PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPV4 A IPV6 EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

EDWIN ROLANDO CAMARGO ACEVEDO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECANICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2006

PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPV4 A IPV6 EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

EDWIN ROLANDO CAMARGO ACEVEDO

Trabajo para optar al título de Ingeniero de Sistemas

Director
SERGIO FERNANDO CASTILLO CASTELBLANCO
Profesor Titular
Escuela de Ingeniería de Sistemas - UIS

Codirector
BENJAMIN PICO MERCHAN
Profesional División de Servicios de Información - UIS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECANICAS
ESCUELA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2006

DEDICATORIA

A mi hija Angie Valentina Camargo Alvarez,
por ser la luz de mi vida, por hacer que todo lo adverso
se convierta en esperanza simplemente con verla reír.
A mi madre Edilia Acevedo Garavito,
por creer en mi y por ser la artífice espiritual y material de todo lo que soy.
A el amor de mi vida Adriana Alvarez,
por entenderme, apoyarme, animarme y principalmente
por alegrarme la existencia.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Sergio Fernando Castillo, director del presente proyecto, por sus valiosos consejos y aportes que permitieron hacer de este proyecto un trabajo útil y profesional.

Benjamín Pico, codirector del presente proyecto, por sus significativos aportes a la realización y mejoramiento continuo del mismo.

Enrique Torres, director de la División de Servicios de Información – UIS, por el apoyo ofrecido a la realización del proyecto y por ser el más firme impulsor del mismo ante la UIS y UNIRED.

A mis compañeros y amigos código 2000, quienes de una u otra forma colaboraron aportando ideas que guiaron la realización del presente proyecto, además de contribuir a mi formación académica y personal durante tanto tiempo.

RESUMEN

TITULO:

PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER*

AUTOR:

EDWIN ROLANDO CAMARGO ACEVEDO**

PALABRAS CLAVE: **Protocolo de Internet (IP), IP versión 4 (IPv4), IP versión 6 (IPv6), mecanismos de transición de IPv4 a IPv6.**

DESCRIPCIÓN:

En este documento se hace una completa revisión al estado del arte del protocolo de red IPv6 haciendo énfasis en los aspectos técnicos que involucra la futura migración a este protocolo por parte de la red institucional UIS.

En el capítulo dos se dan las generalidades respectivas a la función e importancia del protocolo de red en el normal funcionamiento de las redes de computadoras. Adicionalmente se establecen las falencias evidenciadas por IPv4 que motivaron al diseño de la nueva versión del protocolo.

En el capítulo tres se encuentra la descripción de los mecanismos de transición básicos que permiten la inclusión de IPv6 en la infraestructura de red IPv4 permitiendo el manejo apropiado de los dos tipos de tráfico.

En el capítulo cuatro se definen las áreas claves de la red institucional UIS involucradas en el proceso de migración a IPv6 y los requerimientos básicos que permiten habilitar el tráfico IPv6 en los dispositivos de red y equipos de usuario final.

En el capítulo cinco se plantea el esquema de conectividad propuesto para la UIS, incluyendo los pasos y mecanismos de transición adecuados que permitan a la División de Servicios de Información evitar traumatismos significativos para cada sección de misión crítica en la red. Así mismo en este capitulo se dan algunas de las conclusiones y recomendaciones más importantes fundamentadas en la viabilidad de la implantación de IPv6 por parte de la UIS.

Por último, en la parte final del documento se incluyen 9 anexos que dada la naturaleza investigativa del proyecto constituyen una completa monografía sobre IPv6.

---

* Trabajo de investigación

** Facultad de Ingenierías Físico – Mecánicas, Escuela de Ingeniería de Sistemas e Informática. PHD. Sergio Fernando Castillo Castelblanco.

SUMMARY

TITLE:

TRANSITION PLAN OF NETWORK PROTOCOL IPv4 TO IPv6 IN UNIVERSIDAD INDUSTRIAL DE SANTANDER*

AUTHOR:

EDWIN ROLANDO CAMARGO ACEVEDO**

KEYWORDS: **Internet Protocol (IP), IP version 4 (IPv4), IP version 6 (IPv6), transition mechanism of IPv4 to IPv6.**

DESCRIPTION:

In this document, will perform a complete revision to the network protocol IPv6 state. Making emphasis in technical aspects that involves the future migration of this protocol by university's institutional network.

In chapter two, will find the generalized aspects, function and importance of network protocol in normal performance computers network. Addicionally, IPv4 faults in service, that motivated the new design of protocolo`s version.

In chapter three, appear the descripción of basic transicion mechanism that allow the entrance of IPv6 in network infrastructure IPv4 accesing the right handle of two kinds of traffic.

In chapter four, defines the important areas in university's institutional network that participate in the process of migration to IPv6 and the basic requerimients that allow activate the IPv6 protocol in network devices and users computers.

In chapter five, suggests the conectivity diagram proposed to the university, including the stages and transicion mechanisms appropiate that allow to Information Services Division avoid significative failures for each section of critical mision in network. Further more in this chapter offers some conclusions and fundamental recommendations in viability to introduce IPv6 protocol by the university.

To finalize, in the last part of the document included 9 attachments, that because of the proyect investigative nature constitute a complete monography about IPv6 protocol.

---

* Investigation work

** Faculty of Physics and Mechanics Engineering, Systems and Informatics school. PHD. Sergio Fernando Castillo Castelblanco.

DESCRIPCIÓN

La Universidad Industrial de Santander consciente de su importante papel en el desarrollo tecnológico, debido a que constituye el principal centro de educación superior en el nororiente colombiano, y a su vez una de las mejores universidades del país, promueve dentro de sus objetivos mantenerse a la vanguardia de las nuevas tecnologías que permitan el fortalecimiento y máximo aprovechamiento de su infraestructura de servicios informáticos.

Siendo la red institucional pieza fundamental en el desarrollo de los procesos académicos y administrativos, y ante la inminente vinculación de la Universidad a las redes académicas de alta velocidad más importantes del mundo, es preciso proveer a la red de las mejores herramientas de desempeño actuales con el fin de agregar valor a los procesos de investigación, transferencia tecnológica, gestión e integración de la Universidad con la sociedad.

El presente proyecto se desarrolló con el firme propósito de dar a conocer a la comunidad UIS las ventajas adicionales que ofrece el protocolo de red IP en su sexta versión – IPv6, sobre la versión más usada en la actualidad – IPv4, además de estudiar los diferentes mecanismos de transición a IPv6 existentes que le permitan a nuestra red de datos ser participe de la nueva generación del Internet.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO[1]

- **Nodo:** un dispositivo que está conectado a una red de datos.

- **Enrutador (Router):** un nodo que reenvía paquetes no explícitamente destinados hacia sí mismo.

- **Host:** cualquier nodo que no es un enrutador.

- **Nodo sólo IPv4:** es un host o router que posee soporte únicamente para IPv4.

- **Nodo IPv4 / IPv6:** es un host o router que posee soporte para ambos protocolos (IPv4 e IPv6).

- **Nodo sólo IPv6:** es un host o router que posee soporte únicamente para IPv6.

- **Nodo IPv6:** es cualquier host o router que implemente IPv6, los nodos IPv4 / IPv6 y los nodos sólo IPv6 son nodos IPv6.

- **Nodo IPv4:** es cualquier host o router que implemente IPv4, los nodos IPv4 / IPv6 y los nodos sólo IPv4 son nodos IPv4.

- **Enlace:** una facilidad de comunicación o medio sobre el cual los nodos pueden comunicarse en la capa de enlace, es decir, la capa inmediatamente debajo del IP.

- **Vecinos:** nodos conectados al mismo enlace.

[1] Términos extraídos de los glosarios incluidos en los principales RFCs.

- **Interfaz:** lo que acopla un nodo a un enlace, una interfaz puede ser un puerto de un router o la tarjeta de red en un host.

- **Dirección:** un identificador de capa IP para una interfaz o un conjunto de interfaces.

- **Paquete IPv4:** una cabecera IPv4 más carga útil.

- **Paquete IPv6:** una cabecera IPv6 más carga útil.

- **Protocolo:** es una descripción formal de un conjunto de reglas y convenciones que gobiernan el modo en que se comunican los dispositivos en una red.

- **Protocolo enrutado:** es cualquier protocolo de red que ofrezca suficiente información en su dirección de capa de red como para permitir que un paquete sea enviado desde un host a otro basado en el esquema de direccionamiento (Ej. IP, Appletalk, IPX).

- **Protocolo de enrutamiento:** es cualquier protocolo que soporte un protocolo enrutado y que suministre los mecanismos necesarios para compartir la información de enrutamiento. Los mensajes de los protocolos de enrutamiento se intercambian entre routers y les permite crear, mantener y actualizar las tablas de enrutamiento (Ej. RIP, IGRP, EIGRP, OSPF).

- **Capa superior:** capa de protocolo inmediatamente encima de IP. Por ejemplo, protocolos de transporte como TCP y UDP, protocolos de control como ICMP, protocolos de enrutamiento como OSPF y protocolos de Internet o de capas mas bajas que son *tunelizados* sobre IP, como IPX, Appletalk o el mismo IP.

- **MTU de enlace:** la unidad de transmisión máxima, es decir, el tamaño del paquete máximo en bytes, que puede transportarse sobre un enlace.

- **MTU de ruta:** la MTU de enlace mínima de todos los enlaces dentro de una ruta entre un nodo origen y un nodo destino.

- **NAT:** *Network Address Translation*, es un método mediante el que las direcciones IP son mapeadas desde un dominio de direcciones a otro, proporcionando encaminamiento transparente a las máquinas finales [RFC 2663].

- **CIDR:** *Classless Inter - Domain Routing,* método que permite reemplazar la generación de direcciones IPv4 mediante clases (A, B y C), en lugar de limitarse a prefijos de red de 8, 16 ó 24 bits, CIDR utiliza prefijos de 13 a 27 bits.

- **Proxy:** un servidor *proxy* es un intermediario entre Internet y los usuarios de una red. Si un cliente necesita información de Internet, el proxy buscará el destino y recuperará la información, si otro cliente necesita esta misma información de este mismo destino, el servidor envía la versión de esa ubicación almacenada en caché.

INTRODUCCIÓN

El origen de la red de computadoras más importante de la actualidad, la red de redes o Internet se remonta a 1957 cuando el gobierno de los Estados Unidos conforma la Agencia Avanzada de Proyectos de Investigación ARPA. El principal objetivo de esta agencia era permitir una comunicación fiable entre los miembros del ejercito, para lo cual se contemplaba la eliminación de cualquier *punto central* de administración que pudiese ser el blanco principal de ataques, en este sentido se pensó en una red descentralizada y diseñada para resistir situaciones hostiles (Guerra fría y la posibilidad de ser atacada con bombas nucleares).

Es así como en 1969 en la Universidad de California (UCLA) se establece la primera red. Poco tiempo después surgen tres redes adicionales dando de esta forma origen a la red de ARPA o ARPANET, antecedente del Internet. En sus inicios ARPANET fue un prototipo muy básico, por 1971 solo constaba de cuatro computadoras o nodos[1], una cifra que se ha ido incrementando hasta hoy en aproximadamente el doble de usuarios por año.

Para lograr esta conexión entre redes, fue fundamental el desarrollo de una arquitectura y unos protocolos que redujeran la complejidad de unir redes heterogéneas en una única red. Este proyecto lleva a que a mediados de la década de los 70 se desarrolle la arquitectura TCP / IP (*Transmision Control Protocol / Internet Protocol*) en la cual se basa Internet.

Durante la década de los 80, esta red conectó principalmente a Universidades e Instituciones, que la utilizaban básicamente para compartir información por

[1] Una completa descripción gráfica de la evolución de ARPANET se encuentra en http://som.csudh.edu/cis/Ipress/history/arpamaps/

medio de utilidades como correo electrónico, transferencia de archivos, acceso a bases de datos, grupos de discusión, etc.

A principios de los noventa comienza a imponerse la que sería la aplicación estrella del Internet, y que daría paso a su popularización masiva, la *World Wide Web* o simplemente Web, la cual se basa en el intercambio de hipertexto con presentaciones gráficas que muestran las posibilidades de Internet para múltiples usos. Durante el resto de la década, Internet creció vertiginosamente en cuanto a número de usuarios y volumen de tráfico, dando lugar a problemas de saturación actuales (sección 2.3).

La solución a estos problemas no implica simplemente aumentar la capacidad de los enlaces, pues está comprobado que se trata de una solución temporal que es absorbida rápidamente por el aumento de usuarios y servicios con mayores necesidades.

Una solución adecuada es aquella que además de poner fin a todos los problemas generados por el enorme éxito de la Web en Internet, soporte la que ha de ser la aplicación estrella de la nueva generación del Internet. Aunque aún está por determinar, las aplicaciones que permiten la colaboración interactiva en tiempo real se distinguen como unas muy fuertes candidatas (Videoconferencias, la Teleinmersión, la Telemedicina, Bibliotecas digitales multimedia y Laboratorios virtuales)[1].

La ingeniería del Internet se enfrenta ahora al reto de hacer posible la coexistencia de todos estos nuevos servicios con el fin de facilitar de nuevo, un medio de colaboración académica entre centros de investigación de todo el mundo, y servir de base para consolidar a Internet como el fenómeno social de

[1] Tecnologías tratadas en la sección 4.6.4.

comunicación, entretenimiento y negocio más importante para la sociedad actual.

Es por esto que el protocolo que soporta la mayor parte de las capacidades actuales de Internet, conocido como IPv4 (Protocolo de Internet en su versión 4) fue sometido a análisis con el fin de determinar mejoras que superen las actuales dificultades y hagan posible el desarrollo de futuras tecnologías en la red. Como resultado de este estudio ha surgido una nueva versión del protocolo IP conocida como IPv6, que ha sido diseñada para permitir la evolución futura de las redes basadas en el protocolo IP.

1. PRESENTACIÓN DEL PROYECTO

1.1 TITULO DEL PROYECTO

Plan de Transición del protocolo de red IPv4 a IPv6 en la Universidad Industrial de Santander.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Planificar la transición del actual protocolo de red IPv4 hacia la versión IPv6 en la Universidad Industrial de Santander.

1.2.2 OBJETIVOS ESPECÍFICOS

- Determinar los posibles escenarios de implantación, mediante el análisis de la infraestructura de servicios informáticos (Equipos y Servicios de Información).

- Seleccionar el mecanismo de transición que ofrezca las mayores ventajas en cuanto a adaptabilidad a la red, eficiencia y facilidad de implantación.

- Dictaminar los requerimientos en los equipos de red y en las aplicaciones informáticas, necesarias para la implantación del mecanismo seleccionado.

- Establecer una serie de lineamientos, recomendaciones y requerimientos para la implantación de IPv6, dirigidos a los nodos de la red institucional.

- Implantar una isla IPv6 dentro de la red institucional UIS, con el fin de tener disponible un laboratorio de pruebas.

- Socializar el plan de transición y su repercusión en la infraestructura de servicios informáticos.

1.3 DESCRIPCIÓN DEL PROBLEMA Y JUSTIFICACIÓN

Los usuarios y las aplicaciones de red cada vez exigen de Internet y sus protocolos funcionalidades para las cuales no fueron diseñados originalmente. En la actualidad es muy común que la sociedad en general use el Internet como el medio de comunicación, entretenimiento y negocios más popular, accesible y rentable del mercado.

Aplicaciones como el chat (con texto, voz y video incluido), el correo electrónico, la voz sobre IP, las aplicaciones punto a punto (*peer to peer*), la descarga de grandes cantidades de archivos, entre otros, han puesto al límite las capacidades de los enlaces y han hecho del ancho de banda uno de los recursos más preciados y demandados por la sociedad del Internet.

Con el fin de responder a las expectativas de negocio generadas por el enorme éxito del Internet, los administradores de redes y servicios se ven obligados a

ofrecer a los usuarios garantías de seguridad, calidad de servicio y movilidad. Dichas demandas no son tan sencillas de satisfacer, debido a que son problemas relativamente nuevos tratados con soluciones de más de treinta años de antigüedad (pila de protocolos TCP / IP). Algunos de estos problemas son:

- La falta de disponibilidad del ancho de banda necesario para soportar los servicios actuales.
- El rápido surgimiento de aplicaciones tales como la voz sobre IP que demandan de la red requisitos estrictos de temporización.
- El uso creciente de Internet como plataforma de negocios hace que la seguridad en la Red sea un punto indispensable si se quiere suplir las expectativas de negocio generadas.
- Se necesitan mecanismos que garanticen unas características determinadas a los diferentes tipos de tráfico. Surge a partir de esta necesidad, un concepto nuevo, la calidad de servicio (QoS, *Quality of Service*).
- Cada día hay más usuarios que acceden a la red y en diversos dispositivos (teléfonos móviles, PDA, automóviles, electrodomésticos, entre otros), esta creciente demanda de conectividad ha hecho que cada vez sean más escasas las direcciones IP públicas.

Es debido a estas razones y algunas más (ver sección 2.3) que la fuerza impulsora de la ingeniería del Internet decidió evaluar y rediseñar el protocolo de red IPv4, cuyo diseño inicial había permanecido invariable desde los años 70. La nueva versión del protocolo de Internet llamada IPv6 ha surgido de este estudio y es la encargada de promover la evolución del Internet del mañana.

“La Universidad Industrial de Santander por pertenecer al ente estatal es consciente que las tecnologías Web permiten difundir, de manera universal cualquier tipo de información, ha contemplado dentro del plan de gestión

institucional la modernización institucional. Es así como los proyectos deben ser destinados a optimizar los conocimientos, los procesos de apoyo y las habilidades de gestión. Al mismo tiempo se definen proyectos enfocados a estimular en las personas el espíritu de la modernidad y a lograr la modernización de la infraestructura tecnológica y física."[1]

La Universidad Industrial de Santander y en especial la División de Servicios de Información, han planteado la necesidad de iniciar la transición de su infraestructura de servicios informáticos (equipos y aplicaciones) hacia IPv6, con el fin de ser participes de la nueva generación de tecnologías que permitirá seguir afianzando a la UIS como el principal referente de calidad académica en el nororiente colombiano, la cual promueve dentro de sus objetivos mantenerse a la vanguardia de las nuevas tecnologías que contribuyan a un mejor desempeño en el manejo de la información y así avanzar en un proceso de modernización que permitirá mejorar la calidad de los servicios que presta.

De la misma forma con IPv6 se busca dar soporte a los requerimientos de calidad de servicio exigidos por las nuevas aplicaciones y servicios de red que surgen de la conectividad con las redes académicas de alto desempeño a las cuales pertenece la UIS (ver sección 4.6).

[1] Tomado del Plan de Gestión Institucional UIS 2004-2006, http://intranet.uis.edu.co

2. MARCO CONCEPTUAL

2.1 IP EN LA ARQUITECTURA DE RED

Antes de profundizar en el estudio de las características del protocolo IP que conciernen al desarrollo de este trabajo, es necesario ubicar en el contexto de las arquitecturas de red y del funcionamiento interno de Internet a la familia de protocolos TCP / IP, con el fin de evidenciar la importancia que tiene el protocolo de Internet en el correcto funcionamiento de las redes de computadores, y por ende en la red institucional UIS.

2.1.1 EL MODELO OSI

La Organización Internacional de Estándares (ISO, *International Standards Organization*) propuso en 1984 el modelo de referencia OSI (*Open Systems Interconection*) con el fin de crear un esquema de red que permitiera normalizar el diseño y la comunicación entre la gran cantidad de redes heterogéneas surgidas por la falta de estandarización.

La ISO decidió atacar el problema de incompatibilidad entre las redes mediante el uso del principio de descomposición funcional, es decir dividió el problema en varios subproblemas, donde cada subproblema es tratado por un *especialista* o en el caso del modelo OSI por un nivel o capa. Gracias a este modelo en capas resulta más fácil comprender como *viaja* la información a través de una red.

El modelo OSI está compuesto por 7 niveles numerados, cada uno de los cuales ejerce una función de red en particular:

Nivel	Descripción
7. Aplicación	Es el nivel más *cercano* al usuario y el único que no ofrece ningún servicio a otro nivel OSI. Es el encargado de suministrar servicios de red a las aplicaciones de los usuarios. Ej. Navegador Web
6. Presentación	Garantiza que la información enviada por la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro, además se ocupa de la encriptación y compresión de los datos.
5. Sesión	Se encarga de las tareas de sincronización, es decir evita que los dos extremos de la comunicación ejecuten la misma operación al tiempo.
4. Transporte	Proporciona confiabilidad en el transporte de datos entre dos hosts, además se encarga de fraccionar la unidad de datos en unidades más pequeñas, lo cual facilita el manejo de los mismos por el nivel de Red.
3. Red	Es el encargado del correcto enrutamiento de los paquetes por la red, lo cual implica evitar la congestión por exceso de paquetes en algún segmento de la red.
2. Enlace	Proporciona tránsito confiable de datos a través de un enlace físico. Se ocupa de aspectos tales como la topología de red, el control de acceso al medio, direccionamiento físico, entrega ordenada de tramas y control de flujo.
1. Físico	Define las especificaciones físicas (tipo de cable y conectores), eléctricas (niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos), de procedimiento y funcionales que permiten activar, mantener y desactivar el enlace físico entre sistemas finales.

Tabla 1 Niveles del modelo OSI

Los datos que se deseen enviar a otro host en el modelo OSI, son pasados en primera instancia al nivel de aplicación, el cual agrega un encabezado delante

de los datos y los envía a la capa de presentación. La capa de presentación a su vez añade su encabezado delante de los datos recibidos de la capa de aplicación y los envía al siguiente nivel, la operación anterior se repite nivel por nivel hasta que los datos son llevados al nivel físico. El nivel físico coloca los datos en el medio de transmisión y los envía al host receptor.

El host receptor realiza la operación inversa a la realizada por el host origen, es decir pasa los datos desde la capa física *ascendentemente* hasta la capa de aplicación. Cuando los datos llegan al nivel n del host receptor, este retira la cabecera puesta por el nivel n del host origen. Al final de este proceso los datos del proceso emisor se entregan al proceso receptor.

2.1.2 LA ARQUITECTURA TCP / IP

Si bien el modelo OSI había sido diseñado teniendo como objetivo ser acogido por la nueva generación de redes, el éxito experimentado por Internet ha hecho que la pila de protocolos basada en TCP / IP sea la más utilizada en la actualidad.

El modelo TCP / IP es una colección de protocolos estándar de la industria, diseñados para la interconexión de redes. Se trata de un conjunto de protocolos donde los más conocidos son el Protocolo de Control de Transmisión (TCP, *Transmision Control Protocol*) y el Protocolo de Internet (IP, *Internet Protocol*).

La característica que hizo del modelo TCP / IP la arquitectura de red más popular en el mundo es la posibilidad que tienen las aplicaciones de correr sobre TCP / IP independientemente de las características físicas de la red.

El modelo TCP / IP consta de 5 niveles, los cuales como se observa en la tabla 2, tienen cierta concordancia con los niveles del modelo OSI:

<table>
<tr><th colspan="3">TCP/IP</th><th rowspan="2">OSI</th></tr>
<tr><th>Nivel</th><th colspan="2">Protocolos</th></tr>
<tr><td rowspan="3">1. Aplicación</td><td colspan="2" rowspan="3">FTP, HTTP, SSH, SSL, Telnet, SMTP, NFS, etc.</td><td>1. Aplicación</td></tr>
<tr><td>2. Presentación</td></tr>
<tr><td>3. Sesión</td></tr>
<tr><td>2. Transporte</td><td colspan="2">TCP</td><td>UDP</td><td>4. Transporte</td></tr>
<tr><td>3. Internet</td><td>IP</td><td>ICMP</td><td>ARP, RARP</td><td>5. Red</td></tr>
<tr><td>4. Acceso a la Red</td><td colspan="3">Ethernet, CSMA, Token-ring, ATM, etc.</td><td>6. Enlace</td></tr>
<tr><td>5. Físico</td><td colspan="3">Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, etc.</td><td>7. Físico</td></tr>
</table>

Tabla 2 Modelo TCP/IP comparado con el modelo OSI

Cuando un mensaje es transmitido por la red, por ejemplo de un host cliente a un equipo servidor, cada nivel TCP / IP se encarga de una tarea en particular apoyado principalmente en los siguientes protocolos:

Nivel de aplicación

- **HTTP:** Protocolo de transmisión de hipertexto (*Hyper Text Transfer Protocol*), el hipertexto es el contenido de las páginas Web, y el protocolo de transmisión es el método mediante el cual se envían las peticiones y respuestas de una página Web, remitiendo la información que se verá en pantalla.
- **FTP:** Protocolo de transmisión de archivos (*File Transfer Protocol*) es utilizado para transferir archivos entre hosts en la red.
- **SSL:** *(Secure Sockets Layer)* permite cifrar la conexión, incluso garantiza la autenticación. Se basa en la criptografía asimétrica y en el concepto de los certificados.
- **Telnet:** Es la posibilidad de acceder remotamente a otro equipo de la Red, y trabajar desde nuestra pantalla como si estuviésemos realmente delante de ese equipo. Además es el mecanismo de prueba más completo que hay, debido a que si se logró establecer una sesión Telnet, todas las capas deben funcionar correctamente.
- **SMTP:** Protocolo simple de transferencia de Correo Electrónico (*Simple Mail Transfer Protocol*) se basa en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras.
- **NFS:** El sistema de archivos de red (*Network File System)* es un sistema de archivos distribuido para un entorno de red de área local. Posibilita que distintos sistemas conectados a una misma red accedan a archivos remotos como si se tratara de archivos locales

Nivel de transporte

- **TCP:** Protocolo de control de transmisión, garantiza que los datos sean entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir

distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. Es utilizado en aplicaciones que necesitan una confirmación o validación ACK (*Acknowledgment*) de los datos recibidos.

- **UDP:** Protocolo de datagrama a nivel de usuario (*User Datagram Protocol*) este protocolo no es tan fiable como TCP, pues se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar el éxito de la transferencia, UDP hace que la máquina de destino envíe un ACK, si no es así, el mensaje se envía de nuevo. Con este protocolo no se establece una conexión entre las dos máquinas.

Nivel de red (Internet)

- **IP:** Es un protocolo enrutado de sistema de máximo esfuerzo de entrega, poco fiable y sin conexión (no es necesaria una conexión de circuito dedicada). IP toma cualquier ruta que sea más eficaz en base a la decisión del protocolo de enrutamiento, para llevar los datos desde un host origen hasta un host destino sobre un sistema interconectado de redes.
- **ICMP:** Protocolo de control de mensajes en Internet (*Internet Control Message Protocol*) se usa principalmente por los routers de Internet para informar de sucesos inesperados, errores. También se usa para hacer pruebas sobre la red (local o Internet), por ejemplo enviando un comando de petición de eco a un equipo y esperar que responda.
- **ARP:** Protocolo de resolución de direcciones (*Address Resolution Protocol*), encargado de encontrar la dirección hardware (MAC[1]) que corresponde a una determinada dirección IP.
- **RARP:** Protocolo de resolución inversa de direcciones (*Reverse Address Resolution Protocol*), es utilizado para resolver la dirección IP de una

[1] Una dirección MAC (Media Access Control) es un identificador físico, único en el mundo, de 48 bits almacenado en fábrica dentro de una tarjeta de red.

dirección física dada, es decir realiza la operación inversa del protocolo ARP.

Nivel de acceso a la red:

- **Ethernet:** Norma (IEEE 802.3) que determina la forma en que los equipos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física.
- **CSMA:** Prueba de portador con acceso múltiple (*Carrier Sense Multiple Access*), protocolo de contienda o algoritmo que controla el derecho a transmitir en la red.
- **Token-ring**: Topología en anillo con paso de testigo, protocolo de contienda que trata de un mensaje o ficha electrónica (testigo) que circula por la red, host que lo recoja tiene derecho a transmitir por un tiempo limitado.
- **ATM:** Modo de Transferencia Asíncrona (*Asynchronous Transfer Mode),* tecnología que aprovecha al máximo el uso de los sistemas de transmisión, la información no se transmite ni se conmuta a través de canales asignados permanentemente, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente mediante el uso de los denominados *canales virtuales* y *trayectos virtuales*.

En la figura 1 se encuentra un ejemplo de cómo los niveles TCP / IP funcionan en conjunto para permitir la transmisión de un mensaje entre un equipo cliente y un equipo servidor a través de una red.

