:el P Internet Protocol (PIP), el Simple Internet Protocol (SIP), y TP / IX. Después de la reunión de marzo de 1992 en San Diego IETF, Simple CLNP convertido en TCP y UDP con Bigger Address (TUBA) y IP Encaps evolucionado en IP Address Encapsulation (IPAE). IPAE se fusionó con el PIP y SIP y se llamó a sí Simple Internet Protocol Plus (SIPP). El TP / IX grupo de trabajo cambió su Common Architecture for the Internet (CATNIP). Las principales propuestas son ahora CATNIP, TUBA, y SIPP. Para una breve discusión de las propuestas, consulte RFC 1752.

El Internet Engineering Steering Group aprobó la recomendación de IPv6 y redactó una norma propuesta el 17 de noviembre de 1994. El conjunto básico de protocolo IPv6 se convirtió en un Proyecto de Norma IETF el 10 de agosto de 1998.

6.3. Ventajas del protocolo IPv6.

Consecuentemente, el diseño de IPv6 fue una forma oportunísima de mejorar Internet, con nuevas ventajas tales como:

- Auto-configuración y re-configuración sin servidores ("enchufar y funcionar", "plug and play"). Con esta característica Internet se simplifica, en el sentido de que es más fácil conectar automáticamente cualquier dispositivo a la red. No hay motivos para pedir a los usuarios que configuren nunca más los dispositivos, especialmente considerando que los nuevos dispositivos no serán "sencillos" ordenadores con teclado y pantalla, sino electrodomésticos, dispositivos de todo tipo, sensores, etc., los cuales no tienen este tipo de interfaces para poder ser configurados. En IPv4 esto no se puede realizar salvo que en la red se haya instalado un servidor (para el protocolo DHCP), lo que implica un coste superior para el propio servidor y su mantenimiento.

- Mecanismos de movilidad más eficientes y robustos. IPv6 ha sido diseñado bajo la perspectiva de un nuevo mundo "nómada". Usuarios y dispositivos tienden a movilizarse más que nunca. La conectividad es importante incluso cuando nos desplazamos, de tal forma que podamos utilizar servicios mejorados, especialmente en entornos sin cables. IPv4 también permite movilidad, pero es muy ineficiente comparada con la movilidad en IPv6.

- Seguridad extremo a extremo con autenticación y encriptación embebidas en la capa IP. IPsec es el protocolo de seguridad, el mismo que en el caso de IPv4. La principal diferencia es que IPv4 no obliga al soporte de IPsec, lo que implica que no siempre está disponible. Además, en IPv4, debido al uso de NAT, a menudo no es posible utilizar IPsec extremo a extremo, salvo que se posean los conocimientos necesarios para configurar un túnel o VPN (Red Privada Virtual, Virtual Private Network), entre las dos estaciones que desean establecer dicha comunicación y se atraviesen los NAT.

- Cabecera con un formato mejorado e identificación de flujos. Los diseñadores del protocolo IPv6 sacaron provecho de los conocimientos adquiridos con la experiencia por el uso de IPv4 durante los últimos años, de forma que pudiera mejorarse la forma en que los datos se codifican para formar la cabecera del protocolo IPv6 consecuentemente mejorar la operación de la red. Al mismo tiempo que la cabecera ha sido simplificada, hemos agregado nuevas funcionalidades, siendo una de ellas la identificación de flujos, lo cual permitirá en un futuro próximo una mejor operación de los mecanismos de calidad de servicio (QoS) en Internet.

- Soporte mejorado de multidifusión. IPv6 incluye soporte mejorado de multidifusión (multicast), dado que se trata de una característica embebida en el protocolo, la cual es fundamental para el uso de redes de banda ancha para la distribución de contenidos.

- Extensibilidad. Soporte mejorado para opciones/extensiones. Por último, pero no menos importante, IPv6 ha sido diseñado teniendo en cuenta las posibilidades para su crecimiento. No deseamos repetir errores y llegar a la situación de descubrir, en unos pocos años, que del mismo modo que diseñamos IPv4 de tal forma que ha

llegado a ser un impedimento para la extensión de Internet, pueda ocurrir con IPv6. La forma en que IPv6 trabaja permite incorporar nuevas características o piezas del protocolo (las que denominamos cabeceras de extensión), sin necesidad de actualizar todos los dispositivos de la red. Sólo aquellos dispositivos que precisen usar determinadas extensiones tienen que ser actualizados, del mismo modo que hoy todos los sistemas operativos y aplicaciones son frecuentemente actualizados, de una forma automática, transparente para el usuario.

6.4. Características del protocolo IPv6[2].

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Algunas de las características más relevantes de IPv6 son:

- Mayor número de direcciones: El tamaño de una dirección aumenta desde 32 a 128 [bits] lo que se traduce en alrededor de ***3,4 x 10 elevado 38*** direcciones disponibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.

- Direccionamiento jerárquico: Las direcciones IPv6 globales están diseñadas para crear una infraestructura eficiente, jerárquica y resumida de enrutamiento basada en la existencia de diversos niveles de ISP. Esto permite contar con tablas de enrutamiento más pequeñas y manejables.

- Nuevo formato de cabecera: Aún cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado campos que en la práctica eran poco usados, de forma de hacer más eficiente el manejo de los paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.

- Autoconfiguración: IPv6 incorpora un mecanismo de auto configuración de direcciones, "stateless address configuration", mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

[2] DEERING, S; HINDEN R. 1998. Protocolo Internet, Versión 6 (IPv6). [en línea]. disponible en: www.rfc-es.org/rfc/rfc2460-es.txt, [Consulta: 5 noviembre 20110].

- Seguridad: IPv6 incluye soporte nativo para una capa de cifrado de red y autenticación, una característica añadida eventualmente a IPv4 por medio de tecnologías como IPsec.

- Nuevo protocolo para interactuar con vecinos: El protocolo de descubrimiento de vecinos, reemplaza a los protocolos ARP y "Router Discovery" de IPV4. Una de sus mayores ventajas es que elimina la necesidad de los mensajes del tipo "broadcast".

- Calidad y Servicio: IPv6 proporciona un medio para especificar la prioridad de un paquete, lo que conllevará a una reducción de la latencia para el caso del vídeo streaming y otras retransmisiones en tiempo real.

Figura 6.4. *Formato de la cabecera IPv6*

Un paquete IPv6 tiene una cabecera de tamaño fijo e igual a 40 [bytes], el doble de la cabecera IPv4. Este aumento se debe a que el tamaño de los campos "Dirección Origen" y "Dirección Destino" aumentaron su tamaño de 32 a 128 [bits] cada uno.

La cabecera IPv6 posee los siguientes 8 campos:

Versión (Version). Es de 4 bits de largo e identifica la versión del protocolo IP, en este caso es igual a 6.

Clase de tráfico (Traffic class). El campo de 8 bits Clase de Tráfico en la cabecera IPv6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y

distinguir entre las diferentes clases o prioridades de paquetes IPv6. Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

- La interface de servicio para el servicio IPv6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por ese protocolo de capa superior. El valor por defecto debe ser cero para todos los 8 bits.

- Los nodos que soportan un uso (experimental o estándar eventual) específico de algunos o todos los bits Clase de Tráfico se les permite cambiar el valor de esos bits en los paquetes que ellos originan, reenvían, o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar a cualquiera de los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

- Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido son los mimos que el valor enviado por el origen del paquete.

Etiqueta de flujo (Flow Level). El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en "tiempo real".

Un flujo es una secuencia de paquetes enviados a un destino unicast o multicast que necesita manejo especial por los routers ipv6 que intervienen. Todos los paquetes pertenecientes a un mismo flujo debe ser enviado con la misma dirección fuente, dirección destino y etiqueta de flujo. Un ejemplo de un flujo sería paquete que soporta un servicio en tiempo real, como audio o vídeo. Etiqueta de flujo es usado por esa fuente para etiquetar esos paquetes que requieren manejo especial por el nodo ipv6. Si un host o router no soporta funciones de Etiqueta de flujo, el campo es fijado a cero en el origen e ignorado en la recepción.

Longitud de carga útil (Payload length). Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos. Nótese que cualquiera de las cabeceras de extensión presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud.

Cabecera siguiente (Next header). Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4.

Límite de saltos (Hop limit). Entero sin signo de 8 bits. Indica el máximo número de saltos que puede realizar el paquete, decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es decrementado hasta cero.

Dirección origen (Source address). Dirección de 128 bits que identifica el originador del paquete. El formato de este campo es más ampliamente definido en el RFC 2373 (Arquitectura de direccionamiento para la versión 6 del IP).

Dirección destino (Destination address). Dirección de 128 bits que identifica el destinatario que tiene la intención de recibir el paquete. Una importante distinción es la de que el destinatario que tiene la intención de recibir el paquete puede no ser el destinatario final, como la *Cabecera de Enrutamiento* puede ser empleado para especificar la ruta que el paquete toma desde su fuente, a través de destinatario(s) intermedio(s), y así hasta su destinatario final.

6.5. Representación de una dirección IPv6[3].

Las direcciones IPv6 están compuestas de 8 campos de 2 bytes (16 bits) de largo separadas por ":" (dos puntos), cada campo está representado por cuatro caracteres hexadecimales (0-F).

Hay tres formas convencionales de representación de direcciones IPv6 como cadenas de texto:

- La forma preferida es x:x:x:x:x:x:x:x, donde la "x"s son los valores hexadecimales de las ocho campos de 16 bits de la dirección.

Ejemplos:

2001: DB8: 7654:3210: FEDC: BA98: 7654:3210
2001:DB8:0:0:8:800:200C:417A

Tenga en cuenta que no es necesario escribir los ceros a la izquierda en un campo individual, pero debe haber al menos un número en cada campo.

[3]JARA SABA., Felipe Ernesto. 2009. Estudio e Implementación de una Red IPv6 en la UTFSM. (Tesis Ing. Civil Telemático) Valparaíso Chile, Universidad Técnica Federico Santa María. Departamento de Electrónica. 25 p.

- Debido a algunos métodos de asignación de ciertos estilos de direcciones IPv6, que será común para las direcciones que contienen cadenas largas de cero bits. Con el fin de hacer la escritura que contiene las direcciones cero bits más fácil una sintaxis especial está disponible para comprimir los ceros a la izquierda.

El uso de "::" indica múltiples grupos de 16-bits de ceros. El "::" sólo puede aparecer una vez en una dirección. El "::" también puede ser utilizado para comprimir el principal y / o ceros en una dirección.

Ejemplos:

Las siguientes direcciones:

2001*:DB8:0:0:0008:800:200C:417A*	***una dirección unicast***
FF01:0:0:0:0:0:0:101	***una dirección multicast***
0:0:0:0:0:0:0:1	***dirección de loopback***
0:0:0:0:0:0:0:0	***direcciones no especificada***

Podrán estar representados por:

2001:DB8::8:800:200C:417A	***una dirección unicast***
FF01::101	***una dirección multicast***
:: 1	***dirección de loopback***
::	***dirección no especificada***

- Una forma alternativa que a veces es más conveniente cuando se trata con un entorno mixto de nodos IPv4 e IPv6 es x: x: x: x: x: x:d.d.d.d, donde la "x"s son los valores de los seis campos hexadecimales de alto orden de 16-bit de la dirección, y las "d"s son los valores los cuatro campos decimales de bajo orden de 8 bits de la dirección (representación estándar IPv4).

Ejemplos:

Las siguientes direcciones:

0:0:0:0:0:0:192.188.49.2

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

O en forma comprimida:

::192.188.49.2

:: FFFF:129.144.52.38

Con el fin de simplificar la escritura y memorización de direcciones, se pueden aplicar las siguientes reglas a las direcciones IPv6:

- No se hace distinción entre mayúsculas y minúsculas. "ABC9" es equivalente a "abc9".
- Tal como en el caso de IPv4, para señalar las secciones de la dirección que identifican a la red y al dispositivo, se utiliza el formato CIDR (Encaminamiento Inter-Dominios sin Clases) en la forma ***<dirección>/<prefijo>***. Por ejemplo, una dirección en la forma ***2001:DB8:c18:1::1/64*** señala que los primeros 64 [bit] identifican a la red (***2001:DB8:c18:1***) y los restantes 64[bit] identifican al dispositivo de dicha red (***::1***).
- Tradicionalmente el uso del símbolo ":" en las dirección IPv4 señala un puerto en un determinado nodo, por ejemplo ***192.168.1.1:80*** señala al puerto 80 (***www***) del nodo ***192.168.1.1***. Esto representa un problema de incompatibilidad al utilizar direcciones IPv6, por lo que se ha establecido que para señalar un puerto en una determinada dirección IPv6, esta debe estar encerrada por paréntesis cuadrados en la forma ***[dirección]:puerto***.

6.6. Representación de los prefijos de las direcciones.

La representación de los prefijos de dirección IPv6 es similar a los prefijos de direcciones IPv4 que están escritos en notación CIDR. Un prefijo de dirección IPv6 se representa con la siguiente notación:

Dirección-ipv6/longitud-prefijo

- ***direccion-ipv6***: Es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.
- ***longitud-prefijo*****:** Es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

Ejemplo:

Las siguientes son representaciones legales de prefijos de 60 bits *2001DB8000000CD30* (hexadecimal):

- *2001: DB8:0000:CD30:0000:0000:0000:0000 / 60*
- *2001:DB8::CD30:0:0:0:0 / 60*
- *2001:DB8:0:CD30:: / 60*

Las siguientes no son representaciones legales de las anteriores prefijo:

- ***2001:DB8:0:CD3 / 60*** - Puede caer ceros a la izquierda, pero no ceros, dentro de cualquier parte de 16 bits de la dirección
- ***2001:DB8::CD30 / 60*** - Dirección a la izquierda de "/" se amplía a *2001:DB8:0000:0000:0000:0000:0000:CD30*
- ***2001::CD3 / 60*** Dirección a la izquierda de "/" se amplía a 2001*:0000:0000:0000:0000:000:0000:0CD3*

Al escribir tanto una dirección de nodo y un prefijo de la dirección de nodo que (Por ejemplo, el nodo del prefijo de subred), los dos pueden combinarse como sigue:

- La dirección del nodo 2001:DB8:0:CD30:123:4567:89AB:CDEF
- Y su número subred 2001:DB8:0:CD30:: / 60
- Puede ser abreviada como 2001:DB8:0:CD30:123:4567:89AB:CDEF / 60

6.7. Modelos de direccionamiento IPv6[4].

Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante que no haya que olvidar. Todas las interfaces han de tener, por los menos, una dirección de enlace local (Link -Local) de tipo unicast. Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope).

Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

6.7.1. Unicast. Identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.

[4]LACNIC. Portal IPv6. [en línea]. disponible en: http://portalipv6.lacnic.net, [Consulta: 22 noviembre 2010].

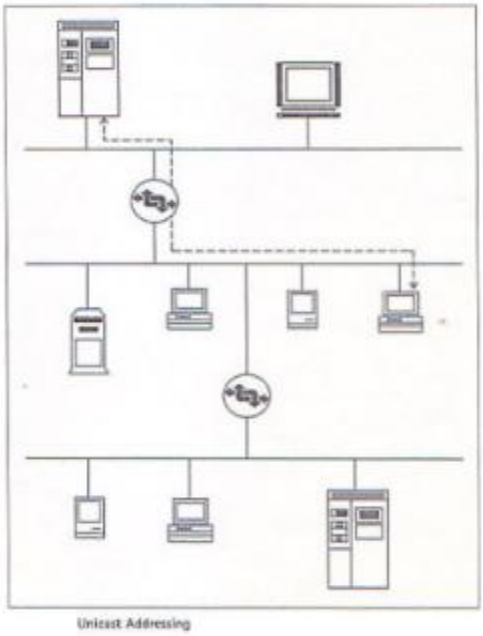


Figura 6.7.1. *Dirección IPv6 Unicast*

6.7.2. Anycast. Identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast (la más cercana, según la medida de distancia del protocolo de ruteo).

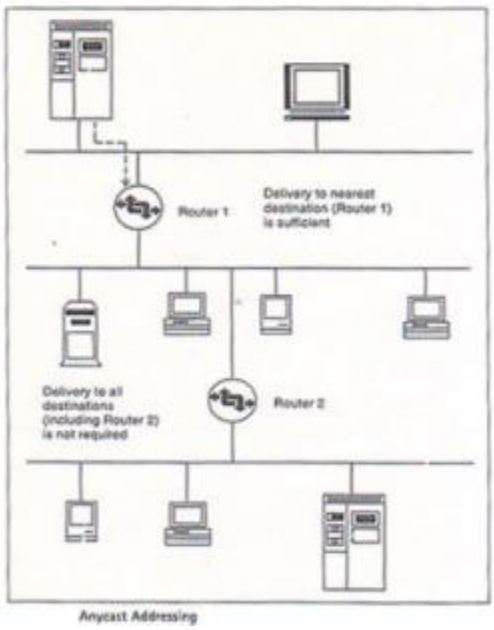


Figura 6.7.2. *Dirección IPv6 Anycast*

6.7.3. Multicast. Identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.

Note que el término difusión (broadcast) no aparece, porque la función de difusión es reemplazada por la definición de multicast. También note que las direcciones de IPv6 de todo tipo son asignadas a interfaces, no nodos; un nodo (como un router) puede tener múltiples interfaces, y así múltiples direcciones unicast. Además, una interfase simple puede estar asignada a múltiples direcciones.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

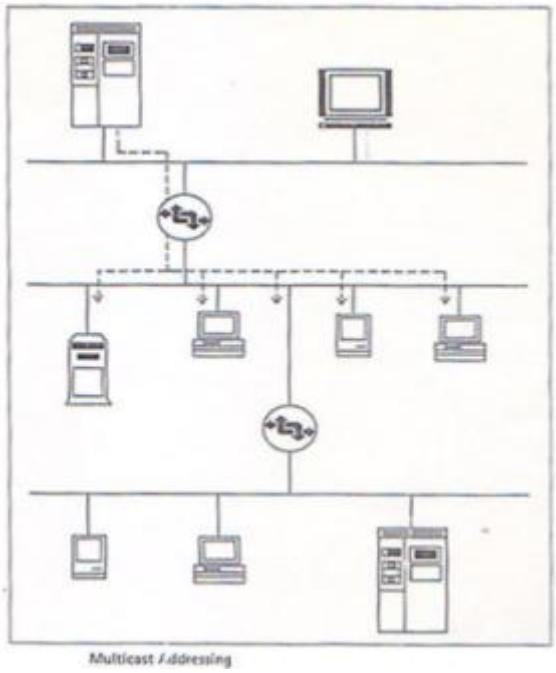


Figura 6.7.3. *Dirección IPv6 Multicast*

6.8. Ámbito de direcciones unicast.

El protocolo IPv6 añade soporte para direcciones de distintos ámbitos, lo que quiere decir que tendremos direcciones globales y no globales. Si bien con IPv4 ya habíamos empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.

Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador único de uno o varias interfaces. El ámbito de cada dirección forma parte de la misma dirección, con lo que vamos a poder diferenciarlos a simple vista. Para las direcciones unicast distinguimos tres ámbitos:

6.8.1. ***Direcciones unicast enlace local (link-local)***[5], que se utilizan entre vecinos en vínculo y en procesos de descubrimiento de vecinos.

Los nodos utilizan direcciones de enlace-local, que se identifican mediante el prefijo de formato ***1111 1110 10*** e incluye un campo Inteface ID de 64 bits y empiezan todas por ***fe80:***, el prefijo de la direcciones de enlace-local siempre es ***FE80::/64***. Es necesaria una dirección de enlace-local para los procesos de descubrimiento de vecinos y siempre se configura automáticamente, incluso si no hay ninguna otra dirección de unidifusión. Los routers nunca reenvían paquetes con la dirección destino u origen de enlace local hacia otras direcciones de enlace. La estructura de una dirección enlace-local es "***fe80:0:0:0:<identificador de interfaz***>". El identificador de interfaz se genera automáticamente a partir de su dirección MAC (IEEE 802), siguiendo el formato IEEE EUI-64.

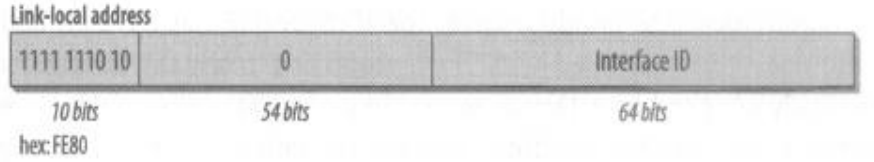


Figura 6.8.1. *Direcciones unicast enlace local*

Nota: *Las direcciones de enlace-local equivalen a las direcciones IPv4 de Direccionamiento IP privado, que utilizan el prefijo* ***169.254.0.0/16****.*

6.8.2. ***Direcciones unicast de sitio local (site-local)***[6], que se utilizan entre nodos que se comunican con otros nodos del mismo sitio.

Para identificar interfaces en un mismo ***sitio-local***. La definición de ***sitio-local*** es un tanto genérica, pero en principio un sitio-local es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Las direcciones de sitio-local no son accesibles desde otros sitios y los enrutadores no deben reenviar tráfico local del sitio

[5] HAGAN, Silvia. 2002. IPv6 Essentials, United States of America
[6] HAGAN, Silvia. 2002. IPv6 Essentials, United States of America

fuera del sitio. Las direcciones de sitio-local se pueden utilizar al mismo tiempo que las direcciones globales unidifusión. Esta dirección comienza con el formato de prefijo ***1111 1110 11***, *l*os primeros 48 bits siempre son fijos en las direcciones locales del sitio y comienzan por ***FEC0::/48***. A continuación de los 48 bits fijos hay un identificador de subred de 16 bits (campo Id. de subred) que proporciona 16 bits con los que se pueden crear subredes en la organización. Al disponer de 16 bits, puede haber hasta 65.536 subredes en una estructura de subredes plana o se pueden subdividir los bits de orden superior del campo Id. De subred para crear una infraestructura de enrutamiento jerárquica y agregable. Después del campo Id. De subred está el campo Id. De interfaz de 64 bits que identifica una interfaz específica de una subred.

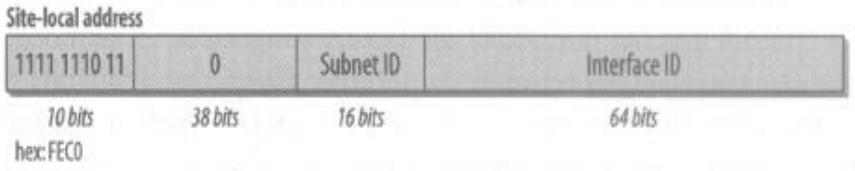


Figura 6.8.2. *Direcciones unicast de sitio local*

Nota: *Las direcciones de sitio-local equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16).*

6.8.3. ***Direcciones unicast globales***[7], para identificar interfaces en todo Internet. Éstas comienzan por ***2001:***. Son el único tipo de direcciones que pueden ser enrutadas a través de Internet. El espacio reservado actualmente para este tipo de direcciones es de ***2001:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001:: /3)***.

Como su nombre indica, las direcciones globales unicast están diseñadas para agregarse o resumirse de forma que produzcan una infraestructura de enrutamiento eficaz. A diferencia de la red Internet actual basada en IPv4, que tiene una mezcla de enrutamiento plano y jerárquico, la red Internet basada en IPv6 se ha diseñado desde la base para admitir direccionamiento y enrutamiento jerárquico eficaz. El ámbito (que es la región del conjunto de redes IPv6 donde la dirección es única) de una dirección global agregable de unidifusión es la red Internet IPv6 completa.

[7] HINDEN, R; DEERING S. 2003. Internet Protocol Version 6 (IPv6) Addressing Architecture. [en línea]. disponible en: www.ietf.org/rfc/rfc3513.txt, [Consulta: 4 noviembre 2010].

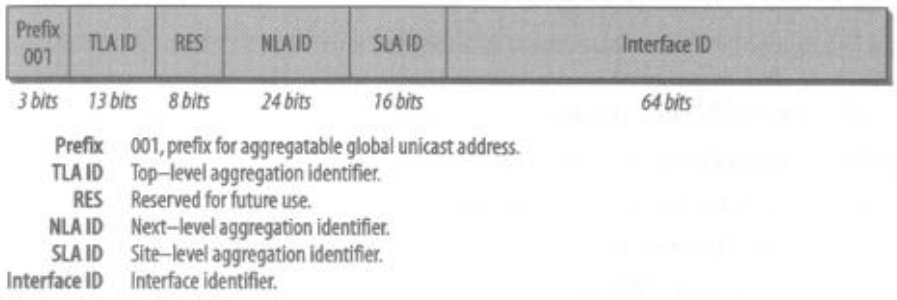


Figura 6.8.3. *Direcciones unicast globales A*

Los campos de una dirección global agregable de unidifusión se describen de la manera siguiente:

- ***Formato 001.*** Prefijo (3 bits) para Aggregatable Global Direcciones Unicast.
- ***TLA ID.*** Indica el Id. de agregación de nivel superior (TLA ID, Level Aggregation Identifier ID) de la dirección. El tamaño de este campo es de 13 bits. TLA identifica el nivel superior en la jerarquía de enrutamiento. Los TLA son administrados por IANA y se asignan a los registros de Internet locales que, a su vez, asignan Id. de TLA individuales a grandes proveedores de servicios Internet (ISP) globales. Un campo de 13 bits permite hasta 8.192 Id. de TLA diferentes. Los enrutadores del nivel superior de la jerarquía de enrutamiento en la red Internet IPv6 (llamados enrutadores libres predeterminados) no tienen una ruta predeterminada, sino rutas con prefijos de 16 bits que corresponden a los TLA asignados.
- ***RES***. Está reservado para su uso futuro en la ampliación del tamaño del Id. de TLA o el Id. de NLA. El tamaño de este campo es de 8 bits.
- ***NLA ID.*** Indica el identificador de agregación de siguiente nivel (NLA ID, Next Level Aggregation ID) de la dirección. El campo Id. de NLA se utiliza para identificar un sitio cliente específico. El tamaño de este campo es de 24 bits. El campo Id. de NLA permite que un ISP cree múltiples niveles de jerarquía de direcciones para organizar el direccionamiento y enrutamiento, así como para identificar sitios. Los enrutadores libres predeterminados no pueden ver la estructura de la red del ISP.
- ***SLA ID.*** Indica el Id. de agregación de nivel de sitio (SLA ID, Site Level Aggregation ID) de la dirección. El campo Id. de SLA sirve para que se identifiquen subredes en el sitio de una organización individual. El tamaño de este campo es de 16 bits. La organización puede utilizar los 16 bits correspondientes a su sitio para crear 65.536 subredes o múltiples niveles de jerarquía de direcciones y una infraestructura de enrutamiento eficaz. Con la flexibilidad de 16 bits para la creación de subredes, un

prefijo global agregable de unidifusión asignado a una organización equivale a asignar a la organización un Id. de red IPv4 de Clase A (siempre y cuando el último octeto se utilice para identificar los nodos en las subredes). El ISP no puede ver la estructura de la red del cliente.

- ***Interface ID.*** Indica la interfaz de un nodo en una subred determinada. El tamaño de este campo es de 64 bits.

En la ilustración siguiente se muestra cómo los campos de la dirección global agregable de unidifusión crean una estructura de topología con tres niveles.

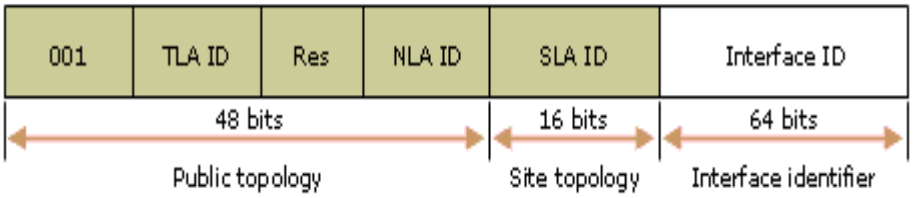


Figura 6.8.3. *Dirección global con tres niveles B*

La topología pública es la colección de grandes y pequeños ISP que proporcionan acceso a la red Internet IPv6. La topología del sitio es la colección de subredes del sitio de una organización. El identificador de interfaz identifica una interfaz específica en una subred del sitio de una organización. Para obtener más información acerca de las direcciones globales agregables de unidifusión, consulte el documento RFC 2374, "An IPv6 Aggregatable Global Unicast Address Format" (Formato de dirección global agregable de unidifusión de IPv6).

Una de las grandes ventajas de los ámbitos es que permitiría la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrían. Tenemos que esperar que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como hemos dicho antes, se trataría siempre que sea posible de mantener las tablas de mayor e invalidando el anterior, porque lo que seguramente sucedería sería que las redes contiguas ya estén asignadas.

Nota: *Las direcciones unicast globales, equivalen a las direcciones públicas IPv4.*

6.9. Direcciones Especiales.

Las siguientes son direcciones IPv6 especiales:

- ***Dirección no especificada.*** La dirección no especificada (***0:0:0:0:0:0:0:0*** *ó* ***::***) sólo se utiliza para indicar la ausencia de dirección. La dirección no especificada se suele utilizar como dirección de origen en paquetes que intentan comprobar la exclusividad de una dirección tentativa. La dirección no especificada nunca se asigna a una interfaz ni se utiliza como dirección de destino.

Nota: *Equivale a la dirección IPv4 no especificada de 0.0.0.0.*

- ***Dirección de bucle de retroceso (loopback).*** La dirección de bucle de retroceso (***0:0:0:0:0:0:0:1 ó ::1***) sirve para identificar una interfaz de bucle de retroceso, lo que permite que un nodo se envíe paquetes a sí mismo, puede ser utilizada por un nodo para enviar un paquete IPv6 a sí mismo. Los paquetes dirigidos a la dirección de bucle de retroceso nunca se envían en un vínculo ni se reenvían mediante un enrutador IPv6.

Nota: *Equivale a la dirección IPv4 de bucle de retroceso de 127.0.0.1.*

6.10. Direcciones IPv6 compatibles con direcciones IPv4.

Para facilitar la migración de IPv4 a IPv6 y la coexistencia de ambos tipos de hosts, se han definido las direcciones siguientes:

6.10.1. ***Dirección compatible con IPv4.*** La dirección compatible con IPv4, ***0:0:0:0:0:0:*****w.x.y.z** o ***::*****w.x.y.z** (donde **w.x.y.z** es la representación decimal con puntos de una dirección IPv4 pública), la utilizan los nodos de pila dual que se comunican con IPv6 a través de una infraestructura IPv4. Los nodos de pila dual son nodos con protocolos IPv4 e IPv6. Cuando la dirección compatible con IPv4 se utiliza como destino IPv6, el tráfico IPv6 se encapsula de forma automática con un encabezado IPv4 y se envía al destino mediante la infraestructura IPv4.

```
|              80 bits                    |  16  |    32 bits     |
+-----------------------------------------+------ ----------------+
| 0000 ............................ 0000 | 0000 | IPv4 dirección |
+-----------------------------------------+----+----- ----------------+
```

Figura 6.10.1. *Dirección compatible con IPv4*

6.10.2. ***Dirección asignada a IPv4.*** La dirección asignada a IPv4, ***0:0:0:0:0:FFFF:*****w.x.y.z** o ***::FFFF:*****w.x.y.z** se utiliza para representar un nodo exclusivo de IPv4 ante un nodo IPv6. Sólo sirve para la representación interna. La dirección asignada a IPv4 nunca se

utiliza como dirección de origen o destino de un paquete IPv6. El protocolo IPv6 no admite el uso de direcciones asignadas a IPv4.

```
|              80 bits                  |  16  |     32 bits    |
+-------------------------------------+---------- ---------------+
| 0000 ............................ 0000 | FFFF | dirección IPv4 |
+-------------------------------------+----+----- ---------------+
```

Figura 6.10.2. *Dirección asignada a IPv4*

6.11. Identificadores de interfaz de IPv6.

Los últimos 64 bits de una dirección IPv6 corresponden al identificador de la interfaz, que es único para el prefijo de 64 bits de la dirección IPv6. Las formas de determinar un identificador de interfaz son las siguientes:

6.11.1. Identificadores de interfaz basados en direcciones EUI-64.

El Institute of Electrical and Electronic Engineers (IEEE) define la dirección EUI-64 de 64 bits. Las direcciones EUI-64 se asignan a un adaptador de red o se derivan de las direcciones IEEE 802.

6.12. Direcciones IEEE EUI-64.

La dirección IEEE EUI-64 representa un nuevo estándar para el direccionamiento de interfaces de red. El Id. De compañía sigue teniendo 24 bits de longitud, pero el Id. De extensión tiene 40 bits, por lo que se crea un espacio de direcciones mucho mayor para los fabricantes de adaptadores de red. La dirección EUI-64 utiliza los bits U/L e I/G de la misma forma que la dirección IEEE 802.

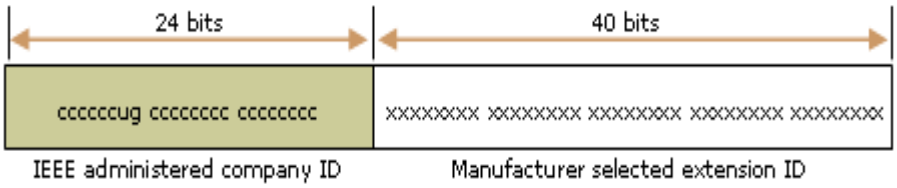


Figura 6.12. *Direcciones IEEE EUI-64.*

6.12.1. Direcciones IEEE 802.

Los identificadores de interfaz tradicionales para los adaptadores de red utilizan una dirección de 48 bits que se llama dirección IEEE 802. Esta dirección consta de un Id de compañía (también llamado Id. de fabricante) de 24 bits y un Id de extensión (también llamado Id. de

tarjeta) de 24 bits. La combinación del Id de compañía, que se asigna de forma única a cada fabricante de adaptadores de red, y el Id de tarjeta, que se asigna de forma única a cada adaptador de red en el momento del ensamblaje, genera una dirección única global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, Media Access Control).

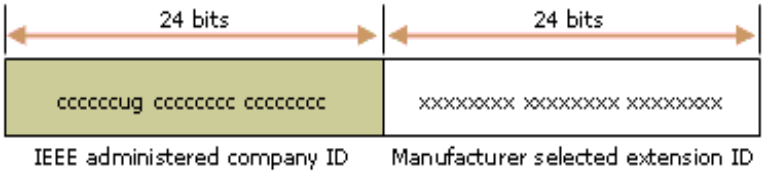


Figura 6.12.1. *Direcciones IEEE 802*

Los bits definidos en la dirección IEEE 802 son los siguientes:

- ***Universal o local (U/L).*** El bit U/L es el séptimo bit del primer byte y se utiliza para determinar si la dirección se administra de forma universal o local. Si el bit U/L está establecido en 0, la administración de la dirección corresponde a IEEE, mediante la designación de un Id. de compañía único. Si el bit U/L está establecido en 1, la dirección se administra de forma local. El administrador de la red ha suplantado la dirección de fábrica y ha especificado una dirección distinta.
- ***Individual o grupo (I/G).*** El bit I/G es el bit de orden inferior del primer byte y se utiliza para determinar si la dirección es individual (unidifusión) o de grupo (multidifusión). Si está establecido en 0, la dirección es de unidifusión. Si está establecido en 1, la dirección es de multidifusión.

En una dirección típica de adaptador de red 802.x, los bits U/L e I/G están establecidos en ***0***, lo que corresponde a una dirección MAC de unidifusión administrada de forma universal.

6.12.2. Asignación de direcciones IEEE 802 a direcciones EUI-64.

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id de compañía y el Id de extensión. En la siguiente ilustración se muestra la conversión de una dirección IEEE 802 en una dirección EUI-64.

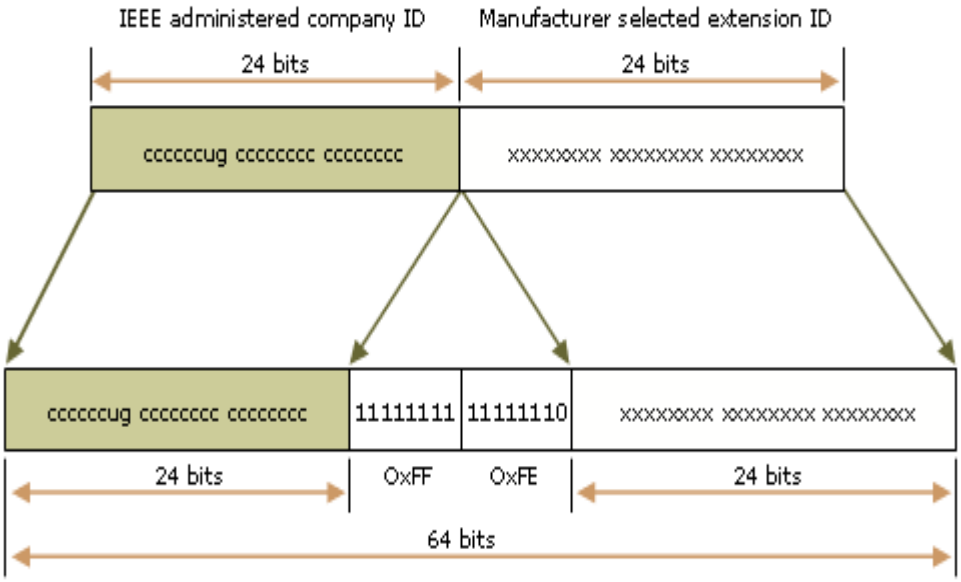


Figura 6.12.2. *Asignación de direcciones IEEE 802 a direcciones EUI-64.*

6.12.3. Asignación de direcciones EUI-64 a identificadores de interfaz IPv6.

Para obtener el identificador de interfaz de 64 bits para las direcciones IPv6 de unidifusión, se complementa el bit U/L de la dirección EUI-64 (si es 1, se establece en 0; y si es 0, se establece en 1). En la ilustración siguiente se muestra la conversión de una dirección EUI-64 de unidifusión administrada de forma universal.

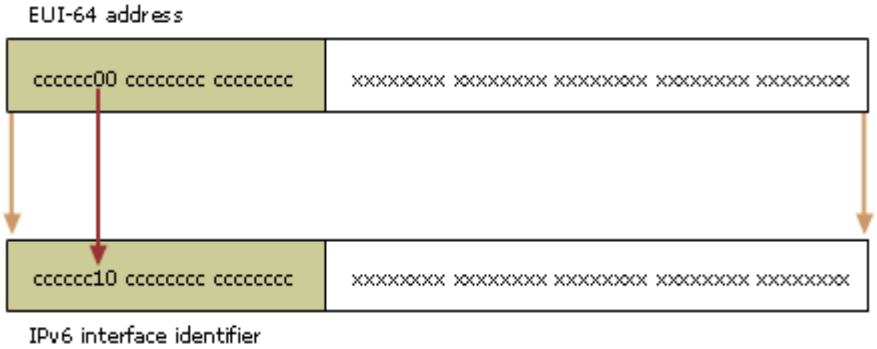


Figura 6.12.3. *Conversión de una dirección EUI-64 de unidifusión administrada de forma universal A.*

Para obtener un identificador de interfaz IPv6 a partir de una dirección IEEE 802, primero se debe asignar la dirección IEEE 802 a una dirección EUI-64 y, después, complementar el bit U/L. En la ilustración siguiente se muestra el proceso de conversión de una dirección IEEE 802 de unidifusión administrada de forma universal.

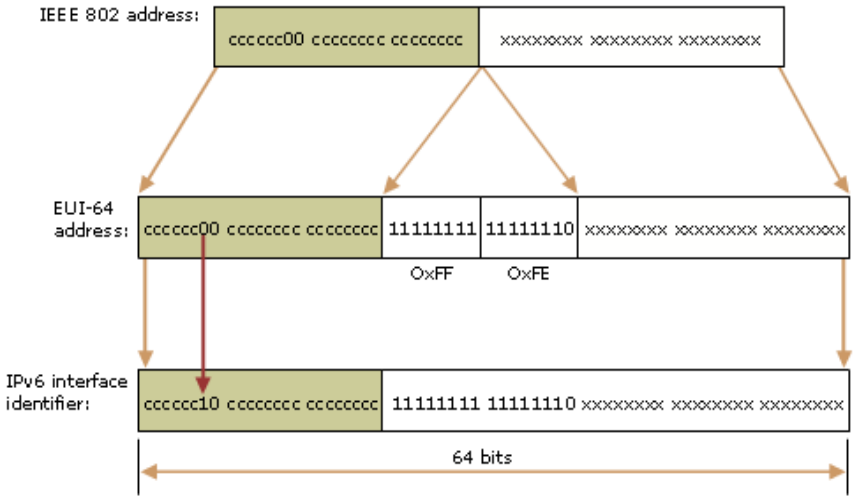


Figura 6.12.3. *Conversión de una dirección IEEE 802 de unidifusión administrada de forma universal B.*

Ejemplo de conversión de una dirección IEEE 802.

El host A tiene la dirección MAC de Ethernet de *00-AA-00-3F-2A-1C*. Primero, se convierte al formato EUI-64 insertando *FF-FE* entre el tercer y cuarto bytes, con el resultado de *00-AA-00-FF-FE-3F-2A-1C*. Después, se complementa el bit U/L, que es el séptimo bit del primer byte. El primer byte en formato binario es *00000000*. Al complementar el séptimo bit, se convierte en *00000010* (0x02). El resultado final es 02-*AA-00-FF-FE-3F-2A-1C* que, cuando se convierte a notación hexadecimal con dos puntos, da como resultado el identificador de interfaz *2AA:FF:FE3F:2A1C*. En consecuencia, la dirección local del vínculo correspondiente al adaptador de red que tiene la dirección MAC de *00-AA-00-3F-2A-1C* es *FE80::2AA:FF:FE3F:2A1C*.

Nota: *Al complementar el bit U/L, se debe sumar 0x2 al primer byte si la dirección EUI-64 se administra de forma universal, y restar 0x2 del primer byte si la dirección EUI-64 se administra de forma local.*

7. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN

7.1. Análisis de la Infraestructura en la Red de Datos de la Universidad Nacional de Loja.

La Universidad Nacional de Loja, ha ido creciendo en los últimos años, buscando mejorar toda su infraestructura, tanto física como tecnológica, eso ha permitido mantener latente la posibilidad de estar siempre a la par de los diferentes avances que se dan en el mundo informático.

Actualmente la institución, cuenta con la Unidad de Telecomunicaciones e Información la cual se compone de cuatro secciones, una de ellas es Redes y Equipos Informáticos, desde donde se llevan a cabo métodos y técnicas para mantener la infraestructura de la red de datos 100% activa y funcional para la transmisión de datos, voz y video, así mismo se dan directrices para mejorar la conectividad entre los diferentes dispositivos de networking y equipos finales; teniendo en cuenta que es función principal velar por la seguridad de la red de datos.

7.1.1. Proveedor de servicios de Internet

El proveedor de servicios de Internet (ISP) es la empresa Telconet S.A que garantiza a la institución la conexión con la red de redes tanto para el uso de Internet, como para que la Universidad Nacional de Loja brinde sus servicios de forma eficaz y eficiente. Actualmente la institución cuenta con un ancho de banda de 80 Mbps.

Backbone Universidad Nacional de Loja

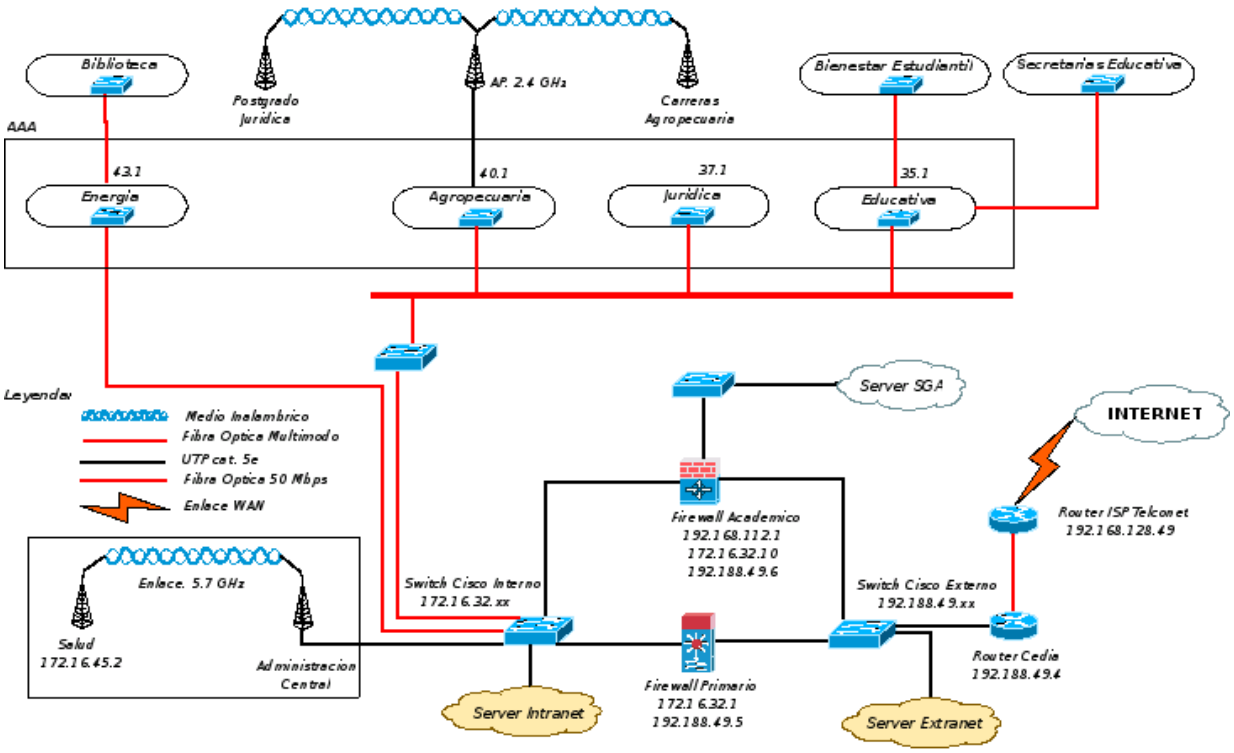


Figura 7.1.1. *Backbone Universidad Nacional de Loja.*

Se muestra el backbone de la infraestructura de la red de datos, en donde se visualizan las principales conexiones troncales tanto de la intranet como extranet y está compuesta de un gran número de switches interconectados que llevan los datos a través de las diferentes dependencias, usando como medio de transmisión fibra óptica, cable UTP cat. 5e, ondas electromagnéticas, etc.

La red de datos se compone de la interconexión de los bloques de Administración Central (bloque 1 y bloque 2) con las Áreas Académico Administrativas (AAA).

En los bloques de Administración Central la red de datos se compone de un "backbone" que utiliza como medio de transmisión fibra óptica multimodo (que comunica las AAA: Educativa, Jurídica, Agropecuaria y Energía) y dispositivos de networking activos para la comunicaciones, principalmente orientado al uso del estándar Fast Ethernet (normas 100Base TX y 100BaseFX) y Gigabit Ethernet (1000Mbps). Este detalle es muy importante, ya que es la columna vertebral de todas las comunicaciones dentro de la institución, como se puede

observar en la figura 7.1.1. Backbone Universidad Nacional de Loja.

Permitiendo de esta manera hacer uso de los diferentes servicios de red que la Universidad Nacional de Loja brinda a cada una de sus dependencias, como son: Internet, Sistema de Gestión Académico, Sistema Financiero, Acceso Inalámbrico, Correo Electrónico, Videoconferencias, etc.

7.1.2. Dispositivos de Networking Cuarto de Telecomunicaciones

Los dispositivos de networking (router, switch, tranceiver, etc) con los que cuenta la institución facilitan la interconexión en todo el campus y permiten mantener una comunicación garantizada con los equipos finales (pc, pda, laptop, impresora, cámara web, etc). Así mismo los servidores, en donde la mayoría son equipos de escritorio y son adaptados a brindar algún servicio de Internet (dns, dhcp, email, proxy, etc), es decir el hardware no cumple con los requisitos necesarios que estipula un servidor. Estos equipos permiten brindar de la mejor manera un servicio eficiente.

7.1.3. Diagrama de topología intranet universitaria

A continuación se ilustra el diagrama de topología, en donde se encuentran los enlaces principales y dispositivos de networking para la comunicación en la red de datos del campus universitario.

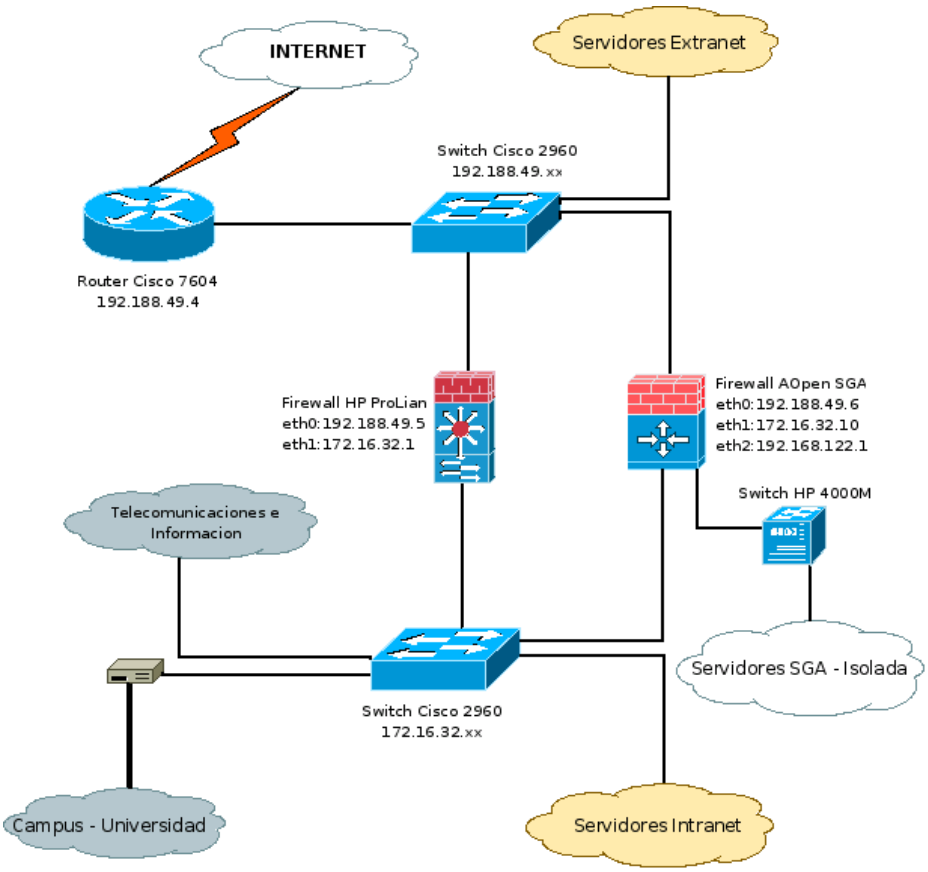


Figura 7.1.3. *Dispositivos de Networking Principales.*

Como se puede visualizar en el diagrama de topología los dispositivos de networking activos principales son: Router cisco 7604, switch cisco 2960 externo, switch cisco 2960 interno, switch hp 4000M, firewall Aopen SGA y firewall Hp ProLiant; detallaremos a continuación la función que cumplen cada uno de ellos.