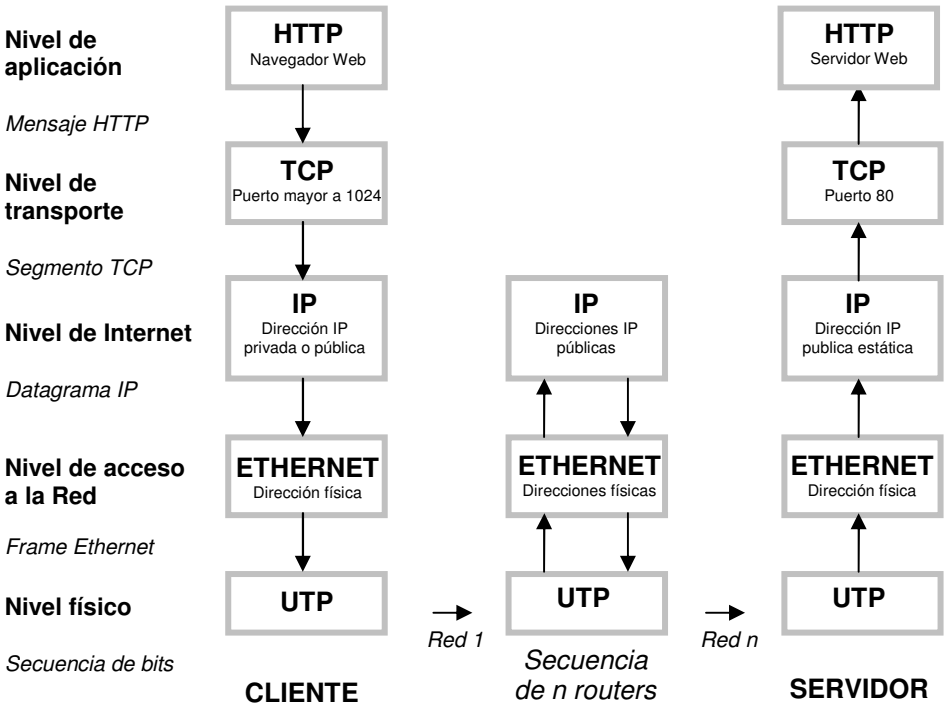

Figura 1 Transmisión de un mensaje TCP / IP

2.2 DIRECCIONAMIENTO IP

Para que la comunicación entre dos computadoras pertenecientes a una red pueda ser posible, cada computadora debe estar identificada con precisión dentro de la red. Dicho identificador lógico se denomina dirección IP. La dirección IP sirve tanto para identificar a la red a la que pertenece una computadora como a la computadora misma dentro de la red.

Una dirección IP está constituida por dos partes, la primera de ellas (cifra más significativa o fracción más a la izquierda) identifica a la red y la otra parte identifica a la computadora dentro de la red. Todas las computadoras pertenecientes a una red requieren el mismo número de red, el cual en el caso de las redes públicas debe ser único en Internet. El número de computadora identifica a un host, servidor, router o cualquier dispositivo con soporte TCP / IP

conectado a la red. El numero de computadora debe ser único para esa red, por tanto en Internet cada maquina debe estar identificado por una dirección irrepetible.

Las direcciones IP se clasifican en:

- **Direcciones IP públicas**. Son visibles en todo Internet. Un host con una dirección IP pública es accesible desde cualquier otro host conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

- **Direcciones IP privadas o reservadas**. Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por enrutadores. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o servidor *proxy*) que tenga una o varias direcciones IP públicas. Sin embargo, desde Internet no se puede acceder directamente a computadoras con direcciones IP privadas. Este es el mecanismo de direccionamiento usado por la LAN UIS, por medio de subredes de la dirección privada clase C 192.168.0.0 [RFC 1918].

A su vez, las direcciones IP pueden ser:

- **Direcciones IP estáticas.** Un host que se conecte a la red con una dirección IP estática siempre lo hará con la misma dirección IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con el fin de estar siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

- **Direcciones IP dinámicas**. Un host que se conecte a la red mediante una dirección IP asignada dinámicamente, es probable que cada vez lo haga con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP.

2.3 IPV4 Y SUS FALENCIAS

El protocolo IP versión 4 [RFC 791] es el protocolo de direccionamiento más usado en la actualidad. Las principales caracteristicas del protocolo IPv4 serán tratadas en paralelo a las caracteristicas de IPv6, con el fin de comprender mejor los cambios incluidos en el nuevo protocolo de Internet.

IPv4 ha superado exitosamente el reto que significa ampliar una red interna (ARPANET) hasta convertirla en un servicio global de las dimensiones actuales de Internet. Sin embargo, en el diseño inicial de este protocolo no fue posible prever los siguientes aspectos:

El crecimiento en usuarios y cobertura experimentado por el Internet y el inminente agotamiento de direcciones IPv4: la falta de direcciones públicas es un problema que no es apreciable por igual en todos los puntos de la red, de hecho es por el momento casi imperceptible en Norteamérica, sin embargo en otras zonas geográficas de Asia, África y parte de Europa el problema se agrava llegando al extremo en el cual una sola universidad de los Estados Unidos posea más direcciones IP públicas que la mayoría de los países Asiáticos.

Además, la creciente proliferación de dispositivos móviles y aparatos electrodomésticos conectados a Internet apunta a que el espacio de direcciones públicas de IPv4 se agotará en los próximos años.

El tamaño excesivo de las tablas de enrutamiento que deben mantener los enrutadores troncales (sin ruta por defecto) de Internet: debido a la forma deficiente en la que se han venido asignando las direcciones de red IPv4, existen generalmente más de 100.000 rutas en la tabla de enrutamiento de los enrutadores del backbone de Internet. Esta situación hace más prolongado el proceso de búsqueda de una ruta en la tabla de enrutamiento y el intercambio de la misma con otros routers, lo cual disminuye considerablemente el rendimiento de la red.

La necesidad de una configuración de direcciones más sencilla: la mayoría de las implementaciones actuales de IPv4 deben configurarse manualmente o mediante un protocolo de configuración de direcciones, como el protocolo de configuración dinámica de host (DHCP, *Dynamic Host Configuration Protocol*). Ante un número mayor de equipos y dispositivos que utilizan IP, existe la necesidad de emplear una configuración de direcciones más sencilla y automática.

La falta de seguridad para el nivel de Red: la comunicación privada a través de un medio público como el Internet requiere de servicios especiales (cifrado y encapsulado) que protejan los datos que se envían ante posibles observaciones o modificaciones durante el tránsito por la red. El uso de estándares de seguridad en IPv4 es opcional.

La necesidad de garantizar la calidad de servicio QoS: aunque existen estándares de QoS para IPv4, el tráfico en tiempo real se basa en el campo *Type of Service* (TOS o Tipo de servicio) de la cabecera IPv4 y en la identificación de la carga, lamentablemente el campo *Type of Service* de IPv4

presenta una funcionalidad limitada y con el tiempo han surgido distintas interpretaciones particulares para su uso.

Las nuevas demandas de movilidad: con IPv4 se tienen las siguientes dificultades al gestionar dispositivos móviles:

- Los dispositivos necesitan una dirección IP nueva en cada punto de conexión y ante la escasez de direcciones es una exigencia muy difícil se suplir.
- Se necesitan buenos elementos de autenticación, para informar la nueva localización del dispositivo móvil.

Siendo conscientes de las anteriores falencias, la comunidad científica a lo largo de los años ha propuesto varios protocolos como sustitutos para IPv4. Los tres más importantes son el PIP [RFC1621] [RFC1622], TUBA (*TCP/UDP With Bigger Addresses*) [RFC1347] [RFC1526] y SIP/SIPP (*Simple Internet Protocol /Simple Internet Protocol Plus*) [RFC1710].

Al mismo tiempo se han desarrollado numerosas extensiones para IPv4, específicamente diseñadas para mejorar la eficacia con que puede utilizarse el espacio de direcciones de 32 bits. Tres de las más importantes son las máscaras de subred de longitud variable (VLSM), los dispositivos NAT y CIDR.

Todos los anteriores protocolos y métodos apoyaron en cierta medida el surgimiento del reemplazo de IPv4, de cada protocolo y práctica eficiente IPv4 se tomó lo mejor y se sintetizó en la siguiente generación del protocolo de Internet.

2.4 LA SIGUIENTE GENERACIÓN DE IP

En respuesta a los inconvenientes nombrados con anterioridad, en julio de 1991 el grupo de trabajo de la ingeniería del Internet (IETF[1], *Internet Engineering Task Force*), emprende el proceso de solicitar a ingenieros y compañías de red alternativas de solución, las cuales se encuentran documentadas en [RFC 1380].

Para diciembre de 1992 ya se disponía de algunas buenas propuestas de solución, razón por la cual el IESG (*Internet Engineering Steering Group*) organizó un consejo llamado IPng (IP *Next Generation*) para debatir y condensar las nuevas proposiciones de IP y publicar su recomendación. Esta publicación hecha en enero de 1995 se denominó *Recommendation for the IP Next Generation Protocol* [RFC 1752].

Este nuevo IP es la versión 6 del protocolo de Internet [RFC 2460] y es el encargado de dirigir la nueva generación del Internet. La razón por la cual no se usó el nombre de IPv5, es que este nombre ya había sido asignado a un protocolo experimental de tiempo real desarrollado en paralelo a IPv6.

2.4.1 LOS CRITERIOS TÉCNICOS PARA IPV6

Los criterios técnicos tenidos en cuenta para el diseño de IPv6 por parte de la IETF han sido definidos en [RFC 1726]. En total se utilizaron 17 criterios en el proceso de evaluación y diseño de IPv6, en los cuales se ve reflejada la intención de mejoría en todos los aspectos clave que involucra el correcto funcionamiento del protocolo de Internet en las redes:

[1] Información detallada en www.ietf.org

1. **Escalabilidad:** La nueva generación de IP debe soportar las nuevas necesidades y aplicaciones que vayan surgiendo, sin ser un impedimento para la nueva generación de Internet.
2. **Flexibilidad Topológica:** La arquitectura de enrutamiento y los protocolos de IPng deben permitir las diversas topologías de red.
3. **Funcionamiento:** Los enrutadores y hosts deben poder procesar el tráfico de IPng sin disminuir su rendimiento normal, es decir a tazas de transferencia y uso de recursos HW similares a IPv4.
4. **Servicio Robusto:** El IPng debe ser un protocolo compacto y robusto que contenga caracteristicas que disminuyan la posibilidad de fallos.
5. **Transición:** El protocolo debe contemplar diversas formas de coexistencia con su predecesor IPv4.
6. **Independencia de los Medios de Transmisión:** El protocolo debe ser diseñado para trabajar a través de una red interna de diversos medios como son redes de área local LAN o redes de área extendida WAN, con velocidades de transmisión que van desde algunos bits por segundo hasta cientos de gigabits por segundo.
7. **Servicio de datagrama poco confiable:** Tal y como ha funcionado en IPv4, el servicio de datagrama no fiable (datagramas que el router envía sin conocer la naturaleza y propósito del mismo) debe seguir funcionando para facilitar una coexistencia con IPv6 y simplificar la administración y mantenimiento de la red.
8. **Configuración, Administración y Operación:** El protocolo debe permitir fácilmente la configuración y administración, en gran parte de manera distribuida.
9. **Operación Segura:** IPng debe proporcionar una capa de red segura. Es vital evitar a toda costa el ingreso de *intrusos* a la red.
10. **Nombramiento Único:** IPng debe asignar a cualquier objeto perteneciente al nivel de red de Internet un identificador único e irrepetible que permita principalmente la identificación de puntos finales.

11. **Acceso:** La totalidad de protocolos que definen el funcionamiento del IPng deben ser claramente definidos y publicados en RFCs, en satisfacción a las especificaciones contenidas en [RFC 1310].
12. **Multicast (Múltiples destinos):** El protocolo debe permitir el envío de paquetes Unicast (Único destino) y Multicast. El Unicast tal y como funcionan las direcciones IPv4 públicas y el Multicast para permitir la transmisión de un mensaje a todos los hosts pertenecientes a la subred.
13. **Extensibilidad:** El protocolo debe ser extensible, es decir debe poder desarrollarse para resolver las necesidades futuras de Internet. Además a medida que IPng se desarrolla debe permitir que las diversas versiones coexistan en la misma red.
14. **Servicios de Red:** El protocolo debe permitir que la red asocie los paquetes a las clases particulares del servicio y provea de ellas los servicios especificados por esas clases.
15. **Movilidad:** el protocolo debe apoyar los hosts y las redes móviles en tareas de enrutamiento en Internet.
16. **Control de Protocolo:** El protocolo debe incluir el soporte elemental para probar y depurar redes punto a punto.
17. **Redes Privadas:** IPng debe permitir a los usuarios construir redes privadas sobre la infraestructura básica de Internet.

2.5 DIFERENCIAS ENTRE IPV4 E IPV6

En esencia no se realizó ningún cambio revolucionario en el protocolo, aparte del aumento en el espacio de direcciones y una estructura de encabezado modificada. Por supuesto que se ha aprovechado la oportunidad para plantear pequeños cambios y mejoras basados en la experiencia obtenida con las operaciones IPv4.

A continuación se encuentran las características en las cuales ha evolucionado el protocolo de Internet en su nueva versión 6 (las cuales serán tratadas a profundidad en los Anexos A y B), en respuesta a las falencias evidenciadas por IPv4:

2.5.1 CABECERA

Los cambios en el encabezado no son drásticos, pero reflejan algunos principios operacionales nuevos que se introducen en IPv6. La cabecera del datagrama IP ha pasado de tener 12 campos en IPv4 a tener solamente 8 en IPv6. La razón principal por la cual se han suprimido algunos campos en el encabezado del protocolo es la excesiva redundancia, por ejemplo IPv4 tiene que calcular los *checksums* en cada uno de los enrutadores presentes en la trayectoria, capas superiores como la TCP envía otros *checksums* en los datagramas salientes con lo que es redundante recalcularlos para la capa de IP.

2.5.2 LA ESCALABILIDAD

IPv6 se puede ampliar fácilmente si se agregan Encabezados de Extensión tras el encabezado de IPv6. A diferencia del campo de Opciones en el encabezado de IPv4, el cual sólo permite entre 0 y 10 palabras de 32 bits para las opciones, el tamaño de los encabezados de extensión de IPv6 sólo está limitado por el tamaño del paquete de IPv6.

Los Encabezados de Extensión se ubican entre el encabezado IPv6 y el encabezado del protocolo de la capa superior. Es debido a los Encabezados de Extensión que podemos garantizar soporte a las futuras aplicaciones, ya que si se requiere definir nuevas opciones, nuevas cabeceras opcionales pueden ser definidas.

2.5.3 ESPACIO DE DIRECCIONES

IPv4 posee un espacio de direcciones de 32 bits lo que significa 2^{32} = 4.294.967.296 direcciones posibles, cantidad que aunque parezca suficiente está limitando el crecimiento de Internet.

Por su parte, IPv6 tiene direcciones IP de origen y destino de 128 bits (16 bytes), el gran espacio de direcciones de IPv6 ha sido diseñado para permitir varios niveles de subredes. Con 128 bits se pueden expresar 2^{128} direcciones diferentes, más de $3{,}4x10^{38}$ combinaciones posibles, y si se estima que el numero de habitantes de la tierra es aproximadamente 6 billones ($6.0x10^{11}$), ¡hay $5.6x10^{26}$ direcciones IPv6 por habitante! Con esta cantidad de direcciones ya no será necesario el uso de dispositivos NAT.

2.5.4 FORMATO DE DIRECCIÓN

Las direcciones IPv4 están conformadas por 4 campos de 8 bits cada uno separados por punto: **X.X.X.X**, donde cada X (por comodidad para los humanos) es expresada en formato decimal.

Ej. **192.168.65.17 -> 11000000 10101000 01000001 00010001**

Por otra parte, las direcciones en IPv6 están conformadas por 8 campos de 16 bits cada uno, separadas por dos puntos: **X:X:X:X:X:X:X:X** donde cada X es expresada en notación hexadecimal. Ahora con IPv6 va a ser mayor la

necesidad e importancia del servicio DNS[1], debido a la dificultad que implica memorizar una dirección del tamaño de las direcciones IPv6.

Ej. **FEDC:BA98:7654:1000:2000:3000:4000:3210**

2.5.5 SEGURIDAD

Aunque se han definido estándares de seguridad para IPv4 ninguno de ellos es obligatorio, es por esto que se han impuesto soluciones propietarias reduciendo así la estandarización de la seguridad en Internet. En IPv6 la compatibilidad con IPSec (Anexo D) es un requisito. IPSec proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6, aporta confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X509v3.

2.5.6 CONFIGURACIÓN DE DIRECCIONES

Para simplificar la configuración de hosts, en IPv6 se permite la configuración de direcciones con estado, como la configuración de direcciones en presencia de un servidor DHCP, y la configuración de direcciones sin estado (en ausencia de un servidor DHCP). Con una configuración de direcciones sin estado, los hosts de un enlace se configuran automáticamente con direcciones IPv6 para el enlace (que se denominan direcciones locales de enlace) y con direcciones

[1] DNS (*Domain Name System*) es un conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

derivadas de prefijos anunciados por enrutadores locales. Incluso en ausencia de un enrutador, los hosts del mismo enlace pueden configurarse automáticamente con direcciones locales de enlace y se comunican sin configuración manual.

2.5.7 LA COMPATIBILIDAD CON LA CALIDAD DE SERVICIO (QOS) Y CLASE DE SERVICIO (COS)

No hay identificación de carga para el control de QoS y CoS por parte de los enrutadores en el encabezado de IPv4, es decir información de gran importancia para una organización no recibe un trato preferencial en la red. Aunque existen estándares de QoS para IPv4, el tráfico en tiempo real se basa en el campo *Type of Service* de la cabecera IPv4 y en la identificación de la carga, normalmente mediante un puerto UDP o TCP. Lamentablemente, el campo *Type of Service* de la cabecera IPv4 presenta una funcionalidad limitada y con el tiempo han surgido distintas interpretaciones locales. Además, la identificación de la carga mediante un puerto TCP o UDP no es posible cuando la carga de paquetes IPv4 se encuentra cifrada. El campo Etiqueta de Flujo del encabezado IPv6 permite identificar y controlar el tráfico con demandas específicas en la red. La identificación del tráfico permite que los enrutadores puedan identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo en particular.

2.5.8 LA INTERACCIÓN CON NODOS VECINOS

En IPv6 las tramas ARP son reemplazadas por el protocolo de descubrimiento de nodo vecino (*Neighbor Discovery),* el cual se encarga de averiguar por que host y redes estamos rodeados. Lo anterior incluye descubrir las características del medio por el cual van a circular los paquetes que enviemos por la red. El

protocolo de descubrimiento de vecino es una combinación entre ARP e ICMPv6, tal como se define en el [RFC 2461].

2.5.9 LA MOVILIDAD

Gracias al amplio espacio de direccionamiento IPv6, es más fácil asignar una dirección nueva en cada punto de conexión a los dispositivos móviles. Se introdujo la seguridad para el tráfico reencaminado y para los procesos de vinculación a las redes. El IPv6 Móvil tiene una implementación más sólida que el IPv4, y además se encuentra incluido en el protocolo.

3. MECANISMOS DE TRANSICIÓN DE IPV4 HACIA IPV6[1]

Aun no se ha definido el día concreto para la implantación definitiva de IPv6 y la consecuente desaparición de IPv4, por lo tanto es necesario seguir manteniendo la infraestructura y aplicaciones IPv4 mientras se avanza en la consolidación de IPv6 como el protocolo encargado del direccionamiento en Internet.

Durante la transición a IPv6, la mayor parte de la red será evidentemente IPv4. Actualmente hay un gran número de hosts y routers que sólo manejan IPv4, pretender cambiar de un día para otro toda esta infraestructura implica esfuerzos económicos y de coordinación a nivel mundial inimaginables que ninguna organización está dispuesta a costear, así que durante un tiempo (probablemente muchos años) IPv4 e IPv6 deberán coexistir.

Por está razón la IETF mediante su grupo de trabajo para la transición (*NgTrans Working Group)* ha definido ciertos mecanismos que permitan a host IPv4 y a host IPv6 comunicarse entre sí. El grupo NgTrans sugiere aplicar técnicas ya probadas, implementadas y optimizadas por compañías, ingenieros y programadores alrededor del mundo.

Se espera que los mecanismos definidos a continuación sean la principal herramienta para hacer de la transición un proceso menos traumático para los usuarios y las aplicaciones. Aplicaciones y sitios deben decidir que técnicas son apropiadas para sus necesidades específicas. Existen tres mecanismos básicos que han sido planteados:

[1] Para un mejor entendimiento de los Mecanismos de Transición tratados en este capítulo, se recomienda examinar con anterioridad el Anexo A (especificación de la versión 6 del Protocolo de Internet) y el Anexo B (arquitectura y ámbito del direccionamiento IPv6)

- *Double stack* IP (doble pila de protocolos).
- Túneles IPv6-sobre-IPv4.
- Traducción de encabezado y de protocolo.

3.1 DOUBLE STACK IP [RFC 4213]

La forma más directa y sencilla de conseguir que un nodo IPv6 sea compatible con un nodo sólo IPv4, es proporcionarle un completo soporte IPv4. Aquellos nodos IPv6 que tienen implementaciones completas de IPv4 e IPv6 son llamados "nodos IPv6 / IPv4". Los nodos IPv6 / IPv4 tienen la capacidad de enviar y recibir ambos tipos de paquetes. Estos nodos pueden interoperar directamente con nodos IPv4 que usan paquetes IPv4, y también interoperar directamente con nodos IPv6 que usan paquetes IPv6. En la siguiente grafica se observa el esquema general de funcionamiento de la pila dual:

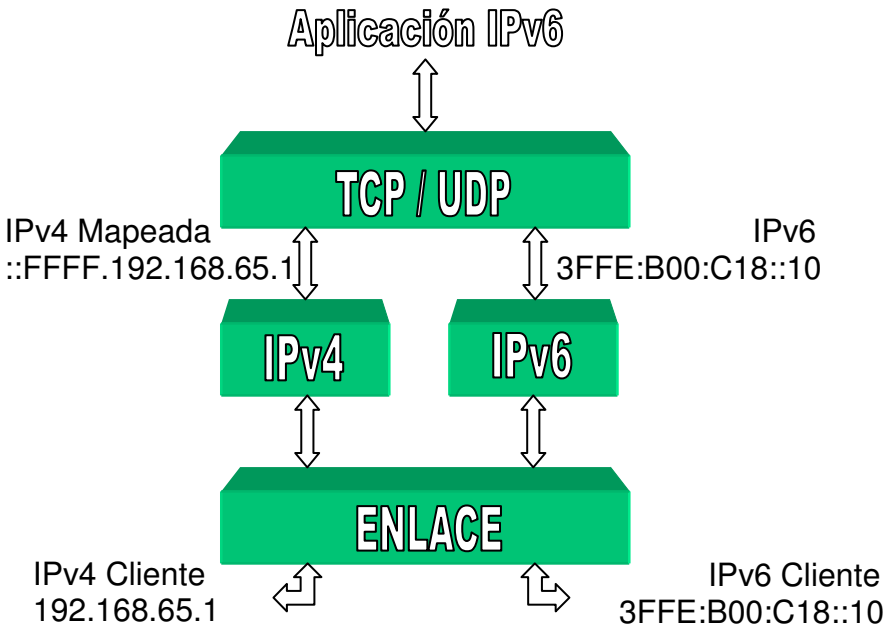

Figura 2 Esquema general del funcionamiento de la pila Dual

Aunque un nodo pueda ser equipado para soportar ambos protocolos, una u otra pila puede ser desactivada por razones operacionales. Así los nodos IPv6/IPv4 pueden operarse en uno de tres modos:

- Con su pila IPv4 habilitada y su pila IPv6 no habilitada.
- Con su pila IPv6 habilitada y su pila IPv4 no habilitada.
- Con ambas pilas habilitadas.

Un nodo IPv6 / IPv4 que tenga su pila IPv6 no habilitada, puede operar nodos solo IPv4, de igual manera un nodo IPv6 / IPv4 con su pila IPv4 no habilitada puede operar con nodos sólo IPv6. Los nodos IPv6 / IPv4 pueden proveer una configuración tipo interruptor para poder activar o desactivar su pila IPv4 o IPv6.

3.1.1 CONFIGURACIÓN DE DIRECCIONES

Debido a que los nodos deben soportar los dos protocolos, un nodo IPv6 / IPv4 debe ser configurado con ambos tipos de direcciones (IPv4 e IPv6). Los nodos IPv6 / IPv4 usan mecanismos IPv4 (Ej. DHCP) para adquirir sus direcciones IPv4, y usar mecanismos IPv6 (Ej. *Stateless Adress Autoconfiguration,* configuración automática sin estado de direcciones (Anexo B - sección 9) y/o DHCPv6) para adquirir sus direcciones IPv6.

IPv6 define mecanismos de autoconfiguración de dirección tanto con estado como sin estado. La autoconfiguración sin estado no requiere configuración manual de servidores, configuración mínima de routers y ninguna de servidores adicionales. El mecanismo sin estado permite que un host genere su propia dirección mediante una combinación de información disponible localmente y anunciada por los routers. Los routers anuncian prefijos que identifican las subredes asociadas a un enlace y las máquinas generan "identificadores de interfaz" que identifican unívocamente a un interfaz en una subred. La dirección

se forma combinando ambos. Si no hay routers, un host tan sólo puede generar direcciones de enlace local. Sin embargo, las direcciones de enlace local son bastante para permitir la comunicación entre nodos conectados al mismo enlace.

En el modelo de configuración con estado, los hosts obtienen direcciones de interfaz y/o información de configuración y parámetros de un servidor. Los servidores mantienen una base de datos que lleva un registro sobre qué direcciones han sido asignadas y a qué host. El protocolo de configuración con estado permite a los hosts obtener direcciones, información de configuración o ambas de un servidor. La configuración automática de direcciones con estado y sin estado son complementarias.

3.1.2 DNS

El sistema de nombres de dominio es usado tanto en IPv4 como en IPv6 para hallar coincidencias entre nombres de host y su dirección IP. Para que los nodos IPv6 / IPv4 puedan interoperar directamente con nodos IPv4 ó IPv6, el DNS debe ser dotado de librerías que le permitan manejar registros IPv4 (A) e IPv6 (A6 / AAAA), registros tratados en el Anexo B – sección 8.

Sin embargo, cuando una solicitud localiza un registro A6 / AAAA de una dirección IPv6, y un registro A que maneja una dirección IPv4, las librerías del DNS pueden filtrar o pedir los resultados devuelta a la aplicación de acuerdo a la versión de los paquetes IP que se comunicaban con ese nodo. En términos de filtrado, el DNS mediante sus librerías tiene tres alternativas: devolver sólo la dirección IPv6 a la aplicación, devolver sólo la dirección IPv4 a la aplicación ó el retorno de ambas direcciones a la aplicación.

Si devuelve sólo la dirección IPv6, la aplicación se comunicará con el nodo que usa IPv6, de igual manera si devuelve sólo la dirección IPv4 la aplicación

se comunicará con el nodo que usa IPv4. Si devuelve ambas direcciones, la aplicación tendrá la opción de escoger que dirección usar, lo cual implica que versión de IP será utilizada. En este caso, la aplicación puede elegir que dirección pedir primero, la IPv6 o la IPv4. Puesto que la mayoría de las aplicaciones prueba las direcciones en el orden en que son devueltas por el DNS, se puede afectar la versión de *preferencia* IP de las aplicaciones. La posibilidad de filtrar u ordenar los resultados del DNS es específica de la aplicación, por lo tanto es necesaria una implementación que permita a la aplicación controlar o no el filtrado.

3.2 TÚNELES

En la mayoría de los escenarios de implantación, la infraestructura de enrutamiento IPv6 será construida con el transcurrir del tiempo. Mientras la infraestructura IPv6 está desplegándose, la infraestructura de enrutamiento IPv4 existente puede permanecer funcional y puede ser usada para llevar tráfico IPv6. Los túneles proveen un modo de utilizar una infraestructura de enrutamiento IPv4 para llevar tráfico IPv6, siendo este proceso transparente para los usuarios finales.

En la figura 3 se observa como lo ocurrido entre los nodos origen y destino (A y F) es completamente transparente para los mismos. A nivel lógico el paquete IPv6 que sale de A, luego de pasar por el nodo B ingresa en un “conducto” especial que lo transporta directamente hasta el nodo E sobre la infraestructura IPv4, y posteriormente el paquete llega tal y como salió al destino final F. A nivel físico el paquete IPv6 luego de pasar por A y B llega al nodo C, el cual ya no recibe un paquete IPv6 sino uno IPv4 (que es lo que el conoce), el paquete IPv4 continua su recorrido hasta D donde el paquete IPv4 es *transformado* nuevamente a IPv6 y llega al destino F como originalmente fue enviado. A nivel de paquetes, los hosts y routers IPv6 / IPv4 pueden establecer un túnel de

datagramas IPv6 sobre las regiones topológicas de enrutamiento IPv4, encapsulando los paquetes IPv6 en paquetes IPv4 (sección 3.2.1).