7.1.4. Descripción dispositivos de networking principales

- ***Router Cisco 7604.*** Dispone de una dirección IP pública (192.188.49.4/24), éste ruteador facilita la interconexión de las diferentes redes con las que cuenta la institución determinando cual es la mejor ruta que deben tomar los paquetes para llegar a su destino. Así mismo permite acceder a Internet comercial e Internet2 que brinda el CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) organización de la cual es miembro la Universidad Nacional de Loja. El ISP Telconet S.A emplea un enlace de fibra óptica multimodo el cual llega hasta el router que se encuentra en el cuarto de telecomunicaciones ubicado en la Unidad de Telecomunicaciones e Información.

- ***Switch Cisco 2960 externo.*** Se ha configurado una dirección IPv4 pública (192.188.49.15/24) para su administración, este dispositivo opera en la capa 2 del modelo OSI el cual facilita la interconexión de dos o más segmentos de red. Una de las interfaces Fast Ethernet 1000 Mbps se encuentra conectado al router cisco 7604, así mismo los puertos 10/100 Mbps establecen una conexión con los servidores públicos (firewall, web, cursos, Med, Sga, videoconferencia, etc).

- ***Switch Cisco 2960 interno.*** Tiene una dirección IP privada (172.16.32.21/19) para realizar la administración, este dispositivo funciona en la capa 2 del modelo OSI y opera con direcciones MAC para el envío de tramas en la red. Una de la interfaces Fast Ethernet 10/100 Mbps principales establece una conexión directa con el firewall HP ProLiant para facilitar el acceso a los servidores públicos e Internet, así mismo algunos de los puertos permite la conexión de los diferentes servicios de Internet (dns, dhcp, email, proxy, sga, quipux, VoIP, etc) y facilita también la comunicación con la diferentes Áreas académico administrativas.

- ***Switch HP 4000M SGA.*** Este dispositivo opera en la capa 2 del modelo OSI, una de la interfaces establece una conexión directa con el firewall AOpen SGA que facilita la comunicación con la intranet, servidores públicos de la Universidad respectivamente e Internet, los servidores del Sistema de Gestión Académico se interconectan por medio de este switch para brindar algún tipo de servicio a la comunidad universitaria y sociedad en general.

- ***Firewall Aopen SGA.*** Este equipo es un balanceador de carga que permite discriminar las conexiones hacia los servidores de trabajo (workers), lo hemos dividido en tres capas (por eso el uso de 3 interfaces de red para isolarlas):

Capa pública. En esta capa se controla un firewall básico que permite servir contenido http y https controlado por el balanceador de carga, aquí el balanceador se comporta como un regulador que regula y dosifica los request (solicitudes) hacia los workers que sirven contenido público, dispone de la dirección IP pública 192.188.49.6/19.

Capa privada. Esta capa permite el acceso controlado de IPs en el rango 172.16.32.0/19 para servicios de intranet, una vez más el balanceador de carga discrimina el acceso a servicios

privados del SGA pero tomando en cuenta el dominio como si se tratase de un virtual server, esto nos permite disponer de muchos dominios en el mismo IP.

Capa isolada. Esta capa permite la conexión hacia la granja de servidores, de esta forma solo recursos con rutas explícitas podrán acceder a la red de servidores, cuyo direccionamiento está en la red IP 192.168.112.0/24.

Aparte de esta división, también existe un cliente VPN usando IPsec para conectarse a recursos del Banco de Loja, este servidor gestiona el tunel de conexión para permitir el acceso de un solo equipo (por políticas del Banco de Loja) hacia la red privada y a un solo servicio con protocolo SOAP.

- ***Firewall HP ProLiant.*** Este dispositivo (router-firewall) dispone de dos direcciones de red, una pública (192.188.49.5/24) y otra privada (172.16.32.1/19) en la cual cada una de sus interfaces Fast Ethernet 10/100 se encuentra conectado a los switch cisco 2960 intranet y externo respectivamente. En el firewall se maneja la configuración de NAT la cual permite que los equipos con direcciones privadas IP compartan una dirección IP enrutable (IP pública), políticas de seguridad (iptables), enrutamiento hacia el exterior de la red y VPN (red privada virtual).

En conjunto dichos equipos de networking componen el núcleo principal de la infraestructura de la red de datos de la institución.

En la siguiente tabla se presenta un resumen de los resultados obtenidos al revisar los dispositivos de networking existentes en el cuarto de telecomunicaciones.

TABLA 7.1.4: DISPOSITIVOS DE NETWORKING ADMINISTRACIÓN CENTRAL			
#	***Dispositivo***	***Marca / Modelo***	***Puertos***
1	Router de Borde	Cisco 7604 ws-sup32-ge-3b	8port Gigabit/Ethernet – 1port 100/1000Mbps
2	Switch Público	Catalyst 2960 Series ws-c2960-24TT-LV02	24port 100Mbps 2port 1000Mbps
3	Switch Privado	Catalyst 2960 Series ws-c2960-24TT-LV02	24port 100Mbps 2port 1000Mbps
4	Switch Interno	3com 3300 - 3c16980A	24port 100Mbps
5	Switch Interno	Dlink DES-3624i	20port 10/100Mbps

6	Switch Interno	Dlink DES-3624	22port 10/100Mbps
7	Switch Interno	Dlink DSS/-4	24port 10/100Mbps
8	Switch SGA	HP ProCurre 4000M HP J4121A	64port 10/100Mbps – 1port 100/1000Mbps – 1port Gigabit SX.
9	Router SDSL	Cisco 673	3port ENET, MGMT y WALL
10	Transceiver	Dlink 300 SC	10/100 Base-Tx / 100 Base-Fx
11	Transceiver	Dlink DFE 855	100 Base-Tx to 100 Base-Fx
12	Transceiver	Dlink DMC 700SC	1000 Base-T / 1000 Base-SX
13	Transceiver	Dlink 300 SC	10/100 Base-Tx / 100 Base-Fx
14	Transceiver	Dlink DFE 855	100 Base-Tx to 100 Base-Fx
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*			

7.1.5. Diagrama de topología servidores públicos

A continuación se ilustra un diagrama de topología en la infraestructura de la red de datos con algunos de los servidores públicos principales de la institución.

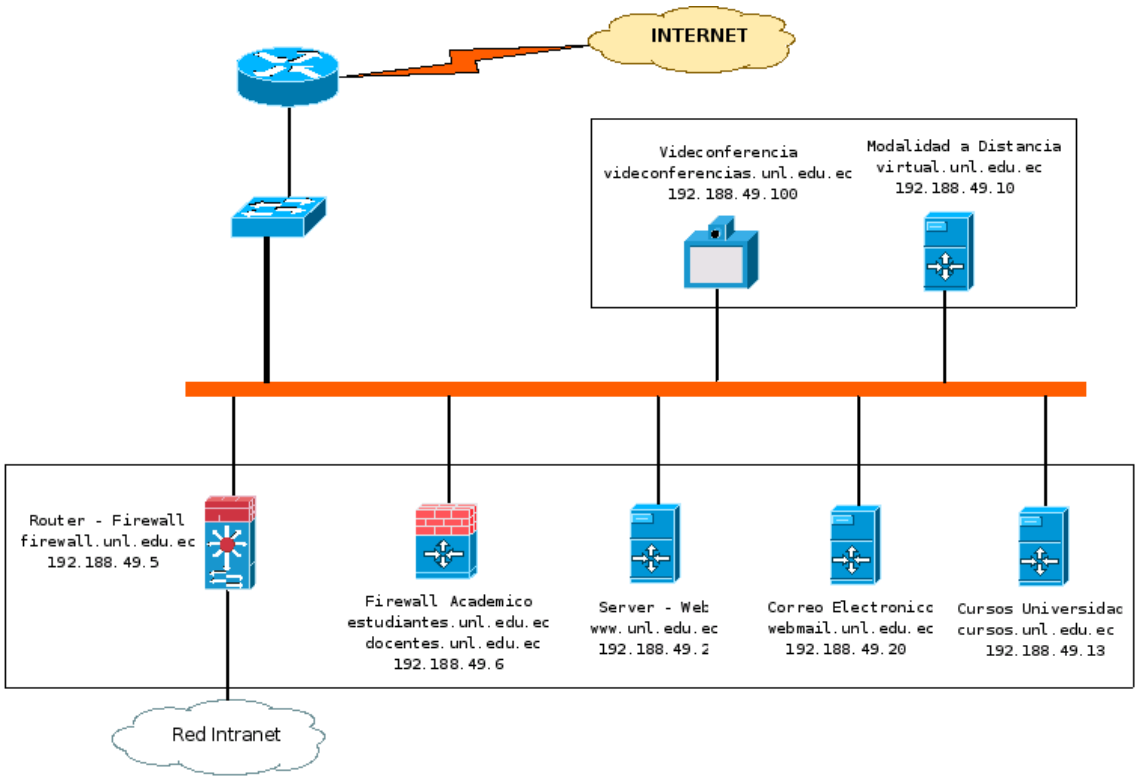


Figura 7.1.5. *Servidores públicos de la Universidad.*

En el diagrama de topología se puede visualizar los diferentes servidores públicos interconectados a través de un switch cisco 2960, aquí se ubican servidores que son necesarios

ser accedidos tanto desde afuera (red de redes) como desde la intranet universitaria, entre los servidores públicos que se encuentran implementados y en producción correo electrónico, web, sistema académico, videoconferencia, modalidad a distancia, etc.

7.1.6. Descripción de servidores públicos de la Universidad Nacional de Loja.

Seguidamente se presenta un resumen de los resultados obtenidos al visitar el cuarto de telecomunicaciones en donde se encuentran los servidores públicos.

Correo electrónico. La institución brinda el servicio de correo electrónico a un número limitado de funcionarios de las diferentes dependencias y Áreas Académico Administrativas (AAA). Este servicio de red permite a los usuarios enviar y recibir mensajes electrónicos rápidamente, así también como anexar documentos digitales para tener una comunicación fiable, lo cual permite cumplir las actividades de manera satisfactoria.

Servidor web. La principal función de este servidor es brindar al mundo entero la vida digital de la Universidad por medio de aplicaciones web dinámicas, blogs, cursos, etc. En las cuales se podrá encontrar acceso a información digital de las diferentes dependencias y AAA, facilitando de esta manera la participación e interacción de los visitantes a dichas páginas.

Sistema académico. Actualmente existe todo un cluster de servidores que cumplen la función de brindar un Sistema de Gestión Académico (SGA) de alto rendimiento y alta disponibilidad acorde a los requerimientos institucionales. Logrando de esta manera automatizar los procesos académicos que antes se venían desarrollando de forma manual. El servicio público del SGA está disponible para estudiantes y docentes.

Videoconferencia. La Universidad Nacional de Loja cuenta con la infraestructura necesaria para llevar a cabo videoconferencias de forma bidireccional simultáneamente de audio, video y contenido, permitiendo mantener reuniones con otras universidades nacionales e internacionales, presentación de conferencias a otros lugares del mundo y asistir a eventos que se desarrollen en otras ciudades y países.

Modalidad a distancia. Los servidores con los que cuenta la Modalidad de Estudios a Distancia (MED) permiten brindar una educación a distancia virtualizada a través de canales electrónicos, utilizando para ello plataformas de e-learning (moodle) las cuales incorporan

aplicaciones: Foros de discusión, blog personales, mensajería instantánea, etc.

En la siguiente tabla se detalla el hardware existente en donde se encuentran funcionando los diferentes servicios de Internet en la red de datos pública de la Universidad Nacional de Loja, aquí se consideran los servidores de mayor prioridad.

TABLA 7.1.6: HARDWARE EXISTENTE DE LOS SERVIDORES PÚBLICOS			
#	***Servidor***	***Marca / Modelo***	***Características***
1	Web Universidad	HP ProLiant ML150	Procesador Intel Xeon 3.2 Ghz, Memoria 1GB, Disco duro 100 GB.
2	Cursos Elearning	HP Proliant ML150	Procesador Intel Xeon 3.2 Ghz, Memoria 1GB, Disco duro 100 GB.
3	Med 1 (Módulos)	HP Compaq	Procesador Core 2Duo Inside, Memoria 5 GB, Disco duro 500 GB.
4	Med 2 (Evaluación)	HP Compaq	Procesador Core 2Duo Inside, Memoria 4 GB, Disco duro 250 GB.
5	Med 3 (Cursos)	HP ProLiant ML115	Procesador Amd Attlon, Memoria 5 GB, Disco duro 250 GB.
6	Sistema Académico 1	Aopen	Procesador Pentium 4, 2.0 Ghz, Memoria 512 MB, Disci duro 60 GB.
7	Sistema Académico 2	Compaq Presario	Procesador Intel Pentium 4 3.6 Ghz, Memoria 512 MB, Disco duro 160 GB.
8	Correo Electrónico	*HP Compaq 6000 Pro MT PC*	*Procesador Intel Core 2 Duo 2.9 Ghz,* *Memoria 2 GB,* *Disco duro 300 GB.*
9	Radio Universitaria	*HP Compaq 6000 Pro MT PC*	*Memoria 1957 MB.* *Disco duro 295 GB*
10	Firewall	HP ProLiant ML370G5	Procesador Intel Xeon 1.8 Ghz, Memoria 2 GB, Disco duro 66 GB.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*			

7.1.7. Diagrama de topología servidores intranet

A continuación se detalla el diagrama de topología en la infraestructura de la red de datos con algunos de los servidores de mayor prioridad en la intranet institucional.

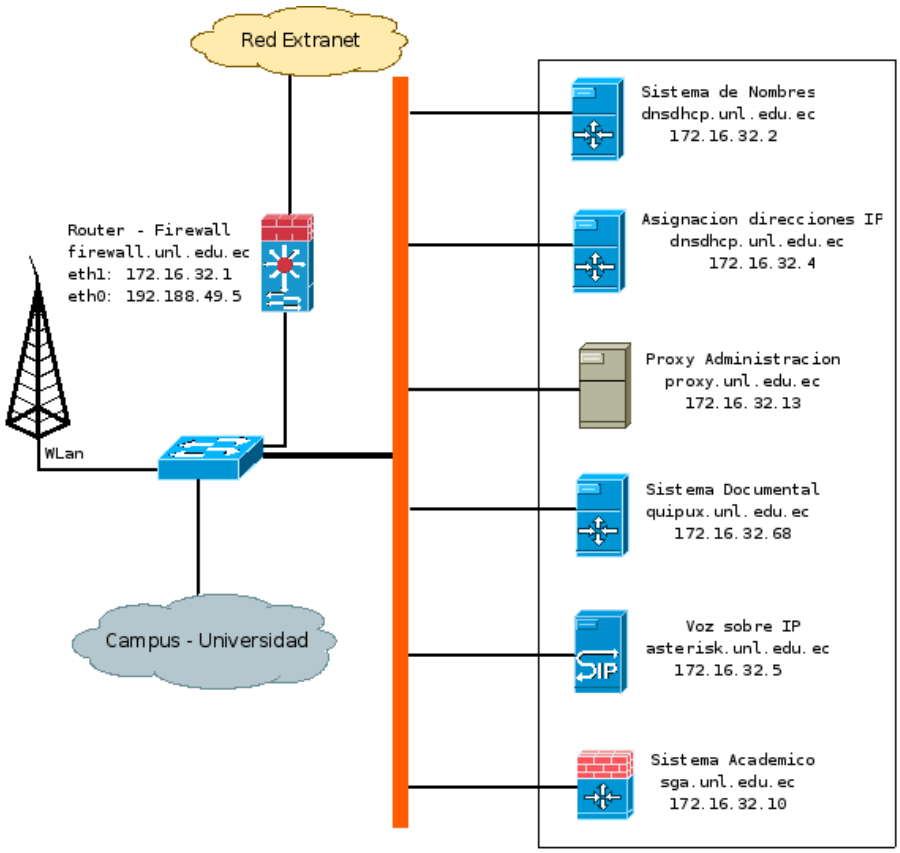


Figura 7.1.7. *Servidores intranet de la Universidad*

En el diagrama de topología se puede apreciar que los servidores de la intranet están interconectados a un switch cisco 2960 y de la misma manera existe un segmento conectado para wireless Lan (WLan). Todos estos servidores se consideran privados por lo que solo pueden ser accedidos desde la misma intranet, visto desde este punto no se puede visualizar los servicios de Internet desde afuera (red de redes). Entre los servidores que se encuentran implementados y en producción existentes: Sistema de nombres (dns), asignación de direcciones IP (dhcp), proxy administración, sistema documental (quipux), voz sobre IP, sistema académico (sga), etc.

7.1.8. Descripción de servidores de la intranet en la Universidad Nacional de Loja.

Seguidamente se presenta un resumen de los resultados obtenidos al visitar el cuarto de telecomunicaciones en donde se encuentran los servidores.

Sistema de nombres. Permite la resolución directa o inversa de las direcciones de Internet, se encuentra configurado como dns primario haciendo uso del dominio unl.edu.ec, facilitando de esta forma la resolución de nombres a los equipos finales en el campus universitario.

Asignación de direcciones IP. Permite a los clientes (pc, impresora, entre otros) de una red que puedan obtener de forma automática sus parámetros de configuración como son: IP, máscara de subred, puerta de enlace, dns y dominio.

Proxy administración. Es un equipo intermedio que facilita el acceso a los servicios de la intranet, servicios públicos e Internet a todos los equipos finales de la institución que no cuentan con una conexión directa a internet. En los servidores de este tipo (proxy) se manejan ciertas políticas de seguridad como es el control de contenido pornográfico, acceso a sitios infectados de virus, etc. Existen un proxy por cada AAA, administración central, modalidad de estudios a distancia y red inalámbrica (proxy transparente).

Sistema documental. Actualmente este servicio denominado "quipux" se encuentra en una etapa de implementación en la institución, cuya función principal es convertirse en una herramienta básica para las dependencias y AAA que soporten el registro, control, circulación y organización de los documentos digitales y/o impresos que se envían y reciben en la Universidad.

Voz sobre IP. A través de este servidor se hace posible que la voz viaje a través de la infraestructura de la red de datos empleando el protocolo IP. Este servicio se brinda a un número limitado de usuarios.

Sistema académico. El Sistema de Gestión Académico que es accesible por medio de la intranet universitaria facilita a los estudiantes, docentes y funcionarios (empleados) cumplir sus actividades académicas de forma eficaz y eficiente.

En la siguiente tabla se detalla el hardware existente en donde se encuentra funcionando los diferentes servicios de Internet en la red de datos de la intranet universitaria, el detalle que se muestra son de los servidores de mayor prioridad.

TABLA 7.1.8: HARDWARE EXISTENTE DE LOS SERVIDORES DE LA INTRANET			
#	**Servidor**	**Marca / Modelo**	**Características**
1	Proxy Administración	HP Compaq	Procesador Pentium D 3.4 Ghz, Memoria 1 GB, Disco duro 145 GB.
2	VoIP Universidad	AOpen	Procesador Pentium III Coppermine, Memoria 256 MB, Disco duro 37 GB.
3	Dns - Dhcp	HP ProLiant ML150	Procesador Intel Xeon 3.2 Ghz, Memoria 1GB, Disco duro 100 GB.
4	Financiero Universidad Nacional de Loja.	HP ProLiant ML150	Procesador XEON Intel Inside, Memoria 2 GB, Disco duro 300 GB.
5	Proxy Transparente	HP Compaq	Procesador Pentium D 3.4 Ghz, Memoria 2 GB, Disco duro 145 GB.
6	Sistema Documental (quipux)	HP Compaq	Procesador Pentium D 3.4 Ghz, Memoria 1GB, Disco duro 150 GB.

Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.*
Fuente: *Unidad de Telecomunicaciones e Información.*

7.1.9. Servicios de Internet que se brindan en el entorno educativo universitario.

Servicios de Internet, es el software o programas necesarios que se encuentran implementados y en producción en los diferentes servidores de la institución. Permiten garantizar el uso de Internet con fines académicos y acceso a los recursos necesarios en la intranet. Actualmente los servicios de Internet permiten: Asignación automática de direcciones IPv4, acceso a Información con fines académicos, correo electrónico institucional, aplicar políticas de seguridad, VoIP, resolución de dominios, sistema académico, etc.

Tallamos a continuación un resumen de los servicios de Internet, los resultados han sido obtenidos de acuerdo a la investigación de campo que se ha realizado.

TABLA 7.1.9: SERVICIOS DE INTERNET (SOFTWARE) EN LA INSTITUCIÓN			
#	**Tipo de Servicio**	**Puertos**	**Sistema Operativo**
1	* dns (bind v. 9.7.0) * dhcp (dhcp v. 3.0.5)	* Dns 53 UDP / 53 TCP * Dhcp 67 UDP	Distribución Centos v. 5.4
Descripción: El servicio de dns (sistema de nombre de dominio) y dhcp protocolo de configuración dinámica de host, está unificado en un solo servidor de producción llamado dnsdhcp.unl.edu.ec el cual permite la resolución directa e inversa y la configuración automática de los parámetros de red en el campus de la Universidad Nacional de Loja. El paquete que permite la resolución de nombres es bind v. 9.7.0 opera en el puerto 53 udp y tcp respectivamente, en cambio que para la asignación de los parámetros de red se emplea el programa dhcp v. 3.0.5.			
2	* smtp (sendmail v. 8.13.8) * pop3 (dovecot v. 1.0.7) * imap (dovecot v. 1.0.7) * ssl (openssl v. 0.9.8)	* Smtp 25 TCP * Pop3 110 TCP * Imap 143 TCP * Smtps 465 pop3s 995 imaps 993	Distribución Centos v. 5.4
Descripción: El servicio de correo electrónico se encuentra implementado en un solo servidor llamado webmail.unl.edu.ec para acceder vía web, y también permite el uso de clientes de correo (thunderbird, evolution, etc) tanto smtps con pop3s como para smtps con imaps haciendo referencia con el mismo nombre webmail.unl.edu.ec. Para el envío de correo (smtp) se hace uso de la herramienta sendmail v. 8.13.8 que opera en el puerto 25 tcp y en el puerto 465 con ssl, en cambio para obtener los mensajes de correo (pop3 e imap) se utiliza la herramienta dovecot v. 1.0.7 que opera en el puerto 110 pop3 y puerto 143 imap en tcp, de igual manera haciendo uso de ssl opera en el puerto 995 pop3s y puerto 993 imaps en tcp.			
3	* http (httpd v. 2.2.3) * mysql (mysql-server v. 5.0.77)	* Http 80 TCP * Mysql 3306 TCP	Distribución Centos v. 5.4
Descripción: La aplicación web de la Universidad se encuentra en el servidor de producción llamado www.unl.edu.ec o también se hace referencia con el nombre unl.edu.ec. En este mismo servidor se encuentra varios subdirectorios que permiten servir con aplicaciones web a las diferentes dependencias de la universidad que así lo requieran y tambien a las AAA. La herramienta que se emplea para poder servir las aplicaciones web es httpd v. 2.2.3 que trabaja en el puerto 80 tcp y la base de datos donde se aloja todo el contenido es mysql-server v. 5.0.77 opera en el puerto 3306 tcp.			

4	* proxy (squid v. 3.0) * dansguardian (dansguardian v. 2.8.0)	* Proxy 5647 TCP * Dansguardian 8080 TCP	Distribución Centos v. 5.4
Descripción: El servicio de proxy se brinda en todo el campus de la Universidad Nacional de Loja, el cual se encuentra implementado en ocho servidores uno por cada Área (Educativa, Jurídica, Agropecuaria, Energía y Salud), administración central, para el acceso inalámbrico funcionando como transparente y la modalidad de estudios a distancia (Med). La herramienta empleada para realizar el control de contenido es dansguardian v. 2.8.0 que escucha en el puerto 8080 tcp y el programa que realiza la función de proxy en si es squid v. 3.0 que opera en el puerto 5647 tcp para establecer un comunicación de uno a uno con dansguardian.			
5	* ftp (vsftpd v. 2.0.5)	* Ftp 20 y 21 TCP	Distribución Centos v. 5.4
Descripción: Este servicio permite la transferencia de archivos, se encuentra implementado en el servidor de cursos llamado cursos.unl.edu.ec. La herramienta utilizada para este fin es vsftp v. 2.0.5 que escucha peticiones en los puertos 20 y 21 tcp.			
	* ssh (ssh-server v. 4.3)	* Ssh 4466 TCP	
Descripción: Ssh es el programa que se ejecuta en los servidores (intranet y públicos) el cual permite acceder desde maquinas clientes por los administradores de la red de forma remota a través de la red de datos permitiendo manejar por completo el servidor mediante un intérprete de comandos (shell). El programa que se está utilizando es ssh-server v. 4.3 que escucha peticiones en el puerto 4466 y 6644 en tcp, dependiendo de las políticas de seguridad que se establezcan en le Sección de redes y equipos informáticos.			
6	* apache (v. 2.0) * postgresql (postgresql v. 8.3) * ssl (openssl v. 0.9.8)	* Apache 80, 81 y 82 TCP * Postgresql 5432 TCP * Https 443 TCP	Distribución Debian 4.0
Descripción: El SGA, usa la herramienta apache v. 2.0 para cada uno de los servidores esclavos por medio de un proxy reverso, por lo general estos esclavos levantan apache en el puerto 80, 81 y 82, pero como son reversos por el otro lado se comunican hacia puertos sin privilegios como el 8080, 8081; en esos puertos tienen cherrypy y pylons que son servidores de aplicaciones web hechos en python y que gobiernan la lógica del controlador del sistema. La base de datos postgresql v. 8.3 está centralizada en un solo nodo, este nodo escucha el			

puerto 5432, tiene acls de control de accesos solo para la red isolada (192.168.112.0/24). Para la página de docentes estan usando openssl v. 0.9.8, el cual nos permite crear un certificado no firmado, pero no lo usa el apache puesto que para este fin y por concepto del puerto https, no se permiten conexiones intermedias, es por esto que el openssl está wrapeado por el balanceador de carga pound.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*

7.1.10. Estructura lógica de la infraestructura red de datos universitaria.

Esta institución educativa cuenta con un rango de direcciones IPv4 privadas para su Intranet el mismo que permite la comunicación entre los diferentes dispositivos de networking, accediendo a los servicios de Internet que se brinda en el campus universitario y así mismo la red de redes Internet por medio de NAT (Traducción de Direcciones de Red), NAT se desarrolló para resolver la falta de direcciones IPv4, lo cual permite que los equipos con direcciones privadas IP compartan una dirección IP enrutable (IP pública). Entonces visto desde afuera prácticamente todos los equipos de la Intranet poseen la misma dirección IPv4 pública. Esto es totalmente transparente desde el punto de vista de los equipos de capa 2 (capa de acceso, modelo de referencia OSI) y equipos finales, en el caso de la Universidad solo es necesario configurar el Firewall-Router que realiza la función de NAT.

7.1.11. Direccionamiento IPv4 privado (intranet)

Se ilustra una tabla del direccionamiento IPv4 privado de clase B que se utilizan en dispositivos de networking, equipos finales, área de servidores, etc.

TABLA 7.1.11: DIRECCIONAMIENTO IPV4 INTRANET A	
Descripción	***Especificación***
Red de clase B	172.16.0.0 / 16
Dominio	unl.edu.ec
Subred en la Universidad	172.16.32.0 / 19
Máscara de subred	255.255.224.0
Dirección de broadcast	172.16.63.255
Puerta de enlace	172.16.32.1
Sistema de nombres (dns)	172.16.32.2
Numero de hosts disponibles	8190

Rangos de direcciones IPv4 Universidad	
Servidores y Dispositivos	17216.32.1 – 172.16.32.255
Administración Central	172.16.33.1 – 172.16.35.255
Área Jurídica	172.16.37.1 – 172.16.39.255
Área Educativa	172.16.41.1 – 172.16.43.255
Área Salud Humana	172.16.45.1 – 172.16.47.255
Área Energía	172.16.49.1 – 172.16.51.255
Área Agropecuaria	172.16.53.1 – 172.16.55.255
Impresoras Intranet	172.16.56.1 – 172.16.56.255
Dispositivos Wireless	172.16.57.1 – 172.16.59.255
Internet Domiciliario	172.16.61.1 – 172.16.61.255
Telefonía IP (VoIP)	172.16.62.1 – 172.16.62.255
Telecomunicaciones e Información	172.16.63.1 – 172.16.63.254
Rangos libres IPv4	172.16.36.1 – 172.16.36.255 172.16.40.1 – 172.16.40.255 172.16.44.1 – 172.16.44.255 172.16.48.1 – 172.16.48.255 172.16.52.1 – 172.16.52.55 172.16.60.1 – 172.16.60.255
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*	

TABLA 7.1.11: DIRECCIONAMIENTO IPV4 SERVIDORES INTRANET B				
Dispositivo	***Interfaz***	***Dirección IPv4***	***Gateway***	***Dns Primario***
Firewall (cortafuegos)	eth1	172.16.32.1 / 19	172.16.32.1	172.16.32.2
Sistema de nombres (dns)	eth0	172.16.32.2 / 19	172.16.32.1	172.16.32.2
Asigación IPv4 (dhcp)	eth0	172.16.32.4 / 19	172.16.32.1	172.16.32.2
Voz sobre IP (asterisk)	eth0	172.16.32.5 / 19	172.16.32.1	172.16.32.2
Financiero	eth0	172.16.32.7 / 19	172.16.32.1	172.16.32.2
Sistema académico (sga)	-	172.16.32.10 / 19	172.16.32.1	172.16.32.2
Proxy Administración	eth0	172.16.32.13 / 19	172.16.32.1	172.16.32.2
Sistema de monitoreo (nagios)	Eth0	172.16.32.20 /19	172.16.32.1	172.16.32.2
Proxy WLan	eth0	172.16.32.27 / 19	172.16.32.1	172.16.32.2
Proxy Med	eth0	172.16.32.28 / 19	172.16.32.1	172.16.32.2
Sistema documental (quipux)	eth0	172.16.32.68 / 19	172.16.32.1	172.16.32.2

Proxy Educativa	eth0	172.16.35.1 / 19	172.16.32.1	172.16.32.2
Proxy Jurídica	eth0	172.16.37.1 / 19	172.16.32.1	172.16.32.2
Proxy Agropecuaria	eth0	172.16.40.1 / 19	172.16.32.1	172.16.32.2
Proxy Energía	eth0	172.16.43.1 / 19	172.16.32.1	172.16.32.2
Proxy Salud	eth0	172.16.45.2 / 19	172.16.32.1	172.16.32.2
Desarrollo IPv6	eth0	172.16.63.7 / 19	172.16.32.1	172.16.32.2
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*				

7.1.12. Direccionamiento IPv4 público

La Universidad también dispone de un rango de direcciones IPv4 públicas asignadas por NIC.EC (Registro de Nombres de Dominio del Ecuador), con dichas direcciones la institución brinda sus servicios de Internet al mundo entero, entre los cuales se menciona aplicación web, med, cursos, videoconferencia, correo electrónico, sistema académico, radio universitaria, etc.

Seguidamente se muestra el esquema de direccionamiento IPv4 público de clase C, el cual se encuentra funcionando actualmente

.

TABLA 7.1.12. DIRECCIONAMIENTO IPV4 PÚBLICO A	
Descripción	***Especificación***
Red de clase C	192.188.49.0 / 24
Dominio	unl.edu.ec
Máscara de subred	255.255.255.0
Dirección de broadcast	192.188.49.255
Puerta de enlace	192.188.49.4
Sistema de nombres (dns) primario	200.93.221.17
Sistema de nombres (dns) secundario	200.93.192.188
Numero de hosts disponibles	254
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*	

TABLA 7.1.12. DIRECCIONAMIENTO IPV4 SERVIDORES PÚBLICOS B				
Dispositivo	***Interfaz***	***Dirección IPv4***	***Gateway***	***Dns Primario***
Servidor web	eth0	192.188.49.2 / 24	192.188.49.4	200.93.222.17
Admisiones (SGA)	eth1	192.188.49.3 / 24	192.188.49.4	200.93.222.17
Router Cedia Telconet	eth0	192.188.49.4 / 24	192.188.49.4	200.93.222.17
Firewall (contafuegos)	eth0	192.188.49.5 / 24	192.188.49.4	200.93.222.17
Sistema académico (SGA)	eth1	192.188.49.6 / 24	192.188.49.4	200.93.222.17
Web cinfa	eth0:0	192.188.49.8 / 24	192.188.49.4	200.93.222.17
Web vinculación	eth0:0	192.188.49.9 / 24	192.188.49.4	200.93.222.17
Web virtual (Med)	eth0	192.188.49.10 / 24	192.188.49.4	200.93.222.17
Web cursos (Med)	eth0	192.188.49.11 / 24	192.188.49.4	200.93.222.17
Web Área Energía	eth0	192.188.49.12 / 24	192.188.49.4	200.93.222.17
Web cursos Universidad	eth0	192.188.49.13 / 24	192.188.49.4	200.93.222.17
Web virtual (Med)	eth0	192.188.49.16 / 24	192.188.49.4	200.93.222.17
Correo electrónico	eth0	192.188.49.20 / 24	192.188.49.4	200.93.222.17
Radio universitaria	eth0	192.188.49.50 / 24	192.188.49.4	200.93.222.17
Videconferencias	eth0	192.188.49.100 / 24	192.188.49.4	200.93.222.17
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*				

7.2. Análisis de los Métodos de Transición a IPv6 y Selección del Método más Eficiente.

Con la creación de un nuevo protocolo (IPv6) para resolver el problema de direccionamiento que presentan actualmente la redes de comunicaciones basadas en IPv4, es necesario que se piense en un mecanismo de transición a IPv6. A continuación presentamos un análisis profundo de los métodos de transición o mecanismos de transición a IPv6 basándonos en los siguientes parámetros:

- Configuración.
- Compatibilidad (hardware y software).
- Integridad.
- Interoperabilidad.
- Desempeño.

Estos parámetros nos permitan determinar el mecanismo de transición a IPv6 más eficiente e idóneo, para la transición a IPv6 en la red de datos de la Universidad Nacional de Loja.

7.2.1. Métodos de transición a IPv6

En la presente investigación haremos mención a tres mecanismos de transición a IPv6 definidos por la IETF: Dual stack (doble pila), túneles y traducción de direcciones (traductores).

7.2.1.1. Dual stack (doble pila)[8].

La pila-dual como su nombre lo sugiere, significa literalmente mantener dos pilas de protocolos que trabajen paralelamente y así permitir al dispositivo trabajar vía ambos protocolos.

El mecanismo de transición doble pila hace uso de las pilas de protocolos de cada uno de ellos, tanto en los host como en los routers; es decir, que un host puede tener configurado los dos protocolos (IPv4 e IPv6) y cuando hace uso de la dirección IPv4 accede a su respectiva pila, de la misma manera cuando se usa la dirección IPv6; en lo correspondiente a los ruteadores, cada protocolo crea y administra su propia tabla de enrutamiento para poder conectarse con otro host o hacia el Internet.

[8] SIXXS. IPv6 Deployment & Tunnel Broker. [en línea]. disponible en: www.sixxs.net, [Consulta: 11 noviembre 2010].

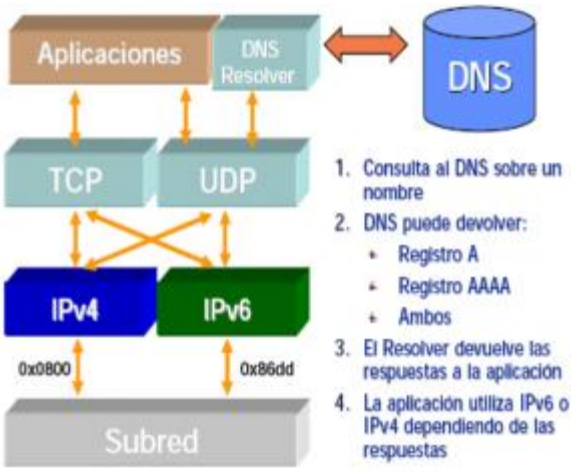


Figura 7.2.1.1: *Esquema de consulta DNS doble pila*

7.2.1.2. Túneles[9]

El túnel es un mecanismo en el que un paquete es encapsulado, dentro de otro tipo de paquete. Es decir podemos encapsular paquetes IPv6 dentro de paquetes IPv4. Es la forma más sencilla de configurar una conexión IPv6 a través de una red IPv4, aunque no es fácil de administrar. La mayoría de hosts doble pila y elementos de red soportan el estándar IPv6 en túneles IPv4

Este encapsulamiento se lleva a cabo en la entrada de un túnel y ese desencapsula a la salida de ese mismo túnel (existe, por lo tanto, una dirección lógica a un túnel dado).

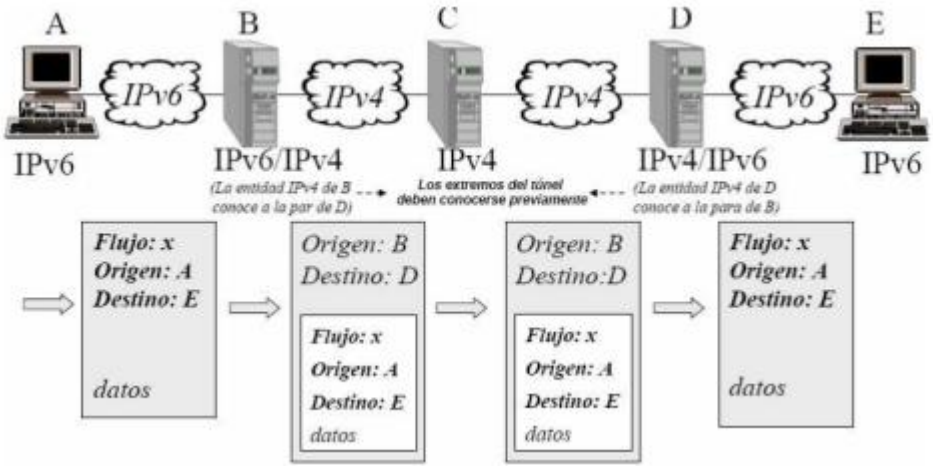


Figura 7.2.1.2: *Proceso de Tunelización A*

[9] ELECTRIC, HURRICANE, Hurricane Electric IPv6. [en línea]. disponible en: http://ipv6.he.net, [Consulta: 2 diciembre 2010].

Tunnel Broker. Este mecanismo actúa como servidor sobre la red IPv4, recibe peticiones de nodos con doble pila para configurar túneles automáticamente, estas peticiones son enviadas vía http sobre IPv4 por el nodo que se quiere configurar el túnel. A continuación se ilustra el diagrama de topología del tunnel broker que se levanto en la Universidad UPAO Trujillo - Perú para la presentación del paper en el II Congreso Internacional de Tecnología 2010 (COINTEC 2010).

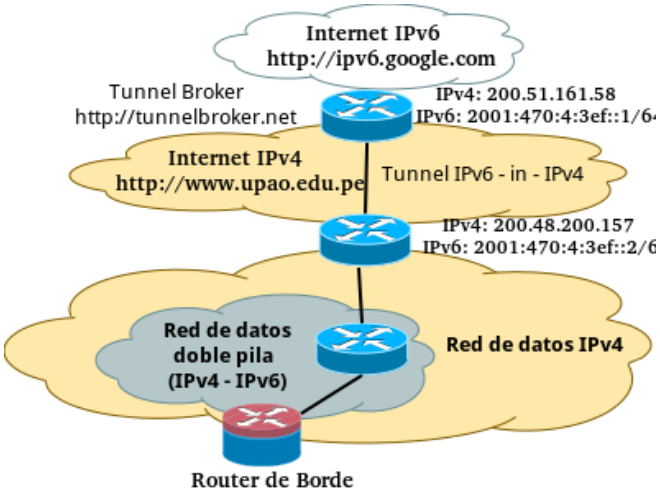


Figura 7.2.1.2: *Tunnel broker desde la Universidad UPAO Trujillo – Perú.B*

Todo el material que se utilizó en el COINTEC 2010 está disponible en la siguiente dirección electrónica:

- [http://www.unl.edu.ec/ipv6/cointec]

7.2.1.3. Traducción de Direcciones[10]

Este mecanismo de transición permite a un nodo que solo cuenta con la pila IPv6 habilitado dentro de una red IPv6 comunicarse con otro nodo que solo tiene la pila IPv4 habilitado dentro de una red IPv4. La cabecera IP ha de ser convertida y puede ser requerido un pool de direcciones IPv4 para proporcionar un alias al host IPv6 durante la comunicación.

Sin embargo, ésta técnica requiere tener también habilitados mecanismos de traducción entre IPv4 e IPv6 en las orillas de ambas redes (enrutadores). La conversión será más

[10] WIKIMEDIA FOUNDATION, Inc. IPv6. Wikipedia, La enciclopedia libre. [en línea]. disponible en: http://es.wikipedia.org/wiki/Ipv6, [Consulta: 2 noviembre 2010].

compleja si la aplicación procesa las direcciones IP. La principal desventaja es que todo el peso de este mecanismo de transición recae en los dispositivos.

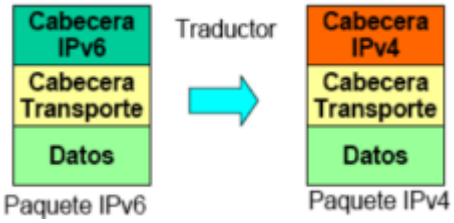


Figura 7.2.1.3: *Esquema básico de traducción de direcciones*. A

Traducción de IPv6 a IPv4. Cuando el traductor recibe un datagrama IPv6 destinado a una dirección IPv4-mapeada, éste traduce el encabezado IPv6 a un encabezado IPv4. Nuevamente, el encabezado original es removido y sustituido, en este caso, por un encabezado IPv4. A continuación se muestra como sucede la traducción de IPv6 a IPv4.

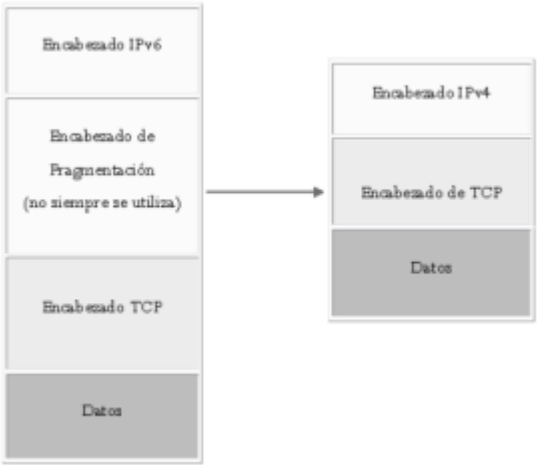


Figura 7.2.1.3: *Traducción de IPv6 a IPv4 B*

Los expertos en desplegar redes de datos IPv6 no recomiendan este mecanismo de transición a IPv6. Por tal motivo, para el posterior análisis y selección del mecanismo de transición más adecuado no será tomada en cuenta el mecanismo "Traducción de Direcciones", por lo tanto el análisis será realizado entre los mecanismos: doble pila y túneles con los parámetros anteriormente mencionados.

7.2.2. Comparación de los mecanismos de transición y selección del más idóneo.

La transición no siempre es la solución. Es importante tener presente que la transición no es la solución a todos los problemas presentes en IPv4. De hecho, algunas aplicaciones innovadoras necesitan IPv6 para su despliegue masivo.

Desplegar mecanismos de transición a gran escala puede además implicar problemas de escalabilidad que podrían limitar enormemente el rendimiento de IPv6 en comparación una solución nativa.

7.2.3. Determinación de los parámetros a evaluar

Configuración. Cada mecanismo de transición tiene su propia manera de estructurar sus procedimientos de comunicación con los dispositivos que soporten la utilización de un determinado mecanismo, que varía según el Sistema Operativo. Esta información ha sido recopilada en los respectivos RFCs (rfc 2893, rcf 2765, rfc 2473, etc) que describen los pasos a seguir para lograr la integración de los protocolos IPv4 e IPv6.

Compatibilidad (hardware y software):

- **Hardware.** Debido al avance tecnológico, los equipos de última generación incorporan funcionalidades que facilitan la configuración de los mecanismos de transición, es decir, soportan la utilización del protocolo IPv4 e IPv6 simultáneamente.
- **Software.** Los Sistemas Operativos actuales incorporan el soporte necesario en sus núcleos, para facilitar la configuración del mecanismo de transición más idóneo.

Integridad. La integridad el flujo de información garantiza que la misma no ha sido modificada durante la transmisión de los paquetes, por medio de los mecanismos de transición.

Interoperabilidad. Es la capacidad de, ejecutar programas o transferir datos entre distintas unidades funcionales de forma que se requiera el mínimo o nulo conocimiento del usuario sobre las características particulares de dichas unidades.

Este concepto ha adquirido gran trascendencia porque la penetración de Internet a nivel universal ha hecho que se convierta en una importante necesidad la interacción entre todos los sitios conectados a la red de redes, en la actualidad se está dando una progresiva migración

del protocolo IPv4 hacia IPv6 y es necesario encontrar el mecanismo de transición que cumpla esta tarea de una manera efectiva.

Desempeño. Hace referencia al comportamiento que tiene un mecanismo de transición específico, una vez que cumple con todos los argumentos y/o especificaciones establecidas para su utilización. Permitiendo de esta manera, comprobar su funcionalidad en entornos de producción reales.

7.2.4. Análisis comparativo entre los mecanismos de transición

A continuación se presenta la tabla de la matriz de valores, bajo la cual se procede a evaluar los mecanismos de transición IPv4 / IPv6. Que permita seleccionar el mecanismo más adecuado.

TABLA 7.2.4: MATRIZ DE EVALUACIÓN DE CRITERIOS		
Factor	**Escala**	**Ponderación**
Óptimo	5	Los argumentos establecidos se cumplen en su totalidad.
Satisfactorio	4	La mayoría de los argumentos establecidos se cumplen.
Aceptable	3	La mitad de los argumentos establecidos se cumplen.
Regular	2	Ciertos argumentos son cumplidos parcialmente.
Inaplicable	1	No se cumple con ningún argumento establecido.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación.*		

7.2.4.1. Evaluación – Requerimientos

Para el análisis a efectuarse, se debe tomar en cuenta varios factores:

- La información documentada sobre cada mecanismo, que permita una configuración adecuada del mismo.
- Los inconvenientes surgidos durante las pruebas de configuración y uso de cada mecanismo de convivencia, en los escenarios de prueba.
- Infraestructura física que permitió la realización de las respectivas pruebas de verificación.

Para la selección del mecanismo de transición más adecuada se analiza los mecanismos dual stack (doble pila) y túneles.

7.2.4.2. Evaluación – Parametrización

Ahora se procede a la evaluación de cada parámetro con los mecanismos de transición seleccionados (doble pila y túnel), con la finalidad de efectuar un análisis específico que permita una evaluación objetiva, tomando como referencia la "Matriz de Evaluación de Criterios" de la tabla anterior.

Parámetro 1: Configuración.

Este parámetro evalúa, si los procedimientos empleados por cada mecanismo de convivencia son los adecuados para su funcionamiento, a continuación se muestra la siguiente tabla.

TABLA 7.2.4.2: EVALUACIÓN CONFIGURACIÓN A			
Mecanismo	**Factor**	**Escala**	**Justificación**
Doble pila	Óptimo	5	No presenta complicaciones de configuración, puesto que su funcionamiento consiste en tener soporte IPv6 en el kernel para su utilización
Túnel	Satisfactorio	4	Este mecanismo está relacionado con Pila Dual puesto que su configuración necesita que los equipos que actúen como extremos del túnel tengan soporte IPv4 e IPv6 simultáneamente. Caso contrario, no es posible su configuración.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación.*			

Parámetro 2:

- **Compatibilidad – Hardware.**

Este parámetro permite evaluar si existe algún tipo de complicación en el hardware, al usar un mecanismo de transición IPv4 e IPv6, se muestra la siguiente la tabla a continuación.

TABLA 7.2.4.2: EVALUACIÓN COMPATIBILIDAD HARDWARE B			
Mecanismo	**Factor**	**Escala**	**Justificación**
Doble pila	Óptimo	5	No hay complicaciones en este método, ya que los dispositivos de última generación cuentan con el soporte necesario para los protocolos IPv4 e IPv6.
Túnel	Óptimo	5	No hay complicaciones en este método, ya que los dispositivos de última generación cuentan con el soporte necesario para los protocolos IPv4 e IPv6.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación*			

- **Compatibilidad Software.**

Este parámetro permite evaluar si existe algún tipo de complicación respecto al software, cuando se usa un mecanismo de convivencia IPv4 e IPv6, ver tabla a continuación.

TABLA 7.2.4.2: EVALUACIÓN COMPATIBILIDAD SOFTWARE C			
Mecanismo	**Factor**	**Escala**	**Justificación**
Doble pila	Óptimo	5	Tomando como referencia el uso de versiones actualizadas de sistemas operativos que brinden soporte hacia IPv6, el uso de este mecanismo de convivencia es factible.
Túnel	Óptimo	5	Tomando como referencia el uso de versiones actualizadas de sistemas operativos que brinden soporte hacia IPv6, el uso de este mecanismo de convivencia es factible.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación*			

Parámetro 3: Integridad.

Se encarga de evaluar que durante el uso de un mecanismo de transición, la información que se transmite por dicho mecanismo no sufre ningún tipo de modificación, ver tabla a continuación.

TABLA 7.2.4.2: EVALUACIÓN INTEGRIDAD D			
Mecanismo	**Factor**	**Escala**	**Justificación**
Doble pila	Óptimo	5	Los equipos que tengan habilitado doble pila, podrán transmitir información entre sí, sin ningún tipo de problema. Asegurando la integridad en los datos que se envíen.

Túnel	Satisfactorio	4	Debido a que este mecanismo hace uso de períodos de tiempo para mantener su conectividad activa. Puede darse el caso, en que durante el envío de paquetes, el tiempo de actividad para el túnel se termine, perdiéndose la información que se estaba transmitiendo.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación*			

Parámetro 4: Interoperabilidad.

Permite evaluar si a hacer uso de un mecanismo de transición determinado, permite la comunicación con dispositivos de red distintos que tengan el soporte necesario a los protocolos IPv4 e IPv6, a continuación se muestra la siguiente tabla.

TABLA 7.2.4.2: **EVALUACIÓN INTEROPERABILIDAD E**			
Mecanismo	**Factor**	**Escala**	**Justificación**
Doble pila	Óptimo	5	Cualquier dispositivo de red administrable que tenga el soporte debido a los protocolos IPv4 e IPv6 puede hacer uso de este mecanismo.
Túnel	Óptimo	5	Cualquier dispositivo de red administrable que tenga el soporte debido a los protocolos IPv4 e IPv6 puede hacer uso de este mecanismo.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación*			

Parámetro 5: Desempeño.

Se encarga de evaluar el comportamiento que tiene un mecanismo de transición, durante su utilización, a continuación se ilustra la siguiente tabla.

TABLA 7.2.4.2: **EVALUACIÓN RENDIMIENTO F**			
Mecanismo	**Factor**	**Escala**	**Justificación**
Doble pila	Satisfactorio	4	Dado que IPv4 e IPv6 son protocolos distintos, la información que se transmita no afecta su desempeño, sin embargo se debe tener en cuenta que este mecanismo debe verificar el tipo de dirección que se usa; es decir, si se trata de una dirección IPv4 o IPv6.
Túnel	Satisfactorio	4	Dado que este mecanismo se encarga de encapsular y desencapsular paquetes IPv6 en paquetes IPv4 y viceversa. El tiempo usado en realizar esta tarea, influye en cierta manera en su desempeño.
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación*			

7.2.5. Resultados

Del análisis efectuado a los Parámetros de Evaluación (Configuración, Compatibilidad (hardware y software), Integridad, Interoperabilidad y Desempeño) con los mecanismos de transición a IPv6 seleccionados (doble pila y túnel), se efectuaron evaluaciones parciales por cada uno de las tablas descritas anteriormente.

Los resultados de las tablas descritas anteriormente se los agrupa la presentación de la siguiente tabla; con la finalidad de obtener un promedio total de los parámetros evaluados para cada mecanismo de transición a IPv6 (doble pila y tunnel) analizado, permitiendo de esta manera obtener sus porcentajes totales de operabilidad respectivos.

TABLA 7.2.5: RESULTADOS TOTALES COMPARACIÓN

		Técnicas de Convivencia Evaluadas	
		Doble pila	**Túnel**
Parámetros de comparación	Configuración	5	4
	Compatibilidad Hardware	5	5
	Compatibilidad Software	5	5
	Integridad	5	4
	Interoperabilidad	5	5
	Desempeño	4	4
	Promedio General	4,43	4,5
	Porcentaje Total	***96,6%***	***90%***
	Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Documentación*		

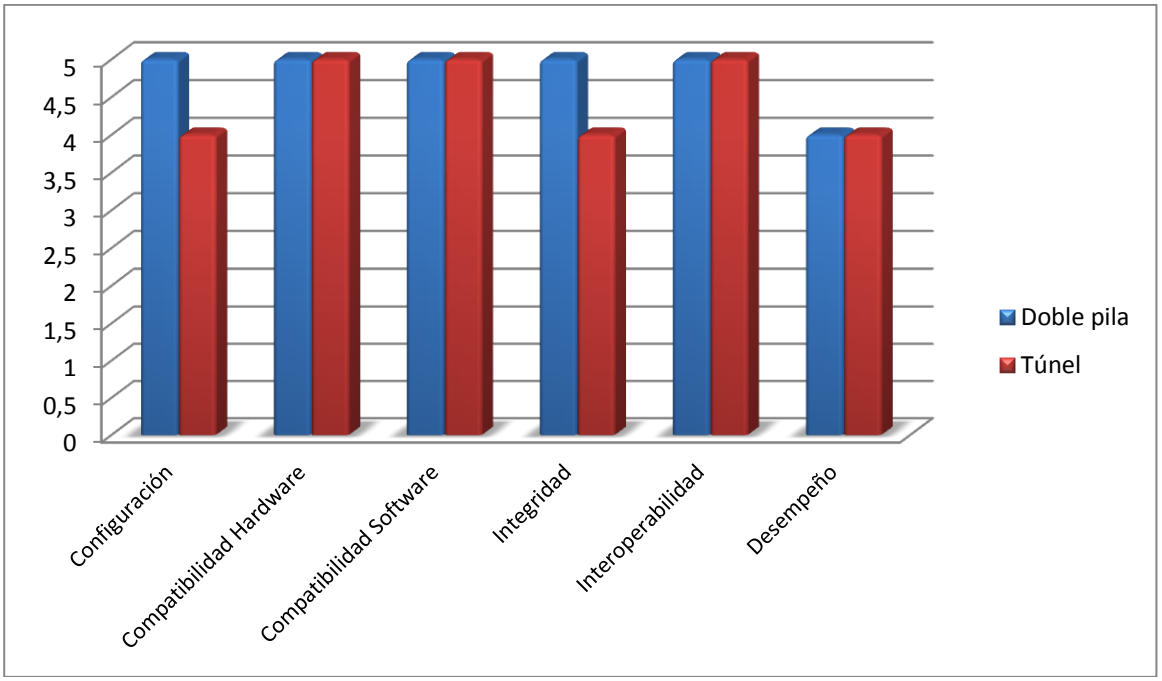


Figura 7.2.5: *Técnicas de Convivencia Evaluadas A*

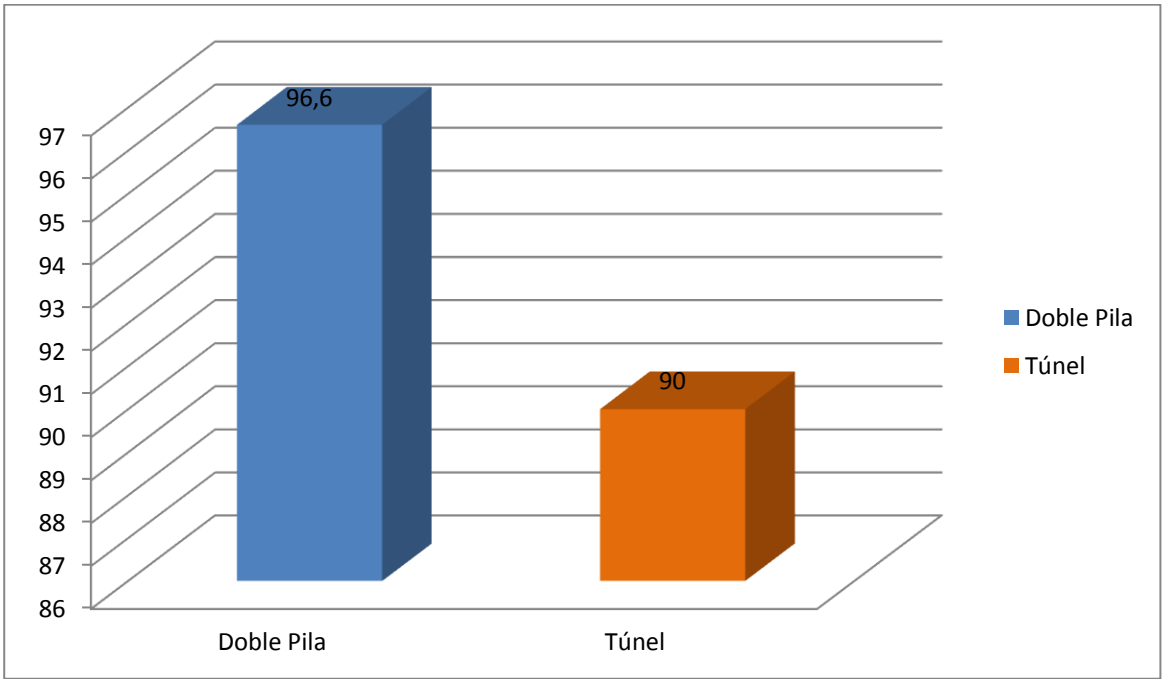


Figura 7.2.5: *Porcentajes entre Comparación de Mecanismos B*

Los resultados finales obtenidos de la evaluación de los mecanismos de transición a IPv6 (doble pila y túnel), son los siguientes:

El mecanismo doble pila presenta un porcentaje de operabilidad del 96.6% mientras que el mecanismo de túnel presenta un porcentaje del 90%. Dichos porcentajes se los obtuvo del promedio general obtenido por cada mecanismo, realizando una aproximación con el valor de escala más alto.

Con los resultados obtenidos se deduce lo siguiente:

- Las evaluaciones parciales efectuadas a cada parámetro, permitieron establecer las condiciones de operación bajo las cuales cada mecanismo se desenvuelve.

- Los argumentos requeridos para la utilización de ambos mecanismos de transición, cumplen con los requerimientos establecidos. Sin embargo, la diferencia existente en los porcentajes totales de ambos mecanismos, se debe a las evaluaciones realizadas, en las cuales se presentaron ciertos argumentos que diferencian un mecanismo del otro. Por ejemplo, en la ***Integridad*** de los datos el mecanismo "túnel" marca una diferencia respecto a "doble pila", debido a que su utilización se basa en períodos de tiempo y si dicho período de tiempo expira, los datos que se transmiten en ese momento tienen algún grado de alteración. Con respecto a la ***Configuración*** de cada mecanismo; "doble pila" no presenta inconvenientes, debido que para su utilización basta con tener el soporte IPv6 en el kernel, mientras que el mecanismo "túnel" debe incorporar equipos con doble pila en sus extremos, para efectuar posteriormente la configuración que el mecanismo túneles usa. Por estas razones, ambos mecanismos se distinguen uno del otro, de ahí la diferencia existente en los porcentajes finales entre ambos mecanismos de transición evaluados.

- La utilización del mecanismo de transición más adecuado, va enfocado al propósito de incorporar dicho mecanismo en una herramienta que provea el soporte necesario para los protocolos IPv4 e IPv6 simultáneamente. Por esta razón y basándonos en los resultados finales de la comparación efectuada entre "Doble pila" y "Túnel", podemos establecer que el mecanismo más adecuado para nuestros requerimientos es ***Doble Pila***, debido a que en el análisis efectuado en las evaluaciones, se demuestra un mejor desempeño del mecanismo de transición a IPv6 ***doble pila*** frente al mecanismo de túneles.

- Como una acotación final, vale mencionar que la utilización de "doble pila" es apto para entornos donde se conoce explícitamente la cantidad de equipos que se usa, es decir en el caso de la institución para la intranet y servidores públicos. Mientras que el uso de "túneles", permite la conectividad entre entornos que se encuentran separados y que se desea la comunicación entre ellos. Como nuestro estudio e implementación IPv6 se enfoca en la infraestructura de la red de datos Ethernet IEEE 802.3, "doble pila" cumple con este requerimiento satisfactoriamente, proporcionando el soporte necesario para los protocolos IPv4 e IPv6 al mismo tiempo.

7.2.6. Simulación transición doble pila (IPv4 e IPv6) en la Universidad Nacional de Loja

Siguiendo como referente el diagrama de topología de la red de datos de la Universidad, hemos armado un entorno de simulación. El programa específico que nos permite realizar esta actividad es Packet Tracert una aplicación propietaria de Cisco System.

La topología física de la red se crea simplemente arrastrando los dispositivos a la pantalla, luego clickando en ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos de Cisco OS.

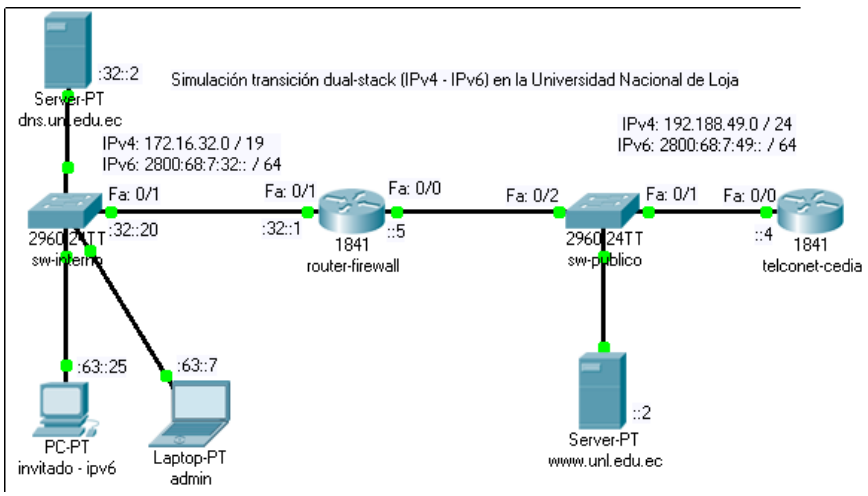


Figura 7.2.6: *Diagrama de topología simplificado en Packet Tracert.*

En el entorno de simulación se utilizaron direcciones IPv6 reales basadas en el prefijo 2800:68:7:: / 48, de dicho prefijo se crearon dos subered:

La primera subred IPv6 la utilizamos en la intranet, 2800:68:7:32:: /64 en donde se

configuran los dispositivos a partir de la interfaz FastEtherner 0/1 (router-firewall) hacia adentro.

La segunda subred IPv6 2800:68:7:49:: /64 la empleamos en los servicios públicos la cual se configura a partir de la interfaz FastEthernet 0/0 (router-firewall) hacia afuera.

Un punto importante a tener en cuenta en la simulación de la transición a IPv6 en la Universidad, nos permite conocer a ciencia cierta la configuración que debe realizar el ISP Telconet en el router de borde (telconet-cedia 7604) para tener conectividad nativa IPv6 hasta el router 7604.

Telconet S.A. realizará la configuración del router 7604, colocando una IPv6 en su interfaz interna (en nuestro ejemplo FastEthernet 0/0), y colocará una ruta estática apuntando hacia adentro a la subred IPv6 2800:68:7:32:: /64 con la IPv6 de gateway 2800:68:7:49::5.

```
router-7604#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router-7604(config)#interface FastEthernet 0/0
router-7604(config-if)#description Conexion-a-Universidad-Nacional-Loja IPv6
router-7604(config-if)#ipv6 enable
router-7604(config-if)#ipv6 address 2800:68:7:49::4/64
router-7604(config-if)#exit
router-7604(config)#
router-7604(config)#
router-7604(config)#ipv6 route 2800:68:7::/48 2800:68:7:49::5
router-7604(config)#ipv6 route 2800:68:7:112::/64 2800:68:7:49::6
router-7604(config)#
router-7604(config)#exit
```

La dirección IPv6 del gateway 2800:68:7:49::5 ya se encuentra configurada en el router-firewall en la interfaz FastEthernet 0/0. A continuación daremos una breve explicación de los comandos aplicados en el router 7604.

- [***ipv6 enable***] Habilitar IPv6 en la interfaz FastEthernet 0/0.
- [***ipv6 address 2800:68:7:49::4/64***] Permite agregar una dirección IPv6 con longitud de prefijo en la interfaz FastEthernet 0/0.
- [***ipv6 route 2800:68:7::/48 2800:68:7:49::5***] Agregar una ruta estática IPv6 a la subred IPv6 de la intranet universitaria.
- [***ipv6 route 2800:68:7:112::/64 2800:68:7:49::6***] Agregar una ruta estática IPv6 a la subred IPv6 isolada del sistema académico (SGA).

Iniciamos una prueba de conectividad IPv6 desde el router-firewall (2800:68:7:49::5) al router 7604 (2800:68:7:49::5).

```
router-fw#ping 2800:68:7:49::4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:7:49::4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/9 ms
```

Ahora probamos conectividad IPv6 desde un equipo de la intranet (2800:68:7:32:63:7) hacia el servidor web IPv6 (2800:68:7:49::2).

```
PC>ipv6config /all

Physical Address.................: 000A.411C.95AD
IPv6 Address....................:   2800:68:7:32:63::7/64
Default Gateway.................: 2800:68:7:32:32::1
DNS Servers.....................:   2800:68:7:32:32::2

PC>ping 2800:68:7:49::2
Pinging 2800:68:7:49::2 with 32 bytes of data:
Reply from 2800:68:7:49::2: bytes=32 time=47ms TTL=126
Reply from 2800:68:7:49::2: bytes=32 time=15ms TTL=126
Reply from 2800:68:7:49::2: bytes=32 time=9ms TTL=126
Reply from 2800:68:7:49::2: bytes=32 time=20ms TTL=126
Ping statistics for 2800:68:7:49::2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 9ms, Maximum = 47ms, Average = 22ms
```

Como se puede apreciar el entorno de simulación se llevo a cabo con todo éxito, el cual nos permitió conocer, entender y practicar de una mejor manera el protocolo de Internet versión 6 (IPv6).

8. DESARROLLO DE LA PROPUESTA ALTERNATIVA

8.1. Diseño del Direccionamiento IPv6 de la Universidad Nacional de Loja.

8.1.1. Diagrama de topología de la red de datos.

A continuación se ilustra el diagrama de topología de la red de datos de la Universidad Nacional de Loja acorde al direccionamiento IPv4 actual.

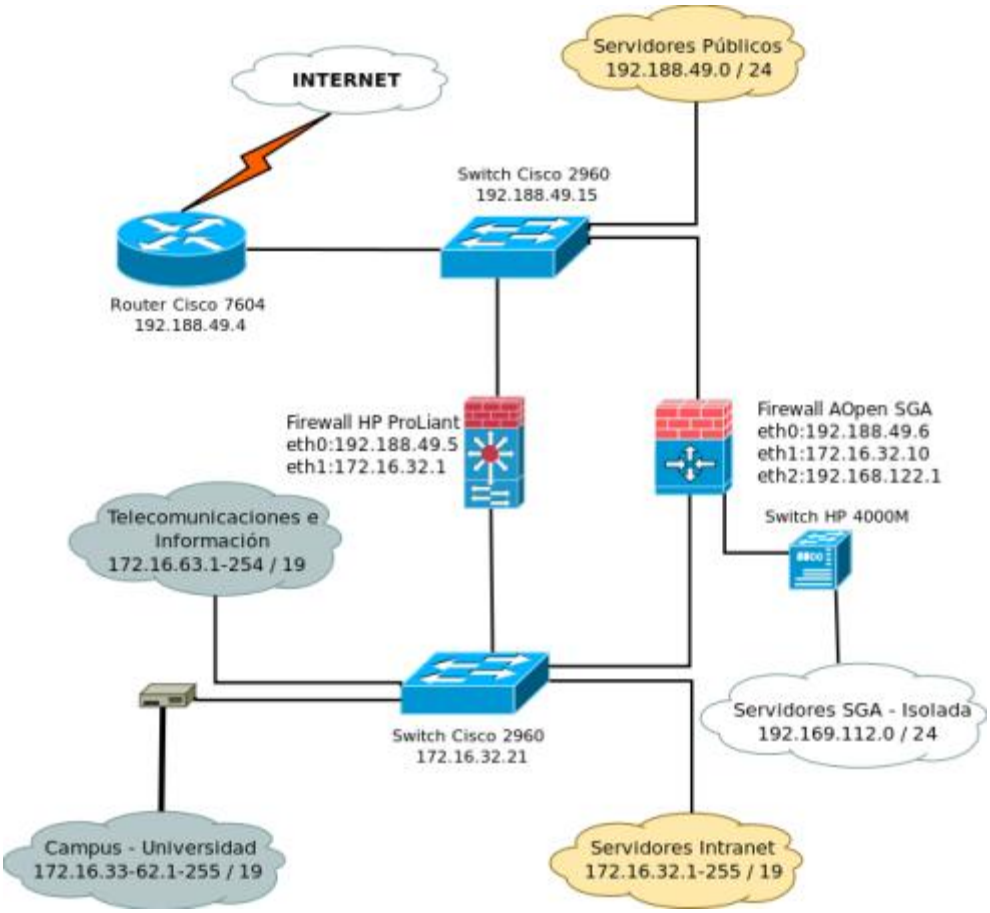


Figura 8.1.1: *Dispositivos de networking direccionamiento IPv4.*

Como se puede apreciar en el diagrama de topología la Universidad cuenta con una subred de clase B IPv4 172.16.32.0 / 19 para toda la intranet universitaria, en donde se divide por rangos de direcciones IPv4 para los dispositivos de networking, AAA y dependencias. A si mismo se dispone de una red de clase C IPv4 192.188.49.0/24 para los servicios de Internet públicos que brinda la institución y puedan ser accedidos desde afuera (red de redes) y desde toda la intranet.

La Univwersidad Nacional de Loja, posee un enlace a Internet mediante IPv4, otorgado por la empresa ISP (Proveedor de Servicios de Internet) Telconet S.A, dicho ISP tiene implementado y en producción IPv6 nativo en sus dispositivos de networking, por lo que no es necesario realizar ningún tipo de túnel IPv6 sobre IPv4 para poder consumir servicios de Internet en IPv6.

La implementación de IPv6 se desarrollará en la Universidad Nacional de Loja, tanto en los servicios de Internet (servidores de la intranet y públicos) como en los dispositivos de networking necesarios para poder brindar servicios de Internet en IPv6 al mundo entero y mismo hacer uso de Internet en IPv6 (navegación).

Prefijo IPv6 para la Universidad Nacional de Loja.

El bloque mínimo asignado por LACNIC es un /48 y el máximo un /32 y para calificar para la asignación inicial, la organización debe:

No ser un LIR (Registro Local de Internet) o ISP.

En caso de anunciar la asignación en el sistema de rutas inter-dominio de Internet, la organización receptora deberá anunciar un único bloque, que agregue toda la asignación de direcciones IPv6 recibida.

Proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses.

Entregar planes de direccionamiento por al menos un año, y números de terminales sobre cada subred.

Entregar una descripción detallada de la topología de la red.

Realizar una descripción detallada de los planes de encaminamiento de la red, incluyendo los protocolos de encaminamiento a ser usados, así también como cualquier limitación existente.

LACNIC asignará bloques de direcciones IPv6 portables directamente a usuarios finales si cuentan con asignaciones de direcciones IPv4 portables previamente realizadas por LACNIC.

En caso de anunciar la asignación en el sistema de rutas inter-dominio de Internet, la organización receptora deberá anunciar un único bloque, que agregue toda la asignación de direcciones IPv6 recibida.

IPv6 actualmente tiene un 13% de su total de direcciones reservado para Internet, este 13% es asignado para Dirección Unicast Global, la direccion es 2000::/3. Cada RIR poseen una /12, en el caso de Latinoamérica y el Caribe, la dirección asignada para LACNIC es 2800:/12.

Prefijo IPv6 2800:68::/32. El CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) dispone del prefijo IPv6 2800:68::/32 asignado por LACNIC, es decir igual que un LIR, este rango se ha subdividido en bloques más pequeños para las instituciones miembros del CEDIA, estos bloques son /48.

Estas asignaciones se han realizado tomando en cuenta el RFC (Request for Comment – Petición de Comentarios) 3177. El CEDIA puede tener hasta 65536 instituciones con redes diferentes, para que se acabe el /32 asignado (por algo se dice que IPv6 tiene IPs para todo mundo).

Prefijo IPv6 2800:68:0007::/48. El prefijo IPv6 asignado por el CEDIA a la Universidad Nacional de Loja es un 2800:68:0007::/48, con ello la institución cuenta con 65536 redes internas diferentes de prefijo IPv6 /64 y cada uno de estos con puede tener 18446744073709551616 direcciones IPv6.

Hay que tener en cuenta que para las asignaciones de prefijos /64 recomendado por el RFC 3177 y los RIRs es: /64 cuando se conoce por diseño que una y sólo una subred es necesaria.

Dual Stack mecanismo de transición para la implementación de IPv6.

De acuerdo al análisis que que se llevó a cabo, sobre los mecanismos de transición a IPv6 se optó por "dual-stack" también conocido como "doble pila" **TABLA 9.2.1** cuyo mecanismo de transición permite que se implementen la pila de ambos protocolos, IPv4 e IPv6 en cada nodo de la red. Cada nodo de doble pila tendrá dos direcciones de red, una en IPv4 y otra en IPv6.

Una de las ventajas que más sobresalen en la técnica de dual-stack, frente a los otros mecanismos de transición (túneles y traducción) es asegurar la conectividad de los nodos de la red, cuando no sea posible utilizar IPv6, se puede utilizar IPv4. Cambien se requiere que todos los sistemas operativos, servicios de Internet y aplicaciones cuenten con soporte IPv6, además los dispositivos de networking principales involucrados en conectar la red de datos institucional al Internet deben contar con soporte para IPv6.

8.1.2. Plan de direccionamiento IPv6 en la Uinersidad Nacional de Loja.

Como ya se mencionó anteriormente el prefijo asignado a la Universidad Nacional de Loja por parte del CEDIA es: 2800:68:0007:0:0:0:0:0/48 agrupando los ceros quedaría el prefijo ***2800:68:7::/48*** lo que permite a la Uiversidad Nacional de Loja contar con 65536 redes IPv6, cada uno de tamaño /64.

Entonces, en general se utilizan /64 para las redes locales (LAN), las redes de área extensa (WAN) y las loopbacks. Con el objetivo de realizar una correcta distribución del gran número de direcciones IPv6 disponibles, se opto por implementar una política basada en los lineamientos de la Sección de Redes y Equipos Informáticos, que se fundamenta en el direccionamiento jerárquico que considera a las distintas AAA (Áreas Académico Administrativas) y demás dependencias de la Universidad Nacional de Loja.

Hay que tener en cuenta que en IPv6 ya no se cuenta terminales (host) en una LAN pues se va asignar a cada una un /64 que se va a enumerar todas las terminales que se deseen. En su lugar, lo que sí se cuenta son las cantidades de redes y subredes a numerar. En el caso particular de la Universidad Nacional de Loja, solo existe un dominio de broadcast por lo que se hace necesario sólo un /64 para la LAN.

Toda dirección unicast globales IPv6 cuenta con tres campos: el prefijo globalmente encaminado, el identificador de subred y el identificador de interfaz, según se indica en el siguiente gráfico.

n bits	m bits	128-n-m bits
Prefijo Global Unicast *n =48 bits*	**Identificador de subred** *m = 16 bits*	**Identificador de interfaz** *128-48-16 = 64 bits*

Figura 8.1.2: *Construcción de una dirección en IPv6 Universidad Nacional de Loja* A

El largo de prefijo Global Unicast asignado a la Universidad Nacional de Loja es /48 ***n=48 bits***. Vamos a escoger un identificador de interfaz igual a un /64 por dos motivos:

Facilitar la autoconfiguración en las redes locales (LAN) que así lo requieran. Respetar que muchas veces el equipo final ha sido especializado para trabajar con direcciones IPv6 /64.

Con esto queda definido que el identificador de subred tendrá una longitud ***m=16 bits,*** y el identificador de interfaz es ***64 bits***, el resultado total nos da: n+m+64=***128 bits*** que es la longitud de una dirección IPv6.

Seguidamente se muestra la tabla, en donde consta la estructura de las direcciones IPv6 a utilizar en la Universidad Nacional de Loja.

TABLA 8.1.2: ESTRUCTURA DIRECCIONES IPV6 EN LA UNIVERSIDAD NACIONAL DE LOJA.				
Nombre campo	***Prefijo UNL***	***ID Subred***	***Dispositivo (id interfaz)***	
Tamaño campo	48 [bits]	16 [bits]	16 [bits] (sección)	48 [btis] (interfaz)
Prefijo	/ 48	/ 64	/ 128	
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*				

Un ejemplo, de dirección IPv6 para un dispositivo de la Universidad Nacional de Loja seria. ***2800:68:7:32:67::2 / 64*** en donde: [2800:68:7] [/48] es el prefijo de ruteo global, [32] [/64] es el identificador de subred y [67::2] indican el identificador de interfaz que incluyen 16 bits [67] para identificar la sección donde pertenece el dispositivo y los restantes 48 bits [::2] identifican plenamente a la interfaz.

Por las razones anteriormente citadas, diremos que nuestras interfaces todas serán de prefijo /64, es decir de los 128 bits totales de cada dirección, los primeros 64bits representarán la red, y los siguientes 64 bits representarán la interfaz (llamado en IPv4, la parte del host).

Ahora al igual que IPv4, debemos sumarizar, ahora la pregunta es como sumarizamos, tenemos del bit 48 al 63 para sumarizar, es decir con estos bits podemos tener 2^16 subredes, lo cual es más que suficiente para la Universidad Nacional de Loja.

En el siguiente gráfico se muestra la mejor regla adaptada a la institución, de una manera fácil de administrar las direcciones IPv6.

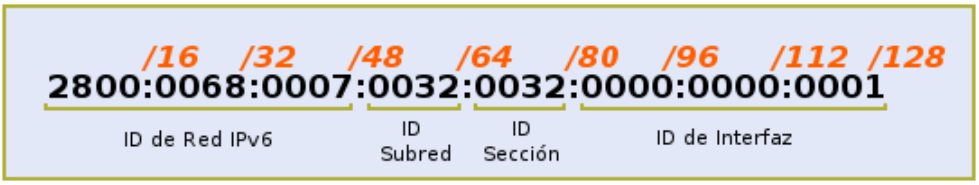


Figura 8.1.2: *Formato de una dirección en IPv6 Universidad Nacional de Loja B.*

La descripción es la siguiente:

- Los primeros 32 bits definen la red del CEDIA [2800:0068:].
- Los siguientes 16 bits definen la red de la Universidad [:0007:].
- Los siguientes 16 bits definen a cada una de las subredes de la Universidad [:0032:].
- Los siguientes 16 bits definen a la AAA, dependencia, etc., de la Universidad [:0032:].
- Los últimos 48 bits son los que definen a una interfaz en específico [:0000:0000:0001:]

8.1.3. Direccionamiento IPv6 intranet.

Como se ilustra una tabla de los rangos de direccionamiento IPv6 unicast globales que se van a implementar en los dispositivos de networking, equipos finales (secciones o áreas), área de servidores, etc de la intranet, basados en el prefijo 2800:68:7:32:: / 64.

TABLA 8.1.3: DETALLE DE RANGOS DE DIRECCIONES IPv6 EN LA UNIVERSIDAD NACIONAL DE LOJA A.		
Rango IPv6 /64	***Identificador***	***Destino***
2800:68:7:32:32::/64	32	Servidores y Dispositivos
2800:68:7:32:33::/64	33	Administración Central
2800:68:7:32:37::/64	37	Área Jurídica
2800:68:7:32:41::/64	41	Área Educativa
2800:68:7:32:45::/64	45	Área Salud Humana
2800:68:7:32:49::/64	49	Área Energía
2800:68:7:32:53::/64	53	Área Agropecuaria
2800:68:7:32:56::/64	56	Impresoras Intranet
2800:68:7:32:57::/64	57	Dispositivos Wireless
2800:68:7:32:61::/64	61	Internet Domiciliario
2800:68:7:32:62::/64	62	Telefonía IP (VoIP)
2800:68:7:32:63::/64	63	Telecomunicaciones e Información
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*		

Los identificadores de la columna 2 hacen referencia al tercer octeto de las direcciones IPv4 de la intranet como se muestra en la ***Tabla 8.1.3***, esto nos permite tener una similitud entre IPv4 e IPv6 para fines de administración de la red de datos. Este identificador se ha considerado en la red IPv6 2800:68:7:32::/48 ubicando el identificador en el quinto campo que es parte del id de la interfaz, quedando de esta forma las direcciones IPv6 2800:68:7:32:32::/64 (rango servidores).

A continuación se mostrará las direcciones IPv6 asignadas a los servidores de la intranet que brindan los servicios de Internet a la comunidad universitaria.

TABLA 8.1.3: DIRECCIONAMIENTO IPv6 SERVIDORES INTRANET B	
Dispositivo	***Dirección IPv6***
Firewall (cortafuegos)	2800:68:7:32:32::1 /64
Sistema de nombres (dns)	2800:68:7:32:32::2 /64
Asigación IPv4 (dhcp)	2800:68:7:32:32::4 /64
Voz sobre IP (asterisk)	2800:68:7:32:32::5 /64
Financiero	2800:68:7:32:32::7 /64
Sistema académico (sga)	2800:68:7:32:32::10 /64
Proxy Administración	2800:68:7:32:32::13 /64
Sistema de monitoreo (nagios)	2800:68:7:32:32::20 /64
Proxy WLan	2800:68:7:32:32::27 /64
Proxy Med	2800:68:7:32:32::28 /64
Sistema documental (quipux)	2800:68:7:32:32::68 /64
Proxy Educativa	2800:68:7:32:35::1 /64
Proxy Jurídica	2800:68:7:32:37::1 /64
Proxy Agropecuaria	2800:68:7:32:40::1 /64
Proxy Energía	2800:68:7:32:43::1 /64
Proxy Salud	2800:68:7:32:45::1 /64
Desarrollo IPv6	2800:68:7:32:63::7 /64
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*	

8.1.4. Direccionamiento IPv6 servidores públicos.

La Universidad dispone de la red IPv4 192.168.49.0/24, de donde partiremos para asignar una subred IPv6 a los servidores públicos basándonos en el campo del tercer octeto, que tenemos como identificador el 49 quedando la subred 2800:68:7:49:: /64 para los servidores.

A continuación se muestra la tabla de direcciones IPv6 asignados a los servidores públicos de la Universidad Nacional de Loja.

TABLA 8.1.4: DIRECCIONAMIENTO IPV6 SERVIDORES PÚBLICOS	
Dispositivo	***Dirección IPv6***
Servidor web	2800:68:7:49::2 /64
Admisiones (SGA)	2800:68:7:49::3 /64
Router Cedia Telconet	2800:68:7:49::4 /64
Firewall (contafuegos)	2800:68:7:49::5 /64
Sistema académico (SGA)	2800:68:7:49::6 /64
Web cinfa	2800:68:7:49::8 /64
Web vinculación	2800:68:7:49::9 /64
Web virtual (Med)	2800:68:7:49::10 /64
Web cursos (Med)	2800:68:7:49::11 /64
Web Área Energía	2800:68:7:49::12 /64
Web cursos Universidad	2800:68:7:49::13 /64
Web virtual (Med)	2800:68:7:49::16 /64
Correo electrónico	2800:68:7:49::20 /64
Radio universitaria	2800:68:7:49::50 /64
Videconferencias	2800:68:7:49::100 /64
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*	

De acuerdo al direccionamiento y el diseño IPv6 que se desarrolló en el presente capítulo, para los diferentes dispositivos, servidores, aplicaciones, etc es necesario presentar un diagrama de topología de la red de datos usando IPv6 como se muestra a continuación.

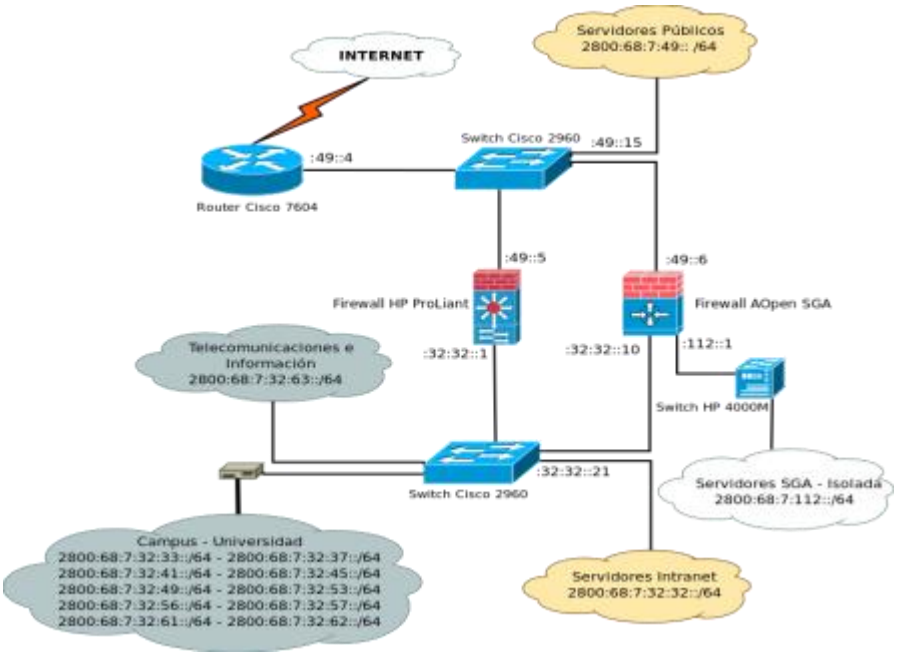


Figura 8.1.4: *Diagrama de topología direccionamiento IPv6.*

Se asignó la red 2800:68:7:32:32::/64 a los servidores de la Intranet, dicha red pertenece al identificador "32" y está bajo la administración de la Sección de Redes y Equipos

Informáticos. Así mismo se considera asignar la red 2800:68:7:49::/64 para los servidores públicos en donde la administración de estos servidores se realiza por parte de personal de la Sección de Redes, SGA y MED. Finalmente el prefijo 2800:68:7:112:: / 64 se considera necesario para la red isolada del Sistema Académico.

8.2. Instalación y Configuración del Harware y Software Necesario que Soporte IPv6.

En este capítulo nos ocuparemos de los procedimientos necesarios para hacer la instalación, configuración y despliegue de IPv6 en los diferentes servicios de Internet de la red datos en la Universidad Nacional de Loja. Prácticamente todos los servicios, aplicaciones y dispositivos de networking de uso mayoritario cuentan con soporte IPv6.

8.2.1. Equipamiento, aplicaciones y servicios.

Se debe tener en cuenta todo el equipamiento, aplicaciones y servicios que funcionan en la red de datos de la Universidad, donde se realizara la instalación y configuración de IPv6. Podemos destacar los siguientes equipos:

1 Router Cisco 7604.
2 Switch Cisco Catalyst 2960.
3 Firewall Hp ProLiant y AOpen SGA.
4 Servidores con sistema operativo Gnu / Linux (distribuciones Centos y Debian).
5 Videoconferencia Polycon VSX 8000.
6 Estaciones de trabajo (Pcs, laptops, otros dispositivos).

En cuanto a los servicios de Internet que se encuentran funcionando y en producción, podemos mencionar que en ellos se realizará la configuración de IPv6.

1 Sistema de nombres (dns).
2 Asignación de parámetros de red (dhcp).
3 Transferencia de archivos (ftp).
4 Correo electrónico (smtp, pop3 e imap).
5 Proxy Administración Central.
6 Servidores web (http).

En función de estos servicios de Internet podemos identificar las aplicaciones que están siendo utilizadas en la Universidad. Nos centraremos especialmente en las soluciones de Software Libre y Open Source ya que ya es una política de institución el uso de soluciones libres.

1 Bind v. 9.7.0
2 Dhcp v. 3.0.5
3 Sendmail v. 8.13.8
4 Dovecot v. 1.0.7
5 Openssl v. 0.9.8
6 Httpd v. 2.2.3
7 Mysql-server v. 5.0.77
8 Squid v. 3.0
9 Dansguardian v. 2.8.0
10 Vsftpd v. 2.0.5
11 Ssh-server v. 4.3
12 Apache 2.0
13 Postgresql v. 8.3

Todos los paquetes de aplicaciones previamente mencionados soportan IPv6 en las versiones expuestas, por lo que debemos tener en cuenta las opciones de configuración que correspondan. Antes de dedicarnos a ello, trataremos el tema de soporte de IPv6 en la infraestructura de la red de datos universitaria.

8.2.2. Soporte IPv6 en la insfraestructura de la red de datos.

Es necesario evaluar el estado actual del soporte IPv6 en los dispositivos de networking, sistemas operativos, servicios de Internet y aplicaciones de uso común, utilizadas por los usuarios de la red de datos universitaria en la Universidad Nacional de Loja.

8.2.3. Soporte IPv6 en dispositivos de networking.

En la actualidad la mayor parte de fabricantes de dispositivos de networking (routers, switchs, etc) incluyen en sus productos soporte nativo IPv6, por el despliegue que ha tenido el protocolo en los últimos años.

Se presenta una tabla de los principales dispositivos de networking que se utilizan en la red de datos.

TABLA 8.2.3: SOPORTE IPV6 EN DISPOSITIVOS DE NETWORKING UNIVERSIDAD NACIONAL DE LOJA.				
#	***Descripción***	***Función***	***IPv4***	***Soporta IPv6 ?***
1	Cisco 7604	Router de borde	Sí	***Sí***
2	Catalyst 2960 Series	Switch público	Sí	***No***
3	Catalyst 2960 Series	Switch privado	Sí	***No***
4	Polycon VSX 8000	Videoconferencia	Sí	***No***
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*				

8.2.4. Soporte IPv6 en sistemas operativos.

La mayor parte de los sistemas operativos en uso en la actualidad disponen de soporte para IPv6 desde el año 2001, Aunque las primeras versiones de estas tecnologías incluían un soporte incompleto o "experimental" del protocolo IPv6, actualizaciones o ediciones posteriores subsanaron esta limitación.

Presentamos un resumen de los sistemas operativos con soporte IPv6 más utilizados por usuarios finales y servidores en la red de datos institucional de la Universidad Nacional de Loja.

TABLA 8.2.4: SOPORTE IPV6 EN SISTEMAS OPERATIVOS DE LA UNIVERSIDAD NACIONAL DE LOJA.				
#	***Nombre SO***	***Función***	***IPv4***	***Soporta IPv6 ?***
1	Gnu / Linux - Centos	Sistema operativo servidores	Sí	***Sí***
2	Gnu / Linux - Debian	Sistema operativo servidores	Sí	***Sí***
3	Gnu / Linux - Ubuntu	Sistema operativo escritorio	Sí	***Sí***
4	Windows Server 2003	Sistema operativo servidor	Sí	***Sí (habilitarlo)***
5	Windows Server 2008	Sistemas operativo servidor	Sí	***Sí***
4	Windows Xp	Sistema operativo escritorio	Sí	***Sí (habilitarlo)***
5	Windows Vista	Sistema operativo escritorio	Sí	***Sí***
6	Windows 7	Sistema operativo escritorio	Sí	***Sí***
7	Mac OS-X	Sistema operativo escritorio	Si	***Si***
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*				

En los sistemas operativos Windows server 2003 y Windows XP con service pack 1 o posteriores, IPv6 está instalado, pero es preciso habilitarlo.

8.2.5. Soporte de IPv6 en servicios de Internet.

De la presente investigación se realizó un análisis de una serie de servicios de Internet de uso común en los servidores de la red de datos de la Universidad Nacional de Loja. El objetivo fue verificar el grado de soporte a IPv6 que estos ofrecen, demostrando que en la actualidad es posible implementarlos en redes que funcionen exclusivamente con IPv6.

A continuación se muestra una tabla de los servicios de Internet que tienen soporte IPv6, los resultados obtenidos es producto de la investigación que se la llevo en la Unidad de Telecomunicaciones e Información.

TABLA 8.2.5: SOPORTE IPV6 EN SERVICIOS DE INTERNET DE LA UNIVERSIDAD NACIONAL DE LOJA.

#	*Descripción*	*Función*	*IPv4*	*Soporta IPv6 ?*
1	Bind v. 9.7.0	Sistema de nombres	Sí	***Sí***
2	Dhcp v. 3.0.5	Asignación de IPs	Sí	***No***
3	Sendmail v. 8.13.8	Envío de correo	Sí	***Sí***
4	Dovecot v. 1.0.7	Obtener correo	Sí	***Sí***
5	Openssl v. 0.9.8	Criptografía asimétrica ssl	Sí	***Sí***
6	Httpd v. 2.2.3	Servidor web http	Sí	***Sí***
7	Mysql-server v. 5.0.77	Base de datos	Sí	***Sí***
8	Squid v. 3.0	Proxy	Sí	***Sí***
9	Vsftpd v. 2.0.5	Transferencia de archivos	Sí	***Sí***
10	Ssh-server v. 4.3	Acceso remoto	Sí	***Sí***
11	Apache 2.0	Servidor web (Sga)	Sí	***Sí***
12	Postgresql v. 8.3	Base de datos (Sga)	Sí	***Sí***

Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.*
Fuente: *Unidad de Telecomunicaciones e Información.*

Como se puede apreciar en el cuadro la mayoría de herramientas que brindan los servicios de Internet cuentan con soporte IPv6, a excepción de Dhcp v. 3.0.5. Es por ello que para la asignación de direcciones IPv6 (dhcpv6) haremos uso del paquete dhcpv6 v. 1.0.10 que si cuenta con soporte para IPv6.

8.2.6. Soporte de IPv6 en aplicaciones de uso común.

Existen en la actualidad innumerables aplicaciones (audio, video, navegación, clientes de correo, acceso remoto, etc) que incluyen algún tipo de soporte para IPv6.

A continuación se mostrará un resumen de la principales aplicaciones de mayor uso en la diferentes AAA y dependencias de la Universidad Nacional de Loja, y si cuentan con soporte IPv6.

TABLA 8.2.6: SOPORTE IPV6 EN APLICACIONES DE USO COMÚN EN LA UNIVERSIDAD NACIONAL DE LOJA.				
#	***Descripción***	***Función***	***IPv4***	***Soporta IPv6 ?***
1	Mozilla Firefox 3.5	Navegador de Internet	Sí	***Sí***
2	Mozilla Thunderbird	Cliente de correo	Sí	***Sí***
3	Evolution	Cliente de coreo	Sí	***Sí***
4	Vlc 1.1	Reproductor multimedia	Sí	***Sí***
5	Google Chrome	Navegador de Internet	Sí	***Sí***
6	Internet Explorer 7.0	Navegador de Internet	Sí	***Sí***
7	Windows Media 9.0	Reproductor multimedia	Sí	***Sí***
8	Outlook Express	Cliente de correo	Sí	***Sí***
Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.* ***Fuente:*** *Unidad de Telecomunicaciones e Información.*				

Es necesario recordar que cuando se utiliza una dirección IPv6 para acceder a un recurso remoto (URI) se utiliza el formato http://[direccion-ipv6]:puerto, la dirección IPv6 debe estar encerrada por paréntesis cuadrados.

Por ejemplo: Para acceder a un sitio web, http://[2800:db8::1] sin dominio.

8.2.7. Servidores de la red de datos.

Los sistemas operativos que se utilizan para brindar servicios de Internet en la Universidad Nacional de Loja son distribuciones del SO Gnu / Linux Centos y Debian. Estos sistemas tienen soporte de IPv6 nativo desde hace muchos años, desde el año 2001 aproximadamente. En los sistemas Gnu / Linux a partir de kernel linux v. 2.6, con versiones muy estables por lo que no representan mayor inconveniente configurarlos.

Cada vez es más frecuente que diversas plataformas o sistemas operativos, no solo incorporen IPv6, sino que además es activado por defecto por el fabricante, sin requerir intervención alguna por parte del usuario.

8.2.8. Instalación mínima de la distribución Centos.

Lo recomendado, sobre todo si se trata de un servidor, es realizar una instalación con el mínimo de paquetes, desactivando todas las casillas para todos los grupos de paquetes, en el siguiente gráfico se aprecia la pantalla de instalación de Centos v. 5.4.

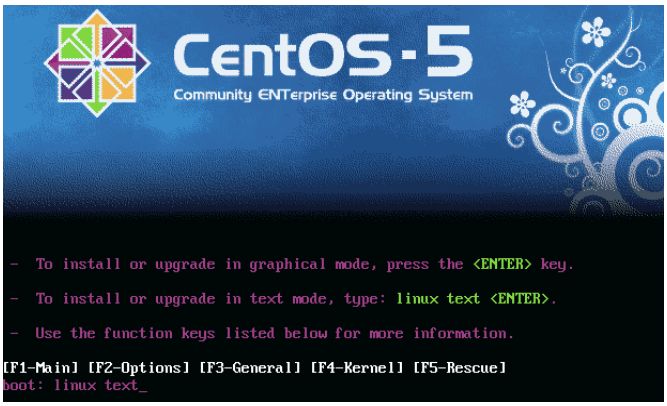


Figura 8.2.8: *Pantalla de inicio instalación Centos modo texto A.*

La idea es instalar lo mínimo necesario para el funcionamiento del sistema operativo Centos (solo paquetes netamente necesarios), y permitir instalar posteriormente solo aquello que realmente se requiera o sea necesario de acuerdo a la finalidad productiva que se le dará al sistema.

Figura 8.2.8: *Selección de los paquetes a instalar B.*

Una vez terminada la selección de los paquetes debemos seleccionar "Aceptar", este proceso tardará aproximadamente de 10 a 15 minutos dependiendo de la cantidad de paquetes, luego será necesario reiniciar el sistema (no olvidar extraer el CD/DVD o disco externo, etc).

Figura 8.2.8: *Finalización correcta instalación Centos v. 5.4.* C

Comprobar soporte de la dirección IPv6 en el sistema.

La distribución de Centos v. 5.4 incluye el soporte necesario para IPv6 en la versión del kernel linux 2.6. Para comprobar el soporte digitamos la siguiente sentencia en el sistema como súper usuario (root).

```
[root@ipv6 ~]# test -f /proc/net/if_inet6 && echo "Existe soporte IPv6 en el kernel de Centos"
Existe soporte IPv6 en el kernel de Centos
```

Si se presentase algún error al realizar el test, cargamos el módulo que nos brinda el soporte IPv6 necesario, de la siguiente manera:

```
[root@ipv6 ~]# modprobe ipv6
```

Una vez realizada la carga del módulo IPv6, lo comprobampos con el siguiente comando:

```
[root@ipv6 ~]# lsmod | grep -w 'ipv6' && echo "Módulo IPv6 cargado con éxito"
ipv6            267361  15 ip6t_REJECT
xfrm_nalgo          13381  1 ipv6
Módulo IPv6 cargado con éxito
```

Con los pasos anteriores se ha comprobado de la manera exitosa el soporte de IPv6 en el kernel Linux v. 2.6.18-164.el5 que incorpora la versión de Centos 5.4.