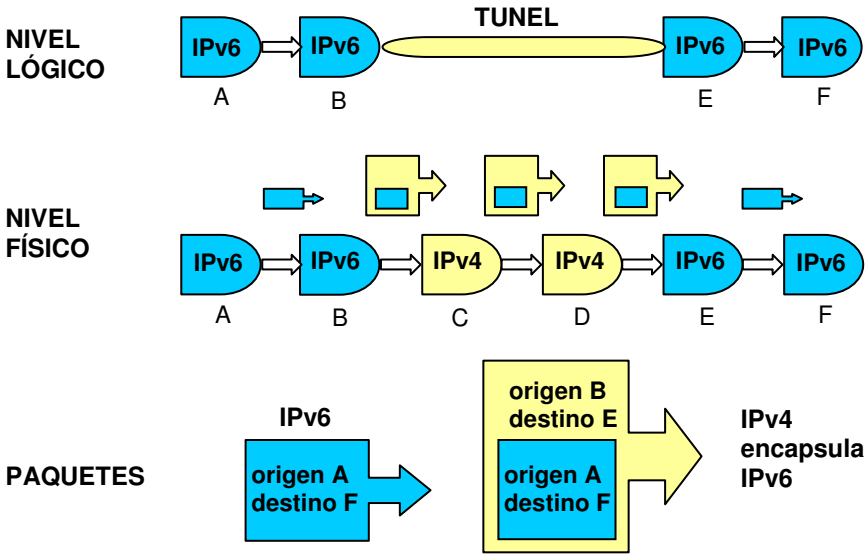

Figura 3 Esquema general del concepto de Túnel

Una analogía que describe claramente la forma en que un túnel opera, haciendo claridad en que con este procedimiento se deja a un lado los beneficios de IPv6 es: supongamos que adquirimos un automóvil con los últimos avances tecnológicos disponibles, el cual alcanza velocidades inimaginables y permite realizar un viaje entre Bucaramanga y Bogotá en tan sólo unos minutos y con muchas garantías de seguridad. El problema es que las vías que comunican a Bucaramanga y a Bogotá, no poseen la infraestructura apropiada para el correcto despliegue del automóvil, adicionalmente las autoridades que controlan el tráfico no permiten autos de este tipo en la vía. Entonces, ¿qué hacer para llegar con este auto hasta Bogotá? Una solución disponible es enviar el auto dentro de un tracto-camión, el cual se demora muchas horas en llegar, no ofrece muchas garantías de seguridad y es el tipo de vehículo que se espera deba transitar por estas vías. Al llegar a

Bogotá el auto es extraído del camión y dejado en una pista moderna y adecuada para su uso. Análogamente, de esta manera funciona un túnel IPv6 sobre IPv4, en el cual los paquetes (el auto) no tienen soporte sobre la infraestructura de red existente IPv4 (las vías), en la cual muchos routers (autoridades de tránsito) no soportan el tráfico IPv6. Para solucionar este problema, se encapsula el paquete IPv6 (auto) en un paquete IPv4 (tracto-camión), el cual viaja transparente por la red IPv4 (las vías) hasta su destino, donde finalmente el paquete es entregado en su forma original.

Los túneles pueden ser usados en una variedad de formas:

Router a router

Los routers IPv6 / IPv4 interconectados por medio de una infraestructura IPv4 pueden establecer un túnel de paquetes IPv6 entre ellos. En este caso, el túnel se extiende de extremo a extremo por el segmento que el paquete tome.

Host a router

Los hosts IPv6 / IPv4 pueden establecer un túnel de paquetes IPv6 a un router intermedio IPv6 / IPv4 que esté asequible por medio de una infraestructura IPv4. Este tipo de túnel se extiende sólo por el primer segmento que el paquete tome en su camino de extremo a extremo.

Host a host

Los hosts IPv6 / IPv4 que están interconectados por medio de una infraestructura IPv4 pueden establecer un túnel de paquetes IPv6 entre ellos.

En este caso, el túnel se extiende palmo a palmo por todo el camino que el paquete tome de extremo a extremo.

Router a host

Los routers IPv6 / IPv4 pueden establecer un túnel de paquetes IPv6 al destino final, en este caso un host IPv6 / IPv4. Este túnel se extiende sólo en el último segmento del camino de extremo a extremo.

Un túnel configurado (sección 3.2.2) puede ser usado en todos los casos anteriormente nombrados, pero la forma más probable de uso es de router a router debido a la necesidad explicita de configurar el túnel en los extremos.

Los mecanismos fundamentales para el *entunelamiento* son:

- El nodo de acceso del túnel (el encapsulador) crea una cabecera IPv4 encapsulando el paquete y transmitiéndolo.
- El nodo de salida del túnel (el desencapsulador) recibe el paquete encapsulado, si es necesario reensambla el paquete, remueve la cabecera IPv4 y procesa el paquete IPv6 recibido.
- El nodo encapsulador puede necesitar mantener alguna información acerca del estado de cada túnel, registrando parámetros como la MTU del túnel y el orden de como procesar los paquetes enviados por el túnel.

Debido a que en algún momento cualquier nodo puede estar usando un número muy grande de túneles, dicha información del estado histórico puede desecharse cuando no se use.

La determinación de qué paquetes encapsular en un túnel se hace generalmente basados en la información de enrutamiento en el nodo encapsulador. Esto se realiza usualmente mediante una tabla de enrutamiento que dirige los paquetes basándose en sus direcciones de destino usando la máscara del prefijo.

Dentro del encabezado IPv4, el campo de Protocolo (Anexo A - sección 1) tendría un valor de 41, identificando así que es IPv6. El nodo desencapsulador confronta los paquetes "protocolo – 41" recibidos con los túneles que el ha configurado, y permite sólo los paquetes en que la dirección origen IPv4 coincida con los túneles configurados en el nodo desencapsulador. Por lo tanto, el operador debe asegurar que la dirección IPv4 con que se configura el túnel sea la misma en los extremos (encapsulador y desencapsulador).

3.2.1 ENCAPSULAMIENTO

Además de agregar una cabecera IPv4, el nodo encapsulador tambien debe ocuparse de otros problemas más complejos:

- Determinar cuando fragmentar y cuando reportar un mensaje de error ICMPv6 "paquete demasiado grande" devuelta al nodo origen.

- Como indicar errores ICMPv4 desde los routers a lo largo del túnel, devuelta al origen el cual sólo espera errores tipo ICMPv6.

El Encapsulamiento de un datagrama IPv6 en uno IPv4 se muestra a continuación:

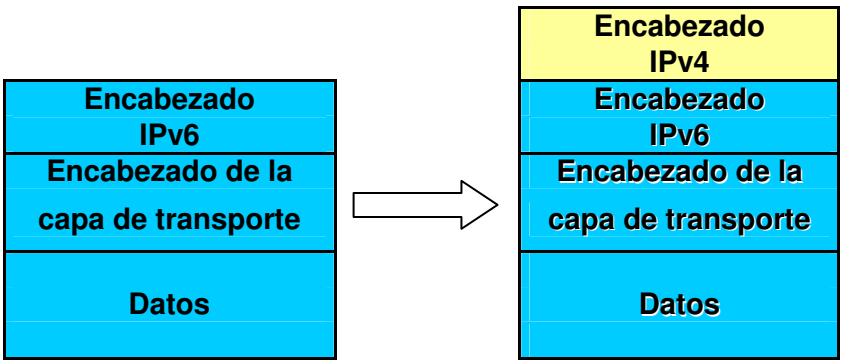

Figura 4 Encapsulamiento en un túnel

3.2.2 TÚNEL CONFIGURADO

Trata de un túnel IPv6 sobre IPv4 cuya dirección del punto final IPv6 está determinada por información de configuración del nodo que realiza el encapsulamiento.

Características

- Se usa fundamentalmente para interconectar islas IPv6 a través de una red IPv4.
- Los extremos son nodos duales que tienen configuradas direcciones IPv4 e IPv6 locales y globales.

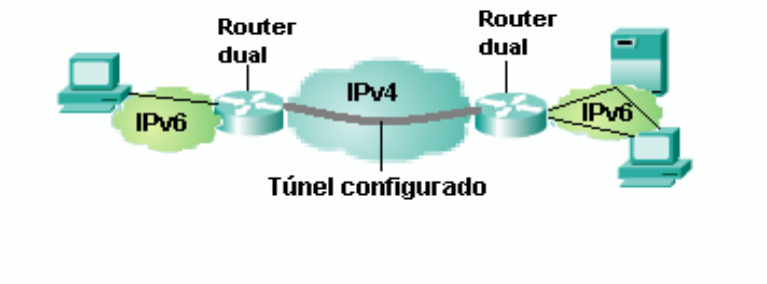

Figura 5 Túnel configurado

Para este caso, el router encapsulador determina la dirección del extremo del túnel basándose en la información de configuración que ha almacenado por cada túnel. Esto se realiza generalmente por medio de la tabla de enrutamiento, basándose en su dirección destino y mascara de prefijo para direccionar los paquetes.

Este tipo de túnel permite a routers duales alcanzar a routers IPv6 con los cuales no disponga de enlaces nativos, lo cual permite a los hosts conectarse con el resto de Internet IPv6. Si es conocida la dirección IPv4 de un router borde IPv6/IPv4 del backbone IPv6, puede ser usada como dirección extremo del túnel. Su aplicación principal es la conexión con ISPv6 remotos a través de Internet.

Las principales desventajas evidenciadas por los túneles configurados radican en la necesidad de configuración manual y la falta de escalabilidad, ya que si se unen N islas y no se establece un nodo central que funcione como switch de túneles, el número de túneles a establecer en cada sitio es N-1. Los sitios que poseen herramientas para gestionar el establecimiento de túneles configurados se denominan *Tunnel Brokers* (sección 4.4.2).

3.2.3 TÚNEL AUTOMÁTICO

Trata de un túnel IPv6 sobre IPv4 cuya dirección IPv4 del punto final está determinada por la dirección IPv4 embebida en la dirección de destino IPv6 (ver Anexo B – sección 4.4) del paquete enviado al túnel.

Características

- Permite a nodos IPv4/IPv6 comunicarse a través de la infraestructura IPv4.
- Los paquetes destinados a direcciones compatibles IPv4, mecánicamente son enviados por un túnel automático.
- La dirección de destino IPv4 se obtiene de la dirección compatible IPv4.

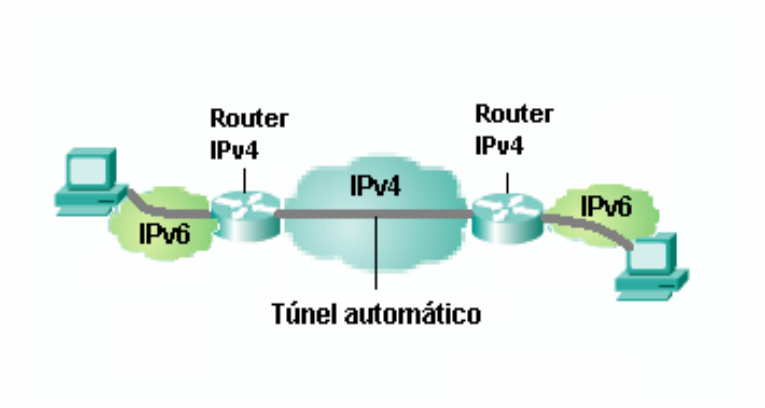

Figura 6 Túnel automático

Pueden utilizarse los túneles configurados y/o automáticos para hosts que se encuentren sin routers IPv6 en el enlace.

3.2.4 TÚNEL 6 TO 4

Un túnel 6 to 4 permite unir islas dispersas a través de la infraestructura IPv4. A cada isla se le asigna un prefijo 2002::/16 más la dirección IP del router frontera. El siguiente salto IPv4 está contenido en la dirección IPv6. El enrutamiento entre las islas se apoya en el enrutamiento IPv4 subyacente.

Al igual que los túneles manuales, son transparentes a nivel IPv6, por lo tanto no afectan a las aplicaciones. Los túneles 6 to 4 se establecen dinámicamente y

sin necesidad de configuración previa. Si se desea conectar N islas IPv6, sólo se establecen los túneles necesarios para las conexiones activas en cada momento.

Los túneles 6 to 4 no son recomendados para redes que sólo necesiten un túnel (por ejemplo a su ISPv6 remoto) o por mucho dos (conexión redundante), en estos casos es preferible establecer túneles configurados manualmente.

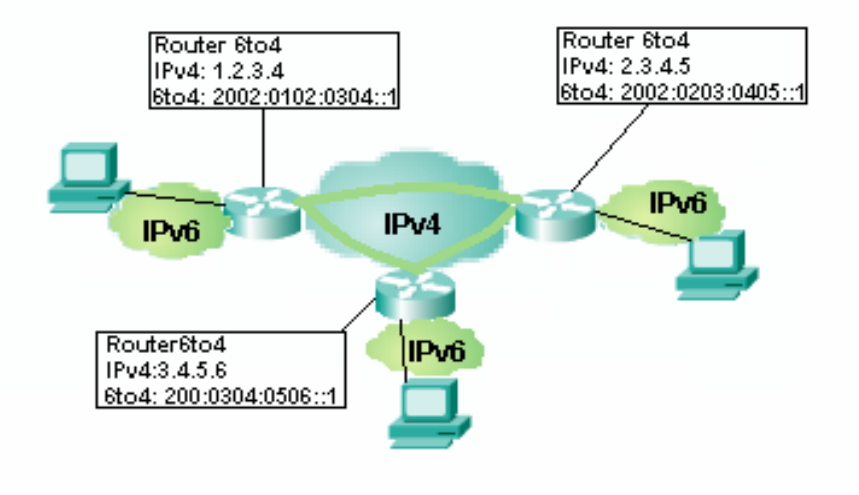

Figura 7 Túnel 6to4

Un túnel 6 to 4 funciona de manera similar a un túnel automático, sólo que los túneles 6 to 4 ofrecen conectividad a toda la isla basado en el prefijo asignado y no sólo a un host basado en una dirección IPv6 con una dirección IPv4 embebida.

3.2.5 TÚNEL 6 OVER 4

Un túnel 6 over 4 se establece cuando un nodo encapsula paquetes IPv6 con cabeceras IPv4, para ser encaminados sobre la infraestructura IPv4.

Características

- Conectan nodos IPv6 dispersos en redes IPv4, formando una LAN virtual IPv6.
- Los procesos de descubrimiento de router y de vecino se realiza empleando multicast.
- Si disponemos de un router dual con acceso al 6bone, todos los nodos podrán acceder al 6bone.

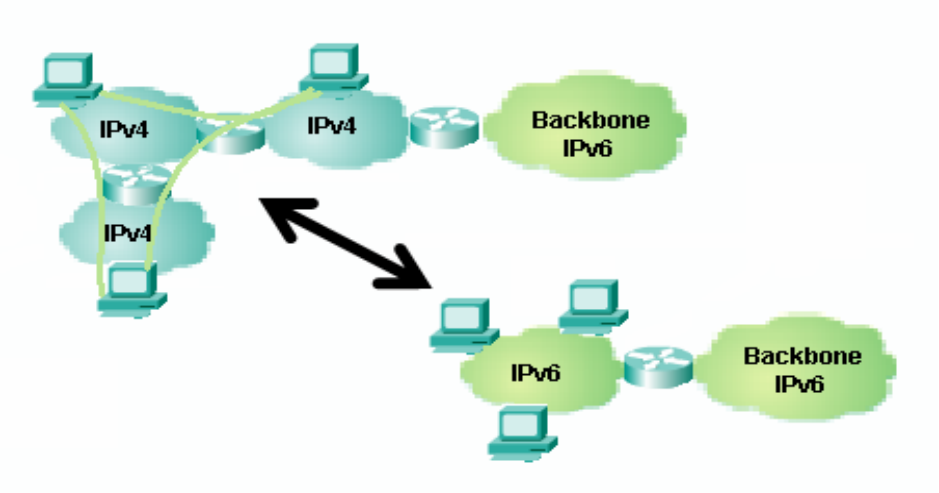

Figura 8 Túnel 6 over 4

Los túneles IPv6 sobre IPv4 son establecidos dinámicamente y sin configuración previa, además permiten la conectividad IPv6 en nodos pertenecientes a una red IPv4 sin necesidad de *tocar* los routers internos.

3.2.6 MTU DEL TÚNEL Y FRAGMENTACIÓN

El encapsulador podría ver el encapsulado como si IPv6 usa a IPv4 como una capa de enlace con un MTU muy grande (65.535 – 20 bytes máximo, se deben restar los 20 bytes necesarios para el encapsulamiento en la cabecera IPv4). El

nodo encapsulador sólo necesita enviar un error ICMPv6 “paquete demasiado grande” hacia el origen para paquetes que excedan este MTU. Sin embargo, tal esquema sería ineficaz o inoperable y no debería ser usado por tres razones:

1. Si se obtiene como resultado fragmentaciones no necesarias. La capa de fragmentación IPv4 debe evitarse debido a los problemas de desempeño causados por la perdida de la unidad más pequeña de transmisión, es decir se generaría una unidad de transmisión menor a la unidad óptima de transmisión.

2. Cualquier fragmentación ocurrida dentro del túnel, es decir entre el nodo encapsulador y desencapsulador, debe ser reensamblado en el punto final del túnel. Para los túneles que terminen en un router, se requeriría memoria adicional y otros recursos extra para reensamblar los fragmentos IPv4 en un paquete completo IPv6 antes de que este paquete sea reenviado a su destino final.

3. El encapsulador no tiene forma de saber que el desencapsulador es capaz de reensamblar los paquetes IPv4, y tampoco tiene manera de saber que el nodo desencapsulador es capaz de ocuparse de una gran MRU (Máxima Unidad de Recibo) IPv6.

Desde aquí, el encapsulador NO DEBE tratar un túnel de una interfaz con una MTU de 64 kilobytes, en cambio puede hacer uso de la MTU fijada estáticamente o una hallada dinámicamente basada en la trayectoria MTU IPv4 en el punto final del túnel. Si los dos mecanismos se llevan a cabo, la decisión de cual usar debe ser configurable básicamente por el extremo final del túnel.

MTU de un túnel estático

Un nodo que usa el MTU de un túnel estático trata la interfaz del túnel como si tuviera un MTU de interfaz fijo. Por defecto, la MTU debe estar entre 1280 y 1480 bytes, pero se recomienda que sea de 1280 bytes. Si por defecto no es 1280, la implementación debe tener configurado un valor que pueda ser usado en cambio del valor MTU.

Un valor MTU fijo de gran tamaño que soporte los anteriores requerimientos, no debe ser configurado a menos que se asegure administrativamente que el desencapsulador puede reensamblar o recibir paquetes de ese tamaño.

La selección de un buen MTU para un túnel depende de muchos factores, entre ellos:

- Si los paquetes protocolo – 41 son transportados sobre medios que puedan tener un camino MTU menor (por ejemplo, redes virtuales privadas IPv4), por lo tanto escoger un valor MTU demasiado alto podría llevar a IPv4 a fragmentar los paquetes.
- Si el túnel se usa para transportar paquetes IPv6 ya *entunelizados* (por ejemplo, un nodo móvil con un túnel configurado IPv6-en-IPv4, y una interfaz de túnel IPv6-en-IPv6), por lo tanto escoger un valor MTU demasiado alto puede llevar a IPv6 a fragmentar los paquetes.

Si se cree que el encapsulamiento por capas es viable hoy por hoy, puede ser prudente considerar el soporte dinámico para la determinación del MTU si esto implica minimizar la fragmentación y optimizar el tamaño de los paquetes.

Cuando se usa un túnel estático MTU, el bit *no fragmentar* no debe ser puesto en la cabecera IPv4 encapsuladora. Como resultado, el encapsulador no

debería recibir ningún mensaje ICMPv4 de “paquete demasiado grande” como consecuencia de los paquetes que el haya encapsulado.

MTU de un túnel dinámico

La determinación dinámica del MTU es opcional. De cualquier modo, si este es implementado, debe proceder tal y como se describe a continuación:

La fragmentación dentro del túnel debe ser reducida al mínimo por tener al nodo encapsulador rastreando el camino MTU IPv4 por el túnel, usando el protocolo de descubrimiento del camino MTU IPv4 [RFC 1911] y registrando el camino MTU resultante. La capa de IPv6 en el encapsulador puede entonces ver un túnel como una capa de enlace con un MTU igual al camino MTU IPv4, menos el tamaño de la cabecera IPv4 encapsuladora.

Nótese que lo anterior no elimina la fragmentación IPv4 en el caso en que el camino MTU IPv4 produzca un camino MTU IPv6 de menos de 1280 bytes [RFC 2460]. En este caso, la capa IPv6 tiene que *ver* una capa de enlace con un MTU de 1280 bytes y el encapsulador tiene que usar fragmentación IPv4 para reenviar los paquetes IPv6 de 1280 bytes.

El nodo encapsulador puede emplear el siguiente algoritmo para determinar cuando reenviar un paquete IPv6 que sea más grande que el MTU del túnel usando fragmentación IPv4, y cuando retornar un mensaje ICMPv6 “paquete demasiado grande” [RFC 1981]:

```
IF (MTU de camino IPv4 – 20) es menor que 1280
        IF el tamaño del paquete es mayor de 1280 bytes
                Enviar mensaje ICMPv6 “paquete demasiado grande” con MTU = 1280.
```

```
            Paquete descartado.
        ELSE
            Encapsular pero no incluir el bit de no fragmentación en la cabecera
            IPv4. Como resultado el paquete IPv4 podría ser fragmentado por la
            capa IPv4 o por algún router a lo largo del camino IPv4.
        END IF
ELSE
        IF el tamaño del paquete es mayor que (MTU de IPv4 - 20)
            Enviar mensaje IPv6 "paquete demasiado grande" con MTU =
            (MTU de camino IPv4 – 20).
            Descartar paquete.
        ELSE
            Encapsular e incluir el bit de no fragmentación en la cabecera IPv4.
        END IF
END IF
```

Los encapsuladores que tengan un gran número de túneles pueden escoger entre MTUs de túneles dinámicos o estáticos fundamentalmente para el punto final de los túneles. En casos donde el número de túneles que cualquier nodo está usando es grande, es útil observar que información de estado de túnel pueda ser guardada, o descartada en caso de no uso.

3.2.7 LIMITE DE SALTOS

Los túneles IPv6-sobre-IPv4 son planeados como un solo salto desde la perspectiva IPv6. El túnel es transparente a los usuarios de red, y no es detectable por herramientas de diagnostico de de red como el *traceroute.*

El modelo del solo-salto es implementado teniendo en cuenta que el nodo encapsulador y desencapsulador sólo decrementan el campo de limite de saltos

de la cabecera IPv6 cuando este paquete es enviado a destinos IPv6, es decir en un túnel ni en los extremos es alterado el valor de limite de saltos.

El valor del campo TTL de la cabecera encapsuladora IPv4 es seleccionado de una manera dependiente de la implementación. Se sugiere los valores publicados por la IANA en http://www.iana.org/numbers.html [RFC 3232].

3.2.8 MANEJO DE LOS ERRORES ICMPV4

En respuesta a paquetes encapsulados y enviados por un túnel, el encapsulador puede recibir mensajes de error ICMPv4 de routers IPv4 dentro del túnel. Estos paquetes son direccionados al encapsulador debido a que este es el origen IPv4 del paquete encapsulado.

El manejo de errores ICMPv4 es solo aplicable a la determinación dinámica del MTU, aunque si las funciones de manejo pueden ser usadas con túneles estáticos MTU, es aún mejor.

Los mensajes de error “paquete demasiado grande” son tratados de acuerdo al descubrimiento del camino IPv4 [RFC 1191] y el camino MTU resultante es grabado en la capa IPv4. El camino MTU grabado es usado por IPv6 para determinar si un error ICMPv6 “paquete demasiado grande” debe ser generado (sección 3.2.6 MTU de un túnel dinámico).

Muchos enrutadores antiguos retornan solo 8 bytes de datos más allá del encabezado IPv4 del paquete en error, que no es suficiente ni para incluir los campos de direcciones del encabezado IPv6. Los routers IPv4 más modernos, probablemente retornen suficientes datos más allá del encabezado IPv4, incluyendo el encabezado IPv6 completo y posiblemente algunos datos adicionales [RFC 1812]. Si los bytes de datos del paquete *ofendido* son

suficientes y están disponibles, el encapsulador puede extraer el paquete IPv6 encapsulado y usarlo para generar un mensaje ICMPv6 dirigido atrás al nodo IPv6 origen, tal y como se muestra en la siguiente gráfica:

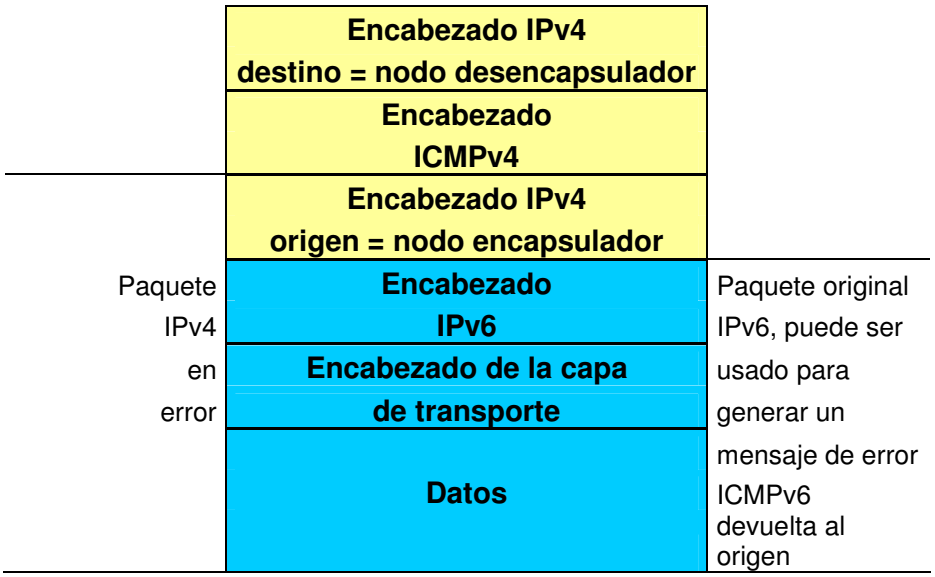

Figura 9 Mensaje de error ICMPv4 devuelto al nodo encapsulador

Cuando los errores ICMPv4 son recibidos como en el ejemplo anterior, y los errores no son del tipo “paquete demasiado grande” sería útil *anotar* o registrar el error como un error relacionado con el túnel. Tambien, si suficientes encabezados están disponibles, entonces el nodo origen puede enviar un error ICMPv6 del tipo “inalcanzable” con un código “dirección inalcanzable” al origen IPv6 [RFC 2463].

Nótese que cuando el MTU del camino es excesivo, y pocos bytes de carga útil asociados con errores ICMPv4 están disponibles, o los errores ICMPv4 no causan la generación de errores ICMPv6 en caso de que haya suficiente carga útil, habrá dos paquetes descartados en lugar de uno (en caso de una sola capa MTU descubierta). Consideremos el caso donde un host IPv6 se conecta a un router IPv4 / IPv6, que es conectado a una red donde un error ICMPv4 sobre el

tamaño excesivo del paquete es generado. Primero, el router necesita aprender el MTU IPv6 desde el router, que ocasiona por lo menos la pérdida de un paquete.

3.2.9 CONSTRUCCIÓN DEL ENCABEZADO IPV4

Cuando se encapsula un paquete IPv6 en un datagrama IPv4, los campos de la cabecera IPv4 son fijados de la siguiente manera:

- **Versión =** 4.
- **Longitud de la cabecera IP en cadenas de 32 bits =** 5 (no se incluyen opciones IPv4 en la cabecera de encapsulamiento).
- **Tipo de servicio =** 0 (a menos que sea especifico en otra parte [RFC 2983] y [RFC 3168] para problemas relacionados con el campo tipo de servicio en un túnel).
- **Longitud total =** la longitud de la carga útil de la cabecera IPv6 mas la longitud de las cabeceras IPv4 e IPv6.
- **Identificación =** generada únicamente por algún paquete IPv4 transmitido por el sistema.
- **Banderas =** Fijar en no fragmentar (DF) o en mas fragmentos (MF) si es necesaria la fragmentación.
- **Desplazamiento de fragmentación =** solo si es necesaria la fragmentación.

- **Tiempo de vida =** debe ser especifica de cada aplicación (ver sección 3.2.7).

- **Protocolo =** 41 (asignado como numero de tipo carga útil para IPv6).

- **Checksum =** calcular la suma de verificación para la cabecera IPv4 [RFC 791].

- **Dirección origen =** una dirección IPv4 del nodo encapsulador: cualquiera configurada por el administrador o la dirección de la interfaz de salida.

- **Dirección destino =** dirección IPv4 del punto final del túnel.

Al encapsular los paquetes, el nodo debe asegurar que usará la dirección origen correcta para que los paquetes sean aceptados en el desencapsulador, tal y como se describe en la sección 3.2.10. Configurar la dirección de origen es particularmente apropiado en los casos en que la selección automática de la dirección de origen pueda producir resultados distintos en un cierto periodo de tiempo. Esto es frecuente en el caso de múltiples direcciones, y múltiples interfaces, o cuando las rutas puedan cambiar a menudo. Por consiguiente, debe ser administrativamente posible especificar la dirección fuente de un túnel.