Ahora comprobamos la asignación de las direcciones IPv6 por default unicast de enlace local (link-local ***fe80:***) en donde podemos apreciar que el identificador de interfaz se genera automaticamente a partir de su dirección MAC (IEEE 802), siguiento el formato IEEE EUI-64.

```
[root@dnsdhcp ~]# ifconfig etho
etho   Link encap:Ethernet  HWaddr 00:12:79:55:8B:86
       inet addr:172.16.32.2  Bcast:172.16.63.255  Mask:255.255.224.0
       inet6 addr: fe80::212:79ff:fe55:8b86/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Comprobamos la conectividad a la dirección IPv6 de la interfaz eth0 (enlace local) usando el comando ¨***ping6***¨ y seguido la dirección IPv6.

```
[root@dnsdhcp ~]# ping6 -I eth0 -c 2 fe80::212:79ff:fe55:8b86
PING fe80::212:79ff:fe55:8b86(fe80::212:79ff:fe55:8b86) from fe80::212:79ff:fe55:8b86 eth0: 56
data bytes
64 bytes from fe80::212:79ff:fe55:8b86: icmp_seq=0 ttl=64 time=0.053 ms
64 bytes from fe80::212:79ff:fe55:8b86: icmp_seq=1 ttl=64 time=0.027 ms

--- fe80::212:79ff:fe55:8b86 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.027/0.040/0.053/0.013 ms, pipe 2
```

Adicionalmente verificamos la dirección de loopback IPv6 [***::1***] y seguidamente comprobamos conectividad.

```
[root@dnsdhcp ~]# ifconfig lo
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
[root@dnsdhcp ~]# ping6 -I lo -c 2 ::1
PING ::1(::1) from ::1 lo: 56 data bytes
64 bytes from ::1: icmp_seq=0 ttl=64 time=0.055 ms
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.025 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.025/0.040/0.055/0.015 ms, pipe 2
```

Cabe resaltar que cuando comprobamos la conectividad de la dirección IPv4 o IPv6, tanto en Windows como en Gnu / Linux se utiliza el comando [ping], pero para el caso de Gnu / Linux es necesario especificar la versión del protocolo con el comando [ping6], además agregar la opción necesaria [-I] que nos permite agregar la interfaz [eth0 o lo] como se mostró en los resultados anteriores.

Activar dirección IPv6 en el sistema operativo Centos.

El archivo [***/etc/sysconfig/network***] es usado para especificar información sobre la configuración de red deseada.

```
[root@dnsdhcp ~]# vim /etc/sysconfig/network
```

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6_AUTOCONF=no
HOSTNAME=dnsdhcp.unl.edu.ec
```

La directiva [***IPV6_AUTOCONF=no***] no habilita la autoconfiguración en los servidores, y la directiva [***NETWORKING_IPV6=yes***] habilita IPv6 en la interfaz.

Configurar la dirección IPv6 en el sistema Centos dual-stack.

En general no haremos autoconfiguración en los servidores, si no que vamos a especificar las direcciones IPv6 estáticas o hacerlo manualmente.

Ingresamos al archivo de configuración [/etc/sysconfig/network-scripts/ifcfg-eth0] de la interfaz deseada en nuestro caso [eth0] para agregar la dirección IPv6.

```
[root@dnsdhcp ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
BOOTPROTO=none
HWADDR=08:00:27:C6:F5:09

IPADDR=172.16.32.2
NETMASK=255.255.224.0
GATEWAY=172.16.63.250
NETWORK=172.16.32.0
BROADCAST=172.16.63.255

IPV6ADDR=2800:68:7:32:32::2/64
IPV6_DEFAULTGW=2800:68:7:32:32::1
IPV6INIT=yes
ONBOOT=yes
```

La directiva [***IPV6INIT=yes***] es para que arranque le módulo IPv6 al iniciar el sistema, la directiva [***IPV6ADDR=***] se pone la dirección IPv6 que se asignará en la interfaz y el parámetro [***IPV6_DEFAULTGW=***] permite especificar cual será la puerta de enlace IPv6. Luego de realizar los cambios pertinentes en los ficheros, es necesario reiniciar la interfaz de red de la siguiente forma:

```
[root@ipv6 ~]# service network restart
Interrupción de la interfaz eth0:                    [  OK  ]
Interrupción de la interfaz de loopback:             [  OK  ]
Activación de la interfaz de loopback:               [  OK  ]
Activando interfaz eth0:                             [  OK  ]
```

Verificamos que la interfaz [eth0] se agrego la dirección IPv6 [2800:68:7:32:32::2/64] esto se lo puede hacer de dos maneras y comprobamos conectividad a la misma interfaz.

```
root@ipv6 ~]# ifconfig eth0 | grep inet6
        inet6 addr: 2800:68:7:32:32::2/64 Scope:Global
        inet6 addr: fe80::a00:27ff:fe07:535c/64 Scope:Link
```

```
[root@ipv6 ~]# ip -6 addr show eth0 | grep inet6
   inet6 2800:68:7:32:32::2/64 scope global
   inet6 fe80::a00:27ff:fe07:535c/64 scope link
```

```
[root@ipv6 ~]# ping6 -I eth0 -c 2 2800:68:7:32:32::2
PING 2800:68:7:32:32::2(2800:68:7:32:32::2) from 2800:68:7:32:32::2 eth0: 56 data bytes
64 bytes from 2800:68:7:32:32::2: icmp_seq=0 ttl=64 time=0.094 ms
64 bytes from 2800:68:7:32:32::2: icmp_seq=1 ttl=64 time=0.115 ms

--- 2800:68:7:32:32::2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.094/0.104/0.115/0.014 ms, pipe 2
```

Configurar la dirección IPv6 en el sistema Debian dual-stack.

Para configurar una dirección IPv6 en el sistema Debian se debe añadir al archivo [/etc/network/interfaces] una nueva definición de interfaz la family ***inet6***, como se muestra a continuación:

```
dxlnx@machute:~$ sudo vim /etc/network/interfaces
```

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
      address 192.168.77.7
      netmask 255.255.255.0
      gateway 192.168.77.1

iface eth0 inet6 static
      address 2800:68:7:32:63::7
      netmask 64
     gateway 2800:68:7:32:32::7
```

Finalmente rreiniciamos la interfaz de red [eth0] para que surjan efecto los cambios hechos en el fichero de configuración, lo hacemos de esta forma:

```
dxlnx@machute:~$ sudo invoke-rc.d networking restart
```

Existe otra forma de agregar la dirección IPv6 de forma temporal, es decir cuando se reinicie la interfaz o el servidor se apague se perderá. La forma de hacerlo es la siguiente:

```
[root@ipv6 ~]# ip -6 addr add 2800:68:7:32:32::2/64 dev eth0
```

8.3. Procedimiento de Instalación y Configuración de Servicios de Internet en la Institución.

8.3.1. Sistema de nombres de dominio (dns).

Existen varios programas de servidor ¨dns¨ que soportan IPv6, los más usados, tanto en IPv4 como en IPv6, son "Bind" para diferentes plataformas (windows, Gnu / Linux, etc). Bind permite el uso indistinto de IPv4 e IPv6 como protocolo de comunicación para realizar consultas al servidor DNS. El protocolo utilizado es independiente del tipo de consulta realizada: se puede consultar con direcciones IPv4 utilizando IPv6 y viceversa.

Para la instalación se pueden utilizar los sistemas habituales de cada distribución Gnu / Linux (apt- get, yum, up2date, rpm, etc.) o descargarse los ficheros fuente desde http://www.isc.org y compilarlo, en nuestro caso haremos uso del paquete ***bind-9.8.0-P2.tar.gz***. La instalación del paquete ***bind*** se la realizó de la siguiente forma:

Descomprimir las fuentes del paquete bind-9.8.0-P2.tar.gz en un directorio.

```
[root@dnsdhcp bind]# tar -xvzf bind-9.8.0-P2.tar.gz
```

Ejecutar el script configure con los parámetros necesarios para verificar que se tienen todos las herramientas necesarias para compilar, permite conocer si existe un error de ser así tendríamos que solucionarlo antes de continuar. El script se ejecuta en el directorio donde descomprimimos las fuentes.

```
[root@dnsdhcp bind]# ./configure --prefix=/usr/local/bind --bindir=/bin --sbindir=/sbin –
sysconfdir=/etc/bind --mandir=/usr/share/man --enable-ipv6 --enable-filter-aaaa
```

Los parámetros principales [--sbindir=/sbin] le indicamos en que directorio instalar los archivos ejecutables para el dns y en el siguiente parámetro [–sysconfdir=/etc/bind] le decimos donde va estar el archivo de configuración principal es decir namef.conf y es el directorio donde ubicamos los archivos de zona de resolución directa en inversa para IPv4 e Ipv6. Una vez terminado procedemos a compilar y realizar la instalación.

```
[root@dnsdhcp bind]# make && make install
```

El fichero [/etc/bind/named.conf] el cual contiene la configuración principal del servidor DNS, será donde cambiaremos algunas directivas para el funcionamiento idóneo de Ipv6.

Partiendo de la instalación exitosa del paquete bind-9.8.0-P2.tar.gz mostraremos a continuación tres fases que se desarrollo en el DNS:

1. Habilitar el atender peticiones sobre IPv6, es decir escuchar IPv6 en el servidor de nombres de dominio (dns).
2. Asociar direcciones IPv6 a nombres de dominio unl.edu.ec es decir registros AAAA (quadA).
3. Resolución inversa de direcciones IPv6 a nombres de dominio unl.edu.ec registro PTR.

Habilitar peticiones IPv6.

Para habilitar correctamente las consultas DNS realizadas a la dirección IPv6 del servidor de nombres, se debe agregar las siguientes directivas en el archivo de configuración principal.

```
[root@dnsdhcp ~]# vim /etc/bind/named.conf

acl intranet6   {
      2800:68:7:32::/64;
      ::1/128;
};

options {
      directory "/etc/bind";
      listen-on port 53 { 127.0.0.1; 172.16.32.2; };
      allow-query { intranet; intranet6; };
      allow-recursion { intranet; intranet6; };
      listen-on-v6 port 53 { ::1; 2800:68:7:32:32::2; };
      query-source-v6 address 2800:68:7:32:32::2;
```

Las directivas [***listen-on-v6 port 53 {::1; 2800:68:7:32:32::2; };***] permite indicarle al servidor Dns en que puerto escuchar para recibir peticiones de clientes IPv6, y la directiva [***query-source-v6 address 2800:68:7:32:32::2;***] indica que puerto usar para las consultas de IPv6 desde el servidor, si no se especifica es aleatorio (recomendado por seguridad).

Comprobar que efectivamente está escuchando peticiones en la dirección IPv6 del servidor y el puerto [53] puerto [udp].

```
[root@dnsdhcp ~]# netstat -anutp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q  Local Address              Foreign Address          State      PID/Program
name
udp        0      0   2800:68:7:32:32::2:53     :::*                                3850/named
```

Resolución directa IPv6.

Respecto a la resolución de nombres a direcciones IPv6, existe el registro ***AAAA*** en el DNS. Todo servidor [dns] tiene lo que se llama ficheros de zona que contiene la información del servidor de nombres relacionada con un dominio. En nuestro caso específico el dominio es: "unl.edu.ec".

El archivo [/etc/named.conf] es donde se configuran las zonas (zone) de las que se encarga el servidor, declaramos la zona que se encuentra en el fichero [/etc/bind/named.unl.edu.ec] se cargue al iniciar el servicio DNS que será master (primario) para el dominio ¨ unl.edu.ec ¨.

```
zone "unl.edu.ec" IN {
      type master;
      file "named.unl.edu.ec";
};
```

Los ficheros de zona para resolución directa pueden contener registros con direcciones IPv4 e IPv6 a la vez. Editamos el fichero [/etc/bind/named.unl.edu.ec] y añadimos lo siguiente:

```
[root@dnsdhcp ~]# vim /etc/bind/named.unl.edu.ec
```

```
        IN      MX    10    webmail.unl.edu.ec.
        IN      MX    10    webmail6.unl.edu.ec.
fw              IN    A          172.16.32.1
fw6             IN    AAAA       2800:68:7:32:32::1
dnsdhcp         IN    A          172.16.32.2
dnsdhcp6        IN    AAAA       2800:68:7:32:32::2
dns             IN    CNAME      dnsdhcp
dns6            IN    CNAME      dnsdhcp6
dhcp            IN    A          172.16.32.4
dhcp6           IN    AAAA       2800:68:7:32:32::4
proxy           IN    A          172.16.32.13
proxy6          IN    AAAA       2800:68:7:32:32::13
v4              IN    A          172.16.63.7
v6              IN    AAAA       2800:68:7:32:63::7

unl.edu.ec.     IN    A          192.188.49.2
unl.edu.ec.     IN    AAAA       2800:68:7:49::2
www             IN    CNAME      unl.edu.ec.
www6            IN    CNAME      unl.edu.ec.
webmail         IN    A          192.188.49.20
webmail6        IN    AAAA       2800:68:7:49::20
```

Hemos configurado que:

1. [www6.unl.edu.ec] se resuelva solamente a una dirección IPv6 [***2800:68:7:32:49::2***] y así a todos los subdominios que terminen en ¨***6***¨ solo y a una única dirección IPv6.

Resolución inversa IPv6.

El registro empleado para resolución inversa de dirección IPv6 es ¨PTR¨ no es nuevo, es el mismo que se utiliza para la resolución inversa de direcciones IPv4 a nombres de dominio. La

diferencia con IPv6 viene en la notación utilizada para representar las direcciones IPv6 y en el nombre de dominio usado para ello [ip6.arpa]. Los ficheros de zona para resolución inversa de direcciones IPv6 contendrán solamente direcciones IPv6 como podra apreciarse en la siguiente configuración.

En el archivo de configuración principal del servidor Dns [/etc/named.conf] se declara la zona de resolución inversa para IPv6 correspondiente al prefijo de la Universidad Nacional de Loja [2800:68:7:32::/64] que hemos delegado para la intranet y servidores públicos el prefijo [2800:68:7:49::/64]. Añadimos lo siguiente a los ficheros de zona inversa.

```
zone "2.3.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa" IN {
      type master;
      file "named.2800.68.7.32";
};

zone "9.4.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa" IN {
      type master;
      file "named.2800.68.7.49";
};
```

Como se observa cada uno de los prefijos (2800:68:7:32::/64 y 2800:68:7:49::/64) se dividen en nibles y se concatenan en orden inverso para declarar las zonas al dominio [ip6.arpa]. Estas zonas permitirán la resolución inversa de las direcciones IPv6, cuyos ficheros son: [named.2800.68.7.32] y [named.2800.68.7.49]. A continuación se añaden las siguientes líneas.

```
[root@dnsdhcp ~]# vim /etc/bind/named.2800.68.7.32
```

```
1.0.0.0.0.0.0.0.0.0.0.0.0.2.3.0.0 IN     PTR    fw6.unl.edu.ec.
2.0.0.0.0.0.0.0.0.0.0.0.0.2.3.0.0 IN     PTR    dnsdhcp6.unl.edu.ec.
4.0.0.0.0.0.0.0.0.0.0.0.0.2.3.0.0 IN     PTR    dhcp6.unl.edu.ec.
3.1.0.0.0.0.0.0.0.0.0.0.0.2.3.0.0 IN     PTR    proxy6.unl.edu.ec.
7.0.0.0.0.0.0.0.0.0.0.0.0.3.6.0.0 IN     PTR    v6.unl.edu.ec.
```

```
[root@dnsdhcp ~]# vim /etc/bind/named.2800.68.7.49
```

```
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN     PTR    www6.unl.edu.ec.
0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN     PTR    webmail6.unl.edu.ec.
```

Lo que significa que:

- La dirección IPv6 [2800:68:7:49::2] resolverá al nombre de dominio [www6.unl.edu.ec] y así para el resto de direcciones IPv6 tanto de la intranet como de los servidores públicos.

Debemos recordar que después de realizar cualquier cambio en las directivas del archivo de configuración [/etc/bind/named.conf] o en los archivos de zona debemos reiniciar el demonio named de la siguiente forma.

```
[root@dnsdhcp ~]# /sbin/named
```

Seguidamente revisamos los sucesos que se generan en el fichero ¨log¨ [/var/log/messages] al iniciar o parar o reiniciar el demonio ¨named¨, esto nos permite verificar la correcta inicialización del DNS así como detectar posibles inconvenientes que se presenten.

```
[root@dnsdhcp ~]# tail -f /var/log/messages
May 14 21:37:30 dnsdhcp named[11910]: starting BIND 9.3.6-P1-RedHat-9.3.6-4.P1.el5 -u named
May 14 21:37:30 dnsdhcp named[11910]: using default UDP/IPv6 port range: [1024, 65535]
May 14 21:37:30 dnsdhcp named[11910]: listening on IPv6 interface lo, ::1#53
May 14 21:37:30 dnsdhcp named[11910]: listening on IPv6 interface eth0, 2800:68:7:32:32::2#53
May 14 21:37:30 dnsdhcp named[11910]: listening on IPv4 interface lo, 127.0.0.1#53
May 14 21:37:30 dnsdhcp named[11910]: listening on IPv4 interface eth0, 172.16.32.2#53

May 14 21:37:30 dnsdhcp named[11910]: zone 2.3.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa/IN: loaded serial 2011051489
May 14 21:37:30 dnsdhcp named[11910]: zone 9.4.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa/IN: loaded serial 2011051496
May 14 21:37:30 dnsdhcp named[11910]: zone unl.edu.ec/IN: loaded serial 2011051491
May 14 21:37:30 dnsdhcp named[11910]: zone 0.0.127.in-addr-arpa/IN: loaded serial 2011051487
May 14 21:37:30 dnsdhcp named[11910]: zone localhost/IN: loaded serial 2011051490
May 14 21:37:30 dnsdhcp named[11910]: running
```

Probando la configuración.

Para comprobar que los cambios se han aplicado y el servidor está escuchando en las direcciones IPv4 e IPv6 en el puerto del DNS [53] en los protocolos TCP y UDP, se lo hace de la siguiente manera:

```
[root@dnsdhcp ~]# netstat -anutp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 2800:68:7:32:32::2:53   :::*                    LISTEN      11910/named
tcp        0      0 ::1:53                  :::*                    LISTEN      11910/named
udp        0      0 2800:68:7:32:32::2:53   :::*                                11910/named
udp        0      0 ::1:53                  :::*                                11910/named
```

Desde el mismo servidor ejecutamos una consulta de resolución directa en IPv6 para el dominio [www6.unl.edu.ec], utilizando la aplicación "dig".

```
[root@dnsdhcp ~]# dig aaaa www6.unl.edu.ec
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5 <<>> aaaa www6.unl.edu.ec
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24997
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www6.unl.edu.ec.            IN      AAAA

;; ANSWER SECTION:
www6.unl.edu.ec.       86400   IN      CNAME   unl.edu.ec.
unl.edu.ec.            86400   IN      AAAA    2800:68:7:49::2

;; AUTHORITY SECTION:
unl.edu.ec.            86400   IN      NS      dnsdhcp.unl.edu.ec.

;; ADDITIONAL SECTION:
dnsdhcp.unl.edu.ec.    86400   IN      A       192.168.77.2
;; Query time: 4 msec
;; SERVER: 2800:68:7:32:32::2#53(2800:68:7:32:32::2)
;; WHEN: Sat May 14 22:01:29 2011
;; MSG SIZE  rcvd: 113
```

Para resolución inversa de la dirección IPv6 [2800:68:7:49::2], usamos la misma aplicación " dig" con el parámetro "-x" como puede apreciarse en la siguiente tabla:

```
[root@dnsdhcp ~]# dig -x 2800:68:7:49::2
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5 <<>> -x 2800:68:7:49::2
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2115
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.4.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.4.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa. 86400 IN PTR
www6.unl.edu.ec.

;; AUTHORITY SECTION:
9.4.0.0.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa. 86400 IN NS dnsdhcp.unl.edu.ec.

;; ADDITIONAL SECTION:
dnsdhcp.unl.edu.ec.    86400   IN     A      192.168.77.2
;; Query time: 11 msec
;; SERVER: 2800:68:7:32:32::2#53(2800:68:7:32:32::2)
;; WHEN: Sat May 14 22:03:39 2011
;; MSG SIZE  rcvd: 157
```

8.3.2. Protocolo de configuración dinámica de host versión 6 (dhcpv6).

Para que un sistema operativo pueda operar en doble-pila (IPv4 e IPv6), es importante que el kernel soporte IPv6 así como las herramientas necesarias para el funcionamiento del servicio, en este caso DHCPv6, cabe recalcar que la configuración del DHCPv4 es independiente de la configuración del servidor DHCPv6.

Como ya hemos mencionado, una de las características de IPv6 frente a IPv4 es la "a***uto configuración***", el proceso de auto configuración consiste en:

- La creación de una dirección de enlace local y comprobar su unicidad en el enlace.
- Determinar qué tipo de información se debe auto configurar (direcciones, otros datos o los dos).
- En el caso de direcciones, determinar qué mecanismo se debe usar para obtenerlas, con control de estado, sin él, o con ambos.

Auto configuración sin control de estado (Stateless).

Se utiliza el mecanismo "anuncios de encaminadores" (o "route advertisements"). Este mecanismo utiliza paquetes ICMPv6 y grupos de multicast locales a la interfaz. A través de este mecanismo se puede configurar la dirección IPv6, la longitud del prefijo y la ruta por

defecto. Sin embargo no es posible configurar elementos adicionales como pueden ser servidores de DNS, de WINS o incluso gateway SIP para la auto-configuración de un teléfono sobre IP. En caso de que no haya enrutadores en el enlace, los *hosts* pueden generar sus propias direcciones de enlace local utilizando el prefijo reservado para las direcciones locales de enlace [FE80::/64] . Estas direcciones le son suficientes para comunicarse entre sí en el enlace.

8.3.3. Auto configuración con control de estado (Stateful).

En este caso la configuración de la dirección IPv6 se hace a través de DHCPv6 igualmente que con IPv4. De esta forma es posible definir un pool de direcciones o incluso asignar direcciones particulares para cada terminal. Utilizando DHCPv6 en su configuración con estados es posible realizar un control de acceso más estricto. Un parámetro que no se obtiene aún (aunque hay trabajos en este sentido) por parte de DHCPv6 es la ruta por defecto. Por esto, aún cuando se utilizar DHCPv6 en modo con estados, es necesario utilizar el mecanismo de anuncio de encaminadores para obtener la ruta por defecto.

El intercambio de mensajes entre clientes y servidores se realiza mediante el protocolo UDP utilizando direcciones de *multicast*. El uso de direcciones *multicast* y no de *broadcast* en la configuración inicial es un detalle ventajoso que ofrece IPv6, haciendo más eficiente el trabajo del protocolo.

8.3.4. Proceso de configuración dinámica de los hosts con DHCPv6.

El proceso de configuración dinámica de los hosts en IPv6 (DHCPv6) ha sido estandarizado en la RFC 3315. Los conceptos básicos del esquema cliente-servidor del DHCPv6 son muy parecidos a los de DHCP para IPv4. A continuación se muestra un esquema representativo de este proceso:

Figura 8.3.4: *Esquema del funcionamiento de DHCPv6*

- Si existe un router en la red este manda un mensaje de RA con los bits "O" o "M" establecidos.
    1. Si el bit "O" está habilitado, pero no así el "M", los hosts podrán solicitar del DHCPv6 otros parámetros de configuración como servidores DNS, SIP, NTP, etc, y utilizar el proceso de auto configuración para establecer los parámetros de la red. Este mecanismo se conoce como "Configuración sin control de estado usando DHCPv6", porque el servidor DHCPv6 no necesita llevar un control de las direcciones IP de la red.
    2. Si el bit "M" está habilitado, los hosts pueden solicitar direcciones **M**anejadas por el servidor DHCPv6. Este se considera el mecanismo de "Configuración con control de estado usando DHCPv6".
- Si un host necesita localizar un servidor DHCPv6 envía un mensaje DHCPv6 "Solicitar" a la dirección multicast de todos los agentes de reenvío y servidores DHCPv6 del enlace [FF02::1:2].
- Los agentes y servidores DHCPv6 envían a la dirección multicast de todos los hosts [FF02::1] mensajes DHCPv6 "Anunciar" anunciando su funcionalidad como servidor DHCPv6.
- Los hosts interesados en recibir la configuración de un servidor DHCPv6 envían un mensaje "Petición" al servidor seleccionado.
- El servidor DHCPv6 le envía al host solicitante los parámetros de configuración solicitados.

8.3.5. Instalación y configuración del servicio de Internet DHCPv6.

Inicialmente vamos a especificar la interfaz [eth0] del servidor DHCPv6, el fichero que no permite hacer esta configuración es: /etc/sysconfig/dhcp6s.

```
DHCP6SIF=eth0
DHCP6SARGS=
```

Para realizar la instalación del servicio DHCPv6 hacemos uso del paquete dhcpv6-1.0.10-17.el5.i386.rpm en formato binario para la distribución centos, tal como se muestra a continuación.

```
[root@dnsdhcp dhcp]# rpm -ivh dhcpv6-1.0.10-17.el5.i386.rpm
advertencia:dhcpv6-1.0.10-17.el5.i386.rpm: CabeceraV3 DSA signature: NOKEY, key ID e8562897
Preparando...           ########################################### [100%]
   1:dhcpv6             ########################################### [100%]
[root@dnsdhcp dhcp]#
```

El fichero de configuración principal del DHCPv6 [/etc/dhcp6s.conf] el cual contiene las direcciones, prefijos y parámetros de configuración de la red para cada interfaz. Se muestra seguidamente como quedo el archivo de configuración, para la asignación de direcciones IPv6 (Stateful) hemos asignado un rango que desde la IP [2800:68:7:32:63::200] a [2800:68:7:32:63::255].

```
[root@dhcp6s ~]# vim /etc/dhcp6s.conf
```

```
interface eth0 {
    server-preference 255;
    renew-time 3600;
    rebind-time 3600;
    prefer-life-time 7200;
    valid-life-time 7200;
    allow rapid-commit;
    option dns_servers 2800:68:7:32:32::2 unl.edu.ec;
    link AAA {
        pool {
            range 2800:68:7:32:63::188 to 2800:68:7:32:63::199/64;
            prefix 2800:68:7:32::/64;
        };
    };
```

Indicamos el significado de cada una de las directivas puestas en el archivo de configuración DHCPv6:

[***interface***] Indica la interfaz a utilizar, es decir la ***eth0***.

[***server-preference***] La prioridad más alta del servidor, por lo general 255.

[***renew-time***] Se indica el tiempo de renovación de la direcciones IPv6 3600 (T1).

[***rebind-time***] Se indica el tiempo de restablecimiento de conexión 3600 (T2).

[***prefer-life-time***] Tiempo de vida preferido para cada dirección IPv6.

[***valid-life-time***] Tiempo de vida válido para cada dirección IPv6.

[***allow rapid-commit***] Permite habilitar al DHCPv6 para permitir una verificación rápida de los mensajes entre el cliente y las solicitudes de respuesta.

[***option dns_servers***] Se determinas direcciones de los servidores DNS.

[***link***] Permite configurar la asignación de pools, rangos y prefijos de direcciones IPv6.

[***pool***] Declara el pool de direcciones a utilizar para la asignación de prefijos.

[***range***] Se indica los rangos de direcciones (donde inicia y termina) que se van asignar.

[***prefix***] Especifica el prefijo de la subred.

Para la asignación de direcciones IPv6 especificas a un cliente (host), **DHCPv6** utiliza básicamente el mismo esquema que DHCPv4, pero hace que el ID de cliente sea obligatorio y le impone una estructura. El ID de cliente de DHCPv6 consta de dos partes: un Identificador único de DHCP [***DUID***] y un Identificador de identidad de asociación [***IAID***]. El DUID identifica el **sistema** cliente (no solo una interfaz, como en DHCPv4), y el IAID identifica la interfaz en ese sistema.

Tal como se describe en RFC 3315, una asociación de identidad es el método que utilizan el servidor y el cliente para identificar, agrupar y gestionar un conjunto de direcciones IPv6 relacionadas. Un cliente debe asociar al menos una asociación de identidad (IA) con cada una de sus interfaces de red, y a continuación utiliza las IA asignadas para obtener información de configuración de un servidor de esa interfaz.

A diferencia de DHCPv4, DHCPv6 no ofrece una opción de "nombre de cliente", así que no hay modo de asignar nombres a sus sistemas basándose únicamente en DHCPv6. Si necesita saber el nombre DNS que corresponde a una dirección proporcionada por DHCPv6, utilice la técnica de determinación inversa de DNS. El host que desea solicitar una dirección IPv6 debe tener un cliente DHCPv6; en la mayoría de Sistemas Operativos ya viene instalado el cliente.

Se detalla las directivas necesarias para hacer la asignación de una dirección IPv6 estática a un equipo en particular.

```
host dhcpv6cleinte {
        duid 00:01:00:01:15:88:24:d7:57:65:25:00:38:75;
        iaidinfo {
            iaid 850100261;
        };
        address {
            2800:68:7:32:63::77/64;
        };
    };
```

[***host***] Se indica la declaración para asignar una dirección IPv6 estática a un host.

[***duid***] Permite indicar un identificador único para el cliente DHCPv6.

[***iaidinfo***] Permite describir la información del IAID.

[***iaid***] Es un identificador de Asociación de Identidad, IA es una colección de direcciones asignadas a un cliente.

[***address***] Se indica la dirección IPv6 que asignaremos al host.

Una vez culminada la configuración del DHCPv6 iniciamos el proceso [***dhcp6s***] en el sistema de la siguiente forma:

```
[root@dhcp6s ~]# service dhcp6s start
Iniciando dhcp6s:                          [  OK  ]
```

Los puertos bien conocidos en el DHCPv6 es: el 547 que permite al servidor escuchar mensajes DHCP usando el protocolo UDP, mientras que el cliente DHCPv6 usa el puerto 546. Entonces vamos a comprobar que efectivamente se está escuchando peticiones en el servidor.

```
[root@dhcp6s ~]# netstat -anutp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address          State      PID/Program name
udp        0      0      :::547                    :::*                          2197/dhcp6s
```

Probando la asignación de direcciones IPv6 desde un cliente DHCPv6, utilizando como sistemas operativo centos obtenemos como resultado algo así:

```
[root@dhcp6c ~]# Jun/14/2011 23:02:42 dhcpv6 doesn't support hardware type 776
Jun/14/2011 23:02:42 doesn't support sito address family 0
Jun/14/2011 23:02:43 status code of this address is: 0 - success
Jun/14/2011 23:02:43 status code of this IA is: 0 - success
Jun/14/2011 23:02:43 duplicated address (2800:68:7:32:63::188/0)
Jun/14/2011 23:02:43  get  DNS address (2800:68:7:32:32::2)
Jun/14/2011 23:02:43 status code of IA: success
Jun/14/2011 23:02:43 assigned address 2800:68:7:32:63::188 prefix len is not in any RAs prefix
length using 64 bit instead
Jun/14/2011 23:02:43 renew time 3600, rebind time 3600
```

En el archivo [***/var/lib/dhcpv6/server6.leases***] que se encuentra alojado en el servidor DHCPv6 podemos apreciar las direcciones IPv6 asignadas a todos los clientes por ejemplo.

```
[root@dhcp6s ~]# vim /var/lib/dhcpv6/server6.leases
```

```
lease 2800:68:7:32:63::188/64 {
        DUID: 00:01:00:01:15:88:24:d7:57:65:25:00:38:75;
        IAID: 850100263        type: 0;
        RenewTime: 0;
        RebindTime: 0;
        state: 1;
        hostname: ;
        (start_date: 3 2011/6/15 4:2:59 UTC);
        start date: 1308110579;
        PreferredLifeTime: 7200;
        ValidLifeTime: 7200;
}
```

8.3.6. Protocolo de transferencia de hipertexto (http).

La navegación web utiliza el protocolo de transferencia de hipertextos (http), generalmente se utiliza el puerto 80 en TCP. Se basa en el modelo cliente-servidor por lo que se hace necesario ambos para establecer la comunicación.

El servidor web que se encuentra en producción en la Universidad Nacional de Loja, utiliza el programa "Apache" para ofrecer este servicio tanto en la Intranet como fuera de la misma. Veremos cómo realizar la instalación y configuración de ambas aplicaciones para que respondan a peticiones sobre IPv6.

El paquete [httpd-2.2.3-31.el5.centos.i386.rpm] es el más entendido de los servidores web actualmente y su entorno de ejecución son las distribuciones de Gnu / Linux. La instalación la realizamos de la siguiente manera:

```
[root@www http]# rpm -ivh httpd-2.2.3-31.el5.centos.i386.rpm
advertencia:httpd-2.2.3-31.el5.centos.i386.rpm: CabeceraV3 DSA signature: NOKEY, key ID
e8562897
Preparando...          ########################################### [100%]
   1:httpd             ########################################### [100%]
```

De la siguiente manera podemos apreciar el archivo de configuración principal del servidor web.

```
[root@www ~]# rpm -qc httpd-2.2.3-31.el5.centos
/etc/httpd/conf.d/proxy_ajp.conf
/etc/httpd/conf.d/welcome.conf
/etc/httpd/conf/httpd.conf
/etc/httpd/conf/magic
```

En el fichero [/etc/httpd/conf/httpd.conf] vamos a poder configurar las directivas necesarias para adaptarlo al servidor web, utilizando el mecanismo de transición doble-pila (IPv4 e IPv6) en un ambiente de producción.

Escuchar peticiones IPv6

A partir de la versión httpd 2.0.x el soporte IPv6 viene habilitado por defecto, así que después de la instalación solo hay que indicarle para que escuche por IPv6. Recordamos que previo a esta configuración deben estar asignados todos los parámetros de IPv6 en el servidor.

La directiva que controla las IPs y puertos por los que escucha el servidor web es: [***Listen***] y se encuentra en fichero [/etc/httpd/conf/httpd.conf].

```
[root@www ~]# vim /etc/httpd/conf/httpd.conf
```

```
Listen  127.0.0.1:80
Listen  192.188.49.2:80
Listen  192.188.49.9:80
Listen  [::1]:80
Listen  [2800:68:7:49::2]:80
Listen  [2800:68:7:49::9]:80
```

La directiva [Listen] ***[2800:68:7:49::2]:80*** permite establecer las direcciones IPv6 y puertos en los que el servidor web acepta peticiones entrantes, en el caso de la Universidad Nacional de Loja se utiliza el puerto "80" y está configurado dos direcciones IPv6.

Para comprobar que efectivamente el servidor web está escuchando por IPv6 en el puerto 80 podemos utilizar la siguiente sentencia.

```
[root@www ~]# netstat -anutp

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0       192.188.49.9:80          0.0.0.0:*              LISTEN      2280/httpd
tcp        0      0       192.188.49.2:80          0.0.0.0:*              LISTEN      2280/httpd
tcp        0      0       127.0.0.1:80             0.0.0.0:*              LISTEN      2280/httpd
tcp        0      0       2800:68:7:49::9:80          :::*                LISTEN      2280/httpd
tcp        0      0       2800:68:7:49::2:80          :::*                LISTEN      2280/httpd
tcp        0      0                ::1:80             :::*                LISTEN      2280/httpd
```

Como se puede apreciar el resultado indica que se está escuchando en las direcciones IPv4 e IPv6 establecidas previamente con la directiva [Listen].

Virtual host IPv6

Para tener múltiples dominios en el mismo servidor web, como es el caso de la Universidad se debe configurar hosts virtuales IPv6.

Iniciamos primero por establecer una dirección IPv6 adicional a la interfaz [eth0] del servidor, de la siguiente forma.

```
[root@www ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
IPV6ADDR=2800:68:7:49::2/64
IPV6ADDR_SECONDARIES=2800:68:7:49::9/64
IPV6_DEFAULTGW=2800:68:7:49::4
IPV6INIT=yes
ONBOOT=yes
```

Una vez que tenemos asignada la dirección IPv6, procedemos a realizar la configuración de los hosts virtuales basados en IPv6 para lo cual hay que utilizar ***[ ]*** para encerrar la dirección IPv6. Detallamos este proceso a continuación.

```
[root@www ~]# vim /etc/httpd/conf/httpd.conf
```

```
# Virtual Host basados en IPv4
<VirtualHost 192.188.49.9>
ServerAdmin soporte@unl.edu.ec
DocumentRoot "/var/www/html/vinculacion"
ServerName vinculacion.unl.edu.ec
</VirtualHost>

# Virtual Host basado en IPv6
<VirtualHost [2800:68:7:49::9]>
ServerAdmin soporte@unl.edu.ec
DocumentRoot "/var/www/html/vinculacion"
ServerName vinculacion6.unl.edu.ec
</VirtualHost>
```

La configuración que realizamos permite al servidor web:

- Atender peticiones sobre IPv4 a la dirección 192.188.49.2 y sobre IPv6 a la dirección [2800:68:7:49::9].
- Las peticiones recibidas a esas direcciones se distinguen por la URL a la que van dirigidas es decir:
  - Las peticiones a vinculacion.unl.edu.ec se atienden por IPv4 sirviendo el contenido de la carpeta /var/www/html/vinculacion. Mientras que las peticiones a vinculacion6.unl.edu.ec se atienden por IPv6, sirviendo el contenido de la misma carpeta.

Adicionalmente agregamos una configuración de hosts virtuales basados en nombres IPv6, que a diferencia de virtual host basados en IPv6 podemos tener la misma IPv6 con diferentes subdominios (URLs) sirviendo el contenido de diferentes carpetas.

```
# Virtual Host basado en nombres IPv6

NameVirtualHost [2800:68:7:49::8]

<VirtualHost [2800:68:7:49::8]>
ServerAdmin soporte@unl.edu.ec
DocumentRoot "/opt/lampp/htdocs/cinfa"
ServerName cinfa6.unl.edu.ec
</VirtualHost>

<VirtualHost [2800:68:7:49::8]>
ServerAdmin soporte@unl.edu.ec
DocumentRoot "/opt/lampp/htdocs/idrisi"
ServerName idirisi6.unl.edu.ec
</VirtualHost>
```

La directiva [NameVirtualHost] permite usar virtual host basado en nombres, para la dirección IPv6 [2800:68:7:49::8] existiendo previamente un ***Listen*** para dicha dirección.

Para la resolución de los subdominios [cinfa6.unl.edu.ec] y [idrisi6.unl.edu.ec] a la dirección IPv6 [2800:68:7:49::8] realizamos la configuración pertinente en el servidor DNS generando un nombre canónico para idrisi6 cuyo registro es CNAME a cinfa6. Como se lo puede apreciar en el siguiente cuadro tanto para resolución directa como inversa.

```
cinfa6     IN    AAAA     2800:68:7:49::8
idrisi6    IN    CNAME    cinfa6
```

```
8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0     IN    PTR    cinfa6.unl.edu.ec.
```

Una vez finalizada la configuración en el fichero principal [/etc/httpd/conf/httpd.conf] del servidor web, procedemos a iniciar el proceso en modo background httpd con la siguiente sentencia.

```
[root@www ~]# service httpd start
Iniciando httpd:                          [  OK  ]
```

8.3.7. Servidor Proxy (squid) IPv6.

Squid es un programa que permite dar la funcionalidad a un servidor de Proxy, actualmente es el más popular y extendido entre los sistemas operativos basados en Gnu / Linux (Centos,

debian, etc), en nuestro caso usaremos Centos como sistema base para correr squid. La Universidad cuenta con algunos servidores que hacen de "proxy" sobre IPv4, por lo que se hace necesaria la activación de IPv6 en dichos servidores en un ambiente de producción, usando el mecanismo de transición doble-pila.

Para la instalación de squid disponemos del paquete [squid-3.1.8-1.el5.i386.rpm] el cual está disponible como un binario "rpm" el viene con soporte nativo (defaut) de IPv6, esta versión de squid detecta el tipo de pila (IPv4 o IPv4) que están usando los clientes. La instalación se la indica a continuación.

```
[root@proxy squid]# rpm -ivh squid-3.1.8-1.el5.i386.rpm
Preparando...          ########################################### [100%]
   1:squid             ########################################### [100%]
```

Configuración y Activación de IPv6 en Squid

El fichero de configuración principal de squid [/etc/httpd/conf.d/squid.conf] nos permite adecuar el servicio de Internet Proxy afines a los requerimientos institucionales.

```
[root@proxy ~]# rpm -qc squid-3.1.8-1.el5
/etc/httpd/conf.d/squid.conf
/etc/logrotate.d/squid
```

Seguidamente ingresamos desde un terminal a archivo de configuración para iniciar la configuración de las directivas necesarias.

```
[root@proxy ~]# vim /etc/squid/squid.conf
```

Escuchar peticiones Proxy IPv6.

Vamos indicar a squid para habilitar la escucha de peticiones en doble-pila (IPv4 y IPv6) y también definir el puerto de escucha.

```
# Puerto de escucha servidor proxy IPv4 e IPv6
http_port 127.0.0.1:8080
http_port 172.16.32.13:8080
http_port [::1]:8080
http_port [2800:68:7:32:32::13]:8080
```

La direcctiva [http_port] nos permite indicar la dirección IPv6 [2800:68:7:32:32::13] y el puerto [8080] en el cual se van a tender las peticiones http por parte de los clientes es decir de toda la subred [2800:68:7:32::/64].

Para comprobar que efectivamente el servidor proxy está escuchando por IPv6 en el puerto 8080 podemos utilizar la siguiente sentencia.

```
[root@proxy ~]# netstat -anutp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0  172.16.32.13:8080     0.0.0.0:*              LISTEN     7948/(squid)
tcp        0      0  127.0.0.1:8080        0.0.0.0:*              LISTEN     7948/(squid)
tcp        0      0  2800:68:7:32:32::13:8080   :::*             LISTEN     7948/(squid)
tcp        0      0  ::1:8080              :::*                   LISTEN     7948/(squid)
```

El resultado obtenido indica que se está escuchando en las direcciones IPv4 e IPv6 establecidas previamente con la directiva [http_port].

Listas de control de acceso IPv6

Las listas de control de acceso nos permite definir las subredes IPv4 e IPv6, de las cuales squid aceptara o negara el tráfico. Iniciamos por definir la ACL que coincida con el tráfico de la maquina local.

```
acl localhost src 127.0.0.1/32
acl localhost6 src ::1/128
```

Aquí definimos la [acl] de nombres [localhost6] y el tipo de acl [src] que especifica la dirección de origen de una conexión en el formato ipv6/prefijo [::1/128].

Seguidamente se indica a squid por medio de una ACL toda la subred IPv6, incorporando el Id de subred IPv6 y la longitud del prefijo.

```
# Lista de subredes IPv4 e IPv6, que se les permite la navegación
acl redunlipv4 src 172.16.32.0/19          # Red intranet IPv4 Universidad
acl redunlipv6 src 2800:68:7:32::/64       # Red intranet IPv6 Universidad
```

Estamos declarando un acl de nombre [redunlipv6] cuyo origen es la subred IPv6 [2800:68:7:32::/64], que corresponde a la intranet IPv6 de la Universidad Nacional de Loja.

Ahora vamos a definir el tipo de política a utilizar: permitir o denegar el acceso en función de las ACLs definidas anteriormente. Mostramos a continuación las reglas que se definieron.

```
# Permite acceso a las subredes de la intranet Universitaria IPv4 e IPv6
http_access allow localhost
http_access allow redunlipv4
http_access allow localhost6
http_access allow redunlipv6
```

Estamos permitiendo el acceso a realizar peticiones al servidor proxy, cuyas ACLs de nombres: [localhost6] que corresponde a la dirección IPv6 [::1/128] y [redunlipv6] es decir la subred IPv6 [2800:68:7:32::/64], cuyas reglas nos permiten saber quiénes exactamente están consultando nuestro servidor proxy.

Adicionalmente en squid también se puede bloquear el tráfico IPv6, pero en nuestro caso no lo estamos haciendo, pero dejamos un precedente de como se lo pude hacer. Les sugerimos ver el siguiente ejemplo:

```
acl to_ipv6 dst ipv6
http_access deny to_ipv6
```

Aquí vemos una [acl] de nombre [to_ipv6] cuyo parámetro [dst] permite especificar una dirección destino de una conexión en formato: ipv6/prefijo, y posteriormente aplicamos una regla de denegar la ACL ***to_ipv6***.

Una vez finalizado el proceso de configuración en el fichero principal [/etc/squid/squid.conf] del servidor proxy, procedemos a iniciar el servicio en modo background squid.

```
[root@proxy ~]# service squid start
Iniciando squid: .                    [  OK  ]
```

El archivo log [/var/log/squid/cache.log] se puede apreciar que a iniciado de manera exitosa el servicio de squid, le mostramos una parte del log de la siguiente manera.

```
[root@proxy ~]# tail -f /var/log/squid/cache.log
2011/06/19 13:58:11| Accepting  HTTP connections at 127.0.0.1:8080, FD 17.
2011/06/19 13:58:11| Accepting  HTTP connections at 172.16.32.13:8080, FD 18.
2011/06/19 13:58:11| Accepting  HTTP connections at [::1]:8080, FD 19.
2011/06/19 13:58:11| Accepting  HTTP connections at [2800:68:7:32:32::13]:8080, FD 20.
```

Servicio de correo electrónico sobre IPv6.

El servicio de email o correo electrónico es uno de los más utilizados. Generalmente utiliza los puertos por defecto: protocolo smtp (puerto 25) para enviar los mensajes de correo, y pop3 (puerto 110) o imap (puerto 143) para obtener los mensajes. El servicio se basa en el modelo cliente-servidor por lo que se requiere ambos para establecer la comunicación. Para trabajar en doble-pila (IPv4 e IPv6) se requiere que las aplicaciones que corren en el servidor y los clientes de correo soporten IPv6.

Instalación y configuración Smtp IPv6.

Utilizaremos el paquete sendmail-8.13.8-2.el5 (smtp) para envió de mensajes de correo el cual viene con soporte nativo para el nuevo protocolo de Internet (IPv6). Sendmail es una de las aplicaciones más populares de servidor SMTP que corre en ambientes de Gnu / Linux.

El proceso de instalación los describimos a continuación para la distribución de Centos v. 5.4, el paquete binario de sendmail es un .rpm.

```
[root@webmail sendmail]# rpm -iUh sendmail-8.13.8-2.el5.i386.rpm
advertencia:sendmail-8.13.8-2.el5.i386.rpm: CabeceraV3 DSA signature: NOKEY, key ID e8562897
########################################### [100%]
el paquete sendmail-8.13.8-2.el5.i386 ya está instalado
```

```
[root@webmail sendmail]# rpm -iUh sendmail-cf-8.13.8-2.el5.i386.rpm
advertencia:sendmail-cf-8.13.8-2.el5.i386.rpm: CabeceraV3 DSA signature: NOKEY, key ID e8562897
########################################### [100%]
########################################### [100%]
```

La instalación se realiza con todo éxito, sin ser necesario instalar dependencias en el server de correo que se encuentra en un estado de producción en la Universidad. Para saber los ficheros de configuración principal del servidor smtp, ejecutamos la sentencia.

```
[root@webmail mail]# vim /etc/mail/sendmail.mc
```

```
[root@webmail ~]# rpm -qc sendmail-8.13.8-2.el5
/etc/mail/Makefile
/etc/mail/access
/etc/mail/sendmail.cf
/etc/mail/sendmail.mc
/etc/mail/submit.cf
/etc/mail/submit.mc
```

Habilitar IPv6 en sendmail.

Sendmail no viene habilitado IPv6 por defecto (por lo menos hasta la versión 8.13.8). Para habilitar el soporte IPv6 debemos aplicar las directivas necesarias en el fichero de configuración principal [/etc/mail/sendmail.mc] para que funcione IPv6, se configura los Agentes de Transferencia de Correo (MTA) de la siguiente forma.

```
dnl # Habilitar escuchar peticiones SMTP para IPv4
DAEMON_OPTIONS(`Port=25, Addr=127.0.0.1, Name=MTA-v4, Family=inet')dnl
DAEMON_OPTIONS(`Port=25, Addr=172.16.49.20, Name=MTA-v4, Family=inet')dnl

dnl # Habilitar escuchar peticiones SMTP para IPv6
DAEMON_OPTIONS(`Port=25, Addr=::1, Name=MTA-v6, Family=inet6')dnl
DAEMON_OPTIONS(`Port=25, Addr=2800:68:7:32:49::20, Name=MTA-v6, Family=inet6')dnl
```

La directiva [DAEMON_OPTIONS] cuyo parámetro [Addr] nos permite adaptar sendmail para escuchar peticiones en una dirección especifica en el caso de IPv6 solo para [2800:68:7:32:49::20], al colocar esta directiva se crea dos listener para el mismo proceso sendmail, uno para la familia [inet] (IPv4) y otro para la familia [***inet6***] (IPv6).

En el servidor de correo de producción en la Universidad, se opto por escuchar peticiones en direcciones específicas tanto, es decir para localhost y una dirección en IPv4 e IPv6.

Finalizada la configuración en el fichero [/etc/mail/sendmail.mc] es necesario generar el fichero [/etc/mail/sendmail.cf] con la herramienta ***m4***.

```
[root@webmail mail]# m4 sendmail.mc > sendmail.cf
```

Una vez generado el fichero procedemos a iniciar el proceso sendmail (demonio del sistema) para correr las configuraciones previamente establecidas.

```
[root@webmail mail]# service sendmail start
Iniciando sendmail:                        [  OK  ]
Inicio de sm-client:                       [  OK  ]
```

Para comprobar que efectivamente el servidor smtp está escuchando por IPv6 en el puerto 25 podemos utilizar la siguiente sentencia.