3.2.10 DESENCAPSULAMIENTO

Cuando un host IPv6 / IPv4 o un router recibe un datagrama IPv4 que es direccionado a una de sus propias direcciones IPv4 o a un grupo de direcciones Multicast, y el valor del campo protocolo es 41, el paquete es un potencial

paquete de túnel y se debe verificar si pertenece a una interfaz de túnel configurado (verificando las direcciones origen y destino), reensamblarlo (si la capa IPv4 fragmentó el paquete), y si luego de remover la cabecera IPv4 el resultado es un datagrama IPv6, este debe ser sometido al código de manejo de la capa IPv6 en el nodo.

El nodo desencapsulador debe verificar que la dirección de origen es correcta antes de procesar los paquetes, para solucionar los problemas con direcciones engañosas (ver sección 3.2.13). Este chequeo tambien se aplica a paquetes que son pasados a los protocolos de transporte en el desencapsulador. Esto se hace verificando que la dirección de origen es la dirección IPv4 del encapsulador configurada en el desencapsulador. Los paquetes para los que la dirección de origen no coincide con la configurada en el desencapsulador, deben ser descartados y ningún mensaje ICMP debe ser generado; sin embargo, si la implementación generalmente envía un mensaje ICMP cuando recibe un paquete de protocolo desconocido, dicho mensaje puede ser enviado (por ejemplo, en presencia de un nodo detrás de un cortafuegos se genera un mensaje ICMPv4 “protocolo 41 inalcanzable”).

Un efecto indirecto de esta comprobación de dirección es que el nodo descarte silenciosamente los paquetes con una dirección de origen incorrecta y paquetes que hayan sido recibidos por el nodo pero no directamente dirigidos a él (por ejemplo, tráfico broadcast).

El nodo desencapsulador debe ser capaz de tener en las interfaces del túnel, un MRU IPv6 de por lo menos 1500 bytes y un gran MTU en la interfaz IPv6 en el desencapsulador. El desencapsulador debe ser capaz de reensamblar un paquete IPv4 que tiene (después del reensamblaje) el máximo MTU de 1500 bytes y un gran MTU en la interfaz IPv4 en el desencapsulador. El número 1500 bytes es el resultado del encapsulado que usa un esquema estático, mientras

que el encapsulado que usa el esquema dinámico, puede ocasionar un MTU de interfaz más grande en el desencapsulador.

El proceso de desencapsulamiento se observa a continuación:

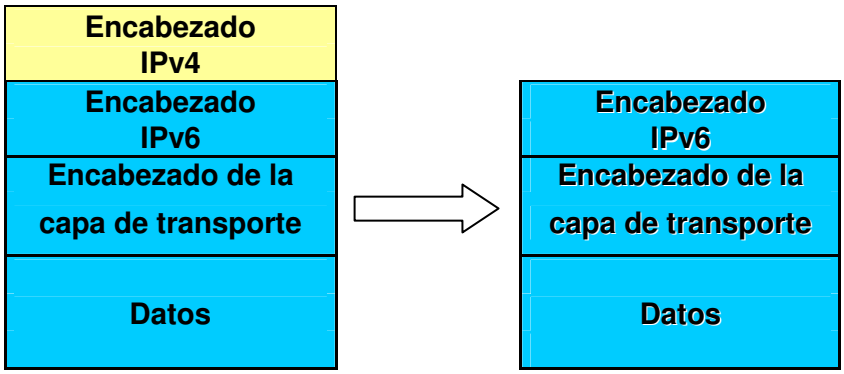

Figura 10 Encapsulamiento en un túnel

El desencapsulador debe reensamblar los paquetes IPv4 antes de desencapsular los paquetes IPv6.

La cabecera IPv4 encapsuladora es descartada, y el paquete resultante es revisado para validar cuando ser tratado por la capa IPv6. Durante la reconstrucción del paquete IPv6, la longitud de la carga útil debe ser determinada desde que el paquete IPv4 es formado (así tenga una longitud que es igual a la longitud del paquete IPv6 mas la cabecera IPv4 que está siendo removida).

Después del desencapsulamiento, el nodo debe descartar silenciosamente los paquetes con una dirección de origen IPv6 no válida. La lista de las direcciones[1] de origen no válidas debe incluir por lo menos:

[1] La arquitectura de direccionamiento IPv6 es definida en el Anexo B.

- Todas las direcciones multicast (FF00:/8)
- La dirección loopback (::1)
- Todas las direcciones IPv4 compatibles con IPv6 [RFC 3513] (::/96), excluyendo la dirección no especifica para la detección de direcciones duplicadas (::/128).
- Todas las direcciones IPv4 mapeadas en una IPv6 (::FFFF:x:x/96).

Adicionalmente, el nodo debe ser configurado para realizar un filtrado del ingreso [RFC 2827] [RFC 3704] en la dirección IPv6 de origen, de manera similar en cualquiera de sus interfaces, por ejemplo:

1. Sí el túnel está configurado a través de Internet, el nodo debe ser configurado para comprobar que los prefijos IPv6 del sitio no son usados como dirección de origen.

2. Sí el túnel es establecido en el borde de una red, el nodo debe ser configurado para comprobar que la dirección de origen pertenece al extremo de la red.

La lista de prefijos generalmente debía ser manualmente configurada, de esta manera el prefijo recientemente incluido podía ser verificado automáticamente, por ejemplo, mediante el uso estricto de un chequeo RPF[1] unicast, mientras una interfaz pueda ser asignada al extremo de la red.

[1] RPF (*Reverse Path Forwarding* – camino inverso de reenvío, método usado para deducir el siguiente salto para paquetes broadcast y multicast.

3.2.11 DIRECCIONES LOCALES DE ENLACE

Los túneles configurados son interfaces IPv6 (sobre la “capa de enlace” IPv4) y por lo tanto deben tener direcciones de Enlace Local (Anexo B – sección 4.6). Las direcciones Locales de Enlace son usadas por ejemplo, por protocolos de enrutamiento que operen sobre los túneles.

El identificador de interfaz para tal interfaz, puede ser basado en los 32 bits de la dirección IPv4 de una interfaz adyacente, o formado usando otros medios, lo importante es que tenga una altísima probabilidad de ser único en el extremo del túnel.

Si una dirección IPv4 es usada para formar una dirección local de enlace IPv6, el identificador de interfaz es la dirección IPv4 precedida de ceros. La dirección local de enlace es formada añadiendo al identificador de interfaz el prefijo FE80::/64.

Cuando el host tiene más de una dirección IPv4 en uso en la interfaz física involucrada en el túnel, una opción para una de estas direcciones IPv4 es formar la dirección local de enlace (ya sea por el administrador o por la aplicación).

3.2.12 DESCUBRIMIENTO DEL VECINO SOBRE UN TÙNEL

Las aplicaciones de túnel configurado deben por lo menos aceptar y responder a la prueba de paquetes usada por la detección del vecino inaccesible (NUD – *Neighbor Unreachability Detection*) [RFC 2461]. Las aplicaciones pueden tambien enviar un paquete de prueba NUD para descubrir cuando un túnel configurado falla, a tal punto que la aplicación puede usar un camino alterno para alcanzar su destino.

Para los propósitos de descubrimiento de vecino, los túneles configurados que se especifican en este documento se asume que no tienen una dirección de capa de enlace, aunque la capa de enlace (IPv4) tenga una dirección. Esto significa que:

- El remitente de paquetes de descubrimiento de vecino, no debe incluir opciones de dirección origen de la capa de enlace u opciones de dirección destino de la capa de enlace, en el enlace del túnel.
- El receptor debe, mientras procesa el paquete de descubrimiento de vecino, ignorar silenciosamente el contenido de alguna opción de dirección de capa de enlace de origen o destino, recibidas en el enlace del túnel.

No usar opciones de dirección de la capa de enlace es consistente con cómo el descubrimiento de vecino es usado en otros enlaces punto-a-punto.

3.2.13 LA AMENAZA RELACIONADA CON LAS DIRECCIONES DE ORIGEN ENGAÑOSAS

La especificación sobre el contenido de las reglas que aplican a la verificación de la dirección origen de un túnel en particular y el ingreso filtrado en general a paquetes antes de ser encapsulados se encuentra en [RFC 2827] y [RFC 3704]. Cuando en un túnel IP-en-IP es usado (independiente de la versión IP), es importante que este no se use para desviar algún ingreso filtrado, en uso por paquetes no entunelizados. Así, las reglas descritas en este documento son basadas en el filtro de ingreso usado por IPv4 e IPv6, el uso de túneles no debe proporcionar un camino fácil para evitar el filtrado.

En este caso, sin especificar la verificación de ingreso filtrado en el desencapsulador, sería posible para un atacante *inyectar* un paquete con:

- Origen IPv4 externo: la dirección IPv4 real del atacante.
- Destino IPv4 externo: dirección IPv4 del desencapsulador.
- Origen IPv6 interno: *nodo-A,* que puede ser el desencapsulador o un nodo cercano.
- Destino IPv6 interno: *nodo-B*.

Aún cuando todos los routers IPv4 entre el atacante y el desencapsulador implementen el filtro de ingreso IPv4, y todos los routers IPv6 entre el desencapsulador y *nodo-A* implementan el filtro de ingreso IPv6, los paquetes engañosos no serán filtrados y desechados. Como resultado *nodo-A* recibirá un paquete que parece haber sido enviado por *nodo-B*, aunque el remitente sea un nodo no determinado.

Una solución a este problema es que el desencapsulador sólo acepte paquetes encapsulados de forma explicita con la dirección de origen configurada (por ejemplo, en el otro extremo del túnel), tal y como se especifica en la sección 3.2.10. Esto no proporciona protección completa en el caso en que el filtro de ingreso no haya sido desplegado, aunque cabe anotar que si aumenta significativamente la seguridad.

3.2.14 CONSIDERACIONES DE SEGURIDAD

Una aplicación de túnel necesita estar al tanto que aunque un túnel es un enlace, el modelo de amenaza para un túnel es mayor y diferente que para cualquier otro enlace, ya que el túnel puede extenderse potencialmente sobre todo el Internet.

Algunos mecanismos (por ejemplo, Neighbor Discovery) dependen de que el contador de saltos sea 255 y/o que la dirección sea local de enlace, para

asegurar que un paquete se originó en un enlace en un ambiente semi-confiable. Los túneles son más vulnerables que un enlace físico, como un atacante puede enviar un paquete IPv6-en-IPv4 al desencapsulador del túnel, causando que este paquete sea inyectado en la interfaz del túnel configurado, a menos que el desencapsulador pueda desechar paquetes enviados de esta manera.

Por consiguiente, es aconsejable que el desencapsulador efectué los siguientes pasos para mitigar esta amenaza:

- La dirección fuente IPv4 del paquete DEBE ser la misma que la configurada para el extremo del túnel.
- Independientemente de cualquier ingreso filtrado IPv4 que el administrador pueda haber configurado, la aplicación PUEDE realizar un ingreso filtrado IPv4 para verificar que los paquetes IPv4 recibidos provienen de una interfaz esperada (pero como esto puede causar algunos problemas, puede estar desactivada por defecto).
- Los paquetes IPv6 con varias direcciones de origen evidentemente inválidas, deben ser desechados.
- El ingreso filtrado puede ser efectuado para verificar que los paquetes IPv6 incluidos en un túnel sean recibidos desde una interfaz esperada o conocida, esto requiere generalmente de una configuración por parte del operador.

Sobre todo la primera verificación es vital: para evitar esta prueba, el atacante debe poder conocer el origen del túnel (pasando de ser difícil a predecible) y ser capaz de engañarlo.

Si se consideran significantes las restantes amenazas de verificación del origen del túnel, un proyecto de túnel con autenticación debe usar en vez de ello, por

ejemplo, IPSec (ver Anexo D) o el Enrutamiento Encapsulado Genérico con una llave secreta pre-configurada (*Generic Routing Encapsulation with a pre-configured secret key* [RFC2890]). Cómo los túneles configurados son fijados más o menos manualmente, establecer el material codificado no debe ser un problema.

Si el entunelamiento se hace dentro de un dominio administrativo, aplicar un filtrado apropiado en el borde del dominio, puede eliminar la amenaza fuera del dominio. Por consiguiente son más recomendables los túneles cortos que los largos.

Además, una aplicación debe tratar las interfaces de diferentes enlaces por separado, por ejemplo, asegurar que los paquetes Neighbor Discovery que lleguen a un enlace no afecten a otros enlaces. Esto es especialmente importante para enlaces del túnel.

Cuando un paquete es descartado por no coincidir con la dirección IPv4 de origen para un túnel, el nodo no debe reconocer la existencia de un túnel, por otra parte esto puede ser usado para sondear si las direcciones de extremo del túnel son aceptables. Por esta razón, la especificación dice que dichos paquetes deben ser descartados y un mensaje de error ICMP no debe generarse, a menos que la aplicación normalmente envíe mensajes ICMP de "destino inalcanzable" para protocolos desconocidos, en este caso el mismo mensaje puede ser enviado. Obviamente, no retornar el mismo mensaje ICMP si un error es retornado por otros protocolos, puede indicar que la pila IPv6 (o el procesamiento de túnel - protocolo 41) ha sido activada, el comportamiento debe ser consistente con cómo la implementación procede de otro modo, en vez de parecer transparente a los sondeos.

3.3 TRADUCCIÓN DE DIRECCIONES DE RED NAT - PT [RFC 2766]

Otra forma de facilitar la coexistencia de IPv4 e IPv6 es mediante el uso de NAT-PT, el cual permite un enrutamiento transparente para comunicar nodos sólo IPv6 con nodos sólo IPv4. Este mecanismo de transición usa una combinación de Traducción de Direcciones de Red (NAT) y Traducción de Protocolos (PT).

El termino NAT usado en este documento [RFC 2766] es muy similar al NAT IPv4 descrito en [RFC 2663], pero no es idéntico. El NAT IPv4 traducía una dirección IPv4 en otra. El NAT que se usa como mecanismo de transición se refiere a la traducción de una dirección IPv4 en una dirección IPv6 y viceversa. Mientras el NATv4 provee enrutamiento entre direcciones privadas IPv4 y un dominio exterior de direcciones IPv4, el NATv6 provee enrutamiento entre un dominio de direcciones IPv6 y un dominio exterior de direcciones IPv4. PT en este documento se refiere a la traducción de un paquete IPv4 en un paquete IPv6 semánticamente equivalente y viceversa. La Traducción de Protocolos es descrita en detalle en [RFC 2765].

Existen dos variaciones del NAT-PT, la primera el NAT-PT tradicional permite a los hosts dentro de una red V6 acceder a hosts en una red V4. En un NAT-PT tradicional, las sesiones son uni-direccionales saliendo de la red V6. El NAT-PT tradicional tiene dos variaciones (NAT-PT básico y NAPT-PT). La segunda variación del NAT-PT es el NAT-PT bidireccional, en el cual las sesiones pueden ser iniciadas desde hosts en una red V4 así como desde una red V6. Las direcciones de red V6 están ligadas a las direcciones V4, estática o dinámicamente cuando las conexiones son establecidas en cualquier sentido. Los hosts del dominio V4 acceden a los hosts del dominio V6 mediante el uso de un DNS para la resolución de direcciones. Un DNS-ALG (*Application Level Gateway* definida en más detalle a continuación) debe estar en capacidad de

traducir direcciones V6 mediante consultas y respuestas DNS, en direcciones V4 válidas y viceversa.

Application Level Gateway

Una pasarela (puerta de enlace) de nivel de aplicación [RFC 2663] es una aplicación específica de agentes que permite la comunicación de un nodo V6 con un nodo V4 y viceversa de una manera transparente para ambas partes de la comunicación. Algunas aplicaciones incluyen las direcciones en campos de carga útil. NAT-PT es una aplicación que no se fija en el contenido de la carga útil. ALG puede trabajar en unión con NAT-PT para proporcionar soporte para muchas aplicaciones.

Las ALG no tienen porqué usar siempre información de estado de NAT. Pueden echar un vistazo a la carga útil y simplemente notificar al NAT para que añada información de estado adicional en ciertos casos. Las ALG son parecidas a los proxys en que, tanto las ALG como los proxys, proporcionan comunicación específica de aplicación entre clientes y servidores. Los proxys utilizan un protocolo especial para comunicarse con clientes proxy y entregar los datos del cliente a los servidores y viceversa. A diferencia de los proxys, las ALG no usan un protocolo especial para comunicarse con las aplicaciones cliente y no necesitan de cambios en las aplicaciones cliente.

Flujo de sesión vs. Flujo de paquete

Los flujos de conexión o sesión son diferentes de los flujos de paquetes. Un flujo de sesión indica la dirección en que se inició la sesión con referencia a una interfaz de red. El flujo de paquetes es la dirección en la que el paquete ha viajado con referencia a un interfaz de red. Por ejemplo, consideremos una

sesión de Telnet saliente. La sesión de Telnet consiste en flujos de paquetes tanto en sentido entrante como saliente. Los paquetes de Telnet salientes llevan las pulsaciones de teclas del terminal y los paquetes entrantes llevan las pantallas desde el servidor de Telnet.

Para los fines de este trabajo, una sesión se define como el conjunto de tráfico que es gestionado como una unidad para su traducción. Las sesiones TCP/UDP se identifican de manera unívoca por una dupla de (dirección IP origen - puerto TCP/UDP origen y dirección IP destino - puerto TCP/UDP destino). Las sesiones para peticiones ICMP se identifican mediante la terna de (dirección IP origen, ID de la petición ICMP, dirección IP destino). El resto de sesiones se caracterizan por la terna (dirección IP origen, dirección IP destino, protocolo IP).

Las traducciones de direcciones realizadas por NAT están basadas en la sesión e incluirían la traducción de los paquetes tanto entrantes como salientes pertenecientes a esa sesión. La dirección de la sesión se identifica mediante la dirección del primer paquete de esa sesión. Démonos cuenta de que no hay garantía alguna de que la idea de una sesión, determinada por NAT como se acaba de explicar, coincida con la idea de sesión de la aplicación. Una aplicación podría ver un puñado de sesiones (sesiones de NAT) como una única sesión y podría incluso no considerar su comunicación con sus interlocutores como una sesión. No se garantiza que todas las aplicaciones funcionen a través de dominios, incluso usando ALG intermedios.

3.3.1 OPERACIÓN DEL NAT-PT TRADICIONAL (V6 A V4)

NAT-PT ofrece una solución de reenvío basado en un enrutamiento transparente y traducción de dirección y protocolo, permitiendo un gran número de aplicaciones en dominios V6 y V4 para interoperar sin requerir algún cambio en dichas aplicaciones. A continuación se describe el funcionamiento de las

variaciones del NAT-PT y la manera en que pueden ser iniciadas las conexiones desde un host en un dominio IPV6 a un host en un dominio IPv4 a través de un NAT-PT tradicional.

Operación del NAT-PT básico

Las direcciones V4 en el pool de direcciones pueden ser asignadas una a una a las direcciones V6 de los nodos finales, todo esto en el caso en que se disponga de tantas direcciones V4 como de nodos finales V6. Como parte del fundamento de este mecanismo, se asume por obvias razones que la red V6 tiene menos direcciones V4 que nodos finales y por esta razón la asignación dinámica de direcciones es requerida para por lo menos algunos de ellos.

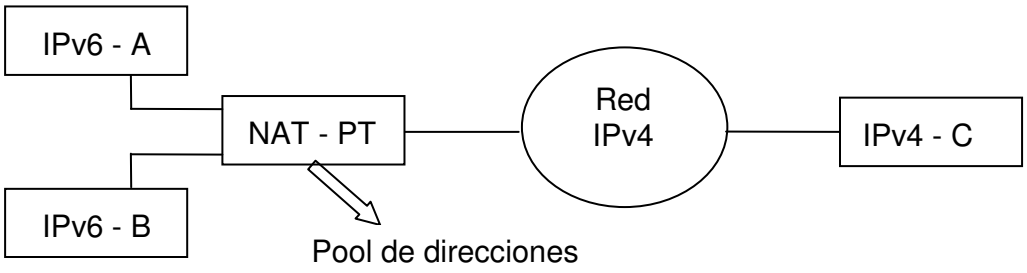

Figura 11 Comunicación IPv6 a Ipv4 a través del NAT

Donde:

- El nodo IPv6 – A tiene la siguiente dirección IPv6: FEDC:BA98::7654:3210
- El nodo IPv6 – B tiene la siguiente dirección IPv6: FEDC:BA98::7654:3211
- El nodo IPv4 – C tiene la siguiente dirección IPv4: 132.146.243.30

- El NAT-PT tiene un pool de direcciones incluyendo la subred IPv4 120.130.26.24/24

Cuando el nodo IPv6 – A necesita comunicarse con el nodo IPv4 – C, el nodo A debe crear un paquete con:

- Dirección de Origen, DO = FEDC:BA98::7654:3210.
- Dirección de Destino, DD = PREFIJO::132.146.243.30

Nótese que el prefijo PREFIJO::/96 es anunciado en el dominio fronterizo por el NAT-PT, y los paquetes direccionados a este PREFIJO deben ser enrutados al NAT-PT. El PREFIJO preconfigurado sólo necesita ser enrutado dentro de los dominios fronterizos IPv6 y como tal puede ser enrutado cualquier prefijo que el administrador de la red escoja.

El paquete es enrutado por medio del gateway del NAT-PT, donde este es traducido a IPv4.

Si el paquete saliente no es un paquete de inicio de sesión, el NAT-PT debe haber almacenado con anterioridad alguna información sobre el estado de la sesión mencionada, incluyendo la dirección IPv4 asignada y otros parámetros para la traducción. Sí esta información de estado no existe, el paquete debe ser descartado silenciosamente.

Si el paquete saliente es un paquete de inicio de sesión, el NAT-PT asigna localmente una dirección (por ejemplo, 120.130.26.10) del pool de direcciones y el paquete es traducido a IPv4. Los parámetros de traducción son guardados durante la sesión y la información de asignación de IPv6 a IPv4 es almacenada por el NAT-PT.

El paquete IPv4 resultante tiene una DO = 120.130.26.10 y DD = 132.146.243.30. Cualquier tráfico devuelto será reconocido como perteneciente a la misma sesión por el NAT-PT. El NAT-PT usará la información de estado para traducir el paquete, y las direcciones resultantes serán DO = PREFIJO::132.146.243.30 y DD = FEDC:BA98::7654:3210. Nótese que este paquete puede ahora ser enrutado dentro de la red sólo IPv6 con normalidad.

Operación del NAPT-PT

El NAPT-PT (*Network Address Port Translation – Protocol Translation*), permite a los nodos V6 comunicarse con nodos V4 de manera transparente usando una sola dirección V4. Los puertos TCP / UDP de los nodos V6 son traducidos en los puertos TCP / UDP de la dirección V4 registrada.

Mientras el soporte de NAT-PT esté limitado a TCP, UDP y otro tipo de puerto multiplexado de aplicaciones, el NAPT-PT resuelve un problema inherente con el NAT-PT. Es decir, el NAT-PT pierde su utilidad cuando su pool de direcciones V4 destinados para la traducción se agota. Una vez el pool de direcciones está agotado, nuevos nodos V6 no pueden establecer sesiones con el mundo exterior. El NAPT-PT por otro lado, permite un máximo de 63k sesiones TCP y UDP por dirección IPv4, antes de tener ningún puerto TCP y UDP por asignar.

Para modificar el ejemplo de la figura 11, se puede tener NAPT-PT en el router de borde (en lugar de NAT-PT) y todas las direcciones V6 pueden ser asignadas a una sola dirección V4 la 120.130.26.10.

El nodo IPv6 –A establece una sesión TCP con el nodo IPv4 – C con lo siguiente:

El nodo A crea un paquete con:

- DO = FEDC:BA98::7654:3210, puerto de origen TCP = 3017, DD = PREFIJO::132.146.243.30 y puerto destino TCP = 23.

Cuando el paquete alcanza el dispositivo NAPT-PT, el NAPT-PT debe asignar uno de los puertos TCP a la dirección V4 asignada para traducir la dupla (dirección origen y puerto de origen TCP) de la siguiente manera:

- DO = 120.130.26.10, puerto de origen TCP = 1025 y DD = 132.146.243.30, puerto de destino TCP = 23.

El trafico retornado desde 132.146.243.30, el puerto TCP 23 debe ser reconocido como perteneciente a la misma sesión y debe ser traducido de manera inversa a V6 de la siguiente manera:

- DO = PREFIJO::132.146.243.30, puerto de origen TCP = 23 y DD = FEDC:BA98::7654:3210, puerto de destino TCP = 3017.

La sesión entrante NAPT-PT es restringida a un servidor por servicio, asignándole el puerto TCP / UDP de manera estática. Por ejemplo, el nodo IPv6 – A de la figura 11 debe ser solamente servidor HTTP (puerto 80) en el dominio V6. El nodo IPv4 – C envía un paquete con:

- DO = 132.146.243.30, puerto de origen TCP = 1025 y DD = 120.130.26.10, puerto de destino TCP = 80.

El NAT-PT traducirá este paquete a:

- DO = PREFIJO::132.146.243.30, puerto de origen TCP = 1025 y DD = FEDC:BA98::7654:3210, puerto de destino TCP = 80.

En el ejemplo anterior, nótese como todas las sesiones que alcanzan el NAPT-PT con un puerto de destino = 80 es remitido al mismo nodo IPv6 – A.

3.3.2 USO DEL DNS - ALG PARA LA ASIGNACIÓN DE DIRECCIONES

Una dirección IPv4 es asignada por el NAT-PT a un nodo V6 cuando el NAT-PT identifica el inicio de una sesión (entrante o saliente). La identificación del inicio de una nueva sesión entrante es realizada de una forma diferente que para una sesión saliente. Sin embargo, el mismo pool de direcciones V4 es usado para ser asignado a nodos V6, sin considerar si una sesión es iniciada saliendo de un nodo V6 o entrando desde un nodo V4. La asignación de nombres a direcciones IPv4 debe ser llevada a cabo en el DNS mediante registros "A". La asignación de nombres a direcciones V6 puede ser concretada en el DNS mediante el uso de registros "AAAA" o "A6" tal y como se especifica en el Anexo B - sección 8.

En cualquier caso, la operación principal del DNS-ALG descrita en esta sección es la misma con cualquier registro (A6 o AAAA). La única diferencia es que la resolución de nombre usada en los registros A6 puede requerir más de una consulta. El DNS-ALG debe en este caso rastrear todas las consultas antes de traducir un registro A6 en un registro A.

Uno de los objetivos del diseño del NAT-PT es que solo se use la traducción cuando no haya ningún otro medio de comunicación disponible. El NAT-PT

además de la conectividad IPv4 que ofrece, permite tener una conexión nativa y/o entunelizada IPv6.

Asignación de direcciones V4 para conexiones entrantes (V4 a V6)

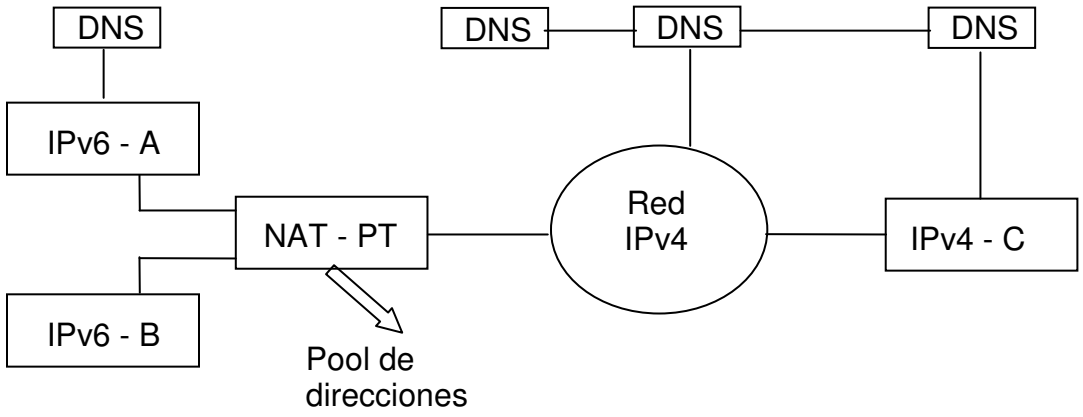

Figura 12 Comunicación IPv6 a Ipv4 a través del NAT incluyendo un DNS

Donde:

- El nodo IPv6 – A tiene la siguiente dirección IPv6: FEDC:BA98::7654:3210
- El nodo IPv6 – B tiene la siguiente dirección IPv6: FEDC:BA98::7654:3211
- El nodo IPv4 – C tiene la siguiente dirección IPv4: 132.146.243.30
- El NAT-PT tiene un pool de direcciones incluyendo la subred IPv4 120.130.26.24/24

En la figura anterior, cuando el nodo C envía una consulta de nombre para el nodo A, la consulta es dirigida al servidos DNS en la red V6. Considerando que el NAT-PT está residiendo en el router frontera entre las redes V4 y V6, este

datagrama de petición habría cruzado a través del router NAT-PT. El DNS-ALG en el dispositivo NAT-PT habría modificado las consultas DNS para registros A salientes del dominio V6 como sigue (nótese que los paquetes DNS TCP/UDP son reconocidos por el hecho de que su puerto de origen o destino es el 53):

a. Para las consultas de Nombre de Nodo a Dirección de Nodo: cambiar el tipo de consulta de “A” a “AAAA” o “A6”.
b. Para las consultas de Dirección de Nodo a Nombre de Nodo: reemplazar la cadena “IN-ADDR.ARPA” por la cadena “IP6.INT”. Reemplazar los octetos de la dirección V4 (en orden inverso) precedidos de la cadena “IN-ADDR.ARPA” por los octetos correspondientes de la dirección V6 en orden inverso.

En la dirección opuesta, cuando una respuesta DNS cruza desde el servidor DNS en la red V6 al nodo V4, el DNS-ALG una vez más intercepta el paquete DNS y hace lo siguiente:

a. Traduce las respuestas DNS para registros “AAAA” o “A6” a registros “A”, (solo traduce registros A6 cuando el nombre esté completamente resuelto).
b. Reemplaza la dirección IPv6 resuelta por el DNS V6 por la dirección V4 internamente asignada por el router NAT-PT.

Si una dirección V4 no está previamente asignada a este nodo V6, el NAT-PT asignará una inmediatamente. Por ejemplo el nodo IPv4 – C intenta inicializar una sesión con el nodo IPv6 – A haciendo una consulta al nombre (registro “A”) para el nodo A. La consulta del nombre sale al DNS local y desde allí esta se propaga al servidor DNS de la red IPv6. El DNS-ALG intercepta y traduce la consulta “A” a una consulta “AAAA” o “A6”, y luego la reenvía hacia el servidor

DNS en la red IPv6 con respuestas de la siguiente manera (este ejemplo usa registros AAAA por conveniencia):

Nodo – A AAAA FEDC:BA98::7654:3210

Esto es devuelto por el servidor DNS y es interceptado y traducido por el DNS-ALG a:

Nodo – A A 120.130.26.1

El DNS-ALG tambien apoya la asignación entre FEDC:BA98::7654:3210 y 120.130.26.1 en el NAT-PT. El registro "A" es entonces retornado al nodo C, el cual puede iniciar una sesión con:

- DO = 132.146.243.30, puerto de origen TCP = 1025 y DD = 120.130.26.1, puerto de destino TCP = 80.

El paquete será enrutado hacia el NAT-PT, que desde ya lleva a cabo una asignación entre FEDC:BA98::7654:3210 y 120.130.26.1 pudiendo traducir el paquete a:

- DO = PREFIJO::132.146.243.30, puerto de origen TCP = 1025 y DD = FEDC:BA98::7654:3210, puerto de destino TCP = 80.

Ahora la comunicación puede proceder de manera normal.

La asignación de direcciones para sesiones entrantes descrita en esta sección, está expuesta a ataques de rechazo de servicio, debido a que se puede hacer

múltiples consultas para nodos residentes en la red V6 causando que el DNS-ALG asigne todas las direcciones V4 en el NAT-PT y así bloquear la entrada de las sesiones legitimas. De esta manera, la asignación de direcciones para sesiones entrantes debe ser interrumpida luego de cierto tiempo para minimizar así los ataques de rechazo de servicio. Adicionalmente, una dirección IPv4 (usando NAPT-PT) puede ser reservada solo para sesiones de salida para minimizar los efectos de tales ataques a las sesiones salientes.

Asignación de direcciones V4 para conexiones salientes (V6 a V4)

Los nodos V6 *aprenden* del servidor DNS en el dominio V4 o del servidor DNS interno de la red V6, las direcciones de los nodos V4. Se recomienda que el servidor DNS interno de los dominios V6 mantenga una asignación de nombres a las direcciones IPv6 para nodos internos y si es posible de algunos nodos externos. En el caso donde el servidor DNS en el dominio V6 contenga un mapa de asignación para nodos externos V4, las consultas DNS no deberían cruzar el dominio V6 y se obviará la necesidad de que intervenga el DNS-ALG. Por otra parte, las consultas que crucen el dominio V6 están sujetas a la intervención del DNS-ALG. Por lo tanto se recomienda que los servidores DNS externos en el dominio V4 capturen la asignación de nombres solamente para nodos externos.

En el caso del NAPT-PT, un puerto de origen TCP/UDP es asignado desde las direcciones V4 registradas cada vez que se detecte una nueva sesión saliente.

Se observa que un nodo V6 que necesite comunicarse con un nodo V4, necesita usar un prefijo especifico (PREFIJO::/96) delante de la dirección IPv4 del nodo V4. La técnica anterior permite el uso de este PREFIJO sin realizar alguna configuración en los nodos.

Para crear otro ejemplo de la figura 12, el nodo – A busca iniciar una sesión con el nodo – C. Para esto el nodo – A inicia haciendo una búsqueda (registro "AAAA" o "A6") de nombre para el nodo – C. Como el nodo – C puede tener una dirección IPv4 y/o una dirección IPv6, el DNS-ALG en el dispositivo NAT-PT reenvía la consulta original AAAA/A6 al DNS externo, así como una consulta A para el mismo nodo. Si un registro AAAA/A6 existe para el destino, este será retornado al NAT-PT quien lo reenviará también inalterado al nodo originador.

Si hay un registro A para el nodo – C la respuesta o contestación será retornada al NAT-PT. El DNS-ALG entonces traducirá la respuesta adicionándole el PREFIJO apropiado y luego lo reenviara al dispositivo originador con cualquier dirección IPv6 que haya aprendido. De esta manera la respuesta seria:

Nodo C	A	132.146.243.30, es traducida a
Nodo C	AAAA	PREFIJO::132.146.243.30 o
Nodo C	A6	PREFIJO::132.146.243.30

Ahora el nodo A puede usar esta dirección como cualquier otra dirección IPv6 y el servidor DNS puede incluso almacenarla, eso si dicho PREFIJO no cambia.

Un problema surgido en este punto es cómo puede el DNS V6 en el dominio fronterizo *hablar* con el dominio V4, afuera del dominio fronterizo IPv6. Recordemos que en este escenario no hay nodos duales. El servidor DNS V4 externo necesita apuntar a una dirección V4, parte del pool de direcciones V4 al NAT-PT disponible. El NAT-PT guarda la asignación una-a-una entre estas direcciones V4 y las direcciones V6 del servidor DNS V6 interno. En el sentido contrario, el servidor DNS V6 apunta a la dirección V6 formada por la dirección V4 del servidor externo V4 y el prefijo (PREFIJO::/96) el cual indica que no son nodos IPv6. Este mecanismo puede ser fácilmente extendido para los servidores DNS secundarios.

3.4 BUMP IN STACK – BIS [RFC 2767]

Este mecanismo funciona como un NAT-PT a nivel de host y es usado en los casos en que las aplicaciones en los nodos no soporten IPv6.

Funciona básicamente añadiendo tres módulos:

- **Un traductor**: el cual traduce direcciones IPv4 en IPv6 y viceversa, usando el mecanismo de conversión IP SIIT definido en [RFC 2765].

- **Una extensión para la resolución de nombres:** la cual retorna una respuesta propia en contestación a la petición de la aplicación IPv4. Cuando la aplicación envía una consulta de registro A al DNS, este crea otra consulta para resolver los dos registros A y AAAA para el nombre del host. Si el registro A es resuelto ya no es necesario enviarlo al traductor IP y puede ser devuelto a la aplicación. Sí sólo el registro AAAA está disponible se solicita al mapeador de direcciones que le asigne una dirección IPv4 correspondiente a la dirección IPv6, luego se crea el registro A para esta dirección IPv4 asignada y es devuelta a la aplicación.

- **Un mapeador de direcciones:** el cual se encarga de mantener un pool de direcciones IPv4, generalmente de ámbito privado. Además mantiene una tabla con los pares de registros para las direcciones IPv4 asignadas a direcciones IPv6, funciona de manera similar al DNS-ALG sección 4.3.2.

La idea fundamental es la siguiente: cuando una aplicación sólo IPv4 necesita comunicarse con un nodo IPv6, su dirección IPv6 se mapea a una dirección IPv4, y los paquetes generados IPv4 son transformados en paquetes IPv6 utilizando SIIT.

Existe otro mecanismo de traducción muy parecido al BIS, se denomina BIA (*Bump in Api*) [RFC 3338], ambos métodos realizan una traducción en el nodo en que se ejecuta la aplicación de información v4 a información v6. La diferencia entre BIA y BIS radica en donde se realiza esta traducción: en el caso de BIA esta traducción se realiza en el nivel del API de trasporte, es decir en la interfaz propia de cada aplicación, y BIS lo hace en la interfaz del nivel de enlace, es decir en la propia interfaz de la tarjeta de red. Lo anterior se puede observar en la figura 13.

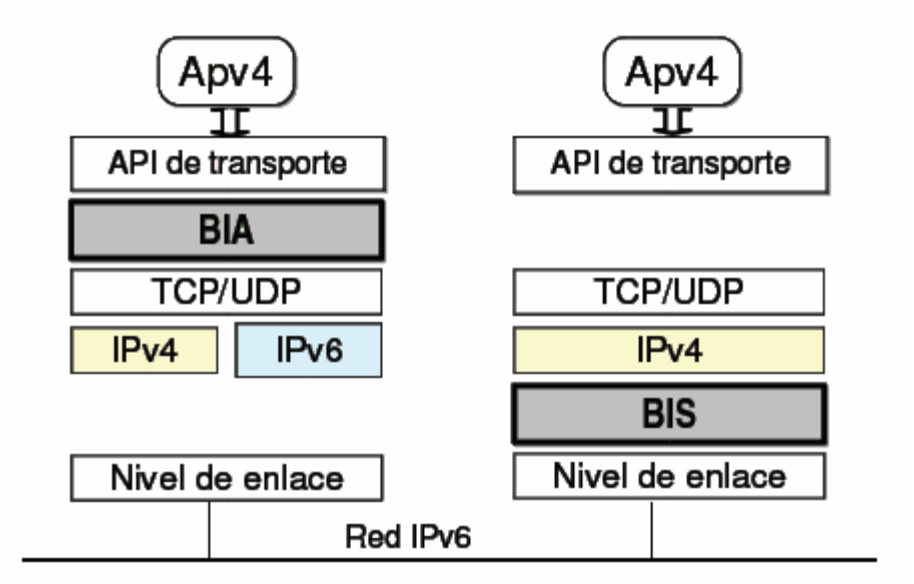

Figura 13 BIS comparado con BIA

4. LA RED DE DATOS UIS FRENTE A IPV6

4.1 SITUACIÓN ACTUAL

En este capítulo se hace una descripción general de la red de datos UIS, haciendo énfasis en los aspectos clave que involucra la futura migración hacia IPv6. De nuestra red es necesario conocer que fortalezas y debilidades posee frente a IPv6, con el fin de evaluar el impacto que tendría la transición sobre los equipos de red (routers y switches), los equipos de usuario, la topología y los enlaces.

Además de los requerimientos físicos, debemos tener en cuenta el soporte IPv6 que posean los diferentes sistemas operativos involucrados en la red (S.O. en equipos cliente, servidores y routers). Asimismo, las diferentes aplicaciones que funcionan sobre la red deben ser sometidas a análisis con el fin de valorar que modificaciones sean requeridas para el correcto funcionamiento de las mismas sobre IPv6.

4.1.1 ESTRUCTURA FÍSICA

La red LAN de datos UIS está definida claramente como un sistema de *backbone* con topología en estrella extendida, es decir la red posee un nodo central desde el cual se irradian todos los enlaces hacia los demás nodos, los cuales a su vez son centro de otra estrella (ver figura 14).

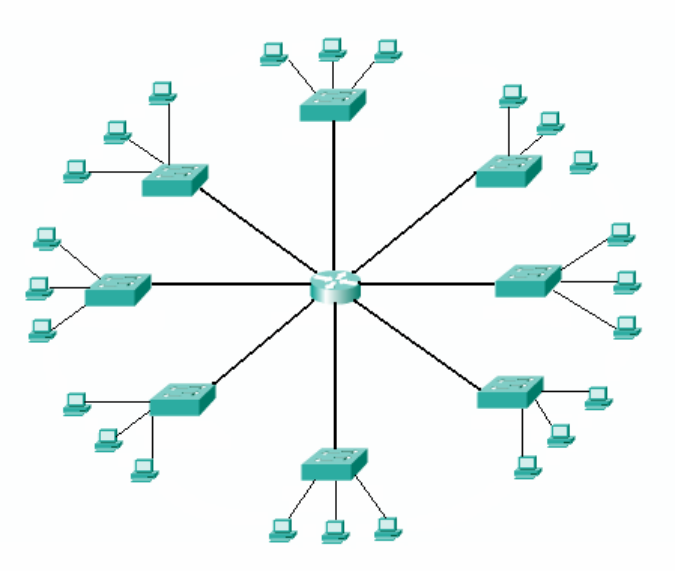

Figura 14 Topología en estrella extendida

Físicamente, la red está constituida por un centro de cableado principal, enlaces de fibra óptica entre el centro de cableado principal y cada uno de los edificios del campus, la facultad de salud, la sede de Guatiguará y la sede de Bucarica, lo que permite conexiones dentro de la red LAN, a velocidades de 100 Mbps y 1.000 Mbps. Las sedes de Barrancabermeja y Socorro se conectan a la red de la UIS a velocidades de 512 Kbps y las sedes de Málaga y Barbosa a 256 Kbps, mediante enlaces contratados con la empresa Colombia Telecomunicaciones Telecom (ver figura 16).

El centro de cableado principal (nodo central) de la red está configurado con un switch de chasis multi-protocolo y multi-capa marca EXTREME NETWORKS, modelo BLACK DIAMOND 6808 con una capacidad de procesamiento de 384 Gbps en switching, alta disponibilidad para redes y enlaces con requerimientos de 10 Gigabit Ethernet, listas de control de acceso (ACLs) y soporte para Jumbogramas. Además, mediante la agregación de chasis o tarjetas de expansión permite obtener un máximo de 672 puertos Fast Ethernet 10 / 100

Base–TX, 168 puertos 10/ 100/ 1000 Base-T, 128 puertos Gigabit Ethernet y 8 puertos 10 Gigabit Ethernet.

Figura 15 Nodo central de la red UIS, ubicado en la planta telefónica

Para permitir el normal funcionamiento de la red aún si ocurre la eventualidad en que el switch BLACK DIAMOND presente fallas, se ha dispuesto que el

switch marca AVAYA P880-R opere como dispositivo emergente (ver figura 15), el cual cuenta con una capacidad de procesamiento de 56 Gbps en switching y 41 millones de paquetes por segundo en enrutamiento, además de una capacidad máxima de 128 puertos Gigabit y 384 puertos 100BaseFX.

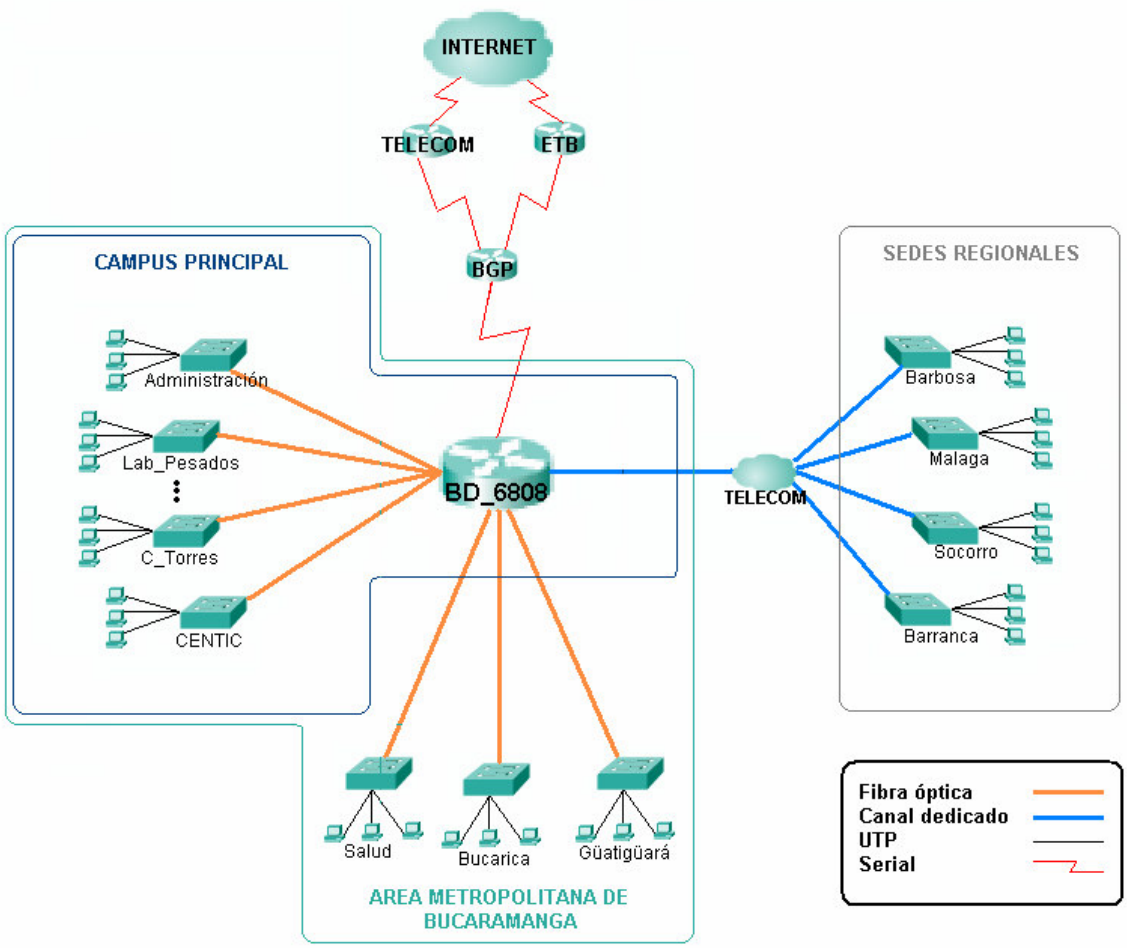

Figura 16 Diagrama esquemático de la red de datos UIS

El centro de cableado principal está ubicado en las dependencias de la planta telefónica de la universidad, que corresponde aproximadamente al centro geográfico del campus, garantizando así la optimización de las distancias del tendido de fibra óptica a cada uno de los edificios del campus.

Todos los edificios del campus principal y las sedes disponen de por lo menos un Centro de Cableado para la interconexión con el Centro de Cableado Principal y para la administración del segmento de red respectivo. Cada uno de estos centros de cableado cuenta con un switch de borde marca AVAYA modelo P333T, configurado con un puerto *uplink* de fibra óptica FastEthernet ó Gigabit Ethernet y 24 puertos 10/100Base-TX *autosensing* para la conexión de concentradores de red, equipos servidores o estaciones de trabajo instalados en el edificio respectivo.

La red LAN de datos de la universidad cuenta actualmente con aproximadamente 3000 puntos de conexión instalados en todos los edificios de sus 4 campus metropolitanos (Central, Facultad de Salud, Bucarica y Guatiguará) y de sus sedes regionales (Barrancabermeja, Socorro, Málaga y Barbosa), implementados como sistemas de cableado estructurado categoría 5, 5e y 6, según las normas técnicas ANSI/TIA/EIA 568A y 569, garantizándose velocidades de transmisión de 100 y 1000 Mbps en los puestos de trabajo.

4.1.2 ACCESO A INTERNET

Para la conexión a Internet, la Universidad cuenta actualmente con dos firmas proveedoras de acceso, Colombia Telecomunicaciones TELECOM, y Empresa de Telecomunicaciones de Bogotá ETB, con las cuales se tienen contratados canales dedicados, utilizando para cada una medios de acceso diferentes y operando con protocolos de balanceo de carga para disponer de un ancho de banda agregado total de 12 (doce) Mbps repartidos actualmente así: 6 (seis) Mbps con la empresa de Colombia Telecomunicaciones, TELECOM, utilizando fibra óptica monomodo como último kilómetro, y 6 (seis) Mbps con la Empresa de Telecomunicaciones de Bogotá, ETB.

El enrutamiento hacia y desde Internet lo realizan 2 enrutadores marca CISCO, modelo 3640 y 3620, los cuales reciben y gestionan el canal de cada uno de los proveedores de acceso a Internet.

Para la protección de la red contra ataques externos, la red cuenta con un firewall marca CISCO, modelo PIX 515 situado entre la red LAN de la Universidad y la red de los proveedores de acceso a Internet.

La optimización del uso de los canales de acceso a Internet se realiza mediante un equipo marca CISCO, modelo Cache Engine 505 que opera como proxy transparente por hardware para la red, y configurado con un disco duro de 10 GB para cache de páginas Web y un puerto FastEthernet de conexión a la red.

Para administrar, controlar, monitorizar y filtrar según políticas institucionales el tráfico y navegación Web, la red dispone de un servidor Websense Enterprise operando sobre un equipo con sistema operativo Microsoft Windows 2000.

4.1.3 SISTEMAS OPERATIVOS

La mayoría de los equipos de usuario ubicados en todas las dependencias de la Universidad operan con el sistema operativo Microsoft Windows XP y en menor medida con Microsoft Windows 98. Estas versiones del sistema operativo Windows, se caracterizan por dar un soporte óptimo a una gran cantidad de aplicaciones ofimáticas, de desarrollo, administrativas, investigativas, lúdicas, entre otras. Las cuales apoyan las labores investigativas de los estudiantes de pregrado, especialización y maestría, además de los docentes, directivos y empleados.

En los equipos servidores de aplicaciones (Ej. gavilán, cóndor, cormorán, dodo, entre otros), se acostumbra usar distribuciones libres de sistemas operativos

derivados de Linux como lo son Red Hat Enterprise y Fedora. Usar estos sistemas operativos aporta un mayor soporte multi-usuario, multi-paginación y sobre todo aumenta la seguridad al permitir el control total sobre las interfaces y procesos de entrada y salida.

4.1.4 SISTEMAS DE INFORMACIÓN

El Sistema Integrado de Información UIS está compuesto por Sistemas de Información Web, Sistemas de Información Intranet y Sistemas de Información de Terminal de usuario. Todas estas aplicaciones apoyan las labores administrativas facilitando así el desarrollo de procesos de misión crítica como lo son: las matriculas, la generación de certificados de notas, el registro de la información financiera, el manejo de inventarios, el manejo de los registros históricos para el recurso humano, catalogar y clasificar libros, tesis, analíticas o revistas en las base de datos, manejar las operaciones relacionadas con la circulación y préstamo del material bibliográfico, recopilar y procesar información que permita realizar la evaluación docente, entre otros.

En este punto cabe resaltar que es gracias a estos Sistemas de Información que la UIS es considerada como una de las instituciones con mejor infraestructura de servicios informáticos del país. Gran parte de este logro se ha obtenido gracias al aporte de los estudiantes de Ingeniería de Sistemas quienes mediante el desarrollo de su proyecto de grado han contribuido con el proceso de modernización institucional, disminuyendo considerablemente la inversión por parte de la UIS en el desarrollo de software.

4.2 DESEMPEÑO ACTUAL

La UIS siendo consecuente con su plan de gestión institucional y apoyada en proyectos importantes e innovadores como ProspeTIC[1] (Soporte al proceso educativo UIS mediante Tecnologías de Información y Comunicación), propende a la modernización de la red institucional mediante el mejoramiento continúo de la misma, garantizándose de esta manera una infraestructura de red de excelente calidad y a la par con las exigencias actuales de los usuarios de Internet.

4.2.1 VENTAJAS

El alto grado de homogeneidad en la distribución y configuración de los nodos de la red permite que la transición hacia IPv6 se realice en un entorno más estandarizado, es decir el mismo escenario básico se repite varias veces en toda la red debido a que los primeros nodos de la estrella utilizan prácticamente los mismos equipos (AVAYA P333T) y los sistemas operativos en los usuarios son los mismos (Windows XP).

Se puede escoger un nodo de la red (preferiblemente el sitio con menos equipos y usuarios) para realizar pruebas con IPv6, en el instante en que este funcione correctamente y se haya aprendido de los errores, se deben generar los pasos para empezar a implantar en los nodos con mayor numero de usuarios.

La mayoría de dispositivos que conforman la red son actualizables por software por lo cual no habría que realizar cambios físicos en la infraestructura, solo es cuestión de actualizar y activar los componentes que requiere IPv6.

[1] Mayor información en http://gavilan.uis.edu.co/~clarenes

4.2.2 LIMITACIONES

Se puede encontrar una excesiva complejidad al momento de ofrecer soporte IPv6 a los nodos y aplicaciones de misión crítica, o en sitios donde se verían afectados muchos usuarios. Con el fin de disminuir los traumatismos ocasionados sobre el normal funcionamiento de las actividades de la Universidad, es necesario empezar a vincular lo más pronto posible a la comunidad UIS para que en poco tiempo comencemos a generar nuevos aportes al manejo de las nuevas tecnologías de red.

4.3 REQUERIMIENTOS PARA LA IMPLANTACIÓN DE IPV6

Ahora que hemos analizado de manera general la situación actual de la red de datos, debemos plantear los requerimientos básicos necesarios para el correcto funcionamiento de IPv6.

4.3.1 HUMANOS

Este es el punto primordial en el cual la UIS debe empezar a trabajar lo antes posible, es necesario que cada una de las personas involucradas en este proyecto posea un amplio dominio de las tecnologías de red y principalmente de IPv6. Aunque IPv6 no sea una tecnología reciente, pudiese no contar con un amplio conocimiento por parte de la comunidad que eventualmente se integre a este proyecto de implantación, por su puesto que los conocimientos sobre IPv4 son primordiales debido a que en IPv6 muchos aspectos tienen su equivalente en IPv4.

Sin importar cual sea nuestra situación se requiere fortalecer ciertos conceptos y prácticas nombradas a continuación:

- Dominio amplio de la pila de protocolos TCP/IP.
- Conocimiento del protocolo IPv6.
- Administración optima de redes mediante el correcto uso de prácticas de gestión consolidadas.
- Destreza en la solución de problemas de red en todas las capas del modelo OSI.
- Funcionalidades y servicios relativos a IPv6 como lo son: la seguridad, ICMPv6, movilidad, Multicast, DNS, QoS entre otros.

4.3.2 TIEMPO

La determinación del tiempo de duración para un proyecto como la implantación de IPv6 resulta ser un aspecto muy ligado a la predisposición al trabajo y a la coordinación por parte de todas las personas involucradas en el mismo. Según Jordi Palet[1] la transición en una red de tamaño medio alto puede tardar entre 6 meses y 2 años, dependiendo del nivel de preparación y entrega por parte de las personas encargadas de la migración.

Un aspecto a favor de la disminución en el tiempo de puesta en marcha de IPv6 en la UIS (además de las ventajas tratadas en la sección 4.2.1), es el interés evidenciado por parte de la Universidad y en especial de la División de Servicios de Información en mantener una infraestructura de servicios de red eficiente y a la par con las tecnologías de punta asequibles en el medio.

Además de esto hay que considerar los tiempos de espera en la asignación de un bloque de direcciones IPv6 para la UIS, los cuales siguen el esquema jerárquico de asignación [RFC 1466] por parte de la IANA a LACNIC, el cual se encarga de asignarlas a los Registros Nacionales de Internet (NIR),

[1] Director de la tecnología IPv6 en Consulintel – España, fuertemente involucrado en el IPv6 forum y director de diversos proyectos IPv6 para la Comisión Europea.

Proveedores de Servicios de Internet (ISP) y estos últimos a los usuarios finales[13]. Afortunadamente los dos ISPs con los que cuenta la UIS, ETB y TELECOM ya tienen asignado por parte de NAP Colombia un bloque de direcciones IPv6, en el caso de TELECOM es el ISP encargado de gestionar las direcciones IPv6 para el proyecto RENATA (ver sección 4.6.2).

4.3.3 HARDWARE

Muchas casas fabricantes de hardware siendo concientes del cambio que se avecina, han decidido implementar IPv6 en sus equipos. Ahora que los sistemas operativos en routers y switches vienen grabados en memoria flash reprogramable y no en ROM, es solo cuestión de actualizar el sistema operativo por una versión compatible con IPv6.