```
[root@webmail mail]# netstat -anutp

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0  172.16.49.20:25        0.0.0.0:*               LISTEN      7232/sendmail: acce
tcp        0      0  127.0.0.1:25           0.0.0.0:*               LISTEN      7232/sendmail: acce
tcp        0      0  2800:68:7:32:49::20:25 :::*                    LISTEN      7232/sendmail: acce
tcp        0      0  ::1:25                 :::*                    LISTEN      7232/sendmail: acce
```

Obtener correo electrónico (dovecot) IPv6.

Para obtener mensajes de correo almacenados en el servidor, utilizaremos el paquete dovecot v. 1.0.7 el cual permite activar el servicio de pop3 (protocolo de la oficina de correo) en el puerto ***110*** e imap (Internet message access protocol) en puerto 143, nos enfocaremos un poco más al protocolo IMAP, ya que cuenta con varias ventajas frente a POP3. Por ejemplo: IMAP permite especificar carpetas en el lado de Servidor.

Actualmente todas las aplicaciones de POP3 e IMAP tanto para el lado del servidor como el lado del cliente están virtualmente soportados. En lado del cliente para obtener correo utilizaremos Thunderbird (aplicación cliente de correo) y squirrelmail (visualizar correos vía web), estas aplicaciones cliente las veremos más adelante con más detalle.

En nuestro caso disponemos de un fichero binario [dovecot-1.0.7-7.el5.i386.rpm] .rpm para la instalación de dovecot en el servidor de producción Centos v. 5.4 de la Universidad, listamos a continuación el proceso de instalación.

```
[root@webmail dovecot]# rpm -ivh dovecot-1.0.7-7.el5.i386.rpm

advertencia:dovecot-1.0.7-7.el5.i386.rpm: CabeceraV3 DSA signature: NOKEY, key ID e8562897
Preparando...          ########################################### [100%]
1:dovecot              ########################################### [100%]
```

La instalación de dovecot no fue necesario instalar ninguna dependencia de paquetes previamente. Para conocer los ficheros de configuración principal ejecutamos desde un terminal del servidor IMAP lo siguiente.

```
[root@webmail mail]# rpm -qc dovecot-1.0.7-7.el5
/etc/dovecot.conf
/etc/pam.d/dovecot
```

El fichero configuración principal [/etc/dovecot.conf] se configura IPv6 en los protocolos pop3 e imap.

Habilitar IPv6 en dovecot.

Las activación de IPv4 e IPv6 en dovecot tanto para POP3 e IMAP son similares, de modo que si estamos utilizando los valores por defecto y se está a la escucha de cualquier dirección disponible, se activa IPv6 en dovecot tras reiniciarse, previo a la habilitación de IPv6 en el Sistemas Operativo.

Dado que en dovecot v. 1.0.7 no es posible especificar varias direcciones IPv4 e IPv6, optamos por utilizar el parámetro **[::]** que lo detallamos a continuación.

```
[root@webmail mail]# vim /etc/dovecot.conf

    protocol imap {
        listen = [::]:143
    }
    protocol pop3 {
        listen = [::]:110
        }
```

Utilizamos la directiva ***listen*** para indicar la escucha de la peticiones en el servidor, con el parámetro [::]:143 y [::]:110 indicamos al servidor que escuche peticiones en todas las interfaces de IPv6 disponibles, en el caso de la Universidad solo existe una interfaz configurada con la dirección IPv6 [2800:68:7:32:49::20]. Con los mismo parámetros de la directiva ***listen*** también se puede escuchar en todas las interfaces IPv4.

Una vez finalizada la configuración para POP3 e IMAP procedemos a iniciar el proceso dovecot en el sistema, como se puede apreciarse.

```
[root@webmail mail]# service dovecot start
Iniciando Dovecot Imap:                    [  OK  ]
```

Después de un inicio satisfactorio de dovecot verificamos que efectivamente se esta escuchando en IPv6 tanto para POP3 (puerto 110) e IMAP (puerto 143).

```
[root@webmail mail]# netstat -anutp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address          State      PID/Program name
tcp        0      0      :::110                  :::*                LISTEN     7707/dovecot
tcp        0      0      :::143                  :::*                LISTEN     7707/dovecot
```

Squirrelmail, cliente de correo IPv6.

Squirrelmail es un webmail, es decir un cliente de correo electrónico, el cual provee una interfaz accesible vía web con el fin de acceder a los mensajes de correo, en el caso de la Universidad Nacional de Loja se utiliza squirrelmail en el servidor de correo, que se encuentra en producción desde donde podemos ingresar, leer, enviar, borrar, etc mensajes de correo vía web.

A demás de ser accesible en IPv4 [http://webmail.unl.edu.ec] realizaremos la implementación necesaria para disponer de acceso vía IPv6 utilizando el subdominio [***http://webmail6.unl.edu.ec***]. La instalación del paquete binario .rpm [squirrelmail-1.4.8-5.el5.centos.7] se realizó en la distribución Centos v. 5.4 la cual detallamos a continuación.

```
[root@webmail squirrelmail]# rpm -ivh squirrelmail-1.4.8-5.el5.centos.7.noarch.rpm
advertencia:squirrelmail-1.4.8-5.el5.centos.7.noarch.rpm: CabeceraV3 DSA signature: NOKEY,
key ID e8562897
Preparando...          ########################################### [100%]
1:squirrelmail         ########################################### [100%]
```

Instalando squirrelmail los directorios y ficheros principales (config, images, plugins, themes, etc) se ubican en [/usr/share/squirrelmail/].

Habilitar IPv6 en squirrelmail.

El fichero de configuración principal [/etc/squirrelmail/config.php] de squirrelmail desde el cual activaremos IPv6, squirrelmail utiliza IMAP (puerto 143) para obtener los mensajes de correo y SMTP (puerto 25) para enviar los mensajes de correo. Estos protocolo son

transparentes para el usuario final, el usuario final solo interactúa con la interfaz web de squirrelmail que será accesible a a través de un subdominio [http://webmail6.unl.edu.ec].

La activación IPv6 en squirrelmail en el servidor de producción de la Universidad Nacional de Loja, tanto para IMAP como para SMTP la mostramos a continuación.

```
[root@webmail ~]# vim /etc/squirrelmail/config.php
$domain                 = 'unl.edu.ec';
$imapServerAddress      = '[2800:68:7:32:49::20]';
$imapPort               = 143;
$useSendmail            = true;
$smtpServerAddress      = '[2800:68:7:32:49::20]';
$smtpPort               = 25;
$sendmail_path          = '/usr/sbin/sendmail';
$sendmail_args          = '-i -t';
$pop_before_smtp        = false;
$imap_server_type       = 'uw';
```

De esta manera estamos indicando a squirrelmail cual es la dirección IPv6 de IMAP y SMTP en este caso coincide que es la misma dirección [2800:68:7:32:49::20], porque se encuentra en el mismo servidor.

Para poder acceder a la dirección [http://webmail6.unl.edu.ec] debemos activar el servicio web instalando el paquete binario httpd-2.2.3-31.el5.centos.i386.rpm cuyo fichero principal de configuración es: [/etc/httpd/conf/httpd.conf], donde activaremos IPv6 para receptar peticiones con la directiva [Listen] a la dirección IPv6 [2800:68:7:32:49::20], usando el puerto 80 por defecto del protocolo http, esto lo realizamos de la siguiente manera.

```
[root@webmail ~]# vim /etc/httpd/conf/httpd.conf
```

```
# Escuchar peticiones Squirrelmail - Webmail IPv6
Listen  127.0.0.1:80
Listen  172.16.49.20:80

# Escuchar peticiones Squirrelmail - Webmail IPv6
Listen  [::1]:80
Listen  [2800:68:7:32:49::20]:80
```

Adicionalmente debemos agregar un registro quad A (AAAA) en el servicio de Internet DNS indicando el subdominio [webmail6.unl.edu.ec] y la dirección IPv6 [2800:68:7:32:49::20],

realizamos la configuración tanto para resolución directa como inversa; seguidamente agregamos nombres canónicos con el registro CNAME para [smtp6.unl.edu.ec] e [imap6.unl.edu.ec]. Esto lo podemos apreciar a continuación.

```
[root@dnsdhcp ~]# vim /etc/bind/named.unl.edu.ec

webmail6    IN    AAAA     2800:68:7:32:49::20
smtp6       IN    CNAME    webmail6
imap6       IN    CNAME    webmail6
```

Una vez finalizado el proceso de configuración en el servidor de correo electrónico procedemos a iniciar todos los procesos: sendmail, dovecot, httpd.

```
[root@webmail ~]# service sendmail start
Iniciando sendmail:                    [  OK  ]
Inicio de sm-client:                   [  OK  ]
```

```
[root@webmail ~]# service dovecot start
Iniciando Dovecot Imap:                [  OK  ]
```

```
[root@webmail ~]# service httpd start
Iniciando httpd:                       [  OK  ]
```

Finalmente verificamos el [***log***] del servidor de correo, utilizando squirrelmail para leer los mensajes de correo y enviar, como se lo aprecia seguidamente.

```
[root@webmail ~]# tail -f /var/log/maillog
```

```
Jun 25 08:29:40 webmail dovecot: imap-login: Login: user=<ipv6>, method=PLAIN, rip=2800:68:7:32:49::20,
lip=2800:68:7:32:49::20, secured
Jun 25 08:29:40 webmail dovecot: IMAP(ipv6): Disconnected: Logged out
Jun 25 08:30:00 webmail sendmail[2823]: p5PDTtrf002823: from=<ipv6@unl.edu.ec>, size=777, class=0,
nrcpts=1, msgid=<34235.2800:68:7:32:63::7.1309008595.squirrel@webmail6.unl.edu.ec>, proto=ESMTP,
daemon=MTA-v4, relay=localhost [127.0.0.1]
Jun 25 08:30:00 webmail sendmail[2822]: p5PDTtDs002822: to=jcalderon@unl.edu.ec, ctladdr=ipv6@unl.edu.ec
(48/48), delay=00:00:05, xdelay=00:00:05, mailer=relay, pri=30553, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0,
stat=Sent (p5PDTtrf002823 Message accepted for delivery)
Jun 25 08:30:00 webmail sendmail[2824]: p5PDTtrf002823: to=<jcalderon@unl.edu.ec>,
ctladdr=<ipv6@unl.edu.ec> (502/502), delay=00:00:00, xdelay=00:00:00, mailer=local, pri=31009, dsn=2.0.0,
stat=Sent
```

Al momento de iniciar sesión en squirrelmail vía web [http://webmail6.unl.edu.ec], podemos ver en el log que hay un parámetro ***rip*** y ***lip*** que hace referencia a la misma dirección IPv6, esto se da porque el servicio de IMAP y HTTP están implementados en el mismo servidor de correo.

8.3.8. Acceso remoto SSH IPv6.

El acceso remoto SSH es uno de los servicios para utilizados por el personal de la Sección de Redes y Equipos Informáticos para llevar a cabo las tareas de administración de los servidores en producción. SSH sustituye a telnet cuando es necesaria la comunicación segura.

El servicio de SSH se encuentra funcionando en todos los servidores sobre IPv4, para lo cual realizamos las adecuaciones necesarias para activar IPv6 en SSH.

Habilitar IPv6 en SSH.

Necesitamos conocer cuál es el fichero de configuración principal ejecutando la siguiente sentencia en el servidor que se requiere activar IPv6.

```
[root@dnsdhcp ~]# rpm -qc openssh-server-4.3p2-36.el5
/etc/pam.d/sshd
/etc/ssh/sshd_config
```

El fichero [/etc/ssh/sshd_config] es el cual efectuaremos los cambios para escuchar peticiones SSH IPv6 para una dirección específica.

```
[root@dnsdhcp ~]# vim /etc/ssh/sshd_config
```

```
# Activar IPv6
ListenAddress [2800:68:7:77::2]:7121
```

La directiva [ListenAddress] le indicamos la dirección IPv6 del servidor la cual la ubicamos entre corchetes y seguidamente establecemos el puerto de escucha.

Una vez efectuados los cambios necesarios iniciamos el servicio sshd y finalmente verificamos si realmente está escuchando en IPv6.

```
[root@dnsdhcp ~]# service sshd start
Iniciando sshd:                                [  OK  ]
```

```
[root@dnsdhcp ~]# netstat -anutp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0  2800:68:7:77::2:7121  :::*                    LISTEN      2545/sshd
tcp        0      0  2800:68:7:77::2:7121  2800:68:7:77::7:55420   ESTABLISHED 2148/0
```

Como se puede apreciar el servidor está escuchando peticiones en IPv6 e incluso se encuentra una conexión establecida desde la dirección IPv6 [2800:68:7:77::7].

Nota: El servicio de acceso remoto utilizando SSH se activa en todos los servidores que se encuentran en producción, tanto en el Intranet como públicos.

8.3.9. Firewall IPv6 en los Diferentes Servicios de Internet.

La herramienta utilizada a nivel de software para levantar el firewall IPv6 en los servicios de Internet (dns, dhcp, proxy, router, http, smtp, pop, imap, etc) es: ***ip6tables*** que viene preinstalado en la distribución Centos v. 5.4, ip6tables incluye un módulo que permite a los administradores de red inspeccionar y restringir conexiones a servicios disponibles en una red IPv6.

En ip6tables, las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes IPv6. Existen tres cadenas básicas INPUT (entrada), OUTPUT (salida) y FORWARD (reenvío), el administrador puede crear tantas como desee.

La tabla filter o tabla de filtros, es la tabla que usaremos para aplicar la mayoría de las políticas de seguridad para un servicio previamente definido. Dicha tabla es la responsable del filtrado (es decir, de bloquear o permitir que un paquete IPv6 continué su camino).

Una breve descripción de las cadenas que utilizaremos para levantar un firewall IPv6.

- Cadena INPUT, nos indica que todos los paquetes IPv6 destinados a este sistema atraviesan esta cadena.
- Cadena OUTPUT, nos indica que todos los paquetes IPv6 creados por este sistema

atraviesan esta cadena.

- Cadena FORWARD, nos indica que todos los paquetes IPv6 que meramente pasan por este sistema para ser encaminados a su destino recorren esta cadena.

Las reglas de ip6tables se crean siguiendo las políticas de seguridad lógicas de la Unidad de Telecomunicaciones e Información, Sección Redes y Equipos Informáticos.

A continuación ilustramos, el formato que siguen todas las reglas ip6tables aplicadas en los diferentes servicios de Internet.

ip6tables [-t tabla] {-A|-D} cadena especificación-regla [opciones...]

Las mencionamos de una manera generalizada, es decir no vamos a repetir algunas reglas ip6tables que prácticamente se aplicarían a cualquier servicio de Internet, por ejemplo las reglas de ::1(localhost6).

Iniciamos el proceso de aplicar las políticas de seguridad firewall ip6tables, vale mencionar que solo utilizaremos la tabla [filter], la cual se la puede incluir en la regla o no puesto que se la reconoce por defecto. En nuestro caso la incluiremos para un mejor aprendizaje.

```
[root@fw ~]# ip6tables -t filter -F
[root@fw ~]# ip6tables -t filter -Z
[root@fw ~]# ip6tables -t filter –X
```

Eliminar todas la reglas que previamente existen en la tabla filter, el significado de: [-f] borrar las reglas una por una, [-Z] poner a cero los contadores de bytes y paquetes en todas las cadenas y [-X] elimina alguna cadena opcional definida por el administrador de la red o del sistema.

```
[root@fw ~]# ip6tables -t filter -P INPUT DROP
[root@fw ~]# ip6tables -t filter -P OUTPUT DROP
[root@fw ~]# ip6tables -t filter -P FORWARD DROP
```

Definimos la política por defecto para cada una de la cadena de la tabla filter con el parámetro [-P] indicamos la cadena y seguidamente el destino de la regla en este caso DROP (descartar).

```
[root@fw ~]# ip6tables -t filter -A INPUT -i lo -j ACCEPT
[root@fw ~]# ip6tables -t filter -A OUTPUT -o lo -j ACCEPT
```

Se aceptan paquetes IPv6 indicando la interfaz de bucle de retroceso cuya dirección IPv6 es [::1], la cual permite que un nodo se envíe paquetes así mismo.

```
[root@fw ~]# ip6tables -t filter -A INPUT -i eth0 -p ipv6-icmp -j ACCEPT
[root@fw ~]# ip6tables -t filter -A OUTPUT -o eth0 -p ipv6-icmp -j ACCEPT
```

Todos los tipos de mensajes de error e informativos, se aceptan en la cadena INPUT y OUTPUT usando el parámetro en la especificación de la regla [-p ipv6-icmp].

Reglas de consultas (queries) IPv6.

Los servidores en producción de la Universidad Nacional de Loja, por seguridad deben realizar consultas (queries) de: DNS (resolución de nombres) y HTTP (para navegación) al exterior.

```
ip6tables -A INPUT -i eth0 -p udp -s 2800:68:7:32:32::2/64 -d 2800:68:7:32:32::13/64 --sport 53 --dport 1024: -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p udp -s 2800:68:7:32:32::13/64 -d 2800:68:7:32:32::2/64 --sport 1024: --dport 53 -j ACCEPT
ip6tables -A INPUT -i eth0 -p tcp -s 2800:68:7:32:32::2/64 -d 2800:68:7:32:32::13/64 --sport 53 --dport 1024: -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s 2800:68:7:32:32::13/64 -d 2800:68:7:32:32::2/64 --sport 1024: --dport 53 -j ACCEPT
```

Estas reglas ip6tables están aplicadas en el servidor proxy, en donde se permite realizar consultas de DNS usando el protocolo UDP y TCP por el puerto 53 que es en el cual escucha el servidor de nombres.

```
ip6tables -t filter -A INPUT -i eth0 -p tcp -s 2000::/3 -d 2800:68:7:32:32::13/64 --sport 80 --dport 1024: -j ACCEPT
ip6tables -t filter -A OUTPUT -o eth0 -p tcp -s 2800:68:7:32:32::13/64 -d 2000::/3 --sport 1024: --dport 80 -j ACCEPT
```

Las reglas ip6tables aplicadas permiten la navegación del servidor en TCP usando el puerto 80, el cual es utilizado por la mayor parte de Internet. Como se puede apreciar en la reglas; la red IPv6 [2000::] y el prefijo [3] es decir 2000::/3 que identifica a todo Internet en IPv6.

Reglas para servicios activos sobre IPv6.

Las reglas de ip6tables definidas a continuación hacen referencia a los distintos servicios de Internet que se brinda desde los servidores en producción en IPv6.

```
ip6tables -A INPUT -i eth0 -p tcp -s 2800:68:7:32:63::7/64 -d 2800:68:7:32:32::2/64 --sport 1024: --dport 7121 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s 2800:68:7:32:32::2/64 -d 2800:68:7:32:63::7/64 --sport 7121 --dport 1024: -j ACCEPT
```

Las reglas ip6tables impuestas están aplicadas en el servidor en el servidor DNS las cuales permiten ingreso al servidor usando SSH por el puerto a la IPv6 de origen [2800:68:7:32:63::7/64].

```
ip6tables -t filter -A INPUT -i eth0 -p tcp -s 2000::/3 -d 2800:68:7:49::2/64 --sport 80 --dport 80 -j ACCEPT
ip6tables -t filter -A OUTPUT -o eth0 -p tcp -s 2800:68:7:49::2/64 -d 2000::/3 --sport 80 --dport 80 -j ACCEPT
```

Estas reglas permiten al servidor web principal de la Universidad Nacional de Loja [www.unl.edu.ec] aceptar petición por el puerto 80, de la red IPv6 2800::/3 cuya longitud de prefijo identifica a todo el Internet en IPv6.

```
ip6tables -A INPUT -i eth0 -p tcp -s 2800:68:7:32::/64 -d 2800:68:7:49::20/64 --sport 1024: --dport 110 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s 2800:68:7:49::20/64 -d 2800:68:7:32::/64 --sport 110 --dport 1024: -j ACCEPT
ip6tables -A INPUT -i eth0 -p tcp -s 2800:68:7:32::/64 -d 2800:68:7:49::20/64 --sport 1024: --dport 143 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s 2800:68:7:49::20/64 -d 2800:68:7:32::/64 --sport 143 --dport 1024: -j ACCEPT
```

Estas políticas están definidas para el servidor de correo electrónico tanto para POP (port 110) e IMAP (port 143), en las cuales por seguridad solo se permite conexiones a la suber IPv6 2800:68:7:32::/64 .

```
ip6tables -A INPUT -i etho -p tcp -s 2800:68:7:32:63::7/64 -d 2800:68:7:49::20/64 --sport 1024: --dport 25 -j ACCEPT
ip6tables -A OUTPUT -o etho -p tcp -s 2800:68:7:49::20/64 -d 2800:68:7:32:63::7/64 --sport 25 --dport 1024: -j ACCEPT
```

Por seguridad, para activar SMTP (envío de correo) solo se crearan reglas para direcciones IPv6 específicas, previamente autorizadas por la Unidad de Telecomunicaciones e Información. Esto es como una medida de seguridad para evitar el SPAM que se realiza por el puerto 25.

Una vez aplicadas la reglas ip6tables en los servidores de producción, de acuerdo a las políticas de seguridad previamente establecidas, procedemos a guardar las reglas en el sistema.

```
[root@fw ~]# service ip6tables save
Guardando las reglas del cortafuegos a :            [  OK  ]
```

En el fichero [/etc/sysconfig/ip6tables] se encuentran todas las reglas de ip6tables anteriormente guardadas. Finalmente iniciamos el proceso que se ejecuta en segundo plano ip6tables, de la siguiente forma.

```
[root@fw ~]# service ip6tables start
Aplicación de las reglas del cortafuegos ip6tables:      [  OK  ]
```

8.4. Plan de activación de IPv6 en las AAA (Áreas Académicas Administrativas) y Administración Central.

En nuevo protocolo de Internet versión 6 (IPv6) se encuentra implementado en los servicios de Internet, tanto de la Intranet como públicos. La asignación de los parámetros de red IPv6 se realiza de forma automática desde el servidor dhcpv6 a los equipos finales que tienen el sistema operativo: Mac OS-X, Windows Vista, Windows 7 y distribuciones de Gnu / Linux.

A las computadoras que tienen el sistema operativo Windows XP no se está realizando la asignación de los parámetros de red IPv6, la razón principal es porque no viene activado IPv6. Por lo que hemos considerado elaborar un plan de activación de IPv6 de acuerdo a los datos obtenidos.

A continuación se ilustra una tabla, en donde se considera el total de computadoras con diferentes sistemas operativos, seguidamente se obtiene el porcentaje de computadoras con sistema operativo XP, se estima el tiempo necesario para realizar la activación de IPv6 y finalmente el número de recursos humanos que se utilizara.

TABLA 8.4. ACTIVACIÓN IPV6 EN LOS SISTEMAS OPERATIVOS WINDOWS XP

#	*Dependencia*	*Total de Computadoras*	*Porcentaje SO - XP*	*Total de Computadoras XP*	*# Días de Activación*	*# Recursos Humanos*
1	Administración Central	346	61 %	211	2	2
2	Área Educativa	324	72 %	233	3	2
3	Área Jurídica	260	75 %	195	2	2
4	Área Agropecuaria	210	65 %	169	2	2
5	Área Energía	153	60 %	91	1	2
6	Área de la Salud Humana	96	68 %	65	1	2
Total		***1389***		***964***	***10***	

Elaborado por: *Jhon Alexander Calderón Sanmartín y Rubi Rafael Cabrera Erreyes.*
Fuente: *Unidad de Telecomunicaciones e Información.*

De acuerdo a los datos proporcionados por la Sección de Redes y Equipos Informáticos y Sección de Mantenimiento Electrónico, hemos determinado que existe un total de 964 computadoras con el sistema operativo XP en todo el campus universitario.

Para realizar la activación de IPv6 en las computadoras con sistema operativo XP se tiene un estimado de 10 días laborables, está activación se realizará físicamente en las computadoras por 2 recursos humanos de la Sección de Redes y Equipos Informáticos de la Universidad Nacional de Loja.

Los proceso de activación de IPv6 en las computadoras con sistema operativo XP se debe realizar manualmente, detallamos a continuación los pasos necesarios.

Antes de nada, sería una buena idea comprobar si **IPv6** ya está activo. Una opción fácil de saberlo es a través del comando "**ipconfig",** que muestra información de los parámetros de red. Para ejecutar el símbolo del sistema existen dos maneras:

- Inicio > Todos los programas > Accesorios > Símbolo del sistema
- Presionamos Windows+r, escribir "cmd" y pulsar Aceptar.

Una vez abierto el símbolo del sistema digitamos el comando "**ipconfig"** para averiguar si IPv6 está disponible en el equipo. Mostramos a continuación el resultado obtenido.

```
C:\Documents and Settings\Happy Hacking>ipconfig
Configuración IP de Windows
Adaptador Ethernet Conexión de área local        :
      Sufijo de conexión específica DNS : machute.ec
      Dirección IP. . . . . . . . . . . : 192.168.77.84
      Máscara de subred . . . . . . . . : 255.255.255.0
      Puerta de enlace predeterminada   : 192.168.77.254
```

Si no se encuentra una entrada de direcciones **IPv6** en el listado, es que no está activado y necesita ser activado. La forma más sencilla de activar el protocolo IPv6 en XP es desde el **símbolo del sistema, para ello se debe digitar** el siguiente comando.

```
C:\Documents and Settings\Happy Hacking>ipv6 install
Instalando...
Finalizado con éxito.
```

Aparecerá un mensaje indicando que se ha configurado correctamente. Para comprobar que ha sido correctamente instalado, usar:

```
C:\Documents and Settings\Happy Hacking>ipv6 if
Interfaz 5: Ethernet: Conexión de área local
  GUID {161D99D0-C134-4852-972E-C9E35C2EF640}
  usa descubrimiento de vecinos
  usa descubrimiento de enrutador
  dirección de capa de enlace: 08-00-27-c3-62-86
    preferred link-local fe80::a00:27ff:fec3:6286, duración infinite
    multidifusión interface-local ff01::1, 1 referencias , no reportable
    multidifusión link-local ff02::1, 1 referencias , no reportable
    multidifusión link-local ff02::1:ffc3:6286, 1 referencias , último informador
  enlace MTU 1500 (enlace MTU 1500)
```

Se mostrará la configuración y los parámetros de red IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

Configurar manualmente una dirección IPv6 en una interfaz lógica del sistema, desde el símbolo del sistema y comprobar que se agrego.

```
C:\>netsh interface ipv6 set address 5 2800:68:7:32:77::102
Aceptar
```

```
C:\>netsh interface ipv6 show address
Consultando el estado activo...
Interfaz 5: Conexión de área local
Tipo dir.  Estado DAD Vida válida  Vida pref.   Dirección
---------  --------- ----------- ----------- ----------------------------
Manual     Preferida  infinite    infinite    2800:68:7:32:77::102
Vínculo    Preferida  infinite    infinite    fe80::a00:27ff:fec3:6286
```

Agregar una ruta estática al sistema por la interfaz definida anteriormente y verificar que se agrego de manera satisfactoria.

```
C:\>netsh interface ipv6 add route 2000::/3 5 2800:68:7:32:32::1
Aceptar
```

```
C:\>netsh interface ipv6 show route
Consultando el estado activo...
Publicar Tipo      Mét  Prefijo              Índ  Interfaz/puerta_enlace
-------- --------  ----  ----------------------  ---  ---------------------
no       Manual     0   2000::/3                5  2800:68:7:32:32::1
```

Configurar manualmente la dirección IPv6 del servidor de nombres y comprobar que se agrego la dirección del DNS.

```
C:\>netsh interface ipv6 add dns "Conexión de área local" 2800:68:7:32:32::2
Aceptar
```

```
C:\>netsh interface ipv6 show dns
Servidores DNS en la interfaz: Conexión de área local
Índ.   Servidor DNS
-----  ----------------------------------------
    1  2800:68:7:32:32::2
```

Probamos conectividad a la dirección IPv6 unicast global configurada en el sistema, con el comando "ping6" y el parámetro "-n 3" que el indicamos el número de paquetes.

```
C:\>ping6 -n 3 2800:68:7:32:77::102
Haciendo ping 2800:68:7:32:77::102
de 2800:68:7:32:77::102 con 32 bytes de datos:

Respuesta desde 2800:68:7:32:77::102: bytes=32 tiempo=1ms
Respuesta desde 2800:68:7:32:77::102: bytes=32 tiempo<1m
Respuesta desde 2800:68:7:32:77::102: bytes=32 tiempo<1m
```

Una vez realizada la activación de IPv6 y configuración necesaria de los parámetros de red IPv6 el usuario final puede empezar a consumir servicios de la Universidad Nacional de Loja e Internet sobre el nuevo protocolo versión 6 de forma transparente. La configuración solo debe realizarse por una vez en el sistema Windows XP.

9. PLAN DE VALIDACIÓN

El proceso de validación se dio inicio desde el mes de mayo del año 2011, realizando la configuración en los diferentes servidores administrados pos la sección de redes y equipos informaticos de la Unidad de Informática, Telecomunicación e información de la Universidad Nacional de Loja, baja la responsabilidad del Lic. Jamil Ramón, Director de la Unidad y del Tecnologo, Daniel Reyes responsable de la Sección de Redes y Equipos Informáticos quienes supervisaron las pruebas de implementación de IPv6 en el campus universitario.

La implementación de IPv6, fue evaluada por los jefes departamentales de la Unidad de Telecomunicaciones e Información y técnicos de la Sección de Redes y Software y ha funcionando correctamente para los usuarios finales, asignando automáticamente las diferentes parámetros de Red de direcciones IPv6, para los cuales va dirigido la implementación de este nuevo protocolo de comunicación que asegura mayor portabilidad, seguridad, mayor números de direcciones IPv6, movilidad entre otros.

Las pruebas de acceso para navegar con IPv6 se han realizado de una manera óptima, sin presentar ningún inconveniente a los usuarios finales, realizando la navegación sin ningún inconveniente.

Las encuestas aplicadas a los diferentes Jefes Departamentales (Anexo N° 1) y técnicos de la Sección de Redes y Software (Anexo N° 2), se las realizó luego de que ellos hayan hecho uso de este nuevo protocolo de comunicación, los cuales emitieron sus apreciaciones en las encuestas entregadas a cada uno de ellos, asignando en las mismas su propia impresión en cuanto a la veracidad de la información visualizada, navegación, seguridad, portabilidad, conexiones de extremo, entre otras características de IPv6.

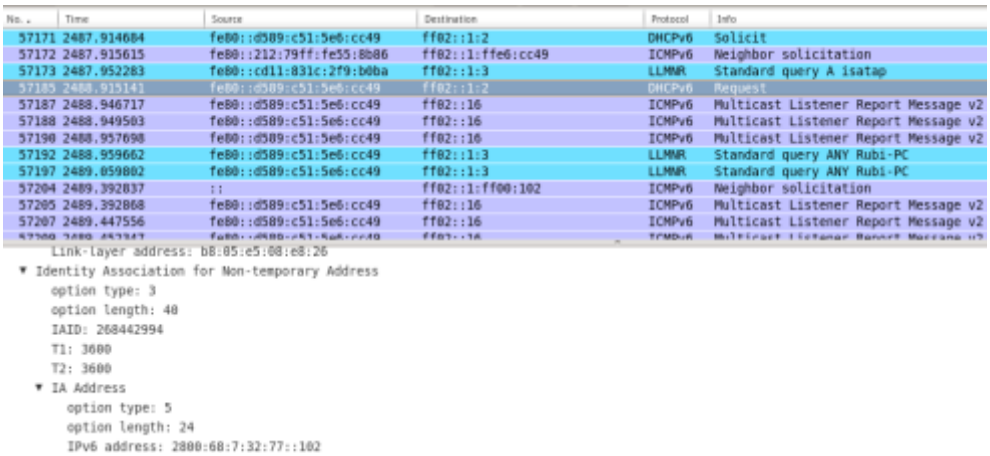
9.1. Pruebas de validación de los servicios de Internet IPv6.

Las pruebas de validación de los servicios de Internet (dns, dhcpv6, proxy, firewall, http, smtp, imap, pop, etc), que actualmente se encuentran implementados en doble (IPv4 e Ipv6) son una parte muy significativa para nuestra investigación, no solo por su importancia en el logro de los resultados correctos sino por el tiempo y recursos requeridos.

Utilizamos un analizador de protocolos "wireshark" el cual nos permitió realizar un análisis del tráfico IPv6 y solucionar problemas en la red de datos Ethernet IEEE 802.3 sobre IPv6.

9.1.1. Asignación de direcciones IPv6.

El cliente dhcpv6 realiza una petición al servidor DHCPv6, los mensajes DHCPv6 en todo este proceso de asignación de los parámetros de red IPv6 se muestran en el siguiente gráfico.



No.	Time	Source	Destination	Protocol	Info
57171	2487.914684	fe80::d589:c51:5e6:cc49	ff02::1:2	DHCPv6	Solicit
57172	2487.915615	fe80::212:79ff:fe55:8b86	ff02::1:ffe6:cc49	ICMPv6	Neighbor solicitation
57173	2487.952283	fe80::cd11:831c:2f9:b0ba	ff02::1:3	LLMNR	Standard query A isatap
57185	2488.915141	fe80::d589:c51:5e6:cc49	ff02::1:2	DHCPv6	Request
57187	2488.946717	fe80::d589:c51:5e6:cc49	ff02::16	ICMPv6	Multicast Listener Report Message v2
57188	2488.949503	fe80::d589:c51:5e6:cc49	ff02::16	ICMPv6	Multicast Listener Report Message v2
57190	2488.957698	fe80::d589:c51:5e6:cc49	ff02::16	ICMPv6	Multicast Listener Report Message v2
57192	2488.959662	fe80::d589:c51:5e6:cc49	ff02::1:3	LLMNR	Standard query ANY Rubi-PC
57197	2489.059802	fe80::d589:c51:5e6:cc49	ff02::1:3	LLMNR	Standard query ANY Rubi-PC
57204	2489.392837	::	ff02::1:ff00:102	ICMPv6	Neighbor solicitation
57205	2489.392868	fe80::d589:c51:5e6:cc49	ff02::16	ICMPv6	Multicast Listener Report Message v2
57207	2489.447556	fe80::d589:c51:5e6:cc49	ff02::16	ICMPv6	Multicast Listener Report Message v2

```
    Link-layer address: b8:85:e5:08:e8:26
  ▼ Identity Association for Non-temporary Address
      option type: 3
      option length: 40
      IAID: 268442994
      T1: 3600
      T2: 3600
    ▼ IA Address
        option type: 5
        option length: 24
        IPv6 address: 2800:68:7:32:77::102
```

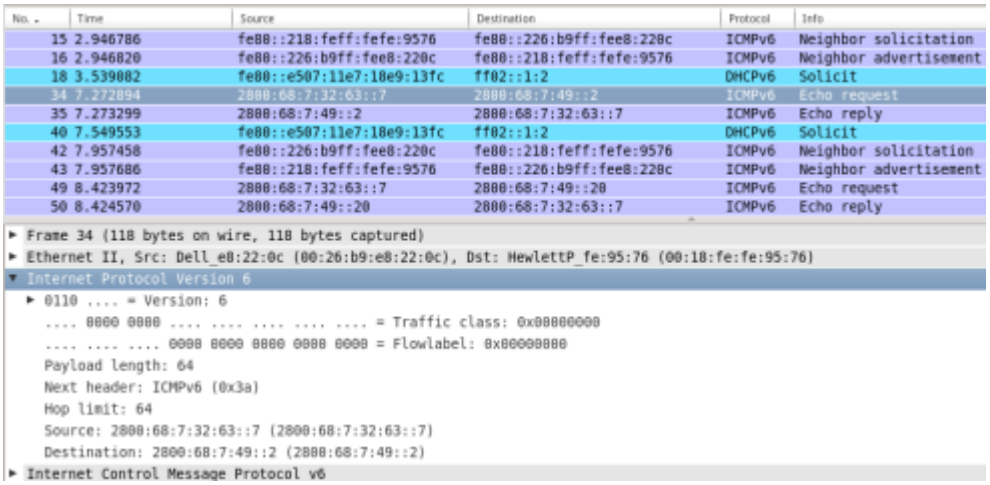
Figura 9.1.1.: *Proceso de asignación dirección IPv6.*

El cliente dhcpv6 ahora cuenta con los parámetros de red IPv6 de manera que se puede acceder a los servicios de Internet tanto de la intranet como servicios públicos de la Universidad.

Dirección física. . . . . : 00-1D-72-E7-88-21
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : ***2800:68:7:32:77::1e0*** (Preferido)
Vínculo: dirección IPv6 local. . . . . : ***fe80::d589:c51:5e6:cc49*** % 12 (Preferido)
IAID DHCPv6 . . . . . : ***268442994***
DUID de cliente DHCPv6. . . . . .: ***00-01-00-01-15-58-E3-79-00-1D-72-E7-88-21***
Servidores DNS. . . . . : ***2800:68:7:32:32::2***

9.1.2. ICMP versión 6.

El protocolo ICMPv6 lo utilizamos tanto en los clientes como en los servidores IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico (ICMPv6 ***ping6***), en el siguiente gráfico se muestra la captura de tráfico al ejecutar la herramienta pin6 para probar conectividad a un equipo remoto.



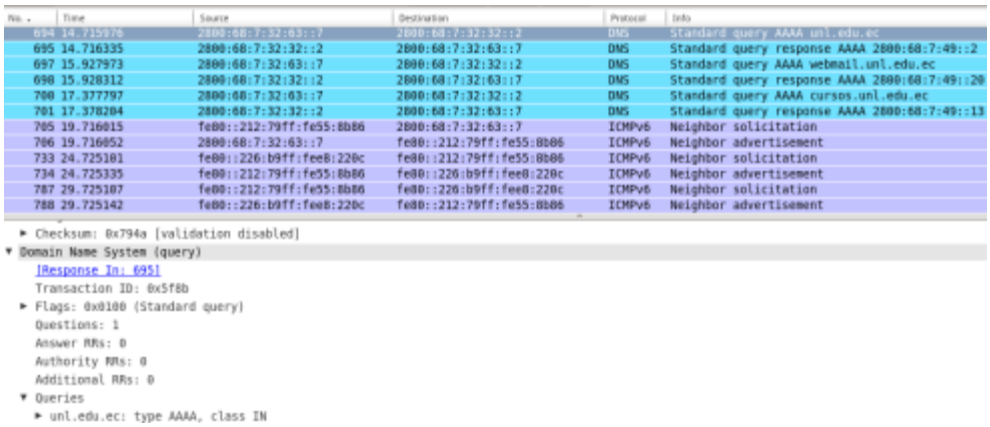
No.	Time	Source	Destination	Protocol	Info
15	2.946786	fe80::218:feff:fefe:9576	fe80::226:b9ff:fee8:220c	ICMPv6	Neighbor solicitation
16	2.946820	fe80::226:b9ff:fee8:220c	fe80::218:feff:fefe:9576	ICMPv6	Neighbor advertisement
18	3.539082	fe80::e507:11e7:18e9:13fc	ff02::1:2	DHCPv6	Solicit
34	7.272894	2800:68:7:32:63::7	2800:68:7:49::2	ICMPv6	Echo request
35	7.273299	2800:68:7:49::2	2800:68:7:32:63::7	ICMPv6	Echo reply
40	7.549553	fe80::e507:11e7:18e9:13fc	ff02::1:2	DHCPv6	Solicit
42	7.957458	fe80::226:b9ff:fee8:220c	fe80::218:feff:fefe:9576	ICMPv6	Neighbor solicitation
43	7.957686	fe80::218:feff:fefe:9576	fe80::226:b9ff:fee8:220c	ICMPv6	Neighbor advertisement
49	8.423972	2800:68:7:32:63::7	2800:68:7:49::20	ICMPv6	Echo request
50	8.424570	2800:68:7:49::20	2800:68:7:32:63::7	ICMPv6	Echo reply

```
▶ Frame 34 (118 bytes on wire, 118 bytes captured)
▶ Ethernet II, Src: Dell_e8:22:0c (00:26:b9:e8:22:0c), Dst: HewlettP_fe:95:76 (00:18:fe:fe:95:76)
▼ Internet Protocol Version 6
  ▶ 0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 64
    Next header: ICMPv6 (0x3a)
    Hop limit: 64
    Source: 2800:68:7:32:63::7 (2800:68:7:32:63::7)
    Destination: 2800:68:7:49::2 (2800:68:7:49::2)
▶ Internet Control Message Protocol v6
```

Figura 9.1.2. : *Conectividad IPv6 utilizando ping6.*

9.1.3. Sistema de nombres de dominio.

El cliente IPv6 realiza una petición "dns" usando el protocolo "udp" para los dominios instituciones, la herramienta utilizada para realizar esta petición es "dig" desde un pc con sistema operativo Gnu / Linux, a continuación se muestra el tráfico IPv6 al realizar este proceso.



No.	Time	Source	Destination	Protocol	Info
694	14.715976	2800:68:7:32:63::7	2800:68:7:32:32::2	DNS	Standard query AAAA unl.edu.ec
695	14.716335	2800:68:7:32:32::2	2800:68:7:32:63::7	DNS	Standard query response AAAA 2800:68:7:49::2
697	15.927973	2800:68:7:32:63::7	2800:68:7:32:32::2	DNS	Standard query AAAA webmail.unl.edu.ec
698	15.928312	2800:68:7:32:32::2	2800:68:7:32:63::7	DNS	Standard query response AAAA 2800:68:7:49::20
700	17.377797	2800:68:7:32:63::7	2800:68:7:32:32::2	DNS	Standard query AAAA cursos.unl.edu.ec
701	17.378204	2800:68:7:32:32::2	2800:68:7:32:63::7	DNS	Standard query response AAAA 2800:68:7:49::13
705	19.716015	fe80::212:79ff:fe55:8b86	2800:68:7:32:63::7	ICMPv6	Neighbor solicitation
706	19.716052	2800:68:7:32:63::7	fe80::212:79ff:fe55:8b86	ICMPv6	Neighbor advertisement
733	24.725101	fe80::226:b9ff:fee8:220c	fe80::212:79ff:fe55:8b86	ICMPv6	Neighbor solicitation
734	24.725335	fe80::212:79ff:fe55:8b86	fe80::226:b9ff:fee8:220c	ICMPv6	Neighbor advertisement
787	29.725107	fe80::212:79ff:fe55:8b86	fe80::226:b9ff:fee8:220c	ICMPv6	Neighbor solicitation
788	29.725142	fe80::226:b9ff:fee8:220c	fe80::212:79ff:fe55:8b86	ICMPv6	Neighbor advertisement