Aun si una organización solo desea renovar sus equipos ya sea por obsolescencia o mejoramiento continuo, obtendrán soporte IPv6 sin pedirlo. En la siguiente tabla se encuentran algunos de los principales productos con soporte IPv6 disponibles en el mercado[14]:

FABRICANTE	PRODUCTOS	VERSIÓN DE SO CON SOPORTE IPV6
EXTREME NETWORS[15]	Series de switches capa 3 Summit, Alpine, y Black Diamond.	Extreme XOS

[13] Las políticas de asignación de direcciones IPv6 son tratadas en mayor detalle en el capitulo 7
[14] Tomado de http://playground.sun.com/pub/ipng/html/ipng-implementations.html
[15] Mayor información en www.extremenetworks.com

CISCO SYSTEMS[16]	Todos	A partir de IOS 12.2(2)T
ALLIED TELESYN[17]	AR (410s, 440s, 450s, 725 y 745) y AT (8948 y 9924Ts más tarjeta aceleradora AT-ACC01)	---
3COM	Routers NETBuilder II y PathBuilder S500	Desde la versión 11.0
6WIND[18]	Serie 6WINDGate 6200	---
HITACHI	Familia de routers Gigabit GR2000	---
NORTEL NETWORKS	Todos	A partir de BayRS 12.0

Tabla 3 Fabricantes de hardware con soporte IPv6

4.3.4 SISTEMAS OPERATIVOS

Al igual que los fabricantes de hardware, las casas desarrolladoras de software en sus últimas versiones de sistemas operativos han decidido brindar soporte Ipv6. Los principales desarrolladores y sus versiones de sistemas operativos con soporte IPv6 se encuentran en la siguiente tabla[19]:

[16] Mayor información en www.cisco.com/ipv6
[17] Mayor información en www.alliedtelesyn.com
[18] Mayor información en www.6wind.com
[19] Tomado de www.ipv6.org/impl/

DESARROLLADOR	SISTEMA OPERATIVO	DESCARGAR DE
WINDOWS	Windows 95/98/NT 4.0	www.trumpet.com.au/ipv6.htm
	Windows 2000	http://msdn.microsoft.com/downloads /sdks/plattform/tpipv6.asp
	Windows XP	Software licenciado
UNIX	AIX 4.3	www.ibm.com/servers/eserver/pseries/software
	OpenBSD 2.7 en adelante	www.openbsd.org
	Linux kernel 2.0 en adelante	www.linux.org
	FreeBSD 4.0	www.freebsd.org
	NetBSD 1.5	www.netbsd.org
	Solaris 8.0	www.sun.com/solaris
	Tru64 UNIX 4.0D/5.1	Software licenciado Compaq
MACINTOSH	Mac OS X 10.2 Jaguar	Software licenciado
IBM	OS/390	http://www.ibm.com/software/enetwork/commserver/downloads/demos/demo_csos390.html.

Tabla 4 Desarrolladores de sistemas operativos con soporte IPv6

4.3.5 APLICACIONES

Es común encontrar en los ambientes operativos de la gran mayoría de redes aplicaciones para el intercambio de hipertexto, DNS, correo y transferencia de archivos. Las siguientes son aplicaciones con soporte IPv6:

SERVICIO	APLICACIÓN	FUENTE
HTTP	Servidores: Apache 2.0 en adelante IIS 6.0 en adelante	Apache: http://httpd.apache.org
	Clientes: Mozilla 5.0 Internet Explorer 5 en adelante	Mozilla:www.mozilla.org/releases/
DNS	BIND 9	www.bind9.net/download
MAIL	Postfix	www.ipnet6.org/postfix/ipv6.html
	Sendmail 8.10	www.sendmail.org
FTP	Servidores: Libre FTP Server	http://libreftp.narod.ru/index.html
	Clientes: NcFTP LFTP 2.0.x	NcFTP: ftp://ftp.kame.net/pub/kame LFTP: http:ftp.yars.free.net/projects/lftp

Tabla 5 Aplicaciones de red con soporte Ipv6

4.4 ESCENARIOS DE TRANSICIÓN A IPV6 EN LA UIS[20]

Durante el despliegue de IPv6 en la red de datos UIS, muchos escenarios posibles surgirán. Áreas descubrirán maneras más eficientes de comunicación con IPv6, mientras otras se adaptarán a los esquemas de interconexión formulados en esta sección. El objetivo de realizar estos planteamientos (escenarios) es abarcar la mayor cantidad posible de detalles con el fin de ofrecer un buen rango de soluciones para los nodos de la red institucional.

Para determinar los diferentes escenarios de implantación en la red, es necesario identificar las variables que establecen la heterogeneidad en los casos de uso de la infraestructura de red, algunos de estos factores son:

- El mecanismo de transición que ofrezca el mayor nivel de adaptación y de facilidad de implantación en la red.
- Los requisitos de conectividad IPv6 o IPv4 dentro y fuera de la red.
- El nivel deseado de coexistencia entre IPv4 e IPv6 en la red.
- El posible interés de otras redes por establecer conexión IPv6 con la UIS.
- Las opciones de conectividad IPv6 ofrecidas por el ISP

En cualquier caso, los principales componentes de la infraestructura de red que van a verse involucrados en la lógica incompatibilidad entre los protocolos y que a si mismo son los puntos críticos de la transición son:

- Configuración de hosts
- Enrutamiento
- Aplicaciones
- Administración de la red

[20] Escenarios adaptados para la UIS en base a [RFC 4057 – Escenarios de implantación IPv6 en redes empresariales]

- Planificación de direcciones
- Soporte ofrecido por el ISP
- DNS
- Seguridad

Para el correcto desarrollo de un escenario de transición establecido en un caso de uso particular, es primordial involucrar al equipo completo de personas implicadas en el funcionamiento de la red, es decir los administradores de red, operarios de red e ingenieros.

Es muy difícil cuantificar todos los posibles escenarios de red que les permitan a los equipos de trabajo planear la transición a IPv6, sólo se pretende describir un grupo de escenarios abstractos que puedan ayudar a la planeación definitiva. A continuación presentamos tres escenarios básicos que servirán de modelo para definir los escenarios específicos:

El primer escenario asume que la Universidad decide desplegar IPv6 en unión con IPv4. En el segundo escenario se asume que la Universidad decide desplegar IPv6 debido a un grupo específico de aplicaciones que se necesita funcionen sobre una red IPv6. Y el tercer escenario asume que la Universidad decide construir una nueva red o reestructurar la red existente, desplegando a IPv6 como el protocolo predominante dentro de la red aunque aun coexista con IPv4.

En el siguiente gráfico se observa como se espera que sea la transición de IPv4 a IPv6 en el mundo, durante este lento proceso cada uno de los escenarios planteados en esta sección va a tomar gran importancia, dependiendo de las necesidades específicas de cada red y de la situación mundial del despliegue IPv6:

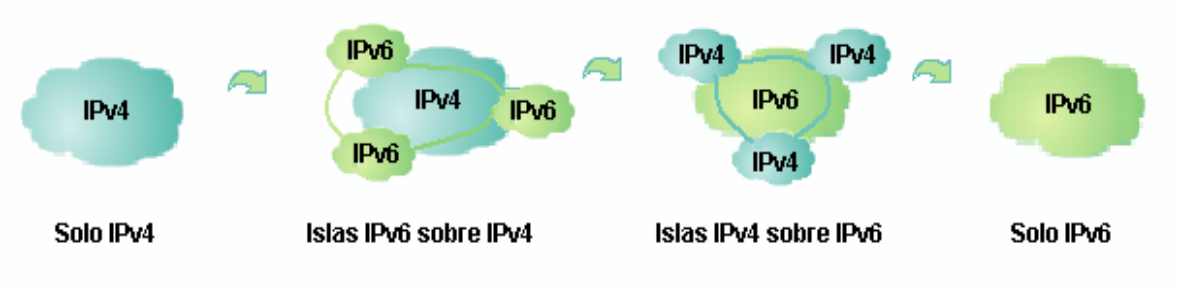

Figura 17 Transición esperada de IPv4 a IPv6

Se puede apreciar como en la primera etapa del gráfico, el mundo del Internet permanecía sólo con IPv4 (hace unos años), posteriormente empiezan a aparecer instituciones o sitios que implantan islas IPv6 aisladas las cuales usan para interconectarse entre sí túneles sobre la infraestructura IPv4 o bien conectadas directamente por canales dedicados (situación actual), luego con el incremento en el desarrollo de servicios y aplicaciones IPv6, IPv4 empieza a ser obsoleto para los requerimientos actuales y a quedar relegado a pocos sitios que usan túneles para comunicarse a través de la infraestructura IPv6, esta tendencia continua por un tiempo indeterminado (puede ser nunca) hasta el punto en que IPv4 desaparece totalmente y se impone IPv6 como el protocolo encargado de dirigir la siguiente generación del Internet.

4.4.1 ESCENARIO 1 (PILA DUAL)

Este escenario implica el despliegue a gran escala de la doble pila de protocolos, es decir todos los hosts en la infraestructura de red deben tener soporte IPv4 e IPv6. Lo anterior con el fin de habilitar la comunicación en un ambiente dual, donde sobre la misma red exista tráfico IPv4 e IPv6. Los paquetes pueden usar direcciones IPv4 entre clientes IPv4, direcciones nativas IPv6 ó direcciones IPv4 - compatibles - IPv6 entre los clientes IPv6, ó clientes IPv4 y direcciones IPv4 - transformadas - a IPv6 entre clientes IPv4. Cada host

equipado con la doble pila de protocolos IP, esta en condición de resolver registros A y A6/ AAAAA.

Para este escenario se pueden deducir tres tipos de tráfico posible (aunque en realidad sólo sean dos, IPv4 o IPv6), por ejemplo si cualquier equipo perteneciente a la red desea establecer comunicación con un sitio IPv4, lo puede hacer usando su dirección IPv4, si otro equipo desea alcanzar un destino IPv6 lo puede hacer usando su dirección IPv6 o su dirección IPv4 mapeada en una IPv6, y por último si cualquier host desea establecer comunicación con otro host IPv4/IPv6 lo puede hacer con cualquiera de las dos pilas de protocolos, la decisión de qué pila activar y cual no, depende de las políticas internas de funcionamiento.

Estos casos de comunicación se representan en la siguiente grafica:

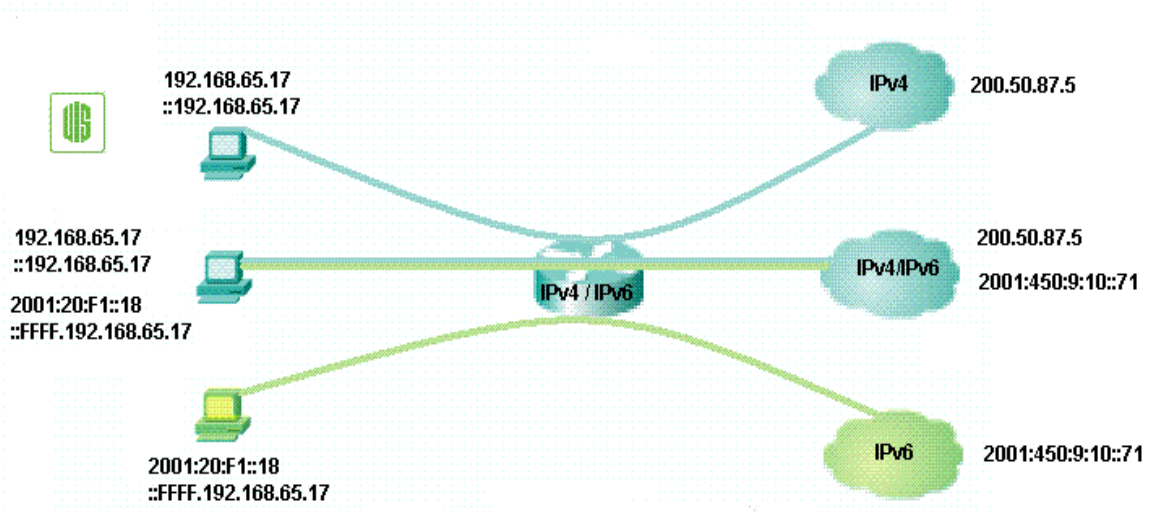

Figura 18 Casos de uso del escenario 1

Requerimientos

Es indispensable no *romper* la infraestructura de red IPv4 existente con la llegada de IPv6. Con IPv6 el funcionamiento de la infraestructura de red debe ser equivalente o mejor que con IPv4, lo anterior nos indica claramente que la red con IPv6 debe poder ofrecer al menos los mismos servicios que ofrecía con IPv4. Sin embargo, se entiende que IPv6 no es requerido para resolver los problemas no resueltos por IPv4 en la infraestructura de red. Tampoco puede ser factible desplegar IPv6 en todas las partes de la red inmediatamente.

Además es necesario que los equipos de usuario funcionen con sistemas operativos con soporte IPv6 (ver tabla 8). Los routers deben tener actualizaciones del sistema operativo para soportar IPv6 (ver tabla 7). Los comandos que permiten instalar IPv6 en plataformas Windows, Linux y FreeBSD se encuentran en los anexos F, G y H respectivamente. El anexo I explica como habilitar IPv6 en routers Cisco.

4.4.2 ESCENARIO 2 (TÚNELES)

La principal funcionalidad de este escenario radica en la necesidad que podrían tener determinados nodos dentro de la UIS de acceder a ciertos servicios o aplicaciones alojadas en redes IPv6. Tambien puede existir el caso en que la Universidad genere un servicio de red IPv6 y obviamente las redes externas para acceder al servicio necesitan conectividad IPv6 por parte de la UIS, por ejemplo en aplicaciones Peer to Peer. Así sólo contemos con algunos nodos IPv6, la LAN puede verse para las redes remotas como una isla IPv6 en un océano IPv4.

Lo anterior implica que el despliegue de IPv6 es limitado al mínimo requerido para operar este grupo de aplicaciones y servicios. Además se asume que los

componentes software / hardware para la aplicación estén disponibles, y que las plataformas para la aplicación tengan soporte IPv6.

Para este escenario es necesario que algunos dispositivos posean soporte dual, por ejemplo el router frontera, además es indispensable configurar un servidor de túneles que permita *viajar* al tráfico saliente IPv6 sobre la infraestructura IPv4, hasta la red IPv6 que ofrezca el servicio de red solicitado. Así mismo, el servidor de túneles debe desencapsular los túneles establecidos en otras redes para permitir la entrada de tráfico IPv6 hacia la UIS. Todo lo anterior se puede observar en el siguiente gráfico:

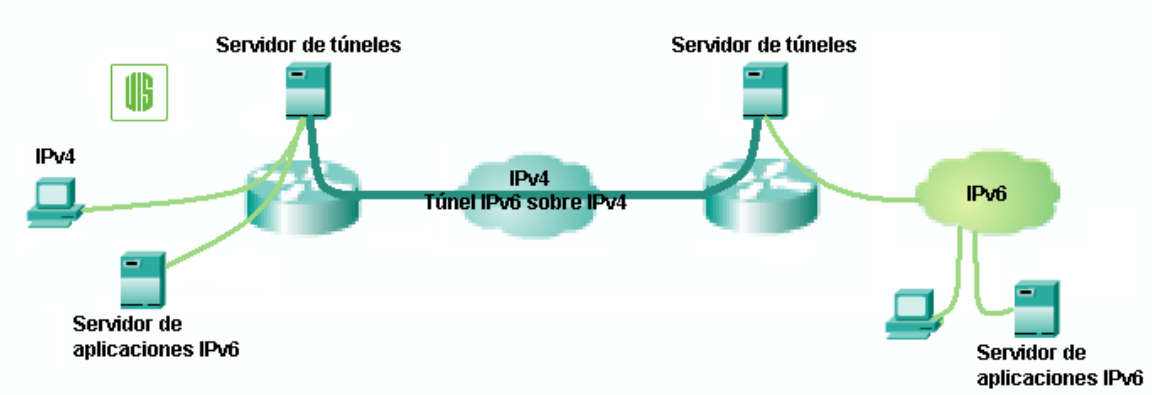

Figura 19 Casos de uso del escenario 2

Para este escenario en particular, el tipo de túnel utilizado es un túnel configurado entre los dos routers (sección 4.2.2). Una variación de este escenario utiliza un túnel automático (sección 4.2.3), el cual es establecido entre los dos hosts en los extremos de la conexión, los cuales deben poseer soporte dual. Este escenario se establece cuando el primer salto del túnel (el router frontera) no dispone de soporte para el tráfico IPv6. Las direcciones finales de los túneles automáticos son del tipo direcciones IPv6 compatibles con IPv4 (Anexo B - sección 4.4).

Requerimientos

El soporte IPv6 para los nodos de la red UIS es opcional, debido a que la red dispondrá de un servidor de túneles el cual realizará el encapsulamiento y desencapsulamiento respectivo, aunque en el caso en que cual la UIS ofrece un servicio IPv6 es aconsejable que todos los nodos tengan soporte dual. Al establecerse un túnel en el servidor UIS, el extremo opuesto de la comunicación tambien deberá configurar un servidor de túneles que desencapsule los paquetes permitiendo la comunicación extremo a extremo IPv6. Además los routers frontera deben tener soporte dual y capacidad para gestionar túneles.

El servicio de *entunelamiento* puede tambien ser ofrecido por *Tunnel Brokers* como el ofrecido por ConsulIntel[21], HexaGO[22], Hurricane Electric[23] entre otros. Básicamente un Tunnel Broker automatiza los scripts que permiten crear un túnel IPv6-sobre-IPv4 (6 over 4, sección 3.2.4) entre nuestro router o host y uno de los routers del Tunnel Broker, el cual obviamente debe poseer conexión directa o ruta por defecto hacia el backbone IPv6. Para usar estos servicios es necesario el soporte IPv6 en el host o router (ver tablas 3 y 4) el cual debe tener conectividad IPv4 con el Internet existente. Si los nodos están ubicados detrás de un dispositivo NAT, es imprescindible que la implementación NAT soporte reenvío de tráfico protocolo 41. El proceso de solicitud de un túnel a través de un Tunnel Broker es similar al proceso solicitar una cuenta de correo, en el cual nos asignan un nombre de usuario (login) y una contraseña con la cual podemos modificar y gestionar opciones del tráfico sobre nuestro túnel.

[21] Mayor información en http://tb4.consulintel.euro6ix.org/in/index.php
[22] Mayor información en http://www.hexago.com/index.php?pgID=step1
[23] Mayor información en http://ipv6tb.he.net/index.php

4.4.3 ESCENARIO 3 (IPV6 NATIVO)

Luego de analizar la situación actual de la UIS, este escenario parece ser el menos consecuente con las necesidades de conexión en la red. Por supuesto que en algún tiempo este va a ser el caso de implantación de IPv6 más común en las redes. Desplegar una nueva red nativa IPv6 teniendo aún la infraestructura IPv4 funcional, sólo tendría sentido en el caso en que la Universidad no desee *arriesgarse* a que cambios relevantes en su red actual IPv4 ocasionen traumatismos en el normal desarrollo de los procesos institucionales.

Debido a que no es posible determinar el día exacto en que IPv4 *desaparezca*, sí ha de llegar el día en que IPv6 sea el protocolo predominante para el enrutamiento entre redes (figura 17 - tercer estado). Es este instante en el cual se hace trascendental este escenario, por que ahora es necesario reestructurar la red para que tanto el enrutamiento interno como el externo se lleve a cabo con IPv6 y además se debe seguir ofreciendo conectividad hacia los pocos sitios IPv4 existentes por medio de túneles IPv4 sobre IPv6.

4.5 TRANSICIÓN DE APLICACIONES A IPV6 [RFC 4038]

Como IPv6 es introducido en el Internet basado en IPv4, serios problemas podrían surgir con el enrutamiento, el direccionamiento, el DNS y los escenarios. Una clave para que la transición a IPv6 sea exitosa, es la compatibilidad con la gran cantidad de aplicaciones IPv4 instaladas en hosts y routers. En el capitulo 3 se describen los mecanismos de transición básicos, sin embargo ninguno de estos mecanismos toma una posición analítica sobre si las aplicaciones soportan IPv6. En el [RFC 4038] son tratados dos aspectos de las aplicaciones en la transición a IPv6:

- Cómo las diferentes técnicas de transición afectan las aplicaciones, y algunas estrategias para que las aplicaciones soporten IPv6 e IPv4.
- Cómo desarrollar aplicaciones con soporte IPv6 o independientes del protocolo, usando APIs[24] estándar [RFC 3493] [RFC 3542].

4.5.1 APRECIACIÓN GLOBAL DE LA TRANSICIÓN DE APLICACIONES

La transición de una aplicación puede ser clasificada en cuatro casos diferentes:

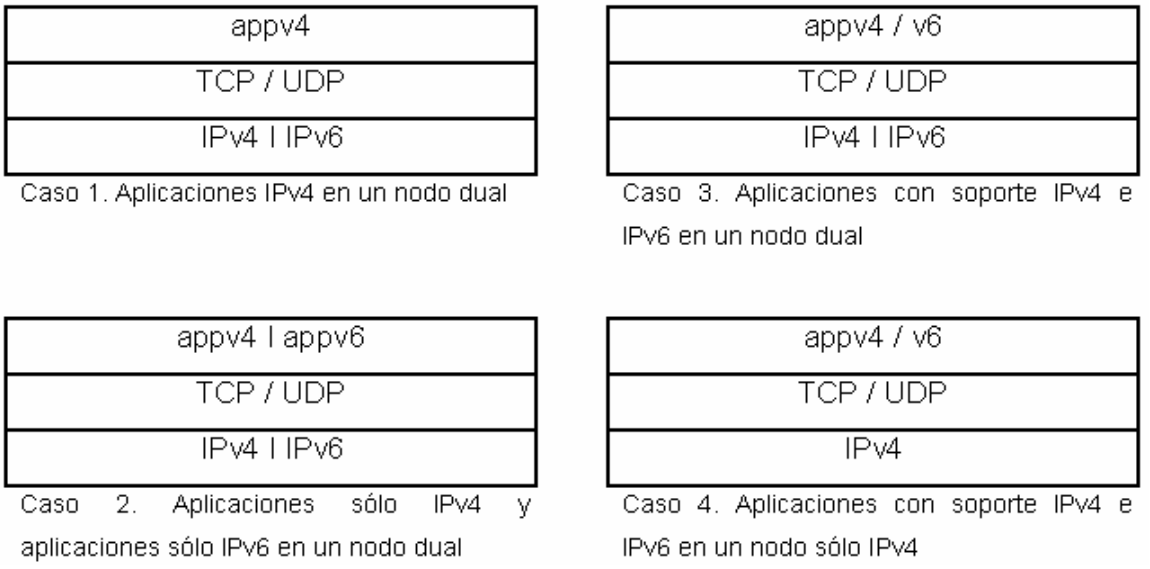

Figura 20 Casos de transición en una aplicación

Donde:

- Caso 1: Aplicaciones sólo IPv4 en un nodo con pila dual. El protocolo IPv6 es introducido en un nodo, pero las aplicaciones aun no han sido portadas para soportar IPv6.

[24] API – Interfaz de programación de aplicaciones, método para conseguir abstracción en la programación

- Caso 2: Aplicaciones sólo IPv4 y aplicaciones sólo IPv6 en un nodo con pila dual. Las aplicaciones han sido portadas sólo para IPv6. Por consiguiente aquí existen dos aplicaciones similares, una para cada versión (Ej.: ping y ping6).

- Caso 3: Las aplicaciones soportan IPv4 e IPv6 en un nodo con pila dual. Las aplicaciones han sido portadas para soportar IPv4 e IPv6. Por lo tanto las aplicaciones IPv4 existentes podrían ser removidas.

- Caso 4: Las aplicaciones soportan IPv4 e IPv6 en un nodo sólo IPv4. Las aplicaciones han sido portadas para soportar IPv4 e IPv6, pero las aplicaciones tambien pueden tener que trabajar cuando IPv6 no está siendo usado (Ej.: desactivado desde el SO).

4.5.2 PROBLEMAS CON LA TRANSICIÓN IPV6 DE APLICACIONES

El soporte IPv6 en el SO y en las aplicaciones no está relacionado

Sí consideramos los casos anteriormente descritos, es muy probable que las pilas de protocolos IPv4 e IPv6 coexistan en un nodo por un largo tiempo. Así mismo, muchas aplicaciones se espera que puedan manejar ambos protocolos durante un periodo largo. En un nodo doble pila, el SO no tiene previsto que deba soportar de los dos tipos de aplicaciones IPv4 e IPv6. Por lo tanto, la transición IPv6 de una aplicación puede ser independiente de las pilas de protocolos en un nodo.

Las aplicaciones con soporte IPv4 e IPv6 probablemente tengan que operar solamente en nodos sólo IPv4 (sí el protocolo IPv6 está desactivado por completo o allí no existe conectividad IPv6 en absoluto).

El DNS no indica que versión de IP va a ser usada

En un nodo, el DNS resuelve nombres recogiendo la lista de direcciones destino. Las consultas y respuestas DNS son enviadas usando IPv4 o IPv6, sin tener en cuenta la versión del protocolo de los datos transportados [RFC 3901].

El problema relacionado con la resolución de nombres del DNS en la transición de aplicaciones es que sólo con hacer una consulta del nombre en el DNS una aplicación cliente no puede establecer con certeza la versión IP de la aplicación servidora. Por ejemplo, si un servidor de aplicaciones aun no soporta IPv6 pero funciona sobre una maquina dual para otros servicios IPv6, y este host esta listado con un registro AAAA en el DNS, la aplicación cliente fallará al intentar conectarse con el servidor de aplicaciones. Esto se debe por una desigualdad entre el resultado de la consulta DNS (Ej.: dirección IPv6) y la versión del servidor de aplicaciones (Ej.: IPv4).

Se podría pensar en una solución operacional, usar nombres de servicio en lugar de nombres de host en el DNS. Si un nodo ofrece múltiples servicios, pero solo algunos de ellos sobre IPv6, un nombre DNS puede ser usado por cada servicio o grupo de servicios (con el registro asociado A / AAAA), y no sólo un nombre para la maquina. Sin embargo, las aplicaciones no pueden depender de esta práctica operacional.

Soportar diferentes versiones de una aplicación es difícil

Durante el periodo de transición de una aplicación, los administradores del sistema pueden tener varias versiones de la misma aplicación (una aplicación sólo IPv4, una aplicación sólo IPv6, o una aplicación que soporte IPv4 e IPv6).

Normalmente uno no puede conocer que versiones de IP puede soportar antes de hacer una consulta DNS y probar la dirección devuelta. Sin embargo si múltiples versiones de la misma aplicación están disponibles, los usuarios locales tienen dificultad en seleccionar la versión correcta que soporta la versión IP requerida.

Para evitar problemas con una aplicación que no soporte la versión especificada del protocolo, es aconsejable tener aplicaciones híbridas que soporten ambos protocolos.
Una alternativa para las aplicaciones cliente locales podría ser tener una aplicación intermedia que realice tareas como averiguar que versión del protocolo es usada afuera, y llame la aplicación que sea necesaria (sólo IPv4 o IPv6). Esta aplicación habrá establecido una conexión y *pasa* el puerto abierto a otra aplicación. Sin embargo, aplicaciones como estas probablemente sean más complejas que una aplicación híbrida ya que debe hacer más que sólo enviar una consulta DNS o determinar literalmente la dirección IP dada.

4.5.3 DESCRIPCIÓN DE LOS ESCENARIOS Y LINEAMIENTOS DE LA TRANSICIÓN DE APLICACIONES

Aplicaciones IPv4 en un nodo doble pila

En este escenario, el protocolo IPv6 es habilitado en un nodo pero el soporte IPv6 en las aplicaciones no está disponible o instalado. Aunque el nodo implementa la doble pila, las aplicaciones IPv4 sólo pueden manejar comunicaciones IPv4 y aceptar / establecer conexiones desde / hacia nodos que implementen IPv4.

Para permitir que una aplicación se comunique con otros nodos usando IPv6, la prioridad es portar la aplicación a IPv6. En algunos casos (Ej.: cuando no se

dispone del código fuente), existen aplicaciones IPv4 que pueden trabajar si el mecanismo BIS – *Bump in the stack* (sección 3.4) o BIA – *Bump in the Api* [RFC 3338] están instalados en el nodo. Es fuertemente recomendado que los desarrolladores de aplicaciones no usen estos mecanismos cuando el código fuente está disponible.

Aplicaciones IPv6 en un nodo dual

El camino más corto para portar las aplicaciones IPv4 es sustituir el antiguo API IPv4 con el nuevo API IPv6 realizando el mapeo de direcciones uno a uno. La mayoría de las implementaciones de doble pila permite aplicaciones sólo IPv6 interoperar con nodos IPv4 e IPv6. Los paquetes IPv4 que van hacia aplicaciones IPv6 en un nodo dual alcanzan su destino debido a que su dirección IPv4 es mapeada en una dirección IPv6. Entonces si llega un paquete IPv4, se mapea su dirección en una IPv6, y si llega un paquete IPv6 puede sin problemas acceder con su dirección IPv6 a las aplicaciones.

A continuación se analiza el comportamiento de las aplicaciones IPv6 que intercambian paquetes IPv4 con aplicaciones IPv4 usando el modelo cliente / servidor:

- **Servidor sólo IPv6:** cuando una aplicación cliente IPv4 envía datos a un servidor de aplicaciones sólo IPv6 que corre sobre un nodo dual, la dirección cliente IPv4 es interpretada como una dirección IPv4 mapeada en una IPv6 en el nodo dual. Esto permite a la aplicación IPv6 manejar la comunicación. El servidor IPv6 usará esta dirección mapeada como si esta fuera una dirección IPv6 regular y una usual conexión IPv6. Sin embargo serán paquetes IPv4 los que sean intercambiados entre los nodos.