```
▶ Checksum: 0x794a [validation disabled]
▼ Domain Name System (query)
    [Response In: 6951]
    Transaction ID: 0x5f8b
  ▶ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ unl.edu.ec: type AAAA, class IN
```

Figura 9.1.3: *Proceso de resolución directa IPv6.*

9.1.4. Servidor proxy IPv6.

Previo a las pruebas realizadas del funcionamiento del proxy IPv6 se configuro en el navegador el proxy [proxy.unl.edu.ec] y el puerto alternativo para pruebas es: 7645. Luego ingresamos a la aplicación web universitaria www.unl.edu.ec. Finalmente mostramos la captura del tráfico IPv6 en la cual se puede apreciar que todo la navegación pasa por el proxy IPv6 previo a su destino.

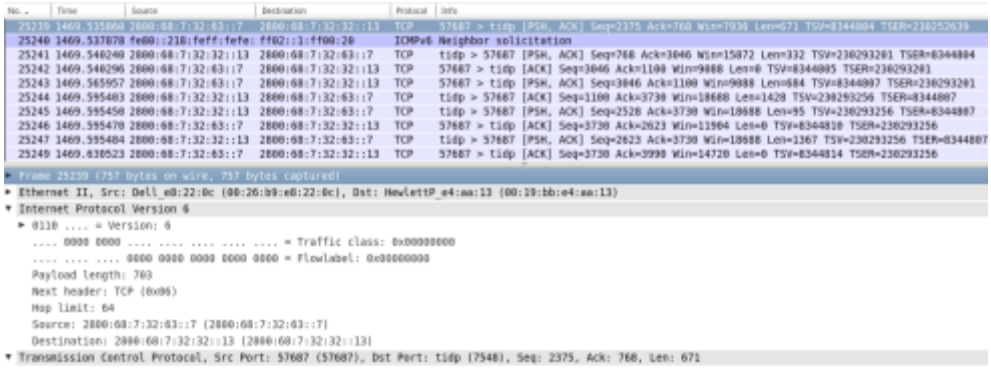


Figura 9.1.4: *Navegación web por medio de un proxy IPv6.*

9.1.5. Navegación web IPv6.

La navegación web IPv6 utiliza el protocolo de transferencia de hipertextos (http), generalmente se utiliza el puerto 80 en TCP. A continuación se muestra el tráfico IPv6 obtenido previo al acceso de la aplicación web universitaria [www.unl.edu.ec].

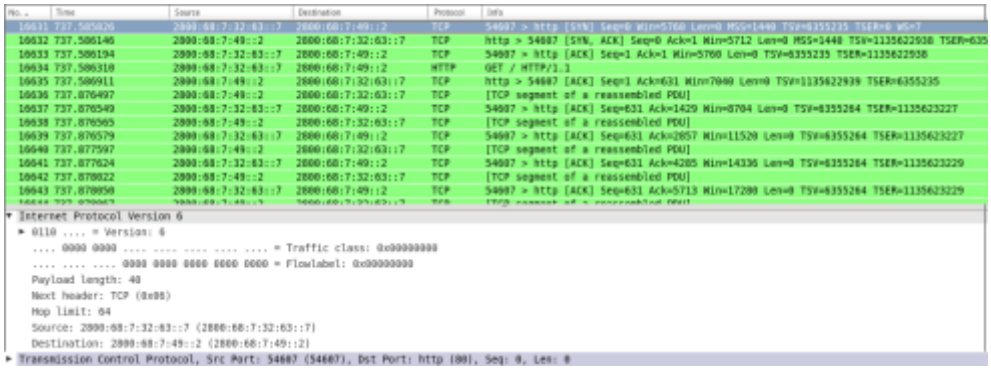


Figura 9.1.5: *Navegación web IPv6.*

9.1.6. Servicio de correo electrónico IPv6.

Un cliente IPv6 puede acceder al correo electrónico IPv6 a través de un navegador o desde un cliente de correo electrónico que soporte IPv6 (thunderbird). El cliente IPv6 envía una

petición al servidor para leer su correo por medio de un navegador, el tráfico que fluye en esta comunicación se muestra a continuación.

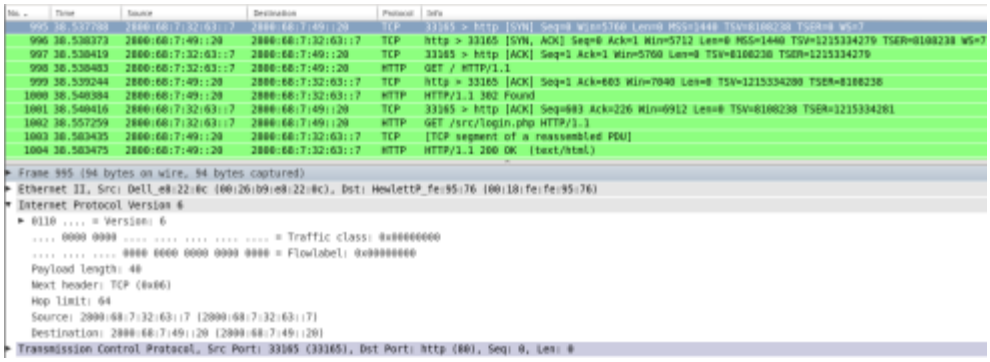


Figura 9.1.6: *Acceso correo electrónico usando http.*

9.1.7. Transferencia de correo SMTP IPv6.

Un cliente de correo electrónico IPv6 envía una petición al servidor SMTP IPv6, por medio del cual se entregara el mensaje de correo electrónico al destinatario. El proceso que se da durante la petición se muestra en el siguiente gráfico.

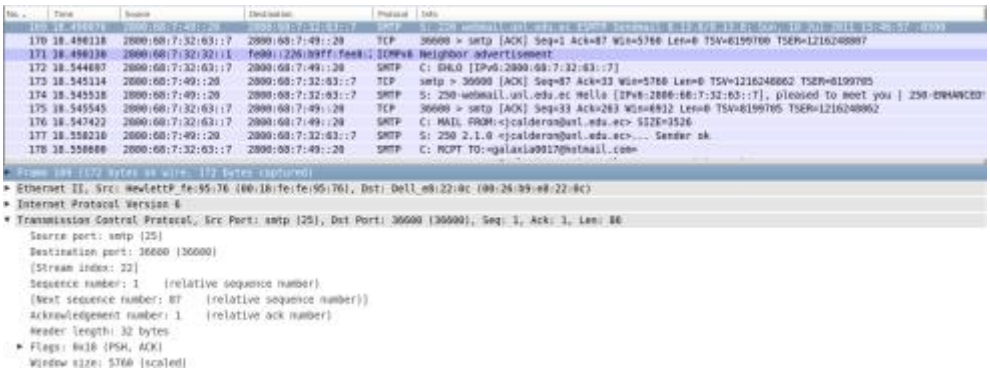


Figura 9.1.7: *Transferencia de correo electrónico SMTP IPv6.*

9.1.8. Acceso a mensajes electrónicos IMAP IPv6.

Un cliente de correo electrónico IPv6 (thunderbird) permitirá tener acceso a los mensajes electrónicos que se encuentran en el servidor de correo por medio del protocolo IMAP IPv6, el cliente IPv6 enviara una petición para acceder a los mensajes y puedan ser vistos por el usuario final. Este proceso se conoce más a detalle en la siguiente figura.

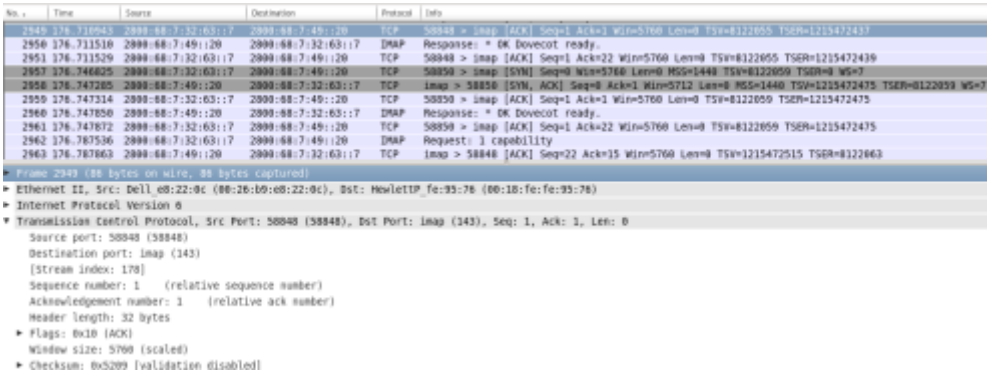


Figura 9.1.8: *Acceso a mensaje electrónicos IMAP IPv6.*

De esta manera damos por concluida las pruebas de validación en los servicios de Internet de la Universidad Nacional de Loja. Dichas pruebas nos permitió comprobar algunos de los beneficiosos del protocolo de Internet versión 6 como: El tiempo de respuesta y retardo de IPv6 disminuyeron con relación a IPv4 porque los paquetes solo se fragmentan y desfragmentan en el origen y destino. Por lo tanto el índice de pérdida de paquetes IPv6 es menor al desaparecer el proceso de fragmentación y desfragmentación en los routers intermedios.

Así mismo podemos concluir en base a la pruebas de validación que el servicio de resolución directa DNS en doble pila se comporta de acuerdo al tipo de cliente que realiza la petición, es decir si el cliente tiene configurado doble pila en su sistema tendrá prioridad IPv6.

Finamente se comprobó con las pruebas de validación realizadas el correcto funcionamiento de IPv6 en la red de datos Ethernet IEEE 802.3 cuyo mecanismo transición a IPv6 fue doble pila.

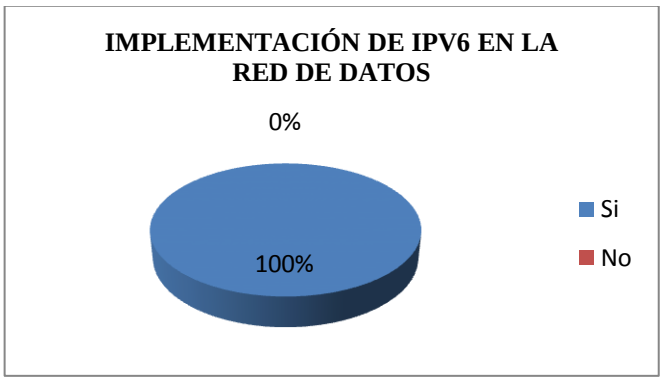
9.2. ENCUESTA APLICADAS A JEFES DEPARTAMENTALES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA.

1. ¿Considera que la implementación de IPv6 en la red de datos de la Universidad Nacional de Loja se realizó de una forma exitosa?

TABLA 9.2.1: IMPLEMENTACIÓN DE IPV6 EN LA RED DE DATOS

Variable	Frecuencia	Porcentaje
Si	3	100%
No	0	0%
Total	**3**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis.

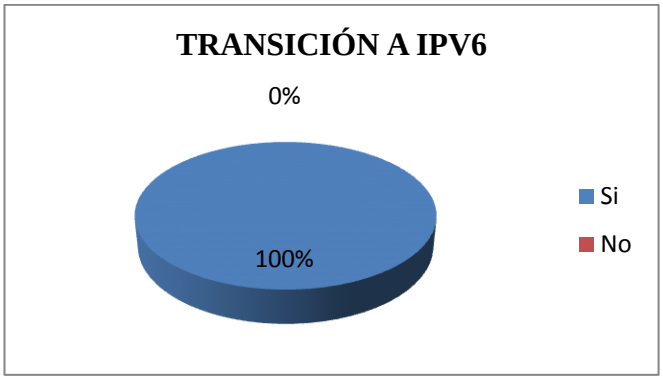
La implementación de IPv6 en la universidad se realizó de una manera exitosa en cada uno de los diferentes servicios los mismo que se encuentran funcionando correctamente como se evidencia en los datos de la pruebas un 100% de los encuestados Jefes departamentales de la Unidad de telecomunicaciones e informática lo manifiestan.

2. ¿Considera importante la transición a IPv6 en el campus de la Universidad, para brindar los servicios de Internet tanto en la intranet, red Pública (Internet) y navegación?

TABLA 9.2.2: TRANSICIÓN A IPV6

Variable	Frecuencia	Porcentaje
Si	3	100%
No	0	0%
Total	**3**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis.

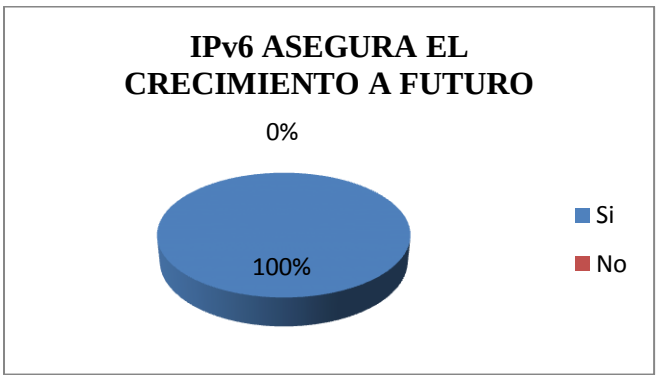
De acuerdo a la encuesta realizada a los Jefes Departamentales de la Unidad De Telecomunicaciones un 100% de los encuestados manifiestan que es muy importante, permitirá brindar servicio de internet con mayor conectividad, seguridad a los diferentes usuarios ya que la tendencia a nivel mundial es la utilización de IPv6

3. ¿Cree necesario que la red IPv6 asignada a la UNL 2800:60:7::/48 por parte del CEDIA es suficiente para conectar todos los nodos de la red Universitaria y garantizar un crecimiento a futuro de unos 20 años ?.

TABLA 9.2.3: IPv6 ASEGURA EL CRECIMIENTO A FUTURO

Variable	Frecuencia	Porcentaje
Si	3	100%
No	0	0%
Total	**3**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis:

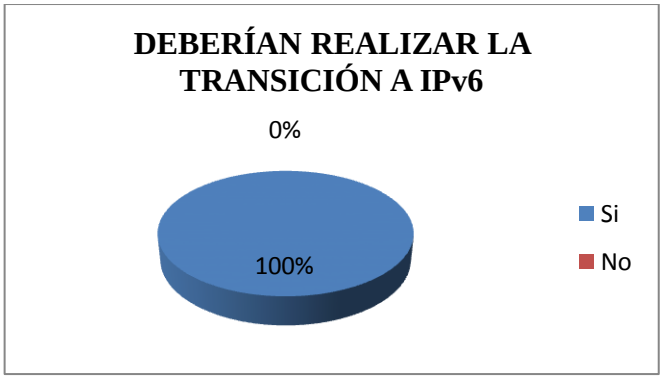
Con el crecimientos que se tendrá en la red y con la asignación del CEDIA, los encuestados manifiestan en un 100% que el prefijo asignado por dicha institución es suficiente por la cantidad de sub redes y host disponibles.

4. **¿Teniendo en cuenta como precedente el agotamiento de direcciones IPv4, considera necesario que las universidades que forman parte del CEDIA empiecen a realizar la transición a IPv6?.**

TABLA 9.2.4: DEBERÍAN REALIZAR LA TRANSICIÓN A IPv6

Variable	Frecuencia	Porcentaje
Si	3	100%
No	0	0%
Total	**3**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis:

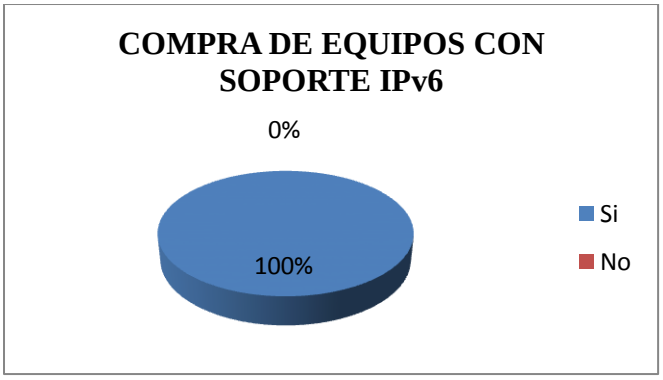
Los encuestados manifiestan en un 100% que es necesario que todas las universidades migren a este nuevo protocolo de internet por el agotamiento de direcciones en IPv4 y por la conectividad, seguridad que brinda IPv6.

5. **¿Si está en su decisión adquirir nuevos dispositivos de networking en la Universidad, tendría en cuenta que vengan con soporte nativo de IPv6 ?.**

TABLA 9.2.5: COMPRA DE EQUIPOS CON SOPORTE IPv6

Variable	Frecuencia	Porcentaje
Si	3	100%
No	0	0%
Total	**3**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis:

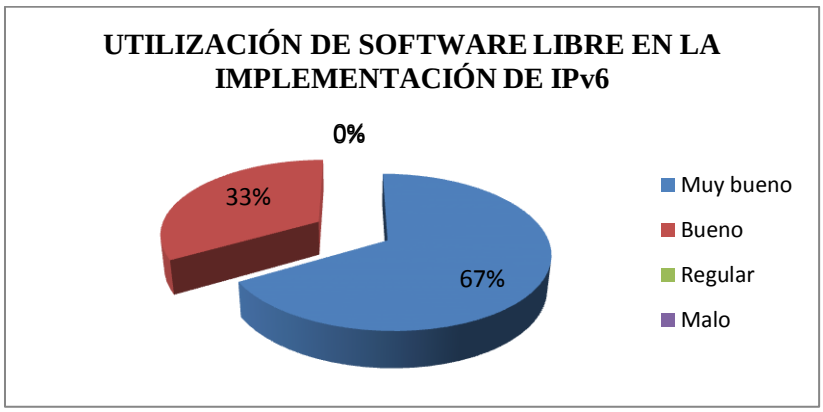
Como se observa en el grafico respectivo el 100% nos dice que es necesario que todos los equipos adquiridos deban soportar esta nueva tecnología que permita su configuración y correcto funcionamiento para brindar un servicio de internet eficiente a los usuarios.

6. ¿El uso de Software Libre y Open Source para la implementación de IPv6 en la Universidad Nacional de Loja, como lo califica?

TABLA 9.2.6: USO DE SOFTWARE LIBRE Y OPEN SOURCE EN IPv6

Variable	Frecuencia	Porcentaje
Muy bueno	2	66,67%
Bueno	1	33,33%
Regular	0	0%
Malo	0	0%
Total	**3**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis.

La implementación de IPv6 se la realizó con herramientas de software libre, los usuarios manifiestan que un 66,67% ha sido muy bueno y un 33,33% manifiesta que ha sido bueno lo que se evidencia que no habido ningún inconveniente en la utilización de Software libre para la implementación de esta nueva tecnología.

9.3. ENCUESTA APLICADAS A LOS TÉCNICOS DE LA SECCIÓN DE REDES Y SOFTWARE DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN.

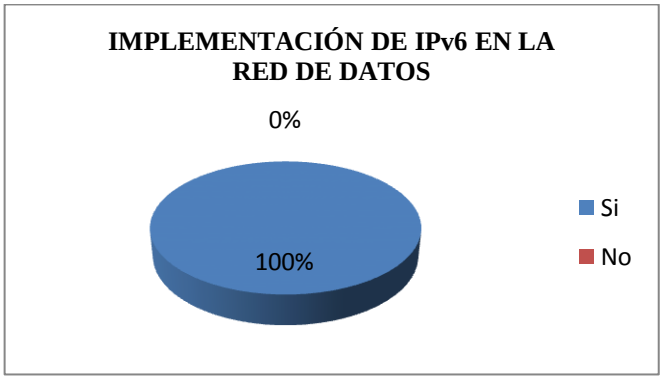
La encuesta de aplico a los diferentes funcionarios de la unidad de telecomunicaciones con la finalidad de de recabar información necesaria que permita comprobar la funcionalidad de IPv6 dentro de la red de datos de la Universidad lo cual se representa en al siguiente información y como constan en los anexos.

1. ¿Considera que la implementación de IPv6 en la red de datos de la Universidad Nacional de Loja se realizó de una forma exitosa?

TABLA 9.3.1: IMPLEMENTACIÓN DE IPv6 EN LA RED DE DATOS

Variable	Frecuencia	Porcentaje
Si	5	100%
No	0	0%
Total	**5**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis.

Los usuarios encuestados manifiestan que la implementación de IPv6 en la Universidad se realizó de una manera exitosa en cada uno de los diferentes servicios los mismo que se

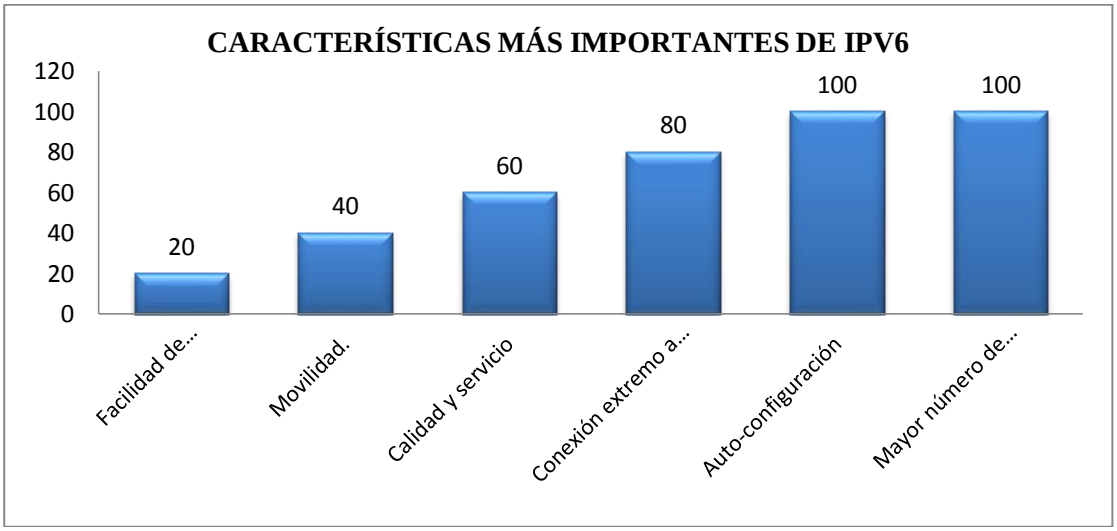
encuentran funcionando correctamente como se evidencia en los datos de la pruebas donde un 100%, afirma que no habido ningún inconveniente.

2. ¿Cuáles cree usted que son la características más importantes de IPv6 ?.

TABLA 9.3.2: TRANSICIÓN A IPv6

Variable	Frecuencia	Porcentaje
Facilidad de administración.	1	20%
Auto-configuración	5	100%
Seguridad	0	0%
Conexión extremo a extremo	4	80%
Movilidad.	2	40%
Mayor número de direcciones	5	100%
Calidad y servicio	3	60%

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis.

De acuerdo a la pregunta realizada sobre cuáles son las características más importantes de IPv6, un 20% manifiesta que es la facilidad de administración y la movilidad, un 100% considera que es la auto configuración, el 80% nos dice que son las Conexión de extremo a extremo, un 100% que es el mayor número de direcciones y el 60% la calidad en el servicio.

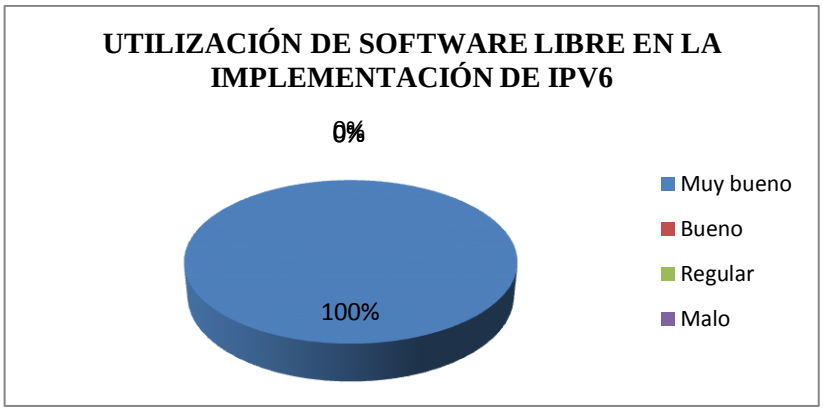
Como se puede evidencia los usuarios consideran diferentes características que posee el nuevo protocolo implementado en el campus universitario de la Universidad nacional de Loja.

3. ¿Qué calificación daría a los servicios de Internet: dns, dhcp, proxy, firewall, web y correo configurados con en el mecanismo de transición doble pila (IPv4 e IPv6)?

TABLA 9.3.3: CALIFICACIÓN DE LOS SERVICIOS DE INTERNET IMPLEMENTADOS (DNS, DHCP, PROXY, FIREWALL, WEB Y CORREO)

Variable	Frecuencia	Porcentaje
Muy bueno	5	100%
Bueno	0	0%
Regular	0	0%
Malo	0	0%
Total	**5**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis.

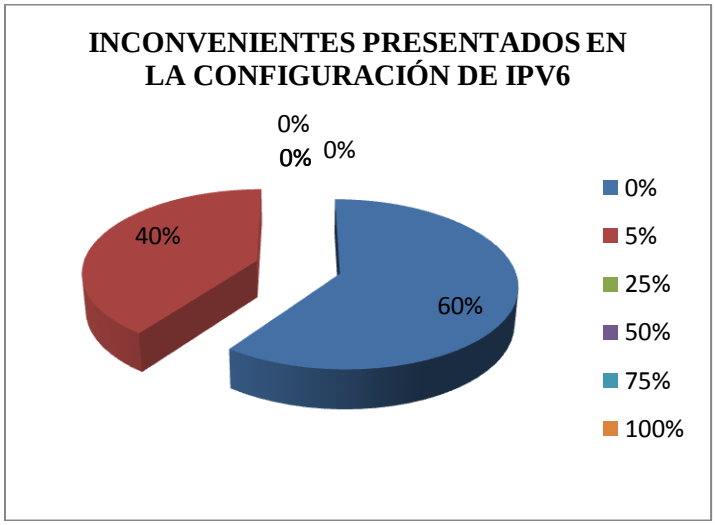
La implementación de IPv6 se la realizó con herramientas de software libre, los usuarios manifiestan en un 100% ha sido muy bueno lo que se evidencia que no habido ningún inconveniente en la utilización los diferentes servicios configurados como son: DNS, DHCP, PROXY, FIREWALL, WEB Y CORREO, mediante el mecanismo de transición de doble pila.

4. ¿En qué porcentaje se le presentaron inconvenientes en la configuración de los parámetros de red IPv6, al momento de configurar su interfaz?

TABLA 9.3.4: INTERFERENCIAS PRESENTADOS EN CONFIGURACIÓN DE IPv6

Variable	Frecuencia	Porcentaje
0%	3	60%
5%	2	40%
25%	0	0%
50%	0	0%
75%	0	0%
100%	0	0%
Total	**5**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis:

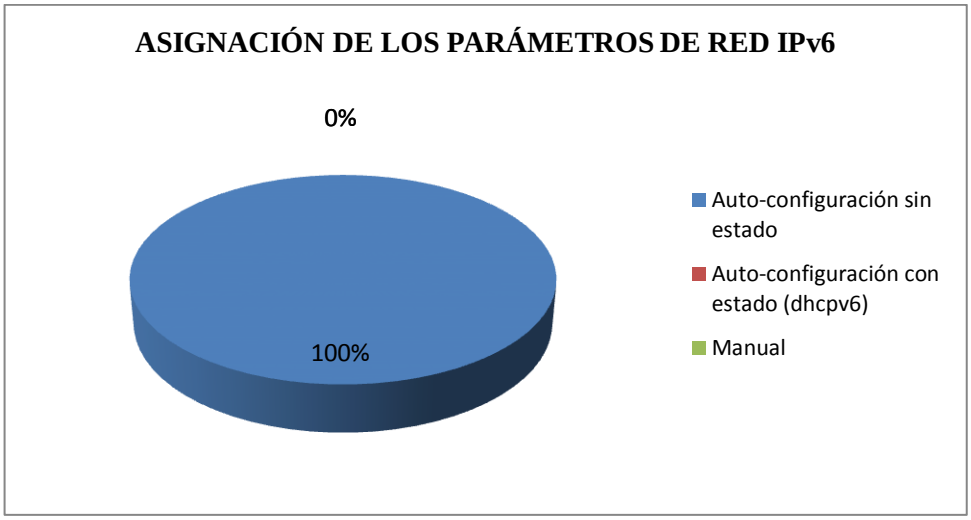
De acuerdo a la pregunta formulada se puede observar que el inconveniente de configurar IPv6 en su computador es mínimo del 5% que es un porcentaje que se encuentra dentro de los márgenes de error, por lo que se puede evidenciar que la transición de IPv4 a IPv6 se ha desarrollado sin ningún inconveniente.

5. ¿De qué forma considera que deberá hacerse la asignación de los parámetros de red IPv6 (dirección IPv6, prefijo, gateway, dns, u otros) a los equipos finales?

TABLA 9.3.5: ASIGNACIÓN DE LOS PARÁMETROS DE RED IPv6

Variable	Frecuencia	Porcentaje
Auto-configuración sin estado	5	0%
Auto-configuración con estado (dhcpv6)	0	100%
Manual	0	0%
Total	**5**	**100%**

Fuente: *Encuestas*
Elaboración: *Los Autores*



Análisis:

Los usuarios entrevistados manifiestan en un 100% que se debería realizar mediante Auto-configuración con estado (dhcpv6), que permita mantener un monitoreo adecuado y eficiente en las asignaciones de IPv6.

Como se puede observar en las encuestas realizadas la implementación de IPv6 se ha desarrollado son ningún inconveniente, como se lo demuestra en los resultados de las pruebas realizadas, no se pudieron notar errores trascendentes. Por lo que se puede afirmar que este nuevo protocolo de internet está apto y funcionando correctamente en la red de datos de la Universidad, así lo demuestran las pruebas realizadas y la certificación dada por el Director de la Unidad de Telecomunicaciones e Información (Anexos) ya que cumple satisfactoriamente con todos los requerimientos planteados en nuestro proyecto.

10. VALORACIÓN TÉCNICA – ECONÓMICA

La implementación de IPv6 en la Universidad Nacional de Loja, contribuye a implementación de nuevas tecnologías para el mejoramiento de los diferentes procesos, lo cual permite tener mayor velocidad y seguridad dentro de la Red de datos.

La misma se la realizó de acuerdo a los requerimientos y las necesidades que fueron expuestos al inicio del proyecto, ya que se utilizaron métodos y herramientas para su desarrollo con eficiencia y eficacia.

Esta nueva tecnología es moderada, ya que la institución cuenta con todos los equipos informáticos que soportan esta nueva tecnología y herramientas utilizadas son gratuitas.

Finalmente los costos de Implementación de IPv6 en su totalidad son:

TABLA 10.1: RECURSOS HUMANOS				
Descripcion	**Cantidad**	**Numero Horas**	**Valor Unitario**	**Valor Total**
Jhon Alexander Calderón S. (Investigador).	1	650	$ 3.50	$ 2275
Rubi Rafael Cabrera (Investigador).	1	650	$ 3.50	$ 2275
Asesor Profesional	1	12	$4.00	$ 48.00
			SUBTOTAL	**$ 4598**

TABLA 10.2: RECURSOS MATERIALES				
Resma de Hojas A4.	7		$3.50	$24.50
Grapadora.	1		$4.00	$4.00
Perforadora.	1		$3.50	$3.50
Borrador.	2		$0.25	$50.00
Lápices, esferos.	10		$0.35	$3.50
Calculadora.	1		$50.00	$50.00
Clips.	1		$0.70	$0.70
Dvds.	25		$0.75	$18.75
Cartuchos de Tinta Negra.	2		$50.00	$100.00
Cartuchos de Tinta de Color.	2		$60.00	$120.00
Anillados.	10		$1.50	$15.50
Empastados.	5		$10.00	$50.00
Transporte.	200		$0.25	$50.00
Consultas (Internet).	400		$0.80	$320.00
Cable de red.	50		$0.40	$20.00
Conectores Rj45.	30		$0.45	$13.50
Jack Modular.	5		$6.00	$30.00
SUB-TOTAL				**$ 873,95**

TABLA 10.3: RECURSOS TÉCNICOS				
Computadores Portátiles.	2		$900.00	$1,800.00
Impresora Hp Color LaserJet 2600n.	1		$450.00	$450.00
Pen Drive Hp 4 GB.	2		$15.00	$30.00
Recursos Técnicos Software:				
Sistema Operativo Gnu / Linux.	3		$0.00	$0.00
Paquete de Ofimática.	2		$0.00	$0.00
Herramientas de diseño de redes.	5		$0.00	$0.00
Software Libre para servicios de Internet.	10		$0.00	$0.00
Software Libre adicional.			$0.00	$0.00
Recursos Técnicos Comunicación:				
Telefonía convencional.	2	15	$6.00	$90.00
Telefonía celular.	2	25	$10.80	$270.00
SUBTOTAL				$ 2640
COSTO TOTAL DEL PROYECTO:				***$8111,95***

11. CONCLUSIONES

- La utilización de las diferentes técnicas de trabajo permitieron realizar la descripción de la situación actual de la red de datos, aplicando la observación directa y entrevista a los administradores de la red de la Universidad Nacional de Loja, los cuales nos dieron a conocer las características técnicas del hardware, software y direccionamiento IP lógico existentes en la toda la infraestructura de la red de datos.

- Se pudo verificar, que el servicio de Internet utilizado para administrar el acceso a sitios web es mediante un servidor proxy y se realiza un filtrado de paquetes (iptables) en cada uno de los servidores.

- Para realizar la transición a IPv6, se optó por el mecanismo de transición doble pila para la implementación de IPv6 en la red de datos, debido a que los nodos tienen la capacidad de enviar y recibir paquetes IPv4 e IPv6, por lo que resulto el mecanismo más óptimo y transparente para la Universidad Nacional de Loja.

- El direccionamiento IPv6 para los servidores de la intranet, servidores públicos, prefijo IPv6 para el sistema académico y equipos finales, se realizó previo a obtener una longitud de prefijo IPv6 por parte del CEDIA 2800:68:7::/48, igualmente se siguieron las normas preestablecidas de la Sección de Redes y Equipos Informáticos para su implementación.

- Los diferentes servicios de Internet, que se realizó la configuración e implementación de IPv6 son: el sistema de nombres (dns), auto-configuración de direcciones IPv6 (dhcpv6), proxy, router firewall (ip6tables), servidor web (http) y correo electrónico (squirrelmail, smtp, pop y imap), los cuales permiten brindar un servicio eficiente y transparente a los usuarios finales.

- Se verificó el correcto funcionamiento de cada servicio de Internet en IPv4 e IPv6 de los servidores de producción, en la fase de pruebas, lo cual es un indicador de que la implementación de IPv6 cumple con los objetivos planteados.

- La asignación de los parámetros de red IPv6 se asignan automáticamente en las diferentes computadoras con el Sistema Operativo Windows 7, Windows Vista y distribuciones de Gnu / Linux, a excepción de Windows XP se lo debe realizar manualmente por los técnicos de la Sección de Redes y Equipos Informáticos.

12. RECOMENDACIONES

- Realizar una planificación a futuro de actualización de la infraestructura de la red de datos a un modelo jerárquico (capa de núcleo, capa de distribución y capa de acceso), que facilite la implementación de nuevas tecnologías.

- Incorporar el tema del protocolo de internet IPv6 en los currículos de las carreras técnicas de la Universidad Nacional de Loja, principalmente en la materia de redes de Internet (TCP/IP) de manera que los estudiantes conozcan y apliquen este nuevo protocolo.

- Es necesario la instalación y configuración de una herramienta Software Libre, para el monitoreo de tráfico IPv6 en la red de datos, que permita obtener estadísticas generales de la utilización de IPv6 en la intranet y navegación hacia servicios de Internet públicos por parte de los equipos finales.

- De adquirir nuevos dispositivos de networking para la red de datos es necesario tener en cuenta que vengan con soporte nativo de IPv6, de tal manera que sean aprovechados en todo su potencial y no tener que hacer actualizaciones de hardware futuras.

- Se sugiere desarrollar charlas y talleres, en donde se capacite a los administradores de la red de datos y docentes de las carreras técnicas, sobre el protocolo de Internet versión 6 y la transición a IPv6 que adopto la Universidad Nacional de Loja.

- Se recomienda realizar la activación de IPv6 en las computadoras con Sistema Operativo Windows XP manualmente o realizar la actualización a Windows 7 dependiendo de las características de la computadora. Este proceso lo detallamos en el plan de activación de IPv6.

- Se propone a la Unidad de Telecomunicaciones e Información, que mediante nuevos tesistas o los técnicos de la Sección de Redes y Equipos Informáticos realicen nuevos estudios que permita la implementación de IPv6 en la red inalámbrica IEEE 802.11 de todo el campus universitario.

12. BIBLIOGRAFÍA Y REFERENCIAS.

Libros:

1. BARRETT, Daniel; SILVERMAN, Riachard; BYRNES, Robert. 2003. Linux Security CookBook. United States of America.
2. HAGAN, Silvia. 2002. IPv6 Essentials, United States of America.
3. SILBERSCHATZ, Abrahan; GALVIN, Peter; GAGNE, Gregne. 2008. Procesos. EN: Sistemas Operativos. 6a. ed. México, Grupo Noriega Editores. pp. 87 – 104.
4. SILBERSCHATZ, Abrahan; GALVIN, Peter; GAGNE, Gregne. 2008. Estructura de Redes. EN: Sistemas Operativos. 6a. ed. México, Grupo Noriega Editores. pp. 469 – 500.
5. SILBERSCHATZ, Abrahan; GALVIN, Peter; GAGNE, Gregne. 2008. El Sistema Linux. EN: Sistemas Operativos. 6a. ed. México, Grupo Noriega Editores. pp. 669 – 715.
6. TANENBAUM, Andrew S. 2003. Redes de Computadoras. 4a. ed. México, Cámara Nacional de la Industria Editorial Mexicana.

Tesis:

1. ESCUELA DE CIENCIAS COMPUTACIONALES. 2008. Implementación de Servicios de Internet sobre IPv6 para UTPL. Ingeniería Investigación Información Internet (i4). No. (2): 141-145. Abril.
2. JARA SABA., Felipe Ernesto. 2009. Estudio e Implementación de una Red IPv6 en la UTFSM. (Tesis Ing. Civil Telemático) Valparaíso Chile, Universidad Técnica Federico Santa María. Departamento de Electrónica. 25 p.

Reporte Técnico:

1. GAGLIANO, Roque. Planificando IPv6. [diapositiva] Lacnic. 25, 50 diap.

Sitios Web:

1. WIKIMEDIA FOUNDATION, Inc. IPv6. Wikipedia, La enciclopedia libre. [en línea]. disponible en: http://es.wikipedia.org/wiki/Ipv6, [Consulta: 2 noviembre 2010].
2. IAB; IESG. 2001. Recommendations on IPv6 Allocations to Site. [en línea]. disponible en: www.ietf.org/rfc/rfc3177.txt, [Consulta: 4 noviembre 2010].
3. HINDEN, R; DEERING S. 2003. Internet Protocol Version 6 (IPv6) Addressing Architecture. [en línea]. disponible en: www.ietf.org/rfc/rfc3513.txt, [Consulta: 4 noviembre 2010].
4. CONTA, A; DEERING S. 2006. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. [en línea]. disponible en: www.ietf.org/rfc/rfc4443.txt, [Consulta: 27 enero 2011].
5. TASK FORCE, IPv6. The Portal IPv6. [en línea]. disponible en: www.ipv6tf.org, [Consulta: 28 enero 2011].
6. FORUM, IPv6. The IPv6 Forum, The New Internet, Driving IPv6 Deploymet. [en línea]. disponible en: www.ipv6forum.com, [Consulta: 24 enero 2011].
7. ELECTRIC, HURRICANE. Hurricane Electric IPv6. [en línea]. disponible en: http://ipv6.he.net, [Consulta: 2 diciembre 2010].
8. HINDEN, R; DEERING S. 1998. IPv6 hace frente a la Arquitectura. [en línea]. Disponible en: http://www.normesinternet.com/normes.php?rfc=rfc2373&lang=es, [Consulta: 25 enero 2011].
9. LACNIC. Portal IPv6. [en línea]. disponible en: http://portalipv6.lacnic.net, [Consulta: 22 noviembre 2010].
10. IPv4 Address Report. 2010. [en línea]. disponible en: http://www.potaroo.net/tools/ipv4, [Consulta: 2 diciembre 2010].
11. DEERING, S; HINDEN R. 1998. Protocolo Internet, Versión 6 (IPv6). [en línea]. disponible en: www.rfc-es.org/rfc/rfc2460-es.txt, [Consulta: 5 noviembre 20110].
12. THOMSON, S; NARTEN T. 1998. Configuración Automática sin Estado de Direcciones IPv6. [en línea]. disponible en: www.rfc-es.org/rfc/rfc2462-es.txt, [Consulta: 23 diciembre 2010].
13. SIXXS. IPv6 Deployment & Tunnel Broker. [en línea]. disponible en: www.sixxs.net, [Consulta: 11 noviembre 2010].

14. ANEXOS

Anexo N° 1

UNIVERSIDAD NACIONAL DE LOJA
UNIDAD TELECOMUNICACIONES E INFORMACIÓN

LIC. JAMIL RAMÓN CARRION

C E R T I F I C A:

Que en la red de datos de Ethernet 802.3 de la Universidad Nacional de Loja, se ha desarrollado la implementación del proyecto de investigación que titula **"ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPv6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE"** de los aspirantes a obtener el título de Ingenieros en Sistemas señores egresados: Jhon Alexander Calderón Sanmartín y Rubí Rafael Cabrera Erreyes. Este proyecto se ha desarrollado en los términos que fue planteado en la propuesta, y en la actualidad tiene el aval respectivo de la Unidad de Telecomunicaciones e Información ya que se encuentra funcionando adecuadamente.

Es cuanto puedo certificar en honor a la verdad.

Loja, 12 de julio de 2011

Lo certifica,

UNIVERSIDAD NACIONAL DE LOJA
JEFATURA DE INFORMATICA

Lic. Jamil Ramón C.
DIRECTOR TELECOMUNICACIONES E INFORMACIÓN

Anexo N° 2
ENCUESTAS A JEFES DEPARTAMENTALES

UNIVERSIDAD NACIONAL DE LOJA
Unidad de Telecomunicaciones e Información
Sección Redes y Equipos Informáticos

Encuestadores:

Jhon Alexander Calderón Sanmartin.
Rubi Rafael Cabrera Erreyes.

Estimado (a), dígnese en llenar la presente encuesta relacionada con la "Implementación del protocolo de Internet versión 6 (IPv6) en la red de datos de la Universidad Nacional de Loja".

1.- ¿Considera que la implementación de IPv6 en la red de datos de la Universidad Nacional de Loja se realizó de una forma exitosa ?.

Si ( )
No ( )

Por qué: .....

2.- ¿Considera importante la transición a IPv6 en el campus de la Universidad, para brindar los servicios de Internet tanto en la intranet, red Pública (Internet) y navegación ?.

Si ( )
No ( )

Por qué: .....

3.- ¿Cree necesario que la red IPv6 asignada a la UNL 2800:60:7:: / 48 por parte del CEDIA es suficiente para conectar todos los nodos de la red Universitaria y garantizar un crecimiento a futuro de unos 20 años ?.

Si ( )
No ( )

Por qué: .....

4.- ¿Teniendo en cuenta como precedente el agotamiento de direcciones IPv4, considera necesario que las universidades que forman parte del CEDIA empiecen a realizar la transición a IPv6 ?.

Si ( )
No ( )

Por qué: .....

5.- ¿Si está en su decisión adquirir nuevos dispositivos de networking en la Universidad, tendría en cuenta que vengan con soporte nativo de IPv6 ?.

Si ( )
No ( )

Por qué: .....

6.- ¿El uso de Software Libre y Open Source para la implementación de IPv6 en la Universidad Nacional de Loja, como lo califica ?.

Muy bueno ( )
Bueno ( )
Regular ( )
Malo ( )

Por qué: .....

Nombre del encuestado (a): ***Firma:***

Anexo N° 3
ENCUESTAS APLICADA A TÉCNICOS DE LA SECCIÓN DE REDES Y SOFTWARE

UNIVERSIDAD NACIONAL DE LOJA
Unidad de Telecomunicaciones e Información
Sección Redes y Equipos Informáticos

Encuestadores:

Jhon Alexander Calderón Sanmartin.
Rubi Rafael Cabrera Erreyes.

Estimado (a), dígnese en llenar la presente encuesta relacionada con la "Implementación del protocolo de Internet versión 6 (IPv6) en la red de datos de la Universidad Nacional de Loja".

1.- ¿ Considera que la implementación de IPv6 en la red de datos de la Universidad Nacional de Loja se realizó de una forma exitosa ?.

Si ( )
No ( )

Por qué: .....

2.- ¿ Cuáles cree usted que son la características más importantes de IPv6 ?.

Facilidad de administración. ( )
Auto-configuración. ( )
Seguridad. ( )
Conexión extremo a extremo. ( )
Movilidad. ( )
Mayor número de direcciones. ( )
Calidad y servicio. ( )
Otros:
.....
.....

3.- ¿ Que calificación daría a los servicios de Internet: dns, dhcp, proxy, firewall, web y correo configurados con en el mecanismo de transición doble pila (IPv4 e IPv6) ?.

Muy bueno ( ) Bueno ( ) Regular ( ) Malo ( )

Por qué: .....

4.- ¿ En que porcentaje se le presentaron inconvenientes en la configuración de los parámetros de red IPv6, al momento de configurar su interfaz ?.

0 % ( )
5 % ( )
25 % ( )
50 % ( )
75 % ( )
100 % ( )

5.- ¿ De qué forma considera que deberá hacerse la asignación de los parámetros de red IPv6 (dirección IPv6, prefijo, gateway, dns, u otros) a los equipos finales ?.

Auto-configuración sin estado ( )
Auto-configuración con estado (dhcpv6) ( )
Manual ( )
Otros:
.....

Por qué: .....

Nombre del encuestado (a): ***Firma:***

Anexo N° 4
ANTEPROYECTO DE TESIS

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE ENERGÍA, INDUSTRIAS Y RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMAS

ANTEPROYECTO DE TESIS

TEMA: *"ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPV6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE."*

AUTORES:

RUBI RAFAEL CABRERA E.
JHON ALEXANDER CALDERÓN S.

LOJA – ECUADOR
2010

1. TÍTULO

"ESTUDIO E IMPLEMENTACIÓN DEL PROTOCOLO INTERNET VERSIÓN 6 (IPV6) EN LA RED DE DATOS ETHERNET IEEE 802.3 DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE Y OPEN SOURCE."

2. PROBLEMÁTICA

2.1.Situación problemática.

La Universidad Nacional de Loja, como uno de los centros de educación superior más grandes del sur del país, viene buscando cada día nuevas alternativas tecnológicas con el objetivo de brindar servicios más eficientes a la comunidad universitaria y a la sociedad.

Esta institución educativa cuenta con un rango de direcciones IPv4 privadas para su Intranet la misma que permite la comunicación entre los diferentes dispositivos de networking, accediendo a los servicios de Internet que se brinda en el campus universitario y así mismo la red de redes Internet por medio de NAT (Traducción de Direcciones de Red), NAT se desarrolló para resolver la falta de direcciones IPv4, lo cual permite que los equipos con direcciones privadas IP compartan una dirección IP enrutable (IP pública). Entonces visto desde afuera prácticamente todos los equipos de la Intranet poseen la misma dirección IPv4 pública.

La Universidad también dispone de un rango de direcciones IPv4 públicas asignadas por NIC.EC (Registro de Nombres de Dominio del Ecuador), con dichas direcciones la institución brinda sus servicios de Internet al mundo entero.

Uno de los principales problemas de IPv4 es la escasez de IPs debido al crecimiento exponencial de hosts en Internet. En un principio la distribución general de IPs se realizó sin ninguna norma es decir se asignaron bloques de direcciones grandes (de 16.271 millones de direcciones) a países e incluso a empresas, dando paso a una estructura mal repartida y desorganizada, y una serie de arreglos sobre otros para intentar solucionar temporalmente el problema. Aunque IPv4 pude proveer hasta 4.294.967.296 direcciones IPs únicas, que en un principio pueden parecer suficientes, no lo es para el concepto de Internet de hoy en día, en la

cual cada dispositivo (router, swicth, pc, PDA, teléfono, cámara fotográfica, webcam, ventilador, etc) pretende tener una IP propia y permanente.

El 20 de junio de 2007, LACNIC (Registro de Direcciones de Internet para América Latina y el Caribe) anuncia el inminente agotamiento de las direcciones IPv4. Se estima que en 3 años se agotarían las direcciones disponibles para conectarse a Internet bajo el protocolo actual. Ante esta situación LACNIC toma medidas para el apoyo y la promoción de la adopción de IP versión 6 en la región. Los pronósticos hechos por varios investigadores, que indican que para el año 2011 el stock central de direcciones de Internet versión 4 (IPv4) podrían estar definitivamente agotadas.

Actualmente existen nuevas tendencias sobre tener una mayor comunicación dentro de la sociedad con servicios más seguros, eficientes y rápidos, nuestro centro de educación superior no puede estar al margen de la innovación tecnológica. Producto de esta innovación tecnológica, se puede contar con una organización de red de datos que funcione de la mejor manera para cubrir necesidades de comunicación de los usuarios, así como la necesidad de estar inmersos en el mundo de la información global como Internet. Es por eso que se ha creído conveniente presentar una alternativa de solución que permita una comunicación rápida, segura y eficiente, entre los diferentes servicios de Internet, dispositivos de networking y usuarios finales de la Universidad Nacional de Loja.

La versión actual del Protocolo de Internet (IPv4) ya presenta algunas limitaciones en el funcionamiento de las redes de hoy y por tanto de la Internet del futuro. Es así como surge el IPv6 que es la versión 6 del Protocolo de Internet como un paso evolutivo del IPv4, para superar deficiencias y ofrecer nuevas y mejores funcionalidades. Representa el fruto de muchas propuestas del grupo de trabajo del Internet (IETF) y de otros grupos centrados en desarrollar un "Protocolo de Internet de Nueva Generación o IPng", con características que están permitiendo tener más y mejores redes, superando las limitaciones del IPv4.

Teniendo en cuenta que es requerimiento institucional, se propone la implementación de IPv6, para no limitar el alcance del consumo de los servicios de Internet no solamente dentro del campus universitario sino también, proporcionando su acceso desde cualquier parte externa de las instalaciones universitarias.

La tecnología IPv6 ofrece beneficios que superan en mucho los ofrecidos por IPv4, mismos que impactarán gradualmente en la adopción de IPv6. El protocolo IPv6 no es una migración o un cambio más bien es una transición a la evolución creado con la finalidad de solucionar los problemas de IPv4 provocado por la gran demanda de direcciones IP y la mala administración que se tuvo al inicio, dio un colapso de dichas direcciones. Los métodos que utiliza IPv4 para determinar la entrega de los paquetes dentro de la red son realmente insuficientes para transportar paquetes que tienen prioridades altas.

La propuesta está basada en la implementación del protocolo Internet versión 6 (IPv6), el mismo que se ha venido impulsando por el CEDIA, y ya se ha implementado en otros centros de educación superior de país permitiendo mejorar los diferentes servicios de internet que ofrecen a sus clientes y usuarios.

Dentro de las principales ventajas de IPv6 se encuentran: un mayor número de direcciones, direccionamiento jerárquico, nuevo formato de cabecera, autoconfiguración de nodos capaces de auto asignarse una dirección IPv6 sin intervención del usuario, seguridad con soporte nativo para una capa de cifrado de red y autenticación, calidad y servicio en la prioridad de un paquete.

2.2.Problema general de investigación.

La falta de direcciones IPv4 globales y la duplicidad ha generado que no se pueda realizar una buena administración de la red de datos en la Universidad Nacional de Loja, lo cual conlleva la implementación de IPv6, que permitirá a la institución estar a la par con la tecnología y brindar servicios de Internet eficientes y eficaces.

2.3.Delimitación.

- **Problemas específicos de investigación.**
  - ✓ Desconocimiento y falta de documentación en la infraestructura de la red de datos Ethernet 802.3 de la Universidad Nacional de Loja.
  - ✓ Desconocimiento de un método de transición que se acople a los requerimientos de la institución universitaria, lo que nos permitirá a través de la investigación determinar el método de transición más eficiente.

- ✓ No se cuenta con un diseño de transición de direcciones IPv4 a IPv6, lo que conlleva a desarrollar un diseño acorde al direccionamiento IP actual de la Universidad Nacional de Loja basado en IPv6.