- **Cliente sólo IPv6:** las aplicaciones cliente sólo IPv6 en un nodo dual no reciben direcciones IPv4 mapeadas de las funciones de resolución de nombres del API, a menos que una indicación especial sea dada. Sí es así, el cliente IPv6 usara la dirección mapeada retornada como si esta fuera una dirección IPv6 regular y una conexión usual IPv6.

Algunas implementaciones duales no permitirán direcciones IPv4 mapeadas para ser usadas para interoperar entre aplicaciones IPv4 e IPv6. En estos casos, se aconseja dos formas de manejar este problema:

1. Desplegar dos diferentes versiones de la aplicación (preferiblemente agregándole el '6' en el nombre).
2. Desplegar sólo una aplicación que soporte ambas versiones del protocolo, como se describe en la siguiente sección.

Aplicaciones IPv4 / IPv6 en un nodo dual

Algunas aplicaciones serán portadas para soportar ambos protocolos. Con el paso del tiempo las aplicaciones IPv4 serán removidas. Entonces la cuestión está en decidir qué aplicación seleccionar y para qué comunicación.

Este caso de transición es el más aconsejable. Durante el periodo de transición IPv6, las aplicaciones con soporte para ambos protocolos deben ser capaces de comunicarse con otras aplicaciones, sin importar la versión IP en la aplicación o en el nodo.
Sí el código fuente está escrito en un lenguaje independiente del protocolo, las aplicaciones deberán habilitar la comunicación con cualquier combinación de aplicaciones y tipos de nodos. Normalmente para las implementaciones se prefiere tener IPv6 por defecto sí el nodo remoto y la aplicación lo soportan. Sin embargo si la conexión IPv6 falla, las aplicaciones independientes de la versión

funcionarán automáticamente según las opciones de conexión brindadas por IPv4.

Sí el código fuente está escrito en un lenguaje dependiente del protocolo, la aplicación soportará explícitamente IPv4 e IPv6 usando dos sockets por separado.

Aplicaciones IPv4 / IPv6 en un nodo sólo IPv4

Como algunas aplicaciones tendrán soporte IPv4 e IPv6 podrán correr en nodos sólo IPv4. Aunque independiente del soporte de la aplicación o del SO, muchas personas ven este caso como muy poco probable y opinan que no tiene sentido que las aplicaciones sean implantadas en este escenario. Un caso común es cuando se necesita una versión de la aplicación que corra sobre SO antiguos, sin embargo muchos parches están siendo desarrollados para dar soporte a plataformas antiguas.

El caso de uso más importante es el soporte para aplicaciones sobre sistemas donde el soporte pueda ser activado / desactivado dinámicamente por los usuarios.

4.5.4 EVOLUCIÓN DE APLICACIONES IPV4[25]

Las aplicaciones actuales IPv4 tienen 3 caminos diferentes para poder conseguir soporte IPv6, siempre y cuando se tenga disponible el código fuente de la aplicación. La primera forma es pasar directamente de IPv4 a IPv6, la

[25] Ponencia completa sobre el porte de aplicaciones a IPv6 en video se encuentra en http://www.6sos.org/eventos.php por Eva Castro Universidad Rey Juan Carlos - España.

segunda es habilitar IPv4 e IPv6 en la aplicación y la tercera es mediante una transición gradual.

A aplicaciones IPv6

Para conseguir el porte total de la aplicación hacia IPv6, se debe inspeccionar el código fuente y sustituir las llamadas o estructuras que dependen de IPv4 por sus pares en IPv6. Como resultado obtenemos dos aplicaciones: una que funciona con IPv4 y la nueva que funciona con IPv6. Con este procedimiento se puede obtener soporte IPv6 de una manera relativamente fácil y rápida.

El inconveniente radica en que al tener dos versiones de la misma aplicación, le estamos trasladando un problema al usuario el cual debe elegir que aplicación usar dependiendo de sus necesidades. A este nivel, un usuario no debería ni saber que se está usando IP o cualquier otra especificación de red. Además si se realiza una modificación en una versión de la aplicación es necesario hacerlo en la otra, disminuyendo así lo práctico del método.

A aplicaciones duales

En este caso se debe añadir a la versión IPv4 de la aplicación soporte para IPv6, consiguiéndose de esta manera una aplicación dual, es decir, que pueda funcionar en nodos IPv4 para comunicaciones IPv4 y en nodos IPv6 para operaciones IPv6. Esto se logra duplicando los procedimientos y llamadas IPv4 con sus procedimientos equivalentes en IPv6. Con este procedimiento obtenemos sólo una versión de la aplicación, facilitándose de esta manera la inclusión de cualquier modificación en el código fuente.

El inconveniente principal radica en que habilitar el soporte dual en una aplicación implica más tiempo y más cambios en el código fuente.

Transición gradual

Este método no introduce caracteristicas nuevas de operación, consta simplemente de un híbrido entre los dos anteriores métodos. Para esto es necesario empezar en paralelo la aplicación dual, pero consiguiendo en un menor periodo de tiempo la aplicación IPv6. Es decir, se hace la sustitución de las llamadas y estructuras IPv4 por las de IPv6 y en paralelo se va diseñando las modificaciones para obtener una aplicación dual, con lo cual el objetivo final que es conseguir una sola aplicación dual más escalable y fácil de mantener se obtiene cuando ya hemos conocido y depurado la aplicación IPv6.

4.6 LA UIS Y LA CONECTIVIDAD CON REDES DE ALTA VELOCIDAD EN EL MUNDO

La UIS está a puertas de contar con conectividad global a través de redes académicas de alta velocidad. El punto inicial de conexión es el enlace con la red UNIRED de Santander, la cual a su vez es parte de la red nacional académica RENATA. RENATA junto a las principales redes nacionales de Latinoamérica conforman la red CLARA, la cual es la red encargada de ofrecer el enlace final hacia las redes de alta velocidad más importantes del mundo: Internet2 y GÉANT.

La principal necesidad que ha motivado a la UIS a decidir implantar IPv6 en su red de datos es la posibilidad de conexión que tiene con estas redes de alta velocidad. Cabe aclarar que IPv6 no es un requisito fundamental para el funcionamiento de ninguna de estas redes, lo que ocurre es que muchas de las

actividades tecnológicas que originan el surgimiento de las redes de alta velocidad tienen un poderoso aliado en las ventajas que ofrece IPv6. Por lo tanto es sólo cuestión de tiempo para que IPv6 sea un requisito para todas las instituciones educativas que deseen acceder a las principales redes académicas del mundo.

Algunos de los grupos técnicos de estas redes han empezado a fomentar el uso de IPv6 por medio de listas de discusión, foros y planes piloto de implantación. Así mismo, los proveedores de conectividad a Internet están empezando a dotar sus redes con una plataforma que soporte la conectividad IPv6, ellos han visualizado en IPv6 una excelente oportunidad de negocio.

La descripción, objetivos y principales servicios de estas redes se encuentran a continuación:

4.6.1 UNIRED

La Corporación de Redes de Universidades del Área Metropolitana de Bucaramanga – UNIRED tiene como objeto fortalecer el sector educativo de la región mediante el correcto aprovechamiento de los recursos de cada uno de sus asociados. Para lograr este objetivo, UNIRED se ha propuesto las siguientes tareas prioritarias[26]:

- Garantizar el mantenimiento, crecimiento y renovación tecnológica de la corporación UNIRED que permita la conexión a redes nacionales e internacionales.

[26] La completa descripción de UNIRED se encuentra en www.unired.edu.co

- Fomentar espacios de articulación e integración de los diferentes agentes y actores del desarrollo alrededor del esfuerzo inter – institucional, buscando así el progreso de la región.
- Promover la utilización masiva de las redes telemáticas a nivel local.

Integrantes

Las siguientes son las instituciones que junto a la UIS son miembro del convenio UNIRED:

- UNAB – Universidad Autónoma de Bucaramanga
- USTA – Universidad Santo Tomás
- UPB – Universidad Pontificia de Bucaramanga
- ICP – Instituto Colombiano del Petróleo
- UDI – Corporación Universitaria de Investigación y Desarrollo
- UDES – Universidad de Santander
- UTS – Unidades Tecnológicas de Santander
- UNISANGIL – Fundación Universitaria de San Gil

El esquema de conectividad de UNIRED funciona básicamente con un enlace de fibra óptica entre cada institución y un switch capa 3 marca CISCO 3550, el cual se encuentra ubicado en las instalaciones de TELECOM. Se ha establecido por TELECOM que a partir de mediados del presente año se ofrecerá una plataforma de conexión IPv6 para todas las instituciones pertenecientes a UNIRED, lo cual implica que cada una de estas instituciones debe empezar a trabajar de inmediato en sus investigaciones sobre IPv6. En la siguiente gráfica se observa el esquema de conectividad que comparte la UIS con los otros miembros de UNIRED:

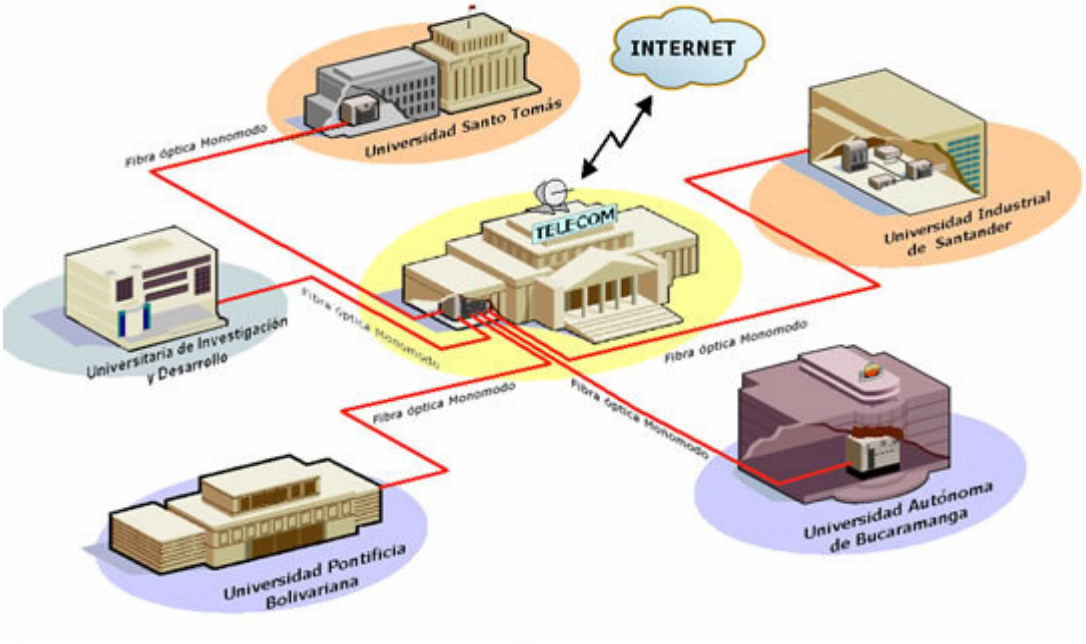

Figura 21 Esquema de conectividad de UNIRED. Imagen tomada de www.unired.edu.co

Servicios

Son dos los principales servicios que ofrece actualmente UNIRED a sus asociados. El primer servicio es un catalogo bibliográfico compartido, el cual permite a la comunidad de cada institución adscrita a UNIRED consultar el material bibliográfico que se encuentra en la biblioteca de cada una de las instituciones para su posterior préstamo y utilización, con lo cual cada institución cuenta con un catálogo bibliográfico distribuido con más de 190.000 documentos. El segundo servicio trata de una librería virtual, el cual cuenta con más de 1.600 documentos de las editoriales UIS, UNAB y USTA.

4.6.2 RENATA[27]

A Comienzos de este año se hizo el lanzamiento de la Red Nacional Académica de Tecnología Avanzada – RENATA, mediante una videoconferencia entre las redes académicas de Barranquilla, Bucaramanga, Popayán, Medellín y Bogotá. El principal objetivo de RENATA es consolidar una red nacional de instituciones académicas y de investigación que hagan uso efectivo de las redes de nueva generación.

Integrantes

RENATA nace como iniciativa de UNIRED y las siguientes redes regionales del país:

- RUMBO – Red Universitaria Metropolitana de Bogotá
- RUANA – Red Universitaria de Antioquia
- RUAV – Red Universitaria del Valle del Cauca
- RUMBA – Red Universitaria Metropolitana de Barranquilla
- RUP – Red Universitaria de Popayán

El esquema de conectividad de RENATA está basado en una topología de estrella cuyo nodo central es la sede Morato de TELECOM en Bogotá, y los nodos en la punta de la estrella lo conforman los nodos principales de las redes anteriormente listadas. El nodo central está configurado con un router Cisco 7606, el cual a su vez ofrece conectividad con la red CLARA por medio de un enlace con la cabecera del Cable Maya en Tolú, entregando el tráfico en el PoP

[27] La completa descripción de RENATA se encuentra en www.renata.edu.co

(punto de conexión a la red) de Red Clara en la estación María Chiquita en Panamá, tal y como se observa en la siguiente gráfica:

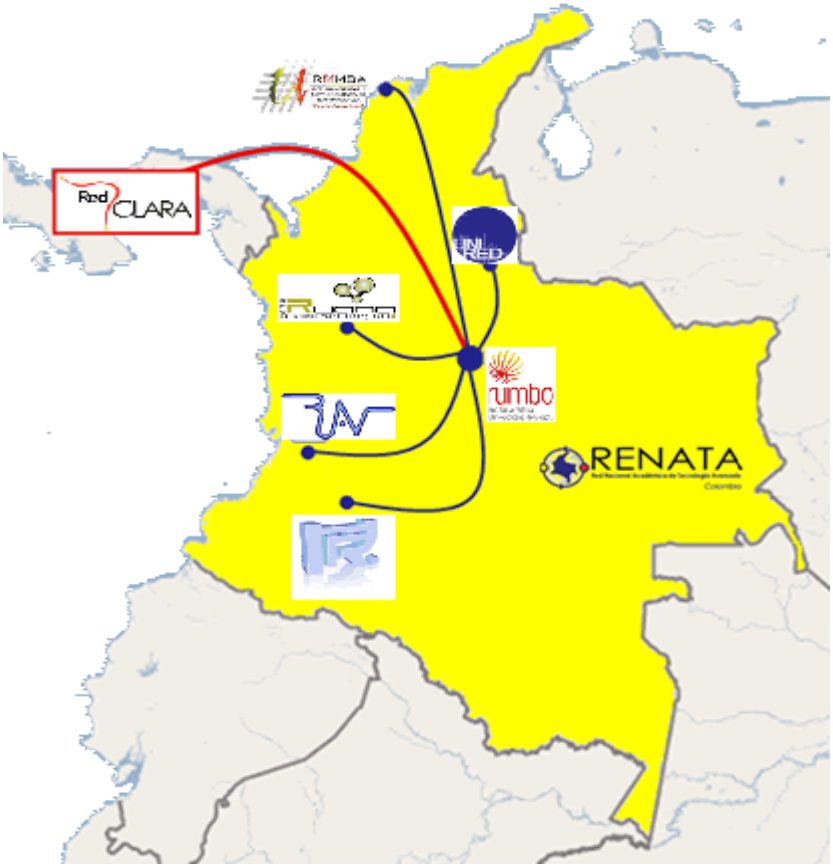

Figura 22 Integrantes de RENATA y conectividad con la red CLARA. Imagen tomada de www.renata.edu.co

Grupos técnicos

Actualmente RENATA está impulsando el desarrollo de su plataforma de comunicaciones apoyado en los siguientes grupos de trabajo:

- Vídeo Conferencia
- VoIP

- IPv6 (en construcción)
- Mediciones
- Multicast
- Enrutamiento avanzado
- Seguridad
- Capacitación
- QoS

La UIS como principal referente de calidad académica e investigativa del oriente colombiano, debe propender por el establecimiento y consolidación de grupos de trabajo similares para UNIRED, que ayuden a consolidar las redes nacionales y además permitan a la UIS y a Santander ser reconocidos en el exterior como semilleros de tecnologías de la información.

4.6.3 CLARA[28]

La Cooperación Latino Americana de Redes Avanzadas – CLARA, es una red regional de alta tecnología que tiene como objetivo primordial interconectar a las redes académicas avanzadas nacionales de América Latina y a estas con sus pares en Europa y Norte América. Los integrantes de está red no son Universidades, ni consorcios, son países enteros representados por su red académica. El listado completo de los países miembros y sus respectivas redes se encuentra en www.redclara.net/01/07.htm.

El backbone de la red CLARA está compuesto por cinco enrutadores principales conectados en topología de anillo. Cada nodo principal representa un PoP de

[28] La completa descripción de CLARA se encuentra en www.redclara.net

CLARA, los cuales están ubicados en Sao Paulo (Brasil), Buenos Aires (Argentina), Santiago (Chile), María Chiquita (Panamá) y Tijuana (México).

La red CLARA logra su conectividad con GÉANT a 622 Mbps por medio del proyecto ALICE[29] (América Latina Interconectada con Europa), para lo cual la Comisión Europea asignó 12.5 millones de euros. La troncal de CLARA está interconectada con la red GÉANT a través del enlace del PoP de CLARA en Sao Paulo, con el punto de acceso de GÉANT en Madrid (España). La conectividad de CLARA con Internet2 en Estados Unidos se logra a través del enlace PoP de CLARA en Tijuana con el punto de acceso CalREN en San Diego, tal y como se observa en la figura 23.

Grupos técnicos

Los grupos de trabajo que apoyan la consolidación de la red CLARA son prácticamente los mismos (en cuanto al nombre y campo de investigación) que los grupos de trabajo de RENATA ver sección 4.6.2. En cuanto al grupo técnico sobre IPv6 denominado GTv6[30], tiene como objetivo primordial apoyar el despliegue y la operación inicial de IPv6 en la red CLARA y las redes nacionales.

Es en este punto donde se puede observar el lento desarrollo de IPv6 en América Latina, debido a que los principales aportes que se han generado por parte del GTv6 se encuentran acotados por la falta de experimentación a gran escala, y son generados fundamentalmente en base a las experiencias y vínculos con otros Task Forces IPv6 principalmente de Europa.

[29] Información detallada en www.alice.dante.net
[30] Mayor información en www.redclara.net/03/06_05.htm

La topología completa de la red CLARA, la cual permite conectar a la UIS con GEANT e Internet2 se observa en la siguiente gráfica:

Figura 23 Topología de CLARA. Imagen tomada de www.renata.edu.co

4.6.4 INTERNET2

Internet2 es un consorcio compuesto por 207 universidades que trabajan junto a la industria y el gobierno en el desarrollo y despliegue de aplicaciones y

tecnologías avanzadas de red, acelerando así la creación del Internet del mañana. Internet2 no es una red superpuesta a Internet, ni tampoco busca sustituirla.

El objetivo primario de Internet2 es proveer a la comunidad del Internet de las aplicaciones revolucionarias que se puedan desarrollar por parte de la comunidad investigativa mundial apoyada en las redes de alta velocidad. Internet2 involucra el uso de nuevas tecnologías de comunicación, protocolos nuevos, gran ancho de banda y la integración de nuevas aplicaciones tales como:

- Software educativo (*Learning-ware*) y el Sistema de Dirección Instruccional (*Instructional Management System* - IMS) para educación a distancia.
- Bibliotecas digitales, mediante un ancho de banda amplio se permite la difusión de videos, audio, catálogos en línea, resúmenes y contenidos en formato digital.
- Teleinmersión, es la transmisión a distancia de escenas tridimensionales representadas empleando técnicas avanzadas de visión y multimedia, dotándolas de texturas y volúmenes que permitan reconocer la presencia y movimiento de objetos tridimensionales. Dichas escenas son proyectadas en salas con el equipamiento necesario (entornos de inmersión) permitiendo a los usuarios finales interactuar sensorialmente con los objetos, como si estuvieran frente a ellos.
- Laboratorios virtuales, permite a investigadores en diferentes lugares del mundo trabajar en proyectos comunes, apoyados en la Teleinmersión.
- Telemedicina, permite utilizar nuevas tecnologías de comunicación para realizar intervenciones quirúrgicas y de diagnostico a distancia.

Se puede observar como los requisitos funcionales de estas aplicaciones concuerdan ampliamente con las caracteristicas principales de IPv6, entre ellas está la QoS, la capacidad de ampliación y la movilidad. Por lo tanto es de esperar que Internet2 haga uso de IPv6 para permitir a las aplicaciones una alta fiabilidad, asignación del ancho de banda adecuado, herramientas de monitoreo y distribución de cargas.

5. RECOMENDACIONES Y CONCLUSIONES

La migración a IP versión 6 por parte de la red de datos UIS es un trabajo no exento de riesgos y costos. Algunos sólo serán percibidos hasta el momento de llevar a cabo la puesta en escena, pero los aspectos tratados en este trabajo y las recomendaciones establecidas en este capitulo, son las herramientas que nos pueden ayudar a conseguir una migración lo menos traumática posible.

Los riesgos se relacionan con la posible pérdida de eficiencia en la red o sectores de la red en que se implante IPv6 en el periodo de transición. Es de esperar que durante el tiempo en que demora la red en converger en prestaciones y servicios IPv6, se presenten traumatismos o inconsistencias en el normal funcionamiento de la infraestructura de red IPv4.

Los posibles costos generados en la transición dependen de los cambios o actualizaciones requeridas en hardware y software, específicamente en equipos de direccionamiento capa 3 (routers o switches capa 3). No obstante, la inclusión de un nuevo protocolo de red no implica que se deban realizar cambios físicos en los dispositivos de red en los equipos de usuarios o en la infraestructura de acceso a la red (tarjetas de red, conectores y tecnología de cableado).

Para el caso del switch central BLACK DIAMOND 6808, su versión de sistema operativo (Extreme Ware) no cuenta con soporte para el enrutamiento IPv6 por defecto. La otra versión de sistema operativo propietario de Extreme Networks, el Extreme XOS sí trae incluido soporte para IPv6, por lo cual es necesaria la actualización del switch central hacia esta versión del sistema operativo[31].

[31] Mayor información en http://www.extremenetworks.com/products/OS/default_spanish.asp

Además debemos ser concientes que el proceso de transición a nivel de red y de servicios es sólo una parte de la migración a IPv6, ya que si queremos sacar provecho a las nuevas caracteristicas del protocolo, es necesario emplear nuevos esfuerzos en extender la red con aplicaciones que soporten QoS, sistemas que gestionen la seguridad en los procesos y la imposición de la movilidad como agente facilitador de servicios a los usuarios, entre otras cosas.

En este contexto, se vislumbra el CENTIC (Centro de Tecnologías de Información y Comunicación) como el lugar propicio para el surgimiento de nuevas aplicaciones basadas en las tecnologías de información y comunicación (TICs) que permitan agregar valor a los procesos de formación académica e investigativa de la UIS. Dado que el contenido de estas herramientas está directamente relacionado con aplicaciones dotadas de novedosos componentes multimedia, requisitos de colaboración en tiempo real y el intercambio de gran cantidad de contenidos por medio de la red, el protocolo de Internet IPv6 se convierte en la mejor opción para garantizar el funcionamiento de un proyecto tan ambicioso e importante para la comunidad UIS en general.

A continuación se encuentran las principales conclusiones, lineamientos y recomendaciones generadas en el desarrollo de esta investigación sobre la viabilidad de IPv6 en la red institucional.

5.1 SOBRE IPV6

- La consolidación de IPv6 como el protocolo encargado de guiar la nueva generación del Internet es sólo cuestión de tiempo, entonces ¿Por qué no empezar ahora?

- IPv6 se encuentra en un estado de madurez suficiente en cuanto a especificaciones y soporte por parte de los fabricantes de software y

hardware de servicios de red, así como en la mayoría de sistemas operativos conocidos.

- IPv6 ha sido diseñado pensando en la coexistencia con IPv4, de ahí la necesidad e importancia de los mecanismos de transición y el surgimiento de nuevos productos y servicios duales

- A pesar de que el uso de los mecanismos de transición deja en un segundo plano las bondades de IPv6, por lo menos estamos consiguiendo conectividad IPv6 de extremo a extremo.

- Las caracteristicas incluidas en el protocolo IPv6 crean el marco adecuado para establecer nuevos modelos de gestión, seguridad, movilidad y soporte para las redes unidas a Internet.

- Lo mejor de IPv6 está por venir, la preocupación aún se centra en cómo obtener conectividad IPv6, y por el momento las mejoras incluidas en el protocolo se encuentran desaprovechadas. De todas formas las funcionalidades más avanzadas de IPv6, no se proporcionan con IPv4, así que no se extrañará ningún servicio habitual y dispondremos de algunos nuevos.

5.2 SOBRE LA RED DE DATOS UIS

- La Universidad Industrial de Santander se encuentra en condiciones propicias para emprender un proceso de migración a IPv6 en su red de datos.

- Emprender el proceso de migración pondría a la Universidad Industrial de Santander en una posición de vanguardia y mostraría su capacidad de

no solo adaptarse sino también de propiciar el adelanto tecnológico en la región.

- El proceso de transición no generaría mayor inversión económica, pues gracias al buen estado de la infraestructura de red en general, el proceso sólo pasaría por la actualización y configuración de los dispositivos de red dependiendo del escenario de transición (sección 4.4).

5.3 SOBRE LA TRANSICIÓN A IPV6

- La transición a IPv6 es una labor lenta y compleja, que ha de verse como un proceso evolutivo que empieza con la implantación del nuevo protocolo en la infraestructura de servicios de red, para continuar luego con la modificación y adaptación de aplicaciones, servicios y sistemas, acabando con la extensión de IPv6 a la mayor parte de dispositivos interconectados a la red.

- Durante el proceso de transición, IPv6 ha de encontrarse con aspectos adversos que retrasen su imposición definitiva, por ejemplo IPv6 concluiría con la carga económica que significa contar con direcciones IPv4 públicas a cargo de los ISPs, además de los negocios que involucran el uso de NAT, Proxy y CIDR.

- Para facilitar y estandarizar el proceso de migración, se deben realizar pruebas en los segmentos de red con menos equipos y usuarios, que aprovechando la homogeneidad de la red, permita afianzar y trasladar la implantación a segmentos de red cada vez más extensos y críticos.

- Una transición ordenada a IPv6 es posible, la clave está en mantener los servicios existentes, adaptar nuevos servicios y evitar traumatismos en el normal funcionamiento de la red.

- La transición a IPv6 debe ir de la mano con la generación o adaptación de aplicaciones IPv6, ya que no tiene mucho sentido dotar la red con IPv6 si no se cuenta con aplicaciones que explotan las ventajas del protocolo.

- Se recomienda continuar con las líneas de investigación relacionadas con IPv6 por parte de la División de Servicios de Información, la Escuela de Ingeniería de Sistemas e Informática y el grupo de investigación GITSI[32].

5.4 SOBRE EL MECANISMO DE TRANSICIÓN ADECUADO PARA LA UIS

El objetivo principal de establecer algunos escenarios de transición para la UIS (sección 4.4) es visualizar de una manera general cómo algunos casos de uso del tráfico IPv4 e IPv6, encuentran el complemento idóneo en los mecanismos de transición básicos (pila dual y túneles).

Hay que tener muy en cuenta que pasar de IPv4 a IPv6 no implica sólo una simple actualización de protocolo, por ejemplo si nosotros decidimos actualizar la versión de nuestro editor de texto, cualquier documento creado con la versión anterior puede ser visualizado con la editor actual. En el caso de IPv6 es necesario seguir ofreciendo soporte IPv4 mientras IPv6 es consolidado en la red.

[32] Grupo de Investigación en Ingeniería Telemática y Sistemas Inteligentes, mayor información en http://cormoran.uis.edu.co/eisi/GruposInvestigacion/gruposinvest.jsp?nom_grup=GITSI

Con el fin de abordar los interrogantes establecidos sobre cual es el mecanismo de transición que se adapte mejor a los casos de uso en la UIS, se podrían establecer dos puntos diferentes de comunicación en la red:

- Internamente (Hosts / Router) - Pila dual
- Externamente (En la red) - Túneles

Así mismo en la red existen hosts solo IPv4 para los cuales no es viable habilitar el tráfico IPv6 desde un principio. En el caso de los diversos servidores alojados en la red, se recomienda sean habilitados con la pila dual con el fin de permitirles el manejo de peticiones por parte de hosts IPv4 e IPv6.

Host / Router

El mecanismo de transición de doble pila implica que cada equipo posea soporte dual sólo para la capa 3, es decir la capa física, la capa de acceso a la red, la capa de transporte y la capa de aplicación permanecen invariables.

Así la mayoría de los equipos posean soporte dual, el tráfico interno de la red es conveniente que continué funcionando sobre IPv4, o al menos mientras IPv6 se consolida en la red. El direccionamiento interno con direcciones privadas IPv4 funciona y por el momento sería un esfuerzo de configuración muy grande e innecesario realizar el direccionamiento interno con direcciones locales IPv6, ha sabiendas que aún existirían equipos sólo IPv4 en la red. Lógicamente el tráfico IPv4 tambien puede ser soportado por los nodos duales.

El router central debe tener soporte dual, con el fin de poder administrar el tráfico dual interno y el posible tráfico IPv6 entrante y saliente; esto en el caso en que por ejemplo, la plataforma de conexión de la UIS con UNIRED funcione

nativamente sobre IPv6. Además no hay que olvidar el tráfico IPv4 que debe existir por un tiempo no determinado.