- ✓ La no existencia de IPv6, conlleva a realizar la instalación y configuración del hardware y software necesario para la red de datos Ethernet 802.3 de la Universidad Nacional de Loja.

- ✓ No se conoce estrategias de implantación de los servicios de Internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.

- **Espacio.**

El desarrollo de la presente investigación e implementación de IPv6, se llevará a cabo en la Universidad Nacional de Loja.

- **Tiempo.**

El tiempo estimado del proyecto son seis meses a partir de la fecha de su aprobación.

- **Unidades de observación.**

Lo más relevante para realizar la implementación de IPv6 son las siguientes unidades de observación:

1. Fuentes bibliográficas, digitales y asesoramiento, acerca del funcionamiento de IPv6.
2. Método de transición de direcciones IPv4 a IPv6.
3. Monitoreo de la red de datos de la Universidad Nacional de Loja.
4. Software y herramientas que soporten IPv6.
5. Sistema Operativo Gnu / Linux.
6. Petición de comentarios (RFC).

3. JUSTIFICACIÓN

3.1.Justificación.

El proyecto **"Estudio e Implementación del Protocolo Internet Versión 6 (IPv6) en la red de datos Ethernet IEEE 802.3 de la Universidad Nacional de Loja utilizando Software Libre y Open Source"**, se justifica plenamente por los siguientes considerandos:

Justificación Académica.

La Universidad Nacional de Loja es una de las instituciones de Educación Superior pioneras en el desarrollo de la región sur del país que ha sustentado su progreso en la investigación permanente de los problemas que se suscitan en las prácticas profesionales y en preparar, por consiguiente, a estudiantes para que estén en capacidad de resolver problemas de la realidad social, razón por la cual el presente proyecto se justifica académicamente, ya que nos permitirá poner en práctica e incrementar los conocimientos adquiridos durante nuestra formación académica, y de esta manera obtener mayor experiencia en el campo informático; además este proyecto servirá como requisito indispensable para obtener el título de Ingenieros en Sistemas.

El "Estudio e Implementación del Protocolo Internet Versión 6 (IPv6) en la red de datos Ethernet IEEE 802.3 de la Universidad Nacional de Loja utilizando Software Libre y Open Source", contribuirá positivamente en el desarrollo académico de los estudiantes y docentes, puesto que podrá brindar mayor cantidad de servicios, necesarios para una educación de alta calidad, también servirá como fuente de consulta para futuras investigaciones.

Justificación Técnica.

Técnicamente el proyecto es justificable, ya que se dispone de la tecnología adecuada que permitirá el desarrollo e implementación del Protocolo de Internet versión 6. Es importante resaltar que se hace necesario el dominio de métodos y técnicas que aseguren el correcto funcionamiento de ambos protocolos (IPv4 e IPv6) en un ambiente de producción.

Justificación Operativa.

Para llevar a cabo este proyecto de investigación se cuenta con la debida autorización del director de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de

Loja en donde se realiza la administración de la red de datos; siendo un requerimiento institucional se dio la apertura necesaria para realizar la ejecución del proyecto investigativo, igualmente se cuenta con el apoyo por parte de los técnicos y el asesoramiento adecuado en el tema.

Justificación Económica.

Según el análisis realizado, nuestro proyecto es económicamente factible ya que la Universidad Nacional de Loja cuenta con una infraestructura de red de datos Ethernet 802.3 base para la implementación del Protocolo de Internet versión 6, resaltando que se utilizará el hardware que posee la Unidad de Telecomunicaciones e Información, Software Libre, Open Source y documentación con licencia libre disponible en Internet; minimizando así considerablemente los costos de implantación.

3.2.Viabilidad.

Es viable porque los conocimientos adquiridos durante la carrera de Ingeniería en Sistemas tanto teóricos como prácticos, nos dan las capacidades y habilidades para el correcto desarrollo del proyecto investigativo, existen los medios necesarios (tecnología, hardware y herramientas de software), que permitirá el funcionamiento y operatividad del mismo.

4. OBJETIVOS

4.1.General.

- ✓ Realizar el estudio e implementación del nuevo Protocolo Internet Versión 6 (IPv6) en la Universidad Nacional de Loja utilizando Software Libre y Open Source.

4.2.Específicos.

- ✓ Describir la situación actual de la infraestructura en la red de datos Ethernet 802.3 de la Universidad Nacional de Loja para la implementación del Protocolo Internet versión 6.

- ✓ Describir el Protocolo de Internet versión 6, que permita determinar el método de transición de IPv4 a IPv6 más eficiente.

- ✓ Diseñar el mecanismo de transición de IPv4 a IPv6, acorde al direccionamiento IP actual de la Universidad Nacional de Loja para su aplicabilidad.

- ✓ Instalar y configurar el hardware y software necesario para la red de datos Ethernet IEEE 802.3 de la Universidad Nacional de Loja que soporten IPv6.

- ✓ Desarrollar e implementar los servicios de Internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.

5. MARCO TEÓRICO

CAPÍTULO I: PROTOCOLO INTERNET VERSIÓN 6 (IPV6).

El Protocolo Internet versión 6 (IPv6) es a veces llamada la siguiente generación de Internet Protocolo, o IPng. Es una nueva versión de IP (Protocolo *Internet*), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, que actualmente esta implementado en la gran mayoría de dispositivos que acceden a Internet.

Aún cuando el protocolo existente, IPv4, proporciona un espacio de direcciones de 32 bits, que teóricamente son 232 direcciones globales únicas (aproximadamente 4.000 millones), en la práctica, el número de direcciones globales IPv4 que pueden ser utilizadas es bastante inferior, debido a las ineficiencias en la asignación y uso de las direcciones. IPv4 tiene una capacidad limitada inherente para permitir la expansión de Internet y por tanto no

permite conectar miles de millones de dispositivos cuando sea apropiado. La traducción de direcciones de red (Network Address Translation, NAT), conjuntamente con direcciones IPv4 privadas, ha permitido la prolongación de la vida útil de IPv4. Sin embargo, NAT añade complejidad al despliegue de nuevos modelos extremo a extremo, inhibiendo el crecimiento de Internet y la innovación, incluyendo aquellos servicios como "siempre-conectado" y "peer-to-peer", que requieren acceso seguro y constante a dispositivos como por ejemplo en redes domésticas. IPv6 ha sido concebido para facilitar estos dos objetivos, proporcionando una capacidad de direccionamiento virtualmente ilimitada que puede direccionar hasta 2128 dispositivos (hasta 340.282.366.920.938.463.463.374.607.431.768.211.456).

1.1.Historia.

El esfuerzo para desarrollar un sucesor del protocolo IPv4 se inició en la década de 1990 por la Internet Engineering Task Force (IETF). Varios esfuerzos paralelos comenzó al mismo tiempo, todos tratando de resolver la limitación de espacio de direcciones previstas, así como proporcionar una funcionalidad adicional. El IETF empezó la zona de IPng en 1993 para investigar las diferentes propuestas y hacer recomendaciones para los procedimientos.

Los directores de área IPng de la IETF recomienda la creación de IPv6 en la reunión de la IETF Toronto en 1994. Su recomendación se especifica en el RFC 1752, "La recomendación para la próxima generación del protocolo IP." Los directores formaron la Address Lifetime Expectation (ALE) grupo de trabajo, cuyo trabajo fue determinar si la duración prevista para el IPv4, que permitiría el desarrollo de un protocolo con la nueva funcionalidad, o si el resto del tiempo sólo permitiría el desarrollo de una solución de espacio de direcciones. En 1994, el grupo de trabajo ALE prevee el agotamiento de direcciones IPv4 que puede ocurrir en algún momento entre 2005 y 2011, basado en las estadísticas de que se disponía en ese momento.

Para aquellos de ustedes que están interesados en las diferentes propuestas, aquí hay más información al respecto (de RFC 1752). Había cuatro principales propuestas que se CNAT, IP Encaps, Nimrod, y Aimple CLNP. Hay más propuestas son el fruto:el P Internet Protocol (PIP), el Simple Internet Protocol (SIP), y TP / IX. Después de la reunión de marzo de 1992 en San Diego IETF, Simple CLNP convertido en TCP y UDP con Bigger Address (TUBA) y IP Encaps evolucionado en IP Address Encapsulation (IPAE). IPAE se fusionó con el PIP y SIP y se llamó a sí Simple Internet Protocol Plus (SIPP). El TP / IX grupo de trabajo

cambió su Common Architecture for the Internet (CATNIP). Las principales propuestas son ahora CATNIP, TUBA, y SIPP. Para una breve discusión de las propuestas, consulte RFC 1752.

El Internet Engineering Steering Group aprobó la recomendación de IPv6 y redactó una norma propuesta el 17 de noviembre de 1994. El conjunto básico de protocolo IPv6 se convirtió en un Proyecto de Norma IETF el 10 de agosto de 1998.

1.2.Ventajas del protocolo IPv6.

Consecuentemente, el diseño de IPv6 fue una forma oportunística de mejorar Internet, con nuevas ventajas tales como:

- ✓ Auto-configuración y re-configuración sin servidores ("enchufar y funcionar", "plug and play"). Con esta característica Internet se simplifica, en el sentido de que es más fácil conectar automáticamente cualquier dispositivo a la red. No hay motivos para pedir a los usuarios que configuren nunca más los dispositivos, especialmente considerando que los nuevos dispositivos no serán "sencillos" ordenadores con teclado y pantalla, sino electrodomésticos, dispositivos de todo tipo, sensores, etc., los cuales no tienen este tipo de interfaces para poder ser configurados. En IPv4 esto no se puede realizar salvo que en la red se haya instalado un servidor (para el protocolo DHCP), lo que implica un coste superior para el propio servidor y su mantenimiento.

- ✓ Mecanismos de movilidad más eficientes y robustos. IPv6 ha sido diseñado bajo la perspectiva de un nuevo mundo "nómada". Usuarios y dispositivos tienden a movilizarse más que nunca. La conectividad es importante incluso cuando nos desplazamos, de tal forma que podamos utilizar servicios mejorados, especialmente en entornos sin cables. IPv4 también permite movilidad, pero es muy ineficiente comparada con la movilidad en IPv6.

- ✓ Seguridad extremo a extremo con autenticación y encriptación embebidas en la capa IP. IPsec es el protocolo de seguridad, el mismo que en el caso de IPv4. La principal diferencia es que IPv4 no obliga al soporte de IPsec, lo que implica que no siempre está disponible. Además, en IPv4, debido al uso de NAT, a menudo no es posible utilizar IPsec extremo a extremo, salvo que se posean los conocimientos necesarios

para configurar un túnel o VPN (Red Privada Virtual, Virtual Private Network), entre las dos estaciones que desean establecer dicha comunicación y se atraviesen los NAT.

- ✓ Cabecera con un formato mejorado e identificación de flujos. Los diseñadores del protocolo IPv6 sacaron provecho de los conocimientos adquiridos con la experiencia por el uso de IPv4 durante los últimos años, de forma que pudiera mejorarse la forma en que los datos se codifican para formar la cabecera del protocolo IPv6 consecuentemente mejorar la operación de la red. Al mismo tiempo que la cabecera ha sido simplificada, hemos agregado nuevas funcionalidades, siendo una de ellas la identificación de flujos, lo cual permitirá en un futuro próximo una mejor operación de los mecanismos de calidad de servicio (QoS) en Internet.

- ✓ Soporte mejorado de multidifusión. IPv6 incluye soporte mejorado de multidifusión (multicast), dado que se trata de una característica embebida en el protocolo, la cual es fundamental para el uso de redes de banda ancha para la distribución de contenidos.

- ✓ Extensibilidad. Soporte mejorado para opciones/extensiones. Por último, pero no menos importante, IPv6 ha sido diseñado teniendo en cuenta las posibilidades para su crecimiento. No deseamos repetir errores y llegar a la situación de descubrir, en unos pocos años, que del mismo modo que diseñamos IPv4 de tal forma que ha llegado a ser un impedimento para la extensión de Internet, pueda ocurrir con IPv6. La forma en que IPv6 trabaja permite incorporar nuevas características o piezas del protocolo (las que denominamos cabeceras de extensión), sin necesidad de actualizar todos los dispositivos de la red. Sólo aquellos dispositivos que precisen usar determinadas extensiones tienen que ser actualizados, del mismo modo que hoy todos los sistemas operativos y aplicaciones son frecuentemente actualizados, de una forma automática, transparente para el usuario.

1.3.Características del protocolo IPv6.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Algunas de las características más relevantes de IPv6 son:

- ✓ Mayor número de direcciones: El tamaño de una dirección aumenta desde 32 a 128 [bits] lo que se traduce en alrededor de ***3,4 x 10 elevado 38*** direcciones disponibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.

- ✓ Direccionamiento jerárquico: Las direcciones IPv6 globales están diseñadas para crear una infraestructura eficiente, jerárquica y resumida de enrutamiento basada en la existencia de diversos niveles de ISP. Esto permite contar con tablas de enrutamiento más pequeñas y manejables.

- ✓ Nuevo formato de cabecera: Aún cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado campos que en la práctica eran poco usados, de forma de hacer más eficiente el manejo de los paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.

- ✓ Autoconfiguración: IPv6 incorpora un mecanismo de auto configuración de direcciones, "stateless address configuration", mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

- ✓ Seguridad: IPv6 incluye soporte nativo para una capa de cifrado de red y autenticación, una característica añadida eventualmente a IPv4 por medio de tecnologías como IPsec.

- ✓ Nuevo protocolo para interactuar con vecinos: El protocolo de descubrimiento de vecinos, reemplaza a los protocolos ARP y "Router Discovery" de IPV4. Una de sus mayores ventajas es que elimina la necesidad de los mensajes del tipo "broadcast".

- ✓ Calidad y Servicio: IPv6 proporciona un medio para especificar la prioridad de un paquete, lo que conllevará a una reducción de la latencia para el caso del vídeo streaming y otras retransmisiones en tiempo real.

1.4.Formato de la cabecera IPv6.

Un paquete IPv6 tiene una cabecera de tamaño fijo e igual a 40 [bytes], el doble de la cabecera IPv4. Este aumento se debe a que el tamaño de los campos "Dirección Origen" y "Dirección Destino" aumentaron su tamaño de 32 a 128 [bits] cada uno.

La cabecera IPv6 posee los siguientes 8 campos:

1.4.1. Versión (Version). Es de 4 bits de largo e identifica la versión del protocolo IP, en este caso es igual a 6.

1.4.2. Clase de tráfico (Traffic class). El campo de 8 bits Clase de Tráfico en la cabecera IPv6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6. Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

- ✓ La interface de servicio para el servicio IPv6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por ese protocolo de capa superior. El valor por defecto debe ser cero para todos los 8 bits.

- ✓ Los nodos que soportan un uso (experimental o estándar eventual) específico de algunos o todos los bits Clase de Tráfico se les permite cambiar el valor de esos bits en los paquetes que ellos originan, reenvían, o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar a cualquiera de los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

- ✓ Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido son los mimos que el valor enviado por el origen del paquete.

1.4.3. Etiqueta de flujo (Flow Level). El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en "tiempo real".

Un flujo es una secuencia de paquetes enviados a un destino unicast o multicast que necesita manejo especial por los routers ipv6 que intervienen. Todos los paquetes pertenecientes a un mismo flujo debe ser enviado con la misma dirección fuente, dirección destino y etiqueta de flujo. Un ejemplo de un flujo sería paquete que soporta un servicio en tiempo real, como audio o vídeo. Etiqueta de flujo es usado por esa fuente para etiquetar esos paquetes que requieren manejo especial por el nodo ipv6. Si un host o router no soporta funciones de Etiqueta de flujo, el campo es fijado a cero en el origen e ignorado en la recepción.

1.4.4. Longitud de carga útil (Payload length). Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos. Nótese que cualquiera de las cabeceras de extensión presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud.

1.4.5. Cabecera siguiente (Next header). Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4.

1.4.6. Límite de saltos (Hop limit). Entero sin signo de 8 bits. Indica el máximo número de saltos que puede realizar el paquete, decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es decrementado hasta cero.

1.4.7. Dirección origen (Source address). Dirección de 128 bits que identifica el originador del paquete. El formato de este campo es más ampliamente definido en el RFC 2373 (Arquitectura de direccionamiento para la versión 6 del IP).

1.4.8. Dirección destino (Destination address). Dirección de 128 bits que identifica el destinatario que tiene la intención de recibir el paquete. Una importante distinción es la de que el destinatario que tiene la intención de recibir el paquete puede no ser el destinatario final, como la *Cabecera de Enrutamiento* puede ser empleado para especificar la ruta que el paquete toma desde su fuente, a través de destinatario(s) intermedio(s), y así hasta su destinatario final.

1.5.Representación de una dirección IPv6.

Las direcciones IPv6 están compuestas de 8 campos de 2 bytes (16 bits) de largo separadas por ":" (dos puntos), cada campo está representado por cuatro caracteres hexadecimales (0 – F).

Hay tres formas convencionales de representación de direcciones IPv6 como cadenas de texto:

- La forma preferida es x:x:x:x:x:x:x:x, donde la "x"s son los valores hexadecimales de las ocho campos de 16 bits de la dirección.

Ejemplos:

2001: DB8: 7654:3210: FEDC: BA98: 7654:3210

2001:DB8:0:0:8:800:200C:417A

Tenga en cuenta que no es necesario escribir los ceros a la izquierda en un campo individual, pero debe haber al menos un número en cada campo.

- Debido a algunos métodos de asignación de ciertos estilos de direcciones IPv6, que será común para las direcciones que contienen cadenas largas de cero bits. Con el fin de hacer la escritura que contiene las direcciones cero bits más fácil una sintaxis especial está disponible para comprimir los ceros a la izquierda.

El uso de "::" indica múltiples grupos de 16-bits de ceros. El "::" sólo puede aparecer una vez en una dirección. El "::" también puede ser utilizado para comprimir el principal y / o ceros en una dirección.

Ejemplos:

Las siguientes direcciones:

2001*:DB8:0:0:0008:800:200C:417A* ***una dirección unicast***

FF01:0:0:0:0:0:0:101 ***una dirección multicast***

0:0:0:0:0:0:0:1	***dirección de loopback***
0:0:0:0:0:0:0:0	***direcciones no especificada***

Podrán estar representados por:

2001:DB8::8:800:200C:417A	***una dirección unicast***
FF01::101	***una dirección multicast***
:: 1	***dirección de loopback***
::	***dirección no especificada***

- Una forma alternativa que a veces es más conveniente cuando se trata con un entorno mixto de nodos IPv4 e IPv6 es x: x: x: x: x: x:d.d.d.d, donde la "x"s son los valores de los seis campos hexadecimales de alto orden de 16-bit de la dirección, y las "d"s son los valores los cuatro campos decimales de bajo orden de 8 bits de la dirección (representación estándar IPv4).

Ejemplos:

Las siguientes direcciones:

0:0:0:0:0:0:192.188.49.2

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

O en forma comprimida:

::192.188.49.2

:: FFFF:129.144.52.38

Con el fin de simplificar la escritura y memorización de direcciones, se pueden aplicar las siguientes reglas a las direcciones IPv6:

- ✓ No se hace distinción entre mayúsculas y minúsculas. "ABC9" es equivalente a "abc9".
- ✓ Tal como en el caso de IPv4, para señalar las secciones de la dirección que identifican a la red y al dispositivo, se utiliza el formato CIDR (Encaminamiento Inter-Dominios sin Clases) en la forma ***<dirección>/<prefijo>***. Por ejemplo, una dirección en la forma ***2001:DB8:c18:1::1/64*** señala que los primeros 64 [bit] identifican a la red (***2001:DB8:c18:1***) y los restantes 64[bit] identifican al dispositivo de dicha red (***::1***).
- ✓ Tradicionalmente el uso del símbolo ":" en las dirección IPv4 señala un puerto en un determinado nodo, por ejemplo ***192.168.1.1:80*** señala al puerto 80 (***www***) del nodo ***192.168.1.1***. Esto representa un problema de incompatibilidad al utilizar direcciones IPv6, por lo que se ha establecido que para señalar un puerto en una determinada dirección IPv6, esta debe estar encerrada por paréntesis cuadrados en la forma ***[dirección]:puerto***.

1.6.Representación de los prefijos de las direcciones.

La representación de los prefijos de dirección IPv6 es similar a los prefijos de direcciones IPv4 que están escritos en notación CIDR. Un prefijo de dirección IPv6 se representa con la siguiente notación:

direccion-ipv6/longitud-prefijo

- ***direccion-ipv6***: Es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.
- ***longitud-prefijo*:** Es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

Ejemplo:

Las siguientes son representaciones legales de prefijos de 60 bits *2001DB8000000CD30* (hexadecimal):

- ✓ *2001: DB8:0000:CD30:0000:0000:0000:0000 / 60*
- ✓ *2001:DB8::CD30:0:0:0:0 / 60*
- ✓ *2001:DB8:0:CD30:: / 60*

Las siguientes no son representaciones legales de las anteriores prefijo:

- ✓ ***2001:DB8:0:CD3 / 60*** - Puede caer ceros a la izquierda, pero no ceros, dentro de cualquier parte de 16 bits de la dirección
- ✓ ***2001:DB8::CD30 / 60*** - Dirección a la izquierda de "/" se amplía a *2001:DB8:0000:0000:0000:0000:0000:CD30*
- ✓ ***2001::CD3 / 60*** Dirección a la izquierda de "/" se amplía a 2001*:0000:0000:0000:0000:000:0000:0CD3*

Al escribir tanto una dirección de nodo y un prefijo de la dirección de nodo que (Por ejemplo, el nodo del prefijo de subred), los dos pueden combinarse como sigue:

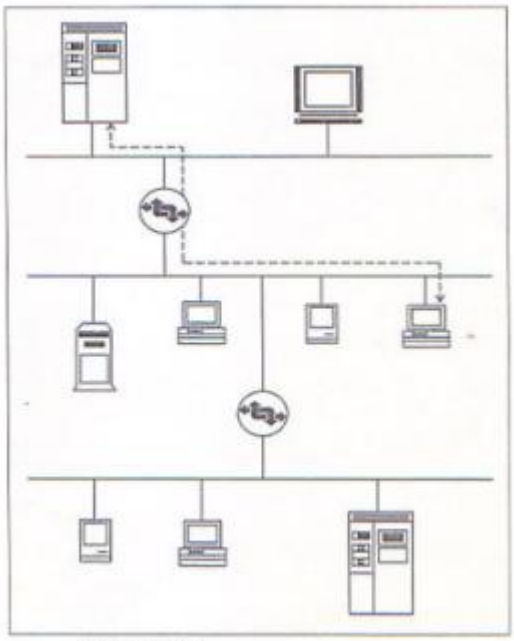
- ✓ La dirección del nodo 2001:DB8:0:CD30:123:4567:89AB:CDEF
- ✓ Y su número subred 2001:DB8:0:CD30:: / 60
- ✓ Puede ser abreviada como 2001:DB8:0:CD30:123:4567:89AB:CDEF / 60

1.7.Modelos de direccionamiento IPv6.

Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante que no haya que olvidar. Todas las interfaces han de tener, por los menos, una dirección de enlace local (Link -Local) de tipo unicast. Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope).

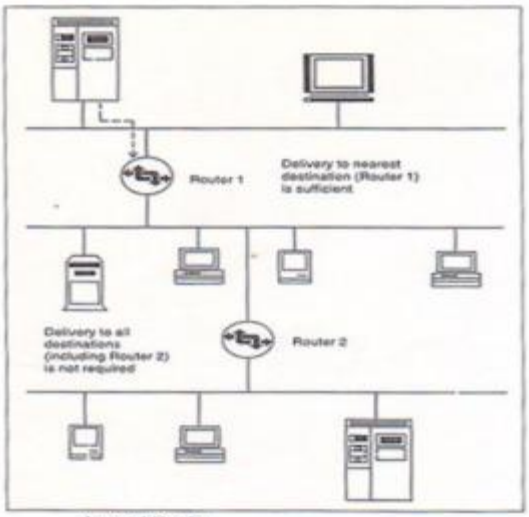
Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

1.7.1. Unicast. Identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.



Unicast Addressing

1.7.2. Anycast. Identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast (la más cercana, según la medida de distancia del protocolo de ruteo).

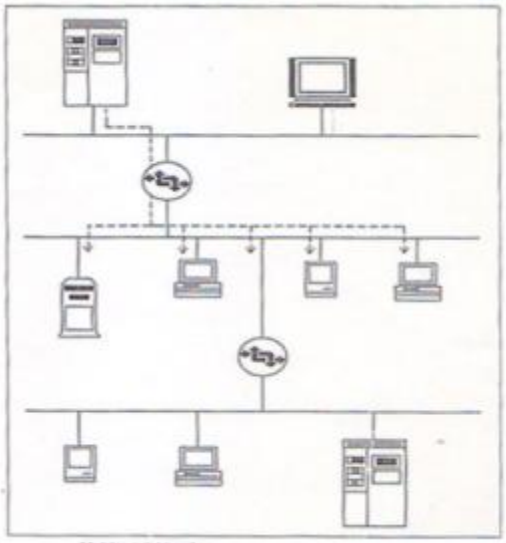


Anycast Addressing

1.7.3. Multicast. Identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.

Note que el término difusión (broadcast) no aparece, porque la función de difusión es reemplazada por la definición de multicast. También note que las direcciones de IPv6 de todo tipo son asignadas a interfaces, no nodos; un nodo (como un router) puede tener múltiples interfaces, y así múltiples direcciones unicast. Además, una interfase simple puede estar asignada a múltiples direcciones.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.


Multicast Addressing

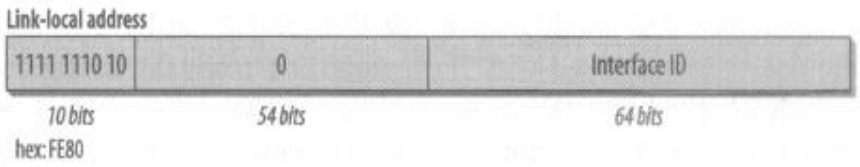
1.8.Ámbito de direcciones unicast.

El protocolo IPv6 añade soporte para direcciones de distintos ámbitos, lo que quiere decir que tendremos direcciones globales y no globales. Si bien con IPv4 ya habíamos empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.

Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador único de uno o varias interfaces. El ámbito de cada dirección forma parte de la misma dirección, con lo que vamos a poder diferenciarlos a simple vista. Para las direcciones unicast distinguimos tres ámbitos:

1.8.1. ***Direcciones unicast enlace local (link-local)***, que se utilizan entre vecinos en vínculo y en procesos de descubrimiento de vecinos.

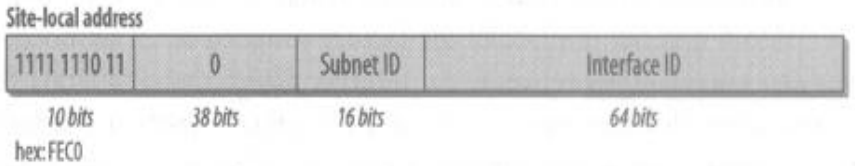
Los nodos utilizan direcciones de enlace-local, que se identifican mediante el prefijo de formato ***1111 1110 10*** e incluye un campo Inteface ID de 64 bits y empiezan todas por ***fe80:***, el prefijo de la direcciones de enlace-local siempre es ***FE80::/64***. Es necesaria una dirección de enlace-local para los procesos de descubrimiento de vecinos y siempre se configura automáticamente, incluso si no hay ninguna otra dirección de unidifusión. Los routers nunca reenvían paquetes con la dirección destino u origen de enlace local hacia otras direcciones de enlace. La estructura de una dirección enlace-local es "***fe80:0:0:0:<identificador de interfaz>***". El identificador de interfaz se genera automáticamente a partir de su dirección MAC (IEEE 802), siguiendo el formato IEEE EUI-64.



Nota: *Las direcciones de enlace-local equivalen a las direcciones IPv4 de Direccionamiento IP privado, que utilizan el prefijo* ***169.254.0.0/16****.*

1.8.2. ***Direcciones unicast de sitio local (site-local)***, que se utilizan entre nodos que se comunican con otros nodos del mismo sitio.

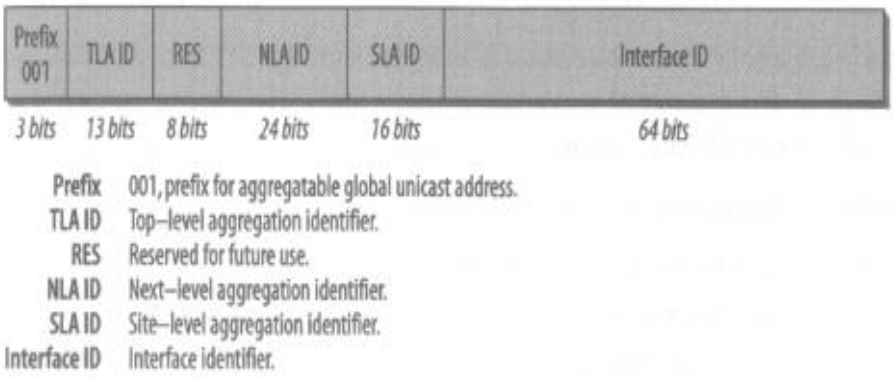
Para identificar interfaces en un mismo ***sitio-local***. La definición de ***sitio-local*** es un tanto genérica, pero en principio un sitio-local es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Las direcciones de sitio-local no son accesibles desde otros sitios y los enrutadores no deben reenviar tráfico local del sitio fuera del sitio. Las direcciones de sitio-local se pueden utilizar al mismo tiempo que las direcciones globales unidifusión. Esta dirección comienza con el formato de prefijo ***1111 1110 11***, *l*os primeros 48 bits siempre son fijos en las direcciones locales del sitio y comienzan por ***FEC0::/48***. A continuación de los 48 bits fijos hay un identificador de subred de 16 bits (campo Id. de subred) que proporciona 16 bits con los que se pueden crear subredes en la organización. Al disponer de 16 bits, puede haber hasta 65.536 subredes en una estructura de subredes plana o se pueden subdividir los bits de orden superior del campo Id. De subred para crear una infraestructura de enrutamiento jerárquica y agregable. Después del campo Id. De subred está el campo Id. De interfaz de 64 bits que identifica una interfaz específica de una subred.



Nota: *Las direcciones de sitio-local equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16).*

1.8.3. ***Direcciones unicast globales***, para identificar interfaces en todo Internet. Éstas comienzan por ***2001:***. Son el único tipo de direcciones que pueden ser enrutadas a través de Internet. El espacio reservado actualmente para este tipo de direcciones es de ***2001:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001:: /3)***.

Como su nombre indica, las direcciones globales unicast están diseñadas para agregarse o resumirse de forma que produzcan una infraestructura de enrutamiento eficaz. A diferencia de la red Internet actual basada en IPv4, que tiene una mezcla de enrutamiento plano y jerárquico, la red Internet basada en IPv6 se ha diseñado desde la base para admitir direccionamiento y enrutamiento jerárquico eficaz. El ámbito (que es la región del conjunto de redes IPv6 donde la dirección es única) de una dirección global agregable de unidifusión es la red Internet IPv6 completa.



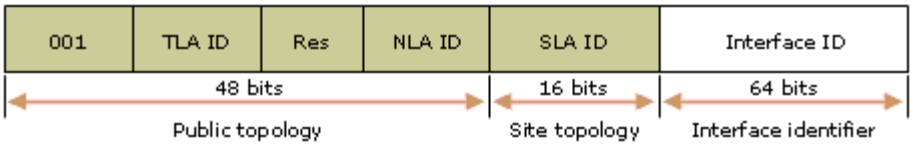
Los campos de una dirección global agregable de unidifusión se describen de la manera siguiente:

- ✓ ***Formato 001.*** Prefijo (3 bits) para Aggregatable Global Direcciones Unicast.
- ✓ ***TLA ID.*** Indica el Id. de agregación de nivel superior (TLA ID, Level Aggregation Identifier ID) de la dirección. El tamaño de este campo es de 13 bits. TLA identifica el nivel superior en la jerarquía de enrutamiento. Los TLA son administrados por IANA y se asignan a los registros de Internet locales que, a su vez, asignan Id. de TLA individuales a grandes proveedores de servicios Internet (ISP) globales. Un campo de 13 bits permite hasta 8.192 Id. de TLA diferentes. Los enrutadores del nivel superior de la jerarquía de enrutamiento en la red Internet IPv6 (llamados enrutadores libres predeterminados) no tienen una ruta predeterminada, sino rutas con prefijos de 16 bits que corresponden a los TLA asignados.
- ✓ ***RES***. Está reservado para su uso futuro en la ampliación del tamaño del Id. de TLA o el Id. de NLA. El tamaño de este campo es de 8 bits.
- ✓ ***NLA ID.*** Indica el identificador de agregación de siguiente nivel (NLA ID, Next Level Aggregation ID) de la dirección. El campo Id. de NLA se utiliza para identificar un sitio cliente específico. El tamaño de este campo es de 24 bits. El campo Id. de NLA permite que un ISP cree múltiples niveles de jerarquía de direcciones para organizar el direccionamiento y enrutamiento, así como para identificar sitios. Los enrutadores libres predeterminados no pueden ver la estructura de la red del ISP.
- ✓ ***SLA ID.*** Indica el Id. de agregación de nivel de sitio (SLA ID, Site Level Aggregation ID) de la dirección. El campo Id. de SLA sirve para que se identifiquen subredes en el sitio de una organización individual. El tamaño de este campo es de 16 bits. La organización puede utilizar los 16 bits correspondientes a su sitio para crear 65.536 subredes o múltiples niveles de jerarquía de direcciones y una infraestructura de enrutamiento eficaz. Con la flexibilidad de 16 bits para la creación de subredes, un

prefijo global agregable de unidifusión asignado a una organización equivale a asignar a la organización un Id. de red IPv4 de Clase A (siempre y cuando el último octeto se utilice para identificar los nodos en las subredes). El ISP no puede ver la estructura de la red del cliente.

- ✓ ***Interface ID.*** Indica la interfaz de un nodo en una subred determinada. El tamaño de este campo es de 64 bits.

En la ilustración siguiente se muestra cómo los campos de la dirección global agregable de unidifusión crean una estructura de topología con tres niveles.



La topología pública es la colección de grandes y pequeños ISP que proporcionan acceso a la red Internet IPv6. La topología del sitio es la colección de subredes del sitio de una organización. El identificador de interfaz identifica una interfaz específica en una subred del sitio de una organización. Para obtener más información acerca de las direcciones globales agregables de unidifusión, consulte el documento RFC 2374, "An IPv6 Aggregatable Global Unicast Address Format" (Formato de dirección global agregable de unidifusión de IPv6).

Una de las grandes ventajas de los ámbitos es que permitiría la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrían. Tenemos que esperar que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como hemos dicho antes, se trataría siempre que sea posible de mantener las tablas de mayor e invalidando el anterior, porque lo que seguramente sucedería sería que las redes contiguas ya estén asignadas.

Nota: *Las direcciones unicast globales, equivalen a las direcciones públicas IPv4.*

1.9.Direcciones Especiales.

Las siguientes son direcciones IPv6 especiales:

- ✓ ***Dirección no especificada.*** La dirección no especificada (***0:0:0:0:0:0:0:0*** *ó* ***::***) sólo se utiliza para indicar la ausencia de dirección. La dirección no especificada se suele

utilizar como dirección de origen en paquetes que intentan comprobar la exclusividad de una dirección tentativa. La dirección no especificada nunca se asigna a una interfaz ni se utiliza como dirección de destino.

Nota: *Equivale a la dirección IPv4 no especificada de 0.0.0.0.*

- ✓ ***Dirección de bucle de retroceso (loopback).*** La dirección de bucle de retroceso (***0:0:0:0:0:0:0:1 ó ::1***) sirve para identificar una interfaz de bucle de retroceso, lo que permite que un nodo se envíe paquetes a sí mismo, puede ser utilizada por un nodo para enviar un paquete IPv6 a sí mismo. Los paquetes dirigidos a la dirección de bucle de retroceso nunca se envían en un vínculo ni se reenvían mediante un enrutador IPv6.

  Nota: *Equivale a la dirección IPv4 de bucle de retroceso de 127.0.0.1.*

1.10. Direcciones IPv6 compatibles con direcciones IPv4.

Para facilitar la migración de IPv4 a IPv6 y la coexistencia de ambos tipos de hosts, se han definido las direcciones siguientes:

- ✓ ***Dirección compatible con IPv4.*** La dirección compatible con IPv4, ***0:0:0:0:0:0:w.x.y.z*** o ***::w.x.y.z*** (donde ***w.x.y.z*** es la representación decimal con puntos de una dirección IPv4 pública), la utilizan los nodos de pila dual que se comunican con IPv6 a través de una infraestructura IPv4. Los nodos de pila dual son nodos con protocolos IPv4 e IPv6. Cuando la dirección compatible con IPv4 se utiliza como destino IPv6, el tráfico IPv6 se encapsula de forma automática con un encabezado IPv4 y se envía al destino mediante la infraestructura IPv4.

```
|              80 bits                    |  16  |    32 bits     |
+-----------------------------------------+---------- ----------------+
| 0000 ............................... 0000 | 0000 | IPv4 dirección |
+-----------------------------------------+----+----- ----------------+
```

- ✓ ***Dirección asignada a IPv4.*** La dirección asignada a IPv4, ***0:0:0:0:0:FFFF:w.x.y.z*** o ***::FFFF:w.x.y.z*** se utiliza para representar un nodo exclusivo de IPv4 ante un nodo IPv6. Sólo sirve para la representación interna. La dirección asignada a IPv4 nunca se utiliza como dirección de origen o destino de un paquete IPv6. El protocolo IPv6 no admite el uso de direcciones asignadas a IPv4.

```
|              80 bits                  |  16  |     32 bits    |
+-------------------------------------+---------- ---------------+
| 0000 ............................ 0000 | FFFF | dirección IPv4 |
+-------------------------------------+----+----- ---------------+
```

1.11. Identificadores de interfaz de IPv6.

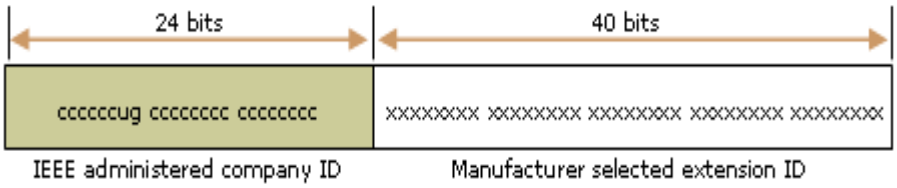
Los últimos 64 bits de una dirección IPv6 corresponden al identificador de la interfaz, que es único para el prefijo de 64 bits de la dirección IPv6. Las formas de determinar un identificador de interfaz son las siguientes:

1.11.1. Identificadores de interfaz basados en direcciones EUI-64.

El Institute of Electrical and Electronic Engineers (IEEE) define la dirección EUI-64 de 64 bits. Las direcciones EUI-64 se asignan a un adaptador de red o se derivan de las direcciones IEEE 802.

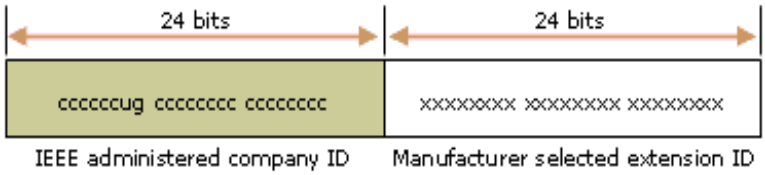
- ✓ ***Direcciones IEEE EUI-64.***

  La dirección IEEE EUI-64 representa un nuevo estándar para el direccionamiento de interfaces de red. El Id. de compañía sigue teniendo 24 bits de longitud, pero el Id. de extensión tiene 40 bits, por lo que se crea un espacio de direcciones mucho mayor para los fabricantes de adaptadores de red. La dirección EUI-64 utiliza los bits U/L e I/G de la misma forma que la dirección IEEE 802.



1.11.2. Direcciones IEEE 802.

Los identificadores de interfaz tradicionales para los adaptadores de red utilizan una dirección de 48 bits que se llama dirección IEEE 802. Esta dirección consta de un Id de compañía (también llamado Id. de fabricante) de 24 bits y un Id de extensión (también llamado Id. de tarjeta) de 24 bits. La combinación del Id de compañía, que se asigna de forma única a cada fabricante de adaptadores de red, y el Id de tarjeta, que se asigna de forma única a cada adaptador de red en el momento del ensamblaje, genera una dirección única global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, Media Access Control).



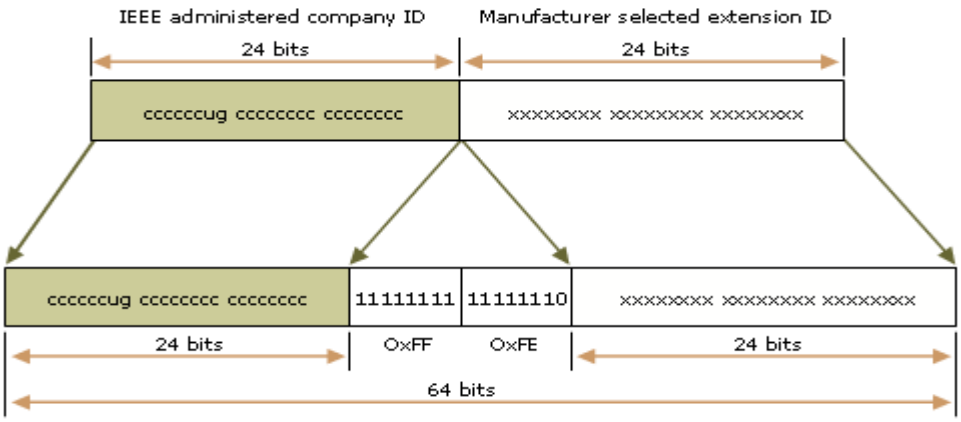
Los bits definidos en la dirección IEEE 802 son los siguientes:

- ✓ ***Universal o local (U/L).*** El bit U/L es el séptimo bit del primer byte y se utiliza para determinar si la dirección se administra de forma universal o local. Si el bit U/L está establecido en 0, la administración de la dirección corresponde a IEEE, mediante la designación de un Id. de compañía único. Si el bit U/L está establecido en 1, la dirección se administra de forma local. El administrador de la red ha suplantado la dirección de fábrica y ha especificado una dirección distinta.
- ✓ ***Individual o grupo (I/G).*** El bit I/G es el bit de orden inferior del primer byte y se utiliza para determinar si la dirección es individual (unidifusión) o de grupo (multidifusión). Si está establecido en 0, la dirección es de unidifusión. Si está establecido en 1, la dirección es de multidifusión.

En una dirección típica de adaptador de red 802.x, los bits U/L e I/G están establecidos en ***0***, lo que corresponde a una dirección MAC de unidifusión administrada de forma universal.

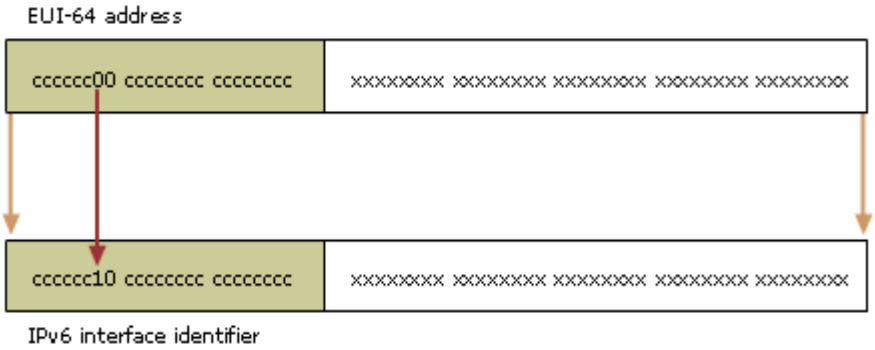
1.11.3. Asignación de direcciones IEEE 802 a direcciones EUI-64.

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id de compañía y el Id de extensión. En la siguiente ilustración se muestra la conversión de una dirección IEEE 802 en una dirección EUI-64.

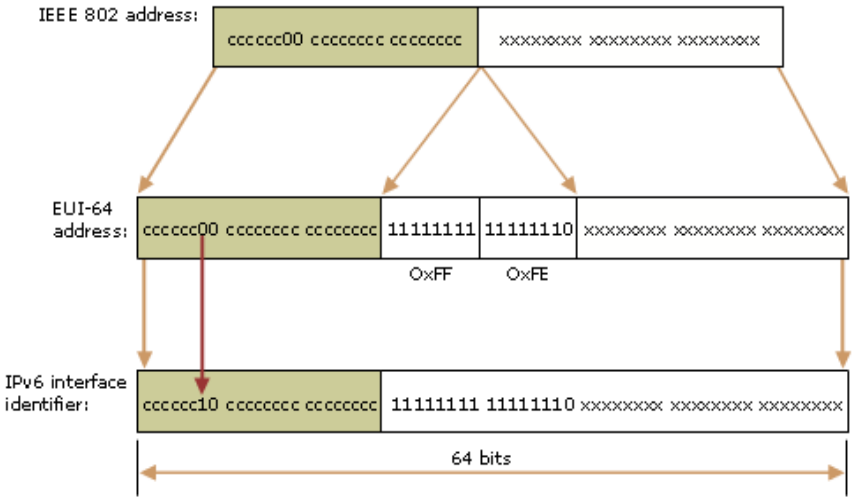


1.11.4. Asignación de direcciones EUI-64 a identificadores de interfaz IPv6.

Para obtener el identificador de interfaz de 64 bits para las direcciones IPv6 de unidifusión, se complementa el bit U/L de la dirección EUI-64 (si es 1, se establece en 0; y si es 0, se establece en 1). En la ilustración siguiente se muestra la conversión de una dirección EUI-64 de unidifusión administrada de forma universal.



Para obtener un identificador de interfaz IPv6 a partir de una dirección IEEE 802, primero se debe asignar la dirección IEEE 802 a una dirección EUI-64 y, después, complementar el bit U/L. En la ilustración siguiente se muestra el proceso de conversión de una dirección IEEE 802 de unidifusión administrada de forma universal.



Ejemplo de conversión de una dirección IEEE 802.

El host A tiene la dirección MAC de Ethernet de ***00-AA-00-3F-2A-1C***. Primero, se convierte al formato EUI-64 insertando ***FF-FE*** entre el tercer y cuarto bytes, con el resultado de ***00-AA-00-FF-FE-3F-2A-1C.*** Después, se complementa el bit U/L, que es el séptimo bit del primer byte. El primer byte en formato binario es ***00000000***. Al complementar el séptimo bit, se convierte en ***00000010*** (0x02). El resultado final es 02-***AA-00-FF-FE-3F-2A-1C*** que, cuando se convierte a notación

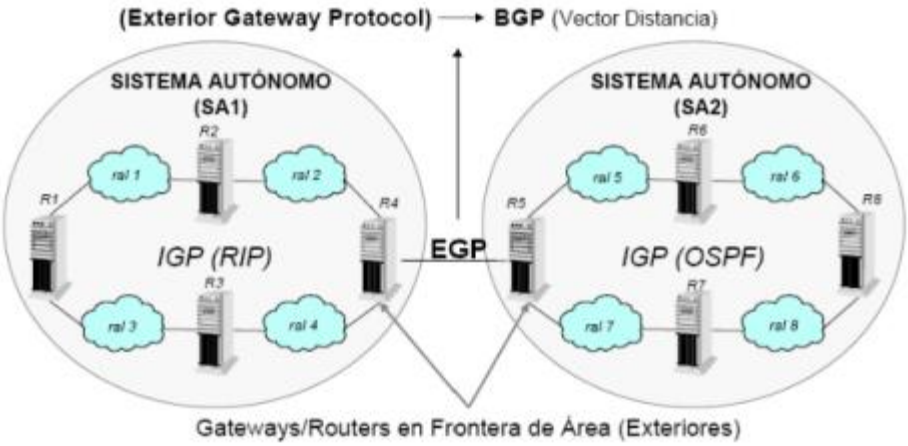
hexadecimal con dos puntos, da como resultado el identificador de interfaz ***2AA:FF:FE3F:2A1C***. En consecuencia, la dirección local del vínculo correspondiente al adaptador de red que tiene la dirección MAC de ***00-AA-00-3F-2A-1C*** es ***FE80::2AA:FF:FE3F:2A1C***.

Nota: *Al complementar el bit U/L, se debe sumar 0x2 al primer byte si la dirección EUI-64 se administra de forma universal, y restar 0x2 del primer byte si la dirección EUI-64 se administra de forma local.*

CAPÍTULO II: PROTOCOLOS DE ENRUTAMIENTO EN IPV6.

En este capítulo nos movemos una capa más arriba y consideraremos temas específicos a los procesos de ruteo en la capa de ***red*** del modelo OSI.

La arquitectura de área extensa de Internet está dividida en un número de sistemas autónomos (AS) conectados arbitrariamente. Un AS es un conjunto de enrutadores y hosts regidos por una administración técnica única (normalmente una entidad comercial única) que utilizan uno o varios protocolos de pasarela interior (IGP) y métricas comunes para encaminar los paquetes dentro del AS y utilizan un protocolo de pasarela exterior (EGP) para encaminar los paquetes hacia y desde otros AS. El uso del término sistema autónomo refuerza en este caso el hecho de que, aunque se utilicen varios IGP y métricas distintas, la administración de un AS tiene para el resto de AS un plan único y coherente de enrutamiento interior y presenta una imagen constante de los destinos que se pueden alcanzar.



El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos

de enrutamiento más utilizados. En la gráfico siguiente se presentan las nuevas versiones desarrolladas para IPv6.

Protocolo enrutamiento	Versión IPv6
RIP	RIPng
EIGRP	EIGRP para IPv6
OSPF	OSPFv3
IS-IS	Integrated IS-IS
BGP	BGP-MP
EIGRP	EIGRP for IPv6

2.1.Interior Gateway Protocol (IGP, Protocolo de pasarela interno).

Los IGPs se utilizan para intercambiar información de encaminamiento entre "routers" con un sólo sistema ***AS***. También lo usan los "routers" que ejecutan protocolos de encaminamiento exterior para recoger información de accesibilidad de la red para el ***AS***.

Los protocolos de pasarela internos se pueden dividir en dos categorías:

- ✓ **Protocolo de enrutamiento Vector-Distancia.**

En los protocolos de este tipo, ningún enrutador tiene información completa sobre la topología de la red. En lugar de ello, se comunica con los demás enrutadores, enviando y recibiendo información sobre las distancias entre ellos. Así, cada enrutador genera una tabla de enrutamiento que usará en el siguiente ciclo de comunicación, en el que los enrutadores intercambiarán los datos de las tablas. El proceso continuará hasta que todas las tablas alcancen unos valores estables. Este conjunto de protocolos tienen el inconveniente de ser algo lentos, si bien es cierto que son sencillos de manejar y muy adecuados para redes compuestas por pocas máquinas. Ejemplos de este tipo de protocolo tenemos: a) Protocolo de Información de Encaminamiento (RIP). b) Protocolo de Enrutamiento de Pasarela Interior (IGRP).

- ✓ **Protocolo de enrutamiento Enlace-Estado.**

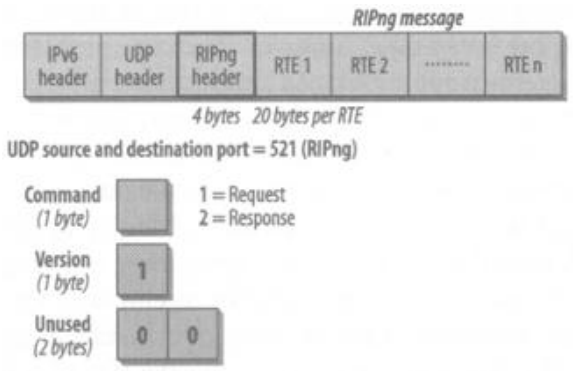
En este caso, cada nodo posee información acerca de la totalidad de la topología de la red. De esta manera, cada uno puede calcular el siguiente salto a cada posible nodo destino de acuerdo a su conocimiento sobre cómo está compuesta la red. La ruta final será entonces una colección de los mejores saltos posibles entre nodos. Esto contrasta con el tipo anteriormente explicado, en el que cada nodo ha de compartir su tabla de enrutamiento con sus vecinos. En los protocolos Enlace-Estado, la única información compartida es aquella concerniente a la

construcción de los mapas de conectividad. Ejemplos de este tipo de protocolo tenemos: a) Open Shortest Path First (OSPF). b) Sistema Intermediario a Sistema Intermediario (IS – IS).

2.1.1. Routing Information Protocol (RIP, Protocolo de encaminamiento de Información).

Es un protocolo de puerta de enlace interna (IGP, Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

- ✓ ***RIPng.*** RIP de siguiente generación está basado en protocolos y algoritmos usados en RIP y RIP2 para IPv4. RIPng es un protocolo de vector de distancia que debe ser implementado solo en Routers: IPv6.



Provee otros mecanismos para descubrimiento de rutas. En cualquier router que usa RIPng se asume que tiene interfaz para una o más redes, de otra forma esto no es realmente un router. Esto está referido a sus redes conectadas directamente.

El protocolo cuenta sobre el acceso de cierta información acerca de cada una de esas redes, de lo cual lo más importante es su métrica. La métrica RIP de una red es un entero entre 1 y 15, inclusivo. Esto es establecido en alguna forma no especificada en este protocolo; sin embargo, dado el máximo número de saltos es de 15, usualmente es usado un valor de 1. Las implementaciones deben permitir al administrador del sistema establecer la métrica de cada red. En adición a la métrica, cada red tendrá un prefijo de dirección destino y la longitud del prefijo asociado a este. Estos son establecidos por el administrador del sistema de una manera no especificada en este protocolo.

RIPng es el protocolo que permite a los routers intercambiar información para computar rutas a través de una red basada en ipv6. Cada router que implementa RIPng es asumida a tener una tabla de ruteo que tiene una entrada para cada destino ipv6 alcanzable. Cada entrada contiene lo siguiente:

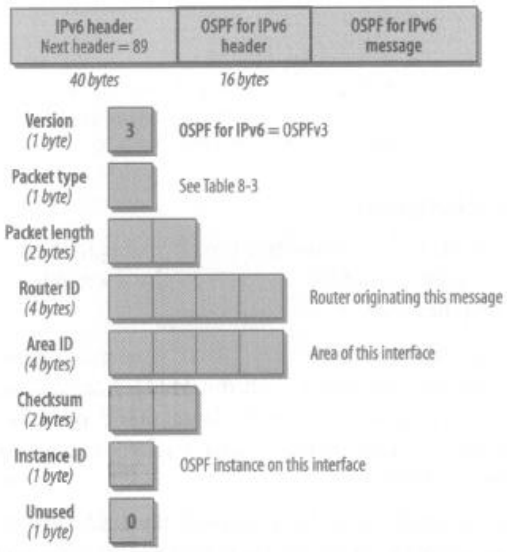
- ✓ El prefijo IPv6 del destino.
- ✓ Una métrica, la cual representa el costo total de obtener un datagrama desde el router a este destino. Esta métrica es la suma de los costos asociados con las redes que serian recorridas para obtener el destino.
- ✓ La dirección IPv6 del próximo router pertenece al camino del destino. Si el destino está sobre una de las redes directamente conectadas, este punto no es necesario.
- ✓ Una bandera para indicar que la información acerca de la ruta, ha cambiado recientemente.
- ✓ Varios timers asociados con la ruta, como un reloj de 30 segundos que apunte la transmisión de la información de la tabla de ruteo a los routers vecinos.
- ✓ Las entradas para las redes directamente conectadas son establecidas por el router usando información recolectada que en ningún caso es especificada en este protocolo. La métrica para una red directamente conectada es establecer el costo de esta red.
- ✓ Los implementadores pueden también permitir al Administrador del Sistema introducir rutas adicionales. Esto sería más parecido a rutear hosts o redes fuera del alcance del Sistema de ruteo. Esto es referido como "Rutas Estáticas". Las entradas para otros destinos que son inicialmente son sumadas y actualizadas por ciertos algoritmos.

2.1.2. Open Shortest Path First (OSPF, Abrir primero la trayectoria más corta).

Es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o sin clases CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

- ✓ **OSPF para IPv6.** La especificación de OSPF para IPv6 se encuentra documentada en el rfc 2740.



OSPF ha sufrido algunas modificaciones para soportar IPv6. El mecanismo fundamental de OSPF permanece sin cambios. Sin embargo, ha sido necesario efectuar algunos cambios, ya sea por diferencias entre las semánticas entre IPv4 e IPv6, o simplemente para manejar el aumento del tamaño de la dirección de IPv6. Los cambios efectuados son los siguientes:

- ✓ Las semánticas de direccionamiento han sido eliminadas de los paquetes OSPF y los LSAs básicos.
- ✓ Los nuevos LSAs han sido creados para llevar las direcciones y los prefijos IPv6.
- ✓ OSPF ahora corre en una base per-link, en lugar de una base per-IP-subnet.
- ✓ El ámbito de flooding para LSAs ha sido generalizado.
- ✓ La autenticación ha sido removida del protocolo OSPF en sí, confiando en la autenticación de la cabecera IPv6 y el Encapsulating Security PayLoad.

- ✓ La mayoría de las limitaciones del campo XSand presentes en OSPF para IPv4 se han disminuido
- ✓ La opción handling se ha hecho más flexible
- ✓ La mayoría de los paquetes en OSPF para IPv6 son casi tan compactos como en OSPF para IPv4, aún con la longitud más larga de IPv6.

Todas las capacidades opcionales de OSPF para IPv4, incluyendo el soporte de circuitos on-demmand, áreas NSSA, y las extensiones multicast para OSPF(MOSPF) también son soportadas en OSPF para IPv6.

2.2.Exterior Gateway Protocol (EGP).

EGP es el protocolo utilizado para el intercambio de información de encaminamiento entre pasarelas exteriores (que no pertenezcan al mismo AS). Posee las siguientes características:

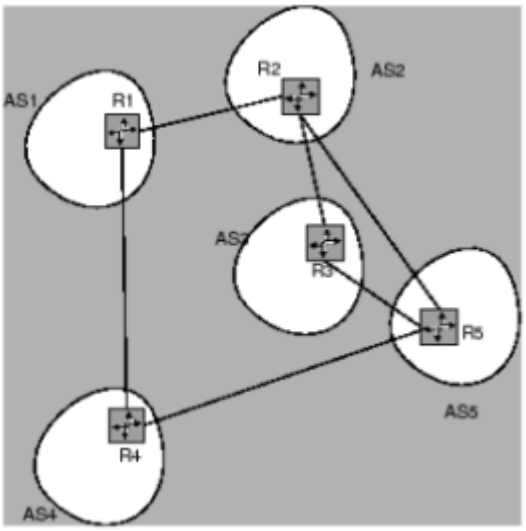
- ✓ Está especificado en los RFC 827 y RFC 904.
- ✓ Rutea en base a los routers vecinos.
- ✓ No utiliza métrica.
- ✓ Los routers se comunican el estado de los enlaces

Las pasarelas EGP sólo pueden retransmitir información de accesibilidad para las redes de su AS. La pasarela debe recoger esta información, habitualmente por medio de un IGP, usado para intercambiar información entre pasarelas del mismo AS.

EGP se basa en el sondeo periódico empleando intercambios de mensajes Hello/I Hear You, para monitorizar la accesibilidad de los vecinos y para sondear si hay solicitudes de actualización. EGP restringe las pasarelas exteriores al permitirles anunciar sólo las redes de destino accesibles en el AS de la pasarela. De esta forma, una pasarela exterior que usa EGP pasa información a sus vecinos EGP pero no anuncia la información de accesibilidad de estos (las pasarelas son vecinos si intercambian información de encaminamiento) fuera del AS.

2.2.1. EGP para IPv6 es MP-BGP4.

MP-BGP4 está documentado en los RFC 2858 y RFC 2545. Razones por la que se decidió que EGP para IPv6 es BGP4, un ejemplo en el que se muestra cómo con EGP pueden aparecer bucles y cómo con BGP se soluciona ese problema.



En la red de la figura, supongamos que usando EGP el encaminador R5 anuncia a R3 y a R2 que tiene alcanzabilidad de AS4 (Sistemas Autónomos). Posteriormente R2 podría anunciar a R3 que tiene alcanzabilidad de AS4, y R3 a su vez anunciar esa alcanzanbilidad a R5. R5 podría decidir que es una mejor forma de alcanzar AS4 es a través de R3 y se formaría el ciclo.

Si se usara BGP, cada anuncio de alcanzabilidad incluye el vector de ruta de Ass que se cruzan hasta llegar al alcanzado. Así, el anuncio de alcanzabilidad de AS4 que le haría R3 a R5 llevaría el vector de ruta: {AS3, AS2, AS5, AS4}. Al ver R5 que su sistema autónomo (AS5) ya está en el vector de ruta, ignoraría el anuncio que le hace R3.

En IPv6 las tablas de encaminamiento son más pequeñas gracias a que las direcciones IP están más jerarquizadas que en IPv4 y se forman a base de agregados. En IPv4 sólo existía la jerarquía red/máquina, en IPv6 hay varios niveles de agregación (al menos 3 niveles más luego la parte de máquina). Esto facilita el uso de prefijos en las entradas de las tablas de encaminamiento que engloben muchas direcciones diferentes.

2.3.Border Gateway Protocol (BGP).

Es un protocolo de ruteo exterior que como función principal tiene intercambiar información entre ASs las cuales son accesibles entre sí.

2.3.1. BGP para IPv6.

No existe BGP para IPv6. El soporte IPv6 deriva de la capacidad de BGP4 para intercambiar información entre los protocolos de la capa de red.

Estas extensiones multiprotocolo de BGP-4 están definidas en el RFC 2858 y el RFC 2545, el cual define las extensiones IPv6 de BGP-4 (que está basado en el RFC 2283).

Es importante entender BGP-4 antes de estudiar sus extensiones multiprotocolo. Las operaciones del BGP-4 están definidas en el RFC 1771.

BGP-4 .

- ✓ Cada AS ejecuta su protocolo de enrutamiento (RIP, OSPF, etc) para distribuir toda la información de ruteo en la AS. El BGP es un protocolo de enrutamiento cuya función primaria es intercambiar información acerca de la accesibilidad entre Ases.

- ✓ Cada AS recibe un único número asignado por la Numbering Authority. Dos routers que intercambian información de enrutamiento con BGP son llamados BGP Peers oBG speakers.

- ✓ Estos establecen una sesión TCP primero, porque TCP garantiza una conexión accesible. Después abren una conexión BGP para intercambiar los mensajes BGP. Los mensajes BGP más importantes son UPDATE (los mensajes de actualización). BGP-4

6. METODOLOGÍA

6.1. Matriz de consistencia general.

Problema General.				
La falta de direcciones IPv4 globales y la duplicidad han generado que no se pueda realizar una buena administración de la red de datos en la Universidad Nacional de Loja, lo cual conlleva la implementación de IPv6, que permitirá a la institución estar a la par de la tecnología y brindar servicios de Internet eficientes y eficaces.				
Tema	***Objeto de Investigación***	***Objetivo General***	***Objetivos Específicos***	***Hipótesis***
Estudio e Implementación del Protocolo Internet Versión 6 (IPv6) en la red de datos Ethernet IEEE 802.3 de la Universidad Nacional de Loja utilizando Software Libre y Open Source.	*Planificación para la implementación de IPv6*	*Realizar el estudio e implementación del nuevo Protocolo Internet Versión 6 (IPv6) en la Universidad Nacional de Loja utilizando Software Libre y Open Source.*	❖ *Describir la situación actual de la infraestructura en la red de datos Ethernet 802.3 de la Universidad Nacional de Loja para la implementación del Protocolo Internet versión 6.* ❖ *Describir el Protocolo de Internet versión 6, que permita determinar el método de transición de IPv4 a IPv6 más eficiente.* ❖ *Diseñar el mecanismo de transición de IPv4 a IPv6, acorde al direccionamiento IP actual de la Universidad Nacional de Loja para su aplicabilidad.* ❖ *Instalar y configurar el hardware y software necesario para la red de datos* Ethernet IEEE 802.3 *de la Universidad Nacional de Loja que soporten IPv6.* ❖ Desarrollar *e implementar los servicios de Internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.*	*La implementación de IPv6, brindara entre sus beneficios calidad de servicio, mayor espacio de direcciones, seguridad, confidencialidad, autoconfiguración y movilidad.*

6.2. Materiales, métodos y técnicas de trabajo.

- **Materiales.**

Los materiales a utilizar en este proceso investigativo, están clasificados de forma general en los siguientes grupos:

- ✓ Materiales de oficina.
- ✓ Equipos de cómputo.
- ✓ Software libre y Open Source.
- ✓ Hardware destinado a servidores.
- ✓ Herramientas libres de diseño.

- **Métodos.**

Los métodos a utilizarse en esta investigación los detallamos a continuación:

- ✓ **Método Científico**: A través de la utilización del método científico que está compuesto de principios, reglas y procedimientos, nos permitirá orientar la investigación a fin de alcanzar un conocimiento objetivo de los procesos y fenómenos concretos y descubrir las relaciones internas y externas de los procesos de la Red de datos de la Universidad Nacional de Loja.

- ✓ **Método Deductivo:** Nos permitirá la recolección de la información relacionada a las actividades, problemas, causas y posibles alternativas en la implementación del protocolo IPv6 en la Universidad Nacional de Loja.

- ✓ **Método Inductivo**: A través de este método permitirá obtener todos los requerimientos necesarios para poder iniciar el diseño de la implementación de IPV6; mediante la entrevista, observación directa y encuestas.

- ✓ **Método descriptivo**: Será utilizado para caracterizar, registrar, analizar e interpretar el manejo de la información existente y de los procesos que se efectúan actualmente.

Además también los métodos a utilizar en esta investigación están detallados en el proceso metodológico redactados anteriormente y son del orden teórico y práctico; como la

observación sistemática, medición, deducción, análisis y síntesis entre otros, debido a los varios campos que implica este estudio.

- **Técnicas de trabajo.**
  - ✓ **Observación.** La observación es un elemento fundamental de todo proceso investigativo que permite observar hechos; en ella se apoya el investigador para obtener el mayor número de datos. Entre las clases de observación tenemos:

  - ✓ **Observación directa.** Mediante la cual nos permitirá identificar la estructura de la red de datos y todos sus componentes, como también el funcionamiento y los servicios que presta a los estudiantes, docentes y servidores universitarios.

  - ✓ **Observación Indirecta.** Cuando el investigador entra en el conocimiento del hecho o fenómeno observado a través de las observaciones realizadas anteriormente por otra persona. (libros, revistas, papers, archivos digitales, etc.)

  - ✓ **Entrevista.** Se realiza con el fin de obtener información por parte de una persona entendida en la materia de la investigación. De hecho la entrevista constituye una técnica indispensable porque permite obtener datos que de otro modo sería muy difícil conseguir y se aplicará al director de la Unidad de Telecomunicaciones e Información, responsables de la sección de redes y equipos informáticos, mantenimiento y electrónica, software y telecomunicaciones y a los técnicos encargados del manejo de la Red de Datos la Universidad Nacional de Loja.

  - ✓ **Mapa Conceptual.** A través de esta técnica sintetizaremos o resumiremos de forma gráfica lo más significativo de un tema determinado que se refleja en un texto. Es una técnica muy útil para hacer evidentes los conceptos clave, para separar la información significativa de la superficial, para establecer conexiones entre conocimientos.

Los mapas conceptuales nos permitirán desarrollar las siguientes tareas:

7. Investigación Bibliográfica en libros sobre IPv6.
8. Investigación en Internet sobre IPv6.
9. Analizar la información recogida.

7. CRONOGRAMA

Nombre de la Tarea	*Duración*	*Inicio*	*Culminación*
Describir el funcionamiento de la red de datos.	*6 días*	*04-10-2010*	*09-10-2010*
Determinar las características del hardware de la red de datos.	*4 días*	*11-10-2010*	*13-10-2010*
Determinar las características del software de la red de datos.	*4 días*	*14-10-2010*	*17-10-2010*
Determinar los tipos de medios de networking existentes en la red de datos.	*6 días*	*18-10-2010*	*23-10-2010*
Investigar la estructura lógica de la red.	*6 días*	*24-10-2010*	*29-10-2010*
Revisión bibliográfica impresa y digital.	*4 días*	*01-11-2010*	*04-11-2010*
Analizar las diferentes técnicas de transición de direcciones a IPv6.	*5 días*	*05-11-2010*	*09-11-2010*
Determinar fortalezas y debilidades del método de transición seleccionado.	*5 días*	*10-11-2010*	*14-11-2010*
Seguir lineamientos establecidos por el CEDIA, para la transición a IPv6.	*5 días*	*15-11-2010*	*19-11-2010*
Realizar pruebas del método de transición seleccionado a IPv6.	*11 días*	*22-11-2010*	*02-12-2010*
Representar gráficamente la infraestructura de la red de datos.	*6 días*	*03-12-2010*	*08-12-2010*
Demostrar una solución de comunicación entre los protocolos de internet IPv4 e IPv6.	*5 días*	*09-12-2010*	*13-12-2010*
Elaborar un esquema de direccionamiento de IPv6.	*4 días*	*14-12-2010*	*17-12-2010*
Investigar acerca de procedimiento que satisfagan la instalación y configuración del hardware y software que soporten IPv6.	*4 días*	*20-12-2010*	*24-12-2010*
Determinar el software necesario para el buen funcionamiento del Protocolo de Internet versión 6.	*4 días*	*27-12-2010*	*30-12-2010*
Disponer del software necesario que soporten IPv6, previo a los requerimientos institucionales.	*3 días*	*03-01-2011*	*05-01-2011*
Proceder a la instalación del software que soporte IPv6.	*11 días*	*06-01-2011*	*16-01-2011*
Establecer parámetros de configuración tanto para el hardware como para el	*5 días*	*17-01-2011*	*21-01-2011*

software en el funcionamiento de IPv6.			
Investigación los servicios de Internet para aplicar en un entorno educativo.	*8 días*	*24-01-2011*	*31-01-2011*
Análisis de los servicios de Internet que permitan convivir ambos protocolos.	*4 días*	*01-02-2011*	*04-02-2011*
Determinar los servicios de Internet en los que se implementara IPv6 en ambos protocolos (IPv4 e IPv6).	*8 días*	*07-02-2011*	*14-02-2011*
Configuración de los servicios de Internet en un ambiente de producción en doble pila.	*14 días*	*15-02-2011*	*28-01-2011*
Realizar pruebas de ejecución para verificar el correcto funcionamiento.	*14 días*	*01-03-2011*	*14-03-2011*
Elaborar un manual sobre el funcionamiento de IPv6 en la Universidad Nacional de Loja.	*2 días*	*15-03-2011*	*16-03-2011*

8. PRESUPUESTO Y FINANCIAMIENTO

Descripción	*Cantidad*	*# Horas*	*V. Unitario*	*V.Total*
Recursos Humanos:				
Rubi Rafael Cabrera (Investigador).	2	*Duración del Proyecto Investigativo.*		
Jhon Alexander Calderón S. (Investigador).				
Director del Proyecto.	1			
Responsable de Redes y Equipos Informáticos.	1	30	$0.00	$0.00
Asesoría Externa.	2	30	$20.00	$600.00
Recursos Materiales:				
Resma de Hojas A4.	7		$3.50	$24.50
Grapadora.	1		$4.00	$4.00
Perforadora.	1		$3.50	$3.50
Borrador.	2		$0.25	$50.00
Lápices, esferos.	10		$0.35	$3.50
Calculadora.	1		$50.00	$50.00
Clips.	1		$0.70	$0.70
Dvds.	25		$0.75	$18.75
Cartuchos de Tinta Negra.	2		$50.00	$100.00
Cartuchos de Tinta de Color.	2		$60.00	$120.00
Anillados.	10		$1.50	$15.50
Empastados.	5		$10.00	$50.00
Transporte.	200		$0.25	$50.00
Consultas (Internet).	400		$0.80	$320.00
Cable de red.	50		$0.40	$20.00
Conectores Rj45.	30		$0.45	$13.50
Jack Modular.	5		$6.00	$30.00
Recursos Técnicos Hardware:				
Computadores Portátiles.	2		$900.00	$1,800.00
Impresora Hp Color LaserJet 2600n.	1		$450.00	$450.00
Pen Drive Hp 4 GB.	2		$15.00	$30.00
Recursos Técnicos Software:				
Sistema Operativo Gnu / Linux.	3		$0.00	$0.00
Paquete de Ofimática.	2		$0.00	$0.00
Herramientas de diseño de redes.	5		$0.00	$0.00
Software Libre para servicios de Internet.	10		$0.00	$0.00
Software Libre adicional.			$0.00	$0.00

Recursos Técnicos Comunicación:				
Telefonía convencional.	2	15	$6.00	$90.00
Telefonía celular.	2	25	$10.80	$270.00
Otros:				
Imprevistos 10 % del total.				$411.03
			Costo total del proyecto:	***$4.524,98***

El costo del presente proyecto es de ***$4.524,98*** dólares americanos, que será financiado en su totalidad con recursos propios de los autores e investigadores; previo a la obtención del título de Ingenieros en Sistemas de la Universidad Nacional de Loja.

9. BIBLIOGRAFÍA

[1] HAGAN, Silvia. 2002. IPv6 Essentials, United States of America.

[2] BARRETT, Daniel; SILVERMAN, Riachard; BYRNES, Robert. 2003. Linux Security CookBook. United States of America.

[3] TANENBAUM, Andrew S. 2003. Redes de Computadoras. 4a. ed. México, Cámara Nacional de la Industria Editorial Mexicana.

[4] SILBERSCHATZ, Abrahan; GALVIN, Peter; GAGNE, Gregne. 2008. Procesos. EN: Sistemas Operativos. 6a. ed. México, Grupo Noriega Editores. pp. 87 – 104.

[5] SILBERSCHATZ, Abrahan; GALVIN, Peter; GAGNE, Gregne. 2008. Estructura de Redes. EN: Sistemas Operativos. 6a. ed. México, Grupo Noriega Editores. pp. 469 – 500.

[6] SILBERSCHATZ, Abrahan; GALVIN, Peter; GAGNE, Gregne. 2008. El Sistema Linux. EN: Sistemas Operativos. 6a. ed. México, Grupo Noriega Editores. pp. 669 – 715.

[7] ESCUELA DE CIENCIAS COMPUTACIONALES. 2008. Implementación de Servicios de Internet sobre IPv6 para UTPL. Ingeniería Investigación Información Internet (i4). No. (2): 141-145. Abril.

[8] JARA SABA., Felipe Ernesto. 2009. Estudio e Implementación de una Red IPv6 en la UTFSM. (Tesis Ing. Civil Telemático) Valparaíso Chile, Universidad Técnica Federico Santa María. Departamento de Electrónica. 25 p.

[9] GAGLIANO, Roque. Planificando IPv6. [diapositiva] Lacnic. 25, 50 diap.

[10] DEERING, S; HINDEN R. 1998. Protocolo Internet, Versión 6 (IPv6). [en línea]. disponible en: www.rfc-es.org/rfc/rfc2460-es.txt, [Consulta: 3 julio 2010].

[11] HINDEN, R; DEERING S. 1998. IPv6 hace frente a la Arquitectura. [en línea]. disponible en: http://www.normes-internet.com/normes.php?rfc=rfc2373&lang=es, [Consulta: 3 julio 2010].

[12] THOMSON, S; NARTEN T. 1998. Configuración Automática sin Estado de Direcciones IPv6. [en línea]. disponible en: www.rfc-es.org/rfc/rfc2462-es.txt, [Consulta: 3 julio 2010].

[13] HINDEN, R; DEERING S. 2003. Internet Protocol Version 6 (IPv6) Addressing Architecture. [en línea]. disponible en: www.ietf.org/rfc/rfc3513.txt, [Consulta: 3 julio 2010].

[14] CONTA, A; DEERING S. 2006. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. [en línea]. disponible en: www.ietf.org/rfc/rfc4443.txt, [Consulta: 17 julio 2010].

[15] IAB; IESG. 2001. Recommendations on IPv6 Allocations to Site. [en línea]. disponible en: www.ietf.org/rfc/rfc3177.txt, [Consulta: 28 agosto 2010].

[16] LACNIC. Portal IPv6. [en línea]. disponible en: http://portalipv6.lacnic.net, [Consulta: 17 julio 2010].

[17] WIKIMEDIA FOUNDATION, Inc. IPv6. Wikipedia, La enciclopedia libre. [en línea]. disponible en: http://es.wikipedia.org/wiki/Ipv6, [Consulta: 28 agosto 2010].

[17] TASK FORCE, IPv6. The Portal IPv6. [en línea]. disponible en: www.ipv6tf.org, [Consulta: 17 julio 2010].

[19] SIXXS. IPv6 Deployment & Tunnel Broker. [en línea]. disponible en: www.sixxs.net, [Consulta: 17 julio 2010].

[20] FORUM, IPv6. The IPv6 Forum, The New Internet, Driving IPv6 Deploymet. [en línea]. disponible en: www.ipv6forum.com, [Consulta: 17 agosto 2010].

[21] IPv4 Address Report. 2010. [en línea]. disponible en: http://www.potaroo.net/tools/ipv4, [Consulta: 14 agosto 2010].

[22] ELECTRIC, HURRICANE. Hurricane Electric IPv6. [en línea]. disponible en: http://ipv6.he.net, [Consulta: 14 agosto 2010].

10. ANEXOS

10.1. Matriz de consistencia específica.

Problema Específico #1: Desconocimiento y falta de documentación en la infraestructura de la red de datos Ethernet 802.3 de la Universidad Nacional de Loja.			
Objetivo Específico	***Hipótesis Específica***	***Unidad de Observación***	***Sistema Categorial***
Determinar la situación actual de la infraestructura en la red de datos Ethernet 802.3 de la Universidad Nacional de Loja para la implementación del Protocolo Internet versión 6.	*Se obtendrá datos reales y objetivos de toda la infraestructura de la red de datos, la cual nos permita determinar la situación actual.*	*Infraestructura de la red de datos.*	❖ *Adquisición de datos.* ❖ *Inventario de equipos informáticos y software.* ❖ *Monitoreo de la red de datos.*

Problema Específico #2: El desconocimiento de un método de transición que se acople a los requerimientos de la institución universitaria, lo que nos permitirá a través de la investigación determinar el método de transición más eficiente.			
Objetivo Específico	***Hipótesis Específica***	***Unidad de Observación***	***Sistema Categorial***
Describir el Protocolo de Internet versión 6, que permita determinar el método de transición de IPv4 a IPv6 más eficiente.	*Mediante el análisis se determinara el método de transición más eficiente que permita convivir IPv4 e IPv6.*	*Protocolo de Internet versión 6.*	❖ *Adquisición de información objetiva sobre IPv6.* ❖ *Factibilidad de la implementación de IPv6.* ❖ *Concretar el método de transición de IPv4 a IPv6.*

Problema Específico #3: No se cuenta con un diseño de transición de direcciones IPv4 a IPv6, lo que conlleva a desarrollar un diseño acorde al direccionamiento IP actual de la Universidad Nacional de Loja basado en IPv6.			
Objetivo Específico	***Hipótesis Específica***	***Unidad de Observación***	***Sistema Categorial***
Diseñar el mecanismo de transición de IPv4 a IPv6, acorde al direccionamiento IP actual de la Universidad Nacional de Loja para su aplicabilidad.	*Es posible diseñar la transición de direcciones IPv4 a IPv6 mediante el método seleccionado.*	*Direcciones IPv4 e IPv6.*	❖ *Conocer la subred de direcciones IPv4.* ❖ *Asignación de direcciones IPv6.* ❖ *Utilizar herramientas para la correcta distribución de las direcciones IPv6.* ❖ *Diagramas de backbone de la red de datos.*

Problema Específico #4: La no existencia de IPv6, conlleva a realizar la instalación y configuración del hardware y software necesario para la red de datos Ethernet 802.3 de la Universidad Nacional de Loja.			
Objetivo Específico	***Hipótesis Específica***	***Unidad de Observación***	***Sistema Categorial***
Instalar y configurar el hardware y software necesario para la red de datos Ethernet IEEE 802.3 *de la Universidad Nacional de Loja que soporten IPv6.*	*Es viable instalar y configurar el hardware y software existente que permitan la implementación de IPv6.*	*Hardware y software que soporten IPv6.*	❖ *Determinar requerimientos de hardware.* ❖ *Conocer el software que tenga soporte nativo de IPv6.* ❖ *Acondicionamiento del hardware y software.* ❖ *Sistema operativo Gnu / Linux.* ❖ *Políticas de seguridad para la red de datos.*

Problema Específico #5: No se conoce estrategias de implantación de los servicios de internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.			
Objetivo Específico	***Hipótesis Específica***	***Unidad de Observación***	***Sistema Categorial***
Desarrollar e implementar los servicios de Internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.	*Con los equipos informáticos y dispositivos de networking existentes en la institución es posible implementar IPv6 con funcionamiento eficiente.*	*Coexistencia de los protocolos IPv4 e IPv6.*	❖ *Instalación del sistema operativo.* ❖ *Herramientas necesarias para los servicios de Internet.* ❖ *Aplicar método de transición de IPv4 e IPv6.* ❖ *Configuración de los servicios de Internet.* ❖ *Navegación en aplicaciones de Internet en IPv6.* ❖ *Adaptabilidad de sistema operativo con IPv4 e IPv6.*

10.2. Matriz de operatividad de objetivos específicos.

Objetivo Específico #1: Describir la situación actual de la infraestructura en la red de datos Ethernet 802.3 de la Universidad Nacional de Loja para la implementación del Protocolo Internet versión 6.

Actividad o Tarea	Metodología	Fecha Inicio	Fecha Final	Responsable	Presupuesto	Resultados Esperados
Describir el funcionamiento de la red de datos.	*Mediante al observación y entrevistas al personal encargado de la red de datos.*	*04-10-2010*	*09-10-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 20.00*	*Información objetiva y organizada para conocer el funcionamiento de la red de datos.*
Determinar las características del hardware de la red de datos.	*Investigación de campo.*	*11-10-2010*	*13-10-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S. .*	*$ 15.00*	*Esquema y características técnicas del hardware para la implementación de IPv6.*
Determinar las características del software de la red de datos.	*Investigación de campo.*	*14-10-2010*	*17-10-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 15.00*	*Esquema y características del software para la implementación de IPv6.*
Determinar los tipos de medios de networking existentes en la red de datos.	*Investigación de campo.*	*18-10-2010*	*23-10-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 20.00*	*Esquema y características técnicas de medios de networking.*
Investigar la estructura lógica de la red.	*Entrevista al responsable de la red de datos.*	*25-10-2010*	*29-10-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 25.00*	*Conocimiento preciso de la estructura lógica de la red de datos.*

Objetivo Específico #2: Describir el Protocolo de Internet versión 6, que permita determinar el método de transición de IPv4 a IPv6 más eficiente.						
Actividad o Tarea	**Metodología**	**Fecha Inicio**	**Fecha Final**	**Responsable**	**Presupuesto**	**Resultados Esperados**
Revisión bibliográfica impresa y digital.	*Se consultas en internet, reportes técnicos y asesoramiento de profesionales que tengan experiencia en el tema.*	*01-11-2010*	*04-11-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 30.00*	*Contar con información necesaria para realizar la transición de IPv4 a IPv6.*
Analizar las diferentes técnicas de transición de direcciones a IPv6.	*Realizar comparaciones de las técnicas de convivencia de protocolos IPv4 a IPv6.*	*05-11-2010*	*09-11-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S. .*	*$ 20.00*	*Seleccionar el método de transición más eficiente.*
Determinar fortalezas y debilidades del método de transición seleccionado.	*Análisis y esquematización sistemática.*	*10-11-2010*	*14-11-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 15.00*	*Puntos fuertes y débiles definidos del método de transición seleccionado.*
Seguir lineamientos establecidos por el CEDIA, para la transición a IPv6.	*Utilización de los requerimientos del CEDIA.*	*15-11-2010*	*19-11-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 25.00*	*Obtener método de transición de acuerdo a lo establecido por el CEDIA.*

Objetivo Específico #3: Diseñar el mecanismo de transición de IPv4 a IPv6, acorde al direccionamiento IP actual de la Universidad Nacional de Loja para su aplicabilidad.

Actividad o Tarea	Metodología	Fecha Inicio	Fecha Final	Responsable	Presupuesto	Resultados Esperados
Realizar pruebas del método de transición seleccionado a IPv6.	*Realizar comparaciones de los métodos de convivencia de protocolos Ipv4 a IPV6.*	*22-11-2010*	*02-12-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 35.00*	*Funcionamiento óptimo del método de transición seleccionado a IPv6.*
Representar gráficamente la infraestructura de la red de datos.	*Conocer el funcionamiento de la red de datos, y esquematizarla técnicamente.*	*03-12-2010*	*08-12-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S. .*	*$ 15.00*	*Obtener diagramas de la infraestructura de la red de datos.*
Demostrar una solución de comunicación entre los protocolos de internet IPv4 e IPv6.	*Analizar mecanismos de solución entre los dos protocolos.*	*09-12-2010*	*13-12-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 20.00*	*Solución óptima de comunicación entre protocolos de internet IPv4 e IPv6.*
Elaborar un esquema de direccionamiento de IPv6.	*Aplicar esquema de direccionamiento de acuerdo al método seleccionando.*	*14-12-2010*	*17-12-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 25.00*	*Diseño eficiente de direccionamiento de la red de datos en Ipv6.*

Objetivo Específico #4: Instalar y configurar el hardware y software necesario para la red de datos Ethernet IEEE 802.3 de la Universidad Nacional de Loja que soporten IPv6.						
Actividad o Tarea	**Metodología**	**Fecha Inicio**	**Fecha Final**	**Responsable**	**Presupuesto**	**Resultados Esperados**
Investigar acerca de procedimiento que satisfagan la instalación y configuración del hardware y software que soporten IPv6.	*Buscar asesoría de profesionales en IPv6 y obtener información impresa y digital.*	*20-12-2010*	*24-12-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 35.00*	*Procesos idóneos para la instalación y configuración de hardware y software que soporten IPv6.*
Determinar el software necesario para el buen funcionamiento del Protocolo de Internet versión 6.	*Análisis minucioso del software que soporten IPv6.*	*27-12-2010*	*30-12-2010*	*Rubi R. Cabrera E. Jhon A. Calderón S.* .	*$ 20.00*	*Software apropiado y características para el funcionamiento de IPv6.*
Disponer del software necesario que soporten IPv6, previo a los requerimientos institucionales.	*Buscar sitios web oficiales del software previo un análisis y su posterior descarga.*	*03-01-2010*	*05-01-2011*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 50.00*	*Software Libre idóneo que necesitaremos para el funcionamiento de IPv6.*
Proceder a la instalación del software que soporte IPv6.	*Basarnos en manuales y tutoriales recomendados por los desarrolladores del software.*	*06-01-2011*	*16-01-2011*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 45.00*	*Instalación correcta del Software que soporte IPv6.*
Establecer parámetros de configuración tanto para el	*Basarnos en las especificaciones técnicas del*	*17-01-2010*	*21-01-2011*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 25.00*	*Esquema apropiado sobre los parámetros de*

hardware como para el software en el funcionamiento de IPv6.	*hardware y software respectivamente.*					*configuración para el funcionamiento de IPv6.*

Objetivo Específico #5: Desarrollar e implementar los servicios de Internet, que permitan convivir ambos protocolos (IPv4 e IPv6) en un ambiente de producción.

Actividad o Tarea	Metodología	Fecha Inicio	Fecha Final	Responsable	Presupuesto	Resultados Esperados
Investigación los servicios de Internet para aplicar en un entorno educativo.	*Consultas en internet, reportes técnicos y asesoramiento de profesionales que tengan experiencia en IPv6.*	*24-01-2011*	*31-01-2011*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 35.00*	*Contar con información necesaria acerca de los servicios de Internet.*
Análisis de los servicios de Internet que permitan convivir ambos protocolos.	*Mediante mecanismos que permitan evaluar rendimiento, eficiencia y eficacia.*	*01-02-2011*	*04-02-2011*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 30.00*	*Parámetros de rendimiento, beneficio y costo sobre los servicios de Internet.*
Determinar los servicios de Internet en los que se implementara IPv6 en ambos protocolos (IPv4 e IPv6).	*A través de parámetros que requiera la institución, evaluando y priorizando los servicios de Internet.*	*07-02-2011*	*14-02-2011*	*Rubi R. Cabrera E. Jhon A. Calderón S.*	*$ 50.00*	*Servicios de Internet para un ambiente educativo por prioridades.*
Configuración de los servicios	*Mediante la modificación de*	*15-02-2011*	*28-02-2011*	*Rubi R. Cabrera E.*	*$ 55.00*	*Servicios de Internet funcionando correctamente*

de Internet en un ambiente de producción en doble pila.	*las diferentes directivas de los archivos de configuración basándonos en los requerimientos de la institución.*			*Jhon A. Calderón S.*		*en un ambiente de producción (IPv4 e IPv6).*
Realizar pruebas de ejecución para verificar el correcto funcionamiento.	*Las pruebas se llevaran a cabo entre los investigadores, responsable de la Unidad de Telecomunicaciones e Información y usuarios finales.*	*01-03-2011*	*14-03-2011*	*Rubi R. Cabrera E.* *Jhon A. Calderón S.*	*$ 50.00*	*Conocer diferentes puntos de vista acerca de la implementación de IPv6 en la Universidad Nacional de Loja.*
Elaborar un manual sobre el funcionamiento de IPv6 en la Universidad Nacional de Loja.	*Mediante la elaboración de un resumen, considerando rfcs, especificaciones, etc sobre IPv6.*	*15-03-2011*	*16-03-2011*	*Rubi R. Cabrera E.* *Jhon A. Calderón S*	*$ 30.00*	*Disponer de un documento entendible para todos sobre IPv6 en la Universidad Nacional de Loja.*

10.3. Matriz de control de resultados.

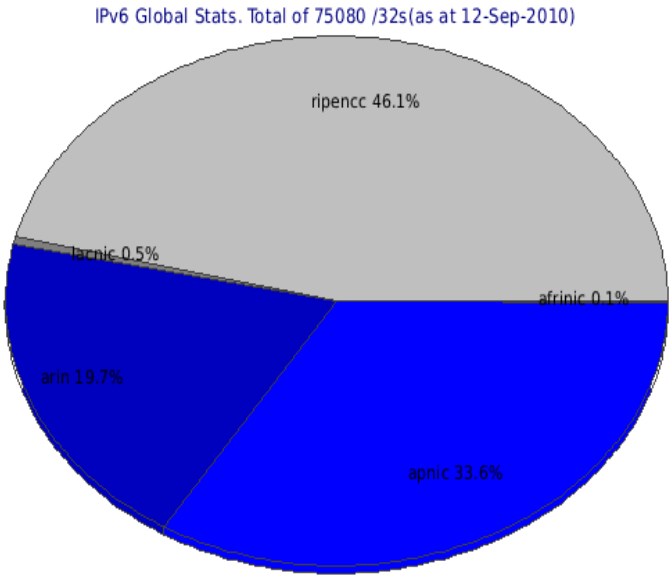
No.	Resultados	Fecha	Firma del Docente
1	*Información objetiva y organizada para conocer el funcionamiento de la red de datos.*		
2	*Esquema y características técnicas del hardware para la implementación de IPv6.*		
3	*Esquema y características del software para la implementación de IPv6.*		
4	*Esquema y características técnicas de medios de networking.*		
5	*Conocimiento preciso de la estructura lógica de la red de datos.*		
6	*Contar con información necesaria para realizar la transición de IPv4 a IPv6.*		
7	*Seleccionar el método de transición más eficiente.*		
8	*Puntos fuertes y débiles definidos del método de transición seleccionado.*		
9	*Obtener método de transición de acuerdo a lo establecido por el CEDIA.*		
10	*Funcionamiento óptimo del método de*		

	transición seleccionado a IPv6.		
11	*Obtener diagramas de la infraestructura de la red de datos.*		
12	*Solución óptima de comunicación entre protocolos de internet IPv4 e IPv6.*		
13	*Diseño eficiente de direccionamiento de la red de datos en Ipv6.*		
14	*Procesos idóneos para la instalación y configuración de hardware y software que soporten IPv6.*		
15	*Software apropiado y características para el funcionamiento de IPv6.*		
16	*Software Libre idóneo que necesitaremos para el funcionamiento de IPv6.*		
17	*Instalación correcta del Software que soporte IPv6.*		
18	*Esquema apropiado sobre los parámetros de configuración para el funcionamiento de IPv6*		
19	*Contar con información necesaria acerca de los servicios de Internet.*		

20	*Parámetros de rendimiento, beneficio y costo sobre los servicios de Internet.*		
21	*Servicios de Internet para un ambiente educativo por prioridades.*		
22	*Servicios de Internet funcionando correctamente en un ambiente de producción (IPv4 e IPv6).*		
23	*Conocer diferentes puntos de vista acerca de la implementación de IPv6 en la Universidad Nacional de Loja.*		
24	*Disponer de un documento entendible para todos sobre IPv6 en la Universidad Nacional de Loja.*		

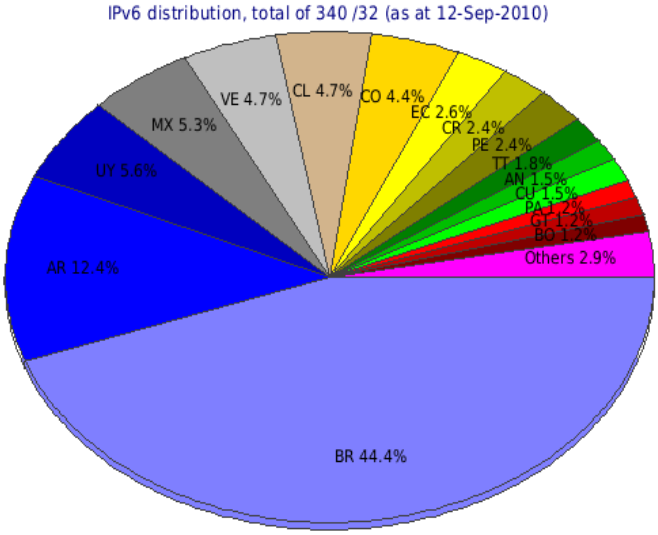
10.4. Esquemas y diagramas de IPv6.

- **Estadísticas Globales de IPv6, distribución de las asignaciones y distribuciones de bloques /32.**



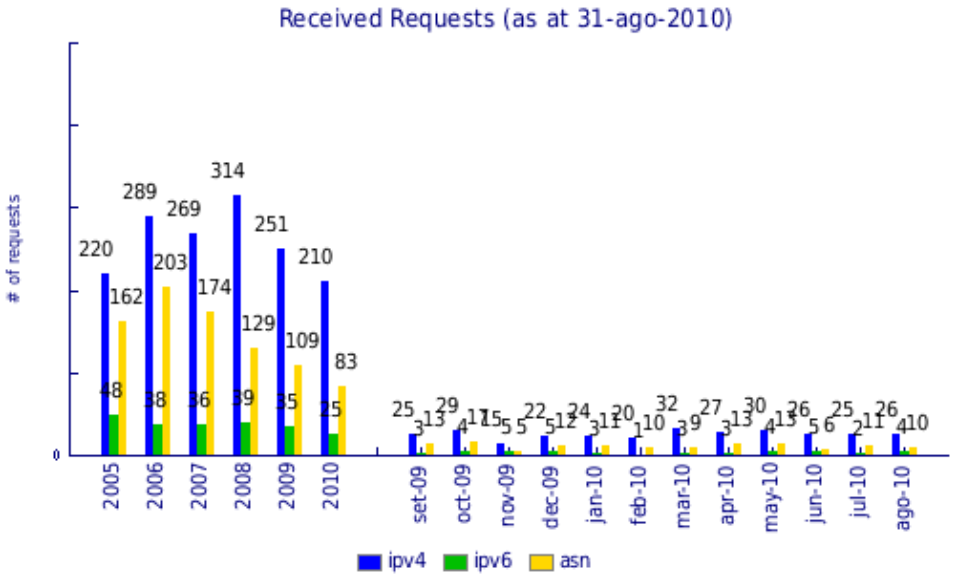
Esa gráfica de torta indica la distribución de la cantidad de bloques IPv6 (en números de "/32") ya asignados entre los RIR.

- **Distribución de IPv6 en la región de LACNIC.**



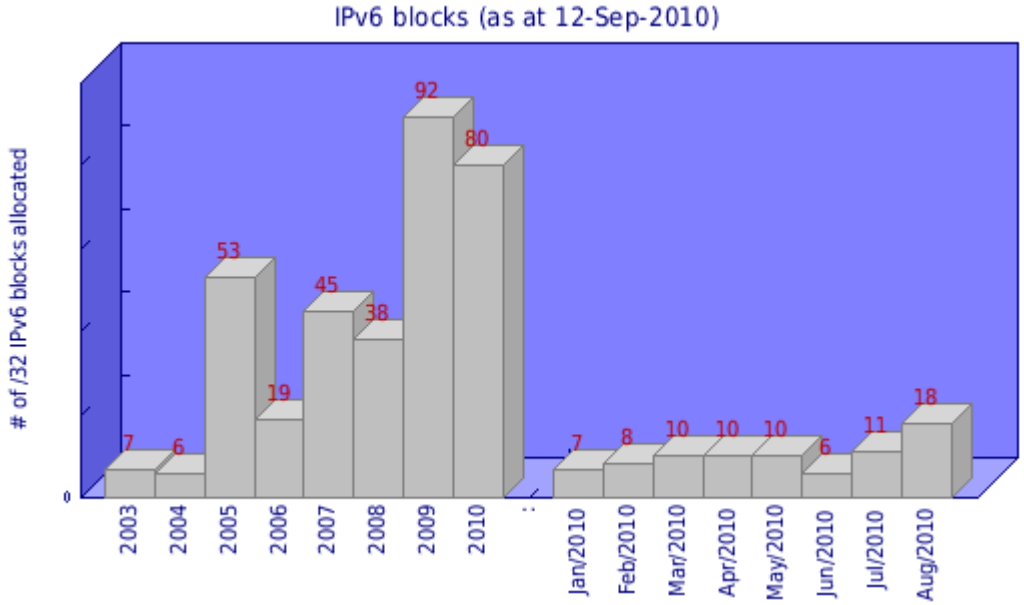
Esta gráfica de torta indica como es la distribución de las direcciones IPv6, en número de /32, ya asignadas por LACNIC entre los países de la región.

- **Solicitudes para recursos de Internet (IPv4, IPv6, ASN).**



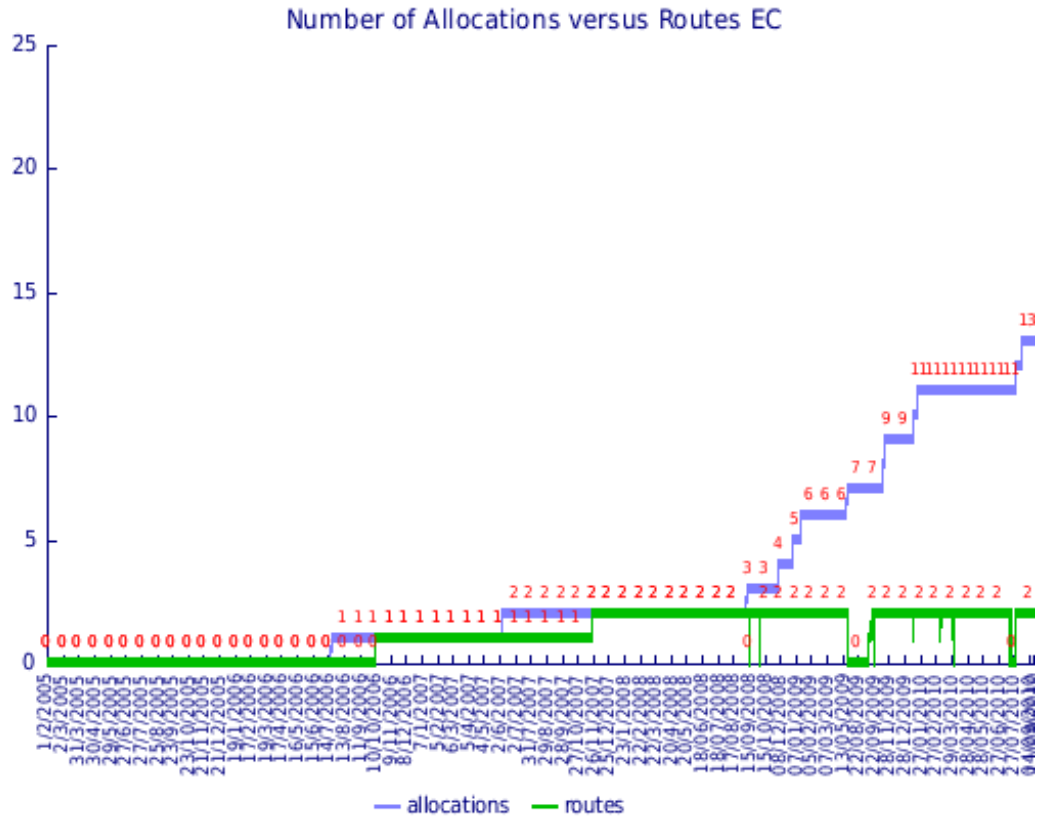
Esta gráfica indica la cantidad de solicitudes para recursos Internet (IPv4, IPv6, ASN) recibidas por LACNIC a cada mes. Y también un comparativo con los años anteriores.

- **Número de Bloques /32 de IPv6 asignados.**



Esta grafica indica la cantidad de direcciones IPv6 asignadas por LACNIC a organizaciones de la región. Dichas asignaciones están representadas en bloques de prefijo /32.

- **Número de Asignaciones en Ecuador por LACNIC.**



Número de Distribuciones y Asignaciones realizadas por LACNIC. Esta métrica mide el número total de distribuciones y asignaciones IPv6 hechas por LACNIC. Se incluyen las hechas a recursos críticos, ISPS y en el futuro a usuarios finales.

Número de Distribuciones y Asignaciones realizadas por LACNIC ruteadas. Esta métrica mide del número total de distribuciones y asignaciones IPv6 hechas por LACNIC cuantas están presentes en la tabla global de direcciones. Se incluyen las hechas a recursos críticos, ISPS y posible PI en el futuro.

- **Ghost Route Hunter : IPv6 DFP visibility : All**

The database currently holds 13 IPv6 DFP allocations for this subselection. The AS is the ASN as found in the All whois database, thus sites which are not entered completely yet show blanks. The current/real origin can be found by following the link behind the last seen field.

Legend

The following colors are used in the table.

- Everything ok.
- Prefix wasn't seen for the last 24 hours.
- /32 is allocated but only a /35 is announced.
- /32 is allocated and both the /32 and the /35 are announced.
- Prefix was returned or reclaimed but is seen.
- Prefix was returned and isn't seen.
- Prefix was reclaimed and isn't seen.
- Less than 100% of the GRH participants saw this route.
- Less than 80% of the GRH participants saw this route.
- Less than 50% of the GRH participants saw this route.
- Less than 30% of the GRH participants saw this route.

LG	Prefix	tld	NetName	Owner	AS	S	Allocated	First seen	Seen by	Last seen (*)
LG	2001:13c7:6006::/48		EC-AEPR-LACNIC	Aeprovi		A	2008-12-05	2009-09-17 02:17:32	0%	2009-10-14 18:17:32
LG	2001:13c7:6f00::/40		EC-AEPR-LACNIC	Aeprovi		A	2009-10-09	2009-10-14 19:32:33	94%	2010-09-13 02:47:44
LG	2800:68::/32		EC-CEDI-LACNIC	CEDIA		A	2006-07-19	2006-10-11 00:47:21	70%	2010-09-13 02:47:45
LG	2800:130::/32		EC-UTPL-LACNIC	Universidad Tecnica Parti...		A	2007-06-07	2007-11-14 15:47:26	8%	2010-09-13 02:47:45
LG	2800:2a0::/32		EC-TESA-LACNIC	Telconet S.A		A	2008-09-08		0%	never
LG	2800:2f0::/32		EC-ETSA-LACNIC	ETAPATELECOM S.A.		A	2009-01-16		0%	never
LG	2800:370::/32		EC-ANSA-LACNIC	CORPORACION NACIONAL DE T...		A	2009-06-04		0%	never
LG	2800:400::/32		EC-ETAP-LACNIC	ETAPA		A	2009-11-16		0%	never
LG	2800:430::/32		EC-CONE-LACNIC	CONECEL		A	2010-01-12		0%	never
LG	2800:440::/32		EC-ECTE-LACNIC	Ecuadortelecom S.A.		A	2010-01-21		0%	never
LG	2800:4f0::/32		EC-EASA-LACNIC	EasyNet S.A.		A	2010-08-03		0%	never
LG	2801:0:20::/48		EC-ESPL-LACNIC	Escuela Superior Politecn...		A	2009-01-02		0%	never
LG	2801:0:60::/48		EC-NISA-LACNIC	NIC.EC S.A.		A	2010-08-19		0%	never

The database currently holds 13 IPv6 DFP's.

Of which 0 (0.00%) are reclaimed, 0 (0.00%) are returned to the pool and 10 (76.92%) IPv6 DFP's didn't have a routing entry.

Thus 3 (23.08%) networks are currently correctly announced.

0 (0.00%) only announced a /35 while they have been allocated a /32.

0 (0.00%) announce both their /32 and their /35.

- **IPv6 DFP's per country**

Total number of countries: 1

Pos	Flag	Country	V	A	VP
1		Equador	3	13	23.08%

V: Visible: Number of Visible Prefixes for this country.

A: Allocated: Number of Allocated Prefixes for this country (excludes returned prefixes).

VP: Visible Percentage: Percentage of visible prefixes against global number of allocated prefixes.

(*) = "Never" in the above "Last seen" columns means: "didn't get a route for this prefix in any of the routing tables since the 1st of December 2002 when this measurement tool was started".IX routes and other /48's where added on 2006-05-05 and thus where not tracked before that date.