El soporte dual en los hosts les permite soportar el tráfico IPv4 e IPv6 interno y externo. Los servidores con soporte dual pueden recibir y enviar cualquier tipo de tráfico, aunque en este caso particular podría utilizarse una traducción de dirección y de protocolos (NAT-PT sección 3.3).

En la red

Para la conexión con redes remotas IPv6, se pueden establecer túneles automáticos o túneles configurados. Esta es la forma más rápida de ofrecer conexión IPv6 de extremo a extremo cuando nuestro ISP no ofrezca conectividad IPv6 nativa y ya nos han asignado un rango de direcciones IPv6, aunque las bondades del protocolo queden relegadas a un segundo plano.

El túnel adecuado para este caso de uso es un túnel configurado de router a router, es decir desde nuestro router frontera hasta el router frontera del ISP o del backbone IPv6, este tipo de túnel se explica es la sección 3.2.2. La unión de las anteriores propuestas de conectividad, de mecanismos de transición y de casos de uso se puede observar en la siguiente grafica:

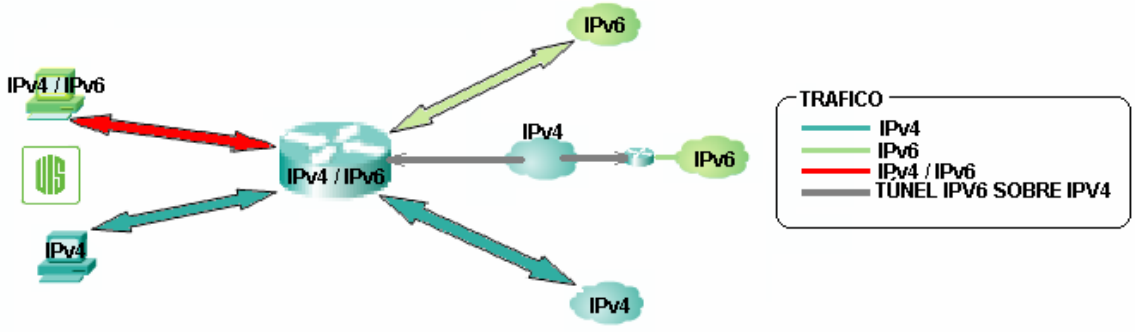

Figura 24 Esquema propuesto de conectividad para la UIS

La clave para el correcto funcionamiento del esquema de conectividad propuesto en la figura 24, radica en el óptimo desempeño del router central. Este dispositivo va a ser el encargado de permitir los tres tipos de tráfico saliente:

- Tráfico IPv4 interno generado desde los hosts duales y desde los hosts sólo IPv4 existentes, hacia el Internet IPv4 que existirá por un tiempo indeterminado.

- Tráfico IPv6 interno generado desde los hosts duales, hacia los posibles destinos IPv6 nativos.

- Tráfico IPv6 interno generado desde los hosts duales, hacia destinos IPv6 remotos (sin conexión nativa IPv6), lo cual implica el establecimiento de túneles IPv6 sobre IPv4.

Para el tráfico saliente descrito anteriormente, el host destino puede pertenecer a cualquier otra dependencia o sede de la UIS. Así mismo, el router debe permitir el tráfico entrante generado de la comunicación establecida por los tres tipos de tráfico saliente.

5.4.1 ESCENARIO BÁSICO DE CONECTIVIDAD

Con el objeto de realizar pruebas de conectividad IPv6, antes de efectuar cambio alguno en el (los) dispositivo(s) de red de misión crítica, es conveniente establecer primero un escenario básico de pruebas como el siguiente:

Se debe establecer un PC que posea dos interfaces o tarjetas de red, como router con dos interfaces Ethernet. Para permitir que el tráfico IPv6 sea enrutado entre las dos interfaces, es necesario disponer de una herramienta software que permita relacionar ambas tarjetas de red. La herramienta sugerida es GNU ZEBRA[33] la cual funciona sobre plataformas LINUX. Luego de haber "convertido" este PC en router, se debe habilitar IPv6 en los 3 PCs los cuales se configuran automáticamente con direcciones Locales de Enlace (FE80::/10), este proceso se describe en la sección 4.1.1. El siguiente paso es realizar pruebas de eco (ping6) y de conectividad remota (Telnet6) entre los dos PCS de los extremos.

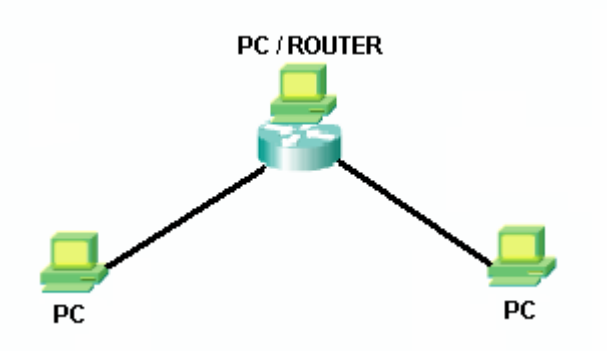

Figura 25 Establecimiento de un PC como router IPv6

Basados en el anterior esquema, se puede conseguir conectividad con el 6Bone (backbone IPv6), para lo cual es necesario tener un número de sistema autónomo y un bloque de direcciones IPv6 (las políticas de asignación de direcciones IPv6 son tratadas en el Anexo E). La UIS debe gestionar el bloque de direcciones IPv6 a través de uno de sus dos proveedores de servicios de Internet (TELECOM o ETB). Además necesitamos los datos de configuración (numero de sistema autónomo y las direcciones IPv4 e IPv6) del router que nos va a enrutar hacia el 6Bone.

[33] Mayor información en www.zebra.org

Mediante la herramienta ZEBRA configuramos los scripts necesarios para establecer el túnel 6 sobre 4 entre nuestro router y el router con enlace directo al 6Bone. La descripción total de este laboratorio se encuentra en el sitio: www.eldemonio.org/extras.php?id=90&archivo=26060513225.html, el proceso de instalación y configuración de ZEBRA se encuentra en el sitio: www.eduangi.com/quagga/quagga-es-2.html.

5.5 METODOLOGÍA GENERAL DE IMPLANTACIÓN IPv6

Basados en el esquema de conectividad propuesto para la red institucional (ver figura 24), se pueden establecer las siguientes áreas básicas de configuración:

- En el router central
- En los dispositivos de usuario final

El esquema propuesto para la red ha de verse como un laboratorio real y evolutivo de pruebas IPv6, más no como el diseño de una arquitectura de red a ser implantada de forma automática y definitiva. El propósito de establecer esta metodología de implantación es analizar desde una perspectiva operacional, que pasos o actividades básicas son necesarias al momento de poner en marcha los objetivos de conectividad establecidos, así como explorar los puntos clave que involucra la habilitación de un nuevo tipo de tráfico en la red.

Como primer requisito en el proceso de transición a IPv6, es necesaria la solicitud y asignación de un bloque de direcciones IPv6 para la UIS por parte de los proveedores de acceso a Internet (las políticas de asignación y delegación de direcciones IPv6 se encuentran en el anexo E).

5.5.1 EN EL ROUTER CENTRAL

El router central es el dispositivo encargado de permitir el tráfico dual entrante y saliente, además de ser el dispositivo encargado de establecer los posibles túneles configurados en la red. Por lo tanto son necesarios los siguientes pasos de configuración en el router central BLACK DIAMOND 6808:

1. Adquirir la versión del sistema operativo propietario de EXTREME NETWORKS llamado Extreme XOS. La adquisición de este software debe ir respaldada por parte del fabricante o distribuidor, con un completo soporte técnico sobre el uso de IPv6 en toda la gamma de switches EXTREME NETWORKS.
2. Actualizar el sistema operativo de su versión actual Extreme Ware por la versión Extreme XOS. Lo anterior es vital para agregar soporte IPv6 en el dispositivo, con lo cual surge la expectativa de conocer como es el funcionamiento de la configuración establecida en el router para la versión Extreme Ware, ahora con la nueva versión del sistema operativo. Se podría presentar el caso en que se sacrifique el correcto funcionamiento del enrutamiento conocido IPv4, con la asignación de nuevo soporte y tráfico IPv6.
3. Es necesario establecer que subred(es) de la LAN UIS va(n) a poseer inicialmente soporte IPv6, con el fin de habilitar el enrutamiento de tráfico IPv6 en la interfaz Ethernet adecuada.
4. Se deben *anunciar* los prefijos de direcciones manejados en nuestra red, con el fin de que los hosts de la subred IPv6 puedan autoconfigurarse con direcciones válidas para ámbitos IPv6 locales y globales (procedimiento explicado en la anexo B sección 9).
5. Es necesario reservar un espacio del direccionamiento IPv4 público de nuestra red, con el fin de ser usadas en los parámetros de configuración de los túneles automáticos (el procedimiento y parámetros que permitan establecer túneles configurados son tratados en el capitulo 3 sección 2.2).

6. Recolectar y configurar nuestro router central con la información necesaria para establecer los túneles configurados (dirección IPv4 e IPv6 del router con acceso al 6Bone, además del bloque de direcciones IPv4 a usar como origen de los túneles en nuestra red).
7. Habilitar el protocolo de enrutamiento en nuestro router que permita anunciar a las demás redes sobre la existencia de nuestra red IPv6, el protocolo de enrutamiento adecuado sólo es posible de establecer luego de revisar la documentación y soporte IPv6 para el router central.
8. Con el fin de obtener mayor experiencia en el manejo interno del direccionamiento IPv6, se recomienda el establecimiento de VLANS en la subred IPv6.
9. Si no es posible establecer túneles automáticos desde nuestro router, se dispone de dos opciones adicionales:

- Establecer un equipo servidor de túneles (preferiblemente que funcione sobre plataformas Linux).
- Establecer los túneles por medio de un túnel broker (sección 4.4.2).

Para cualquiera de estas opciones es necesario que el router permita el reenvío de paquetes protocolo-41.

Luego de realizar los anteriores pasos se tendrá configurado el router central con las caracteristicas básicas que le permitan manejar el tráfico IPv6 saliente y entrante, además de tener la posibilidad de establecer túneles IPv6 sobre IPv4.

5.5.2 EN LOS EQUIPOS DE USUARIO

El siguiente paso para conseguir que la red converja en servicios básicos de conectividad IPv6 es habilitar el protocolo en los equipos de usuario final y

servidores de la red. Los comandos que permiten habilitar IPv6 en plataformas Windows y Linux se encuentran en los anexos F y G respectivamente.

Luego de conseguir que la conectividad IPv6 en la LAN funcione, es necesario realizar pruebas de conectividad WAN (la opción más viable es con cualquier universidad perteneciente a UNIRED – sección 4.6.1), por lo tanto se recomienda socializar parte de los avances establecidos en la transición a IPv6 por parte de la UIS con los demás integrantes de UNIRED con el fin de establecer posibles escenarios de conectividad por túneles o por enlace dedicado con redes conocidas y cercanas.

Si no es posible establecer al router central como nuestro servidor de túneles, es necesario configurar en los hosts de usuario los scripts de configuración facilitados por los servidores del túnel broker para permitir establecer la comunicación remota con el mundo IPv6.

Las siguientes son las aplicaciones básicas clientes y servidoras que interesan a cualquier entorno de red, con el fin de ofrecer servicios para el funcionamiento normal de la red:

- Servidores de aplicaciones Web
- Exploradores de páginas Web
- Servidores de nombres de dominio – DNS
- Servidores de archivos – FTP
- Servidores de correo electrónico

Se requiere descargar cada una de las aplicaciones incluidas en la Tabla No. 5, con el fin de realizar pruebas básicas de funcionamiento, además de permitir a los usuarios nacientes IPv6 contar con los servicios de red más conocidos y demandados.

6. BIBLIOGRAFÍA

Libros:

DR. SYDNEY FEIT, **TCP/IP**, **Arquitectura, Protocolos e implementación, además de IPv6 y seguridad de IP.** *Editorial Mc Graw Hill* 2001. Biblioteca UIS, signatura topográfica 004.62f 311/t, numero de inventario 98380.
Introducción general a TCP/IP. También contiene una parte con información o referencias concretas, para continuar estudiando TCP/IP.

CISCO SYSTEMS, **Academia de Networking de Cisco Systems,** PEARSON EDUCACIÓN S.A. Madrid 2004.
Soporte completo a las tecnologías y procesos enrutamiento para las redes TCP/IP.

Artículos:

MUÑOZ, JOAQUIN. **Implementación de IPv6 para la Red Académica de Centros de Investigación y Universidades Nacionales.** www.nic.ve/view/docs/CNTI_IPv6.pdf. Documento que ilustra el Plan de implementación de REACCIUN en Venezuela.

Tesis:

CESAR CARPETA PAEZ, LEONARDO JIMENEZ BARRIENTOS grupo GITUN[34]. **Estudio sobre la Migración de La Red de Datos de La Universidad Nacional de Colombia De IPv4 hacia IPv6.**
Trabajo válido por proyecto de grado en el cual se realiza un análisis detallado de la situación actual de la Red de datos de la UNAL, con el fin de analizar los cambios requeridos para la implantación de IPv6.

Sitios Web:

www.ipv6.org
www.ipv6-es.com
www.6sos.org
www.cisco.com
www.microsoft.com/ipv6
www.rfc-editor.org
www.rfc-es.org

Principales RFCs sobre IPv6:

[RFC 2460] – Internet Protocol, Versión 6 (IPv6)
[RFC 3513] – Internet Protocol Versión 6, Addressing Architecture
[RFC 4038] – Application Aspects of IPv6 Transition
[RFC 4057] – IPv6 Enterprise Network Scenarios
[RFC 4213] – Basic Transition Mechanism for IPv6 Hosts and Routers
[RFC 4294] – IPv6 Node Requirements

[34] Grupo de Investigación de Teleinformática de la Universidad Nacional, Colombia

Videos[35]:

Javier Sedano, Ágora Systems - **Panorámica de los mecanismos de transición a IPv6**

Eduardo Jacob, Universidad del País Vasco - **Implantando IPv6 en un departamento universitario: Transición de la red y los servicios**

Esther Robles, RedIris - **La transición de las redes académicas: RedIris**

Eva Castro, Universidad Rey Juan Carlos - **Porte de aplicaciones y Servicios a IPv6**

Jordi Palet, Consulintel - **Sacando partido a IPv6 con redes IPv4**

Alberto Cabellos, Universidad Politécnica de Cataluña - **El papel de IPv6 en el soporte a la Movilidad IP**

[35] Tomados de: www.6sos.org/eventos.php

ANEXOS

TABLA DE CONTENIDO DE ANEXOS

ANEXO A. PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6)[36]

1. ENCABEZADO

Para comprender mejor el propósito de los cambios incluidos en la cabecera de IPv6, veamos a continuación la descripción de la cabecera IPv4:

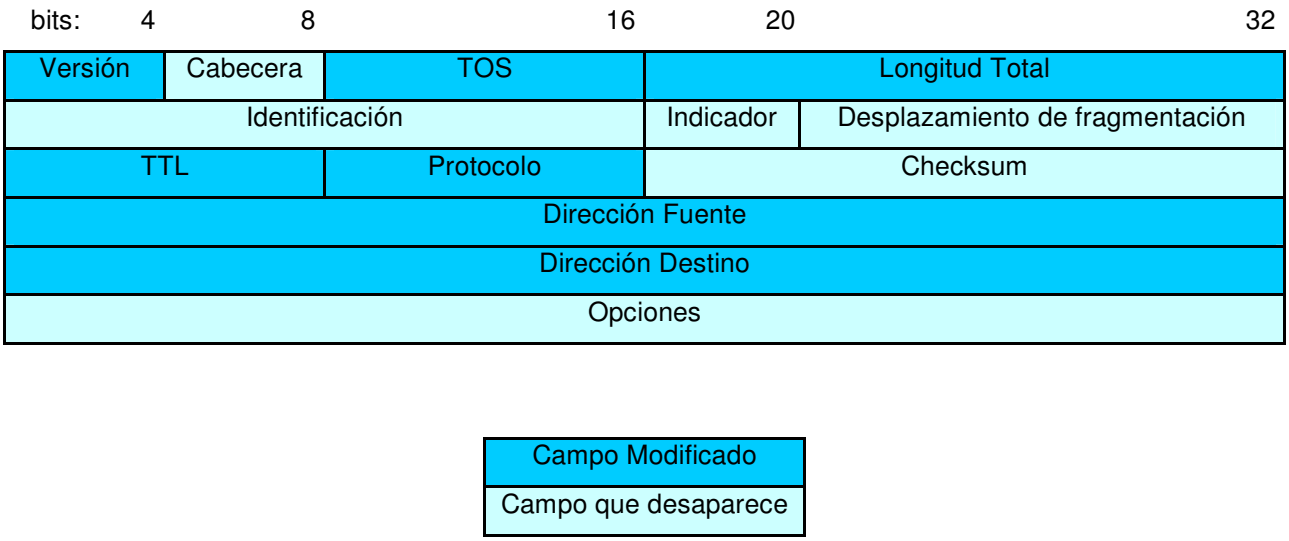

Figura 26 Cabecera IPv4

En la gráfica anterior se puede observar que algunos campos fueron sometidos a modificaciones y otros han sido eliminados, el disponer de una cabecera con menos campos implica una mayor facilidad para su procesado por parte de enrutadores, lo cual a su vez disminuye la latencia (tiempo que un paquete emplea para viajar del origen al destino) en la red.

[36] Anexo basado en [RFC 2460]

Los cambios realizados en el encabezado son los siguientes:

- La cabecera de IPv6 tiene una longitud fija de 40 bytes, la cabecera IPv4 posee una longitud variable debido a que el campo llamado *opciones* permite incluir desde información útil para el enrutamiento hasta bits de relleno en cero (sino se utilizan palabras enteras de 32 bits). Una cabecera de tamaño fijo mejora el rendimiento de los procesos de consulta en dispositivos de conmutación de paquetes. Además elimina la necesidad de un campo de *longitud del encabezado* en el encabezado de los paquetes.

- No se permite que los enrutadores intermedios fragmenten los paquetes, solamente el nodo de origen puede fragmentar la información con base al camino MTU descubierto. Esta limitación también es beneficiosa para los routers, ya que la fragmentación tiene un impacto en el rendimiento del reenvío y utiliza dispositivos adicionales. Esta limitación elimina la necesidad de los campos de *Identificación, Indicador y desplazamiento del fragmento*.

- Se considera que en las redes IPv4, la suma de comprobación del encabezado *cabecera y checksum* no era realmente útil, por lo tanto el campo se eliminó y la función se estableció en el nivel de transporte específicamente a TCP.

- El protocolo IPv6 tiene un nuevo campo, la *Etiqueta de Flujo*, el cual ofrece opciones para mejorar la Calidad de Servicio mediante la inclusión de etiquetas que identifiquen los paquetes que demanden trato preferencial en la red.

- Las opciones de encabezado utilizadas en el protocolo IPv4 se trasladaron a *encabezados* en IPv6, estos encabezados se denominan

encabezados de extensión y pueden ofrecer mayor flexibilidad en la implementación de nuevas características o mejorar las características existentes.

Con todas las anteriores modificaciones, un paquete IPv6 tiene el siguiente encabezado:

Figura 27 Cabecera IPv6

1.1 EL CAMPO VERSIÓN

Su tamaño es de 4 bits y sirve para especificar la versión del protocolo IP, para IPv6, versión = 6 (0110). Este campo es el único que permanece con la misma posición y función que en IPv4.

La razón por la cual este campo es el primero de la cabecera es para permitir una rápida identificación de la versión del protocolo y el paso del paquete al protocolo de proceso apropiado IPv4 ó IPv6.

1.2 EL CAMPO CLASE DE TRÁFICO

Su tamaño es de 8 bits y está disponible en la cabecera de IPv6 para que nodos origen y/o routers identifiquen o distingan entre distintas clases o prioridades de paquetes de IPv6. Este campo antes llamado *priority* en la primera definición para IPng [RFC 1883] tenía un tamaño de 4 bits, el cual fue aumentado posteriormente a 8 bits al disminuir el campo Etiqueta de Flujo de 24 a 20 bits. El nuevo término Traffic Class identifica mejor el propósito de este campo.

Este campo reemplaza las funciones que fueron establecidas para el campo Type of Service de IPv4, permitiendo la diferenciación entre categorías del servicio de transferencia de paquetes.

En [RFC 2460] se definen los 3 requerimientos generales que se aplican al campo Traffic Class:

- Paquetes que sean originados por un nodo perteneciente a una capa superior a IP, deben suministrar los valores de los bits del campo Clase de Tráfico. El valor por defecto de los 8 bits es 0 (el paquete no pertenece a ningún flujo, por lo tanto no requiere tratamiento especial).

- Nodos que soporten un uso experimental o eventual de algunos bits del campo Clase de Tráfico se les es permitido cambiar el valor de estos bits en paquetes que envíen, reciban o reenvíen. Si algún nodo no soporta este uso particular del campo Clase de Tráfico, no debe modificar ninguno de los bits del campo.

- Los protocolos de capas superiores no deben asumir que el valor de los bits del campo Clase de Tráfico de un paquete recibido, son los mismos valores que fueron originalmente transmitidos.

1.3 EL CAMPO ETIQUETA DE FLUJO

Los 20 bits del campo Flow Label de la cabecera de IPv6 son usados para que los nodos origen puedan etiquetar secuencias de paquetes (flujo) para que reciban un trato especial por parte de routers IPv6, como es la Calidad de Servicio *no-default* o servicio en tiempo real. Todos los paquetes que pertenecen a un mismo flujo, deben ser enviados con la misma dirección de origen, dirección de destino y Etiqueta de Flujo. Si un host o router no soporta funciones de *Flow Label,* los bits del campo Etiqueta de Flujo deben ser fijados en 0 en el origen y ser ignorados en el destino.

El apéndice A incluido en [RFC 2460] describe la semántica y la intención de uso del campo Etiqueta de Flujo:

- La naturaleza del manejo especial que demanda un flujo de paquetes, puede ser llevado a los routers por un protocolo de reserva de recursos en el origen, o por información adicional que lleven los paquetes del flujo (Ej. En una cabecera de opción Salto a Salto, Anexo A - sección 2.3).

- Un flujo es identificado de manera univoca por la combinación entre la dirección de origen y una Etiqueta de Flujo diferente de cero. Paquetes que no pertenecen a un flujo llevan la etiqueta de flujo en cero. La idea es que un router simplemente con examinar la Etiqueta de Flujo y al confrontarla con una tabla, sepa como enrutar y enviar el datagrama sin la necesidad de examinar el resto de la cabecera.

- Una Etiqueta de Flujo es asignada a un flujo por el nodo origen del flujo. Nuevas Etiquetas de Flujo deben escogerse al azar y uniformemente entre el rango 1 a FFFFF en hexadecimal. El propósito de la asignación aleatoria del grupo de bits de la Etiqueta de Flujo es hacer una

conveniente llave hash[37] para routers, con el fin de buscar el estado asociado al flujo.

- El tiempo de vida máximo asignado a un flujo con tratamiento especial (por defecto son 120 segundos), debe ser definido como parte de la descripción en el mecanismo de estado establecido, por ejemplo en el protocolo de reserva de recursos o la opción de Salto a Salto del flujo. Una fuente no puede re-usar una Etiqueta de Flujo para un nuevo flujo, hasta que toda la información del estado anterior de la etiqueta haya sido liberada por todos los routers en Internet [RFC 1809].

En la definición inicial del campo *Flow Label* se advirtió inconsistencias en 3 aspectos, que posteriormente fueron tratados por el *Network Working Group* en [RFC 1809], los problemas y conclusiones son las siguientes:

1. ¿Que debe hacer un router si recibe un datagrama con una Etiqueta de Flujo diferente de cero, y no posee una definición clara de esta Etiqueta en particular?

   La especificación de IPv6 permite a estos routers ignorar las Etiquetas de Flujo lo cual no implica que el router no vaya a ofrecer trato preferente a este flujo, ya que se le permite a los datagramas llevar esta información adicionalmente en cualquier encabezado de opciones, así se asegura que de una u otra forma este flujo reciba el trato preferencial que demanda.

   Una solución inapropiada para este problema sería dejar *caer* el datagrama y generar un mensaje de error ICMP, en este caso un paquete

[37] Es una función resumen que genera claves o llaves que representen de manera univoca a un documento, la función hash puede tomar parámetros tales como nombre, tamaño, fecha de creación, etc. aplicándole transformaciones y operaciones matemáticas.

con Etiqueta de Flujo en cero recibiría un mejor trato, lo cual contradice totalmente la intención de uso del campo Flow Label.

2. ¿Cómo hace Internet para liberar etiquetas ya usadas?
   Se asume que cuando la fuente termina de usar un flujo, siempre envía un mensaje que elimina la Etiqueta de Flujo. Esto no siempre puede ocurrir, por ejemplo si la fuente se *cae* antes de enviar el mensaje de eliminación o el mensaje se pierde durante el trayecto, el punto es que un router no puede esperar siempre este mensaje para desechar una etiqueta antigua, se debe contar con algún mecanismo que le permita a los routers eliminar etiquetas usadas.

   El mecanismo obvio es utilizar un *timer,* es decir que el router puede desechar una etiqueta cuyo estado no haya sido actualizado en algún tiempo definido, además si la fuente *cae* debe esperar un tiempo muerto en el cual no cree nuevos flujos, hasta que el tiempo de vida de todas las etiquetas creadas anteriormente haya expirado (las fuentes pueden evitar las restricciones que implica un tiempo muerto, si almacenan información sobre las etiquetas que se enviaron antes de su caída).

3. ¿Que datagramas deben llevar Etiquetas de Flujo diferente de cero?
   Los intercambios de pocos datos deben tener la Etiqueta de Flujo en cero, por que no vale la pena crear un flujo para pocos datagramas. Los flujos de tiempo real, obviamente siempre deben tener una Etiqueta de Flujo diferente de cero. El problema es que hacer cuando pares envían gran cantidad de tráfico que demande el mayor esfuerzo (Ej. Conexiones TCP).

   El argumento a favor del uso de Etiquetas de Flujo en conexiones TCP, es que incluso si la fuente no solicita trato preferencial, el router puede identificar que se trata de una gran cantidad de tráfico y utiliza una Etiqueta preestablecida que establezca una ruta especial que da a la

conexión TCP el mejor servicio (poco retraso y gran ancho de banda).Un argumento en contra del uso de Etiquetas de Flujo en conexiones TCP es que un router puede tener una ruta hacia un host en cache, sin tener en cuenta la cantidad de fuentes que puedan estar enviando a ese host, en este caso ninguna fuente tendría garantizada una optima conexión TCP. Una opción para aminorar este problema es manejando la ruta en cache como una ruta almacenada en una URL en la que las Etiquetas de Flujo usadas en menor frecuencia sean descartadas.

1.4 EL CAMPO LONGITUD DE LA CARGA ÚTIL

Los 16 bits del campo Payload Lenght en la cabecera IPv6 sirven para medir la longitud dada en octetos (bytes) de la carga útil. Los encabezados de extensión opcionales son considerados parte de la carga útil, junto con cualquier protocolo de capa superior. El campo Longitud de la Carga Útil es similar al campo Longitud Total de la cabecera IPv4, excepto que en IPv4 el campo mide los datos y el encabezado, en IPv6 el campo Payload Lenght mide los datos después del encabezado permitiendo así un tamaño mayor de carga útil.

Con 16 bits se puede tener un tamaño teórico máximo de carga útil de 65.535 bytes, las cargas mayores a este valor son llamadas Jumbogramas. Para indicar una carga jumbo, el valor de Payload Lenght es fijado en cero y la longitud de la carga es especificada en una opción cargada en el encabezado de extensión Salto a Salto.

1.5 EL CAMPO SIGUIENTE CABECERA

Su tamaño es de 8 bits y sirve para identificar el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo

Protocolo del IPv4 [RFC 1700], claro que en [RFC 3232] se especifica que los números de protocolo actualizados se encuentran en una base de datos en línea en http://www.iana.org/assignments/protocol-numbers.

En la siguiente tabla se encuentran algunos de los números de protocolo más conocidos:

Valor Decimal	Protocolo
0	Opción Salto a Salto IPv6
1	ICMP
4	IP en IP (Encapsulación)
6	TCP
17	UDP
43	Cabecera de enrutamiento IPv6
44	Cabecera de Fragmentación IPv6
50	ESP - Encapsulado seguro de la carga
51	AH – Cabecera de autenticación
55	IP móvil
59	IPv6NoNxt – No hay siguiente cabecera para IPv6
133	Cabecera de movilidad
138 - 252	No asignadas
253, 254	Uso experimental
255	Reservada

Tabla 6 Valores más conocidos para el campo Siguiente Cabecera

Algunos de los encabezados de extensión que se pueden adicionar a la cabecera IPv6 tambien utilizan un campo llamado *next header* tal y como se puede observar en la figura 27.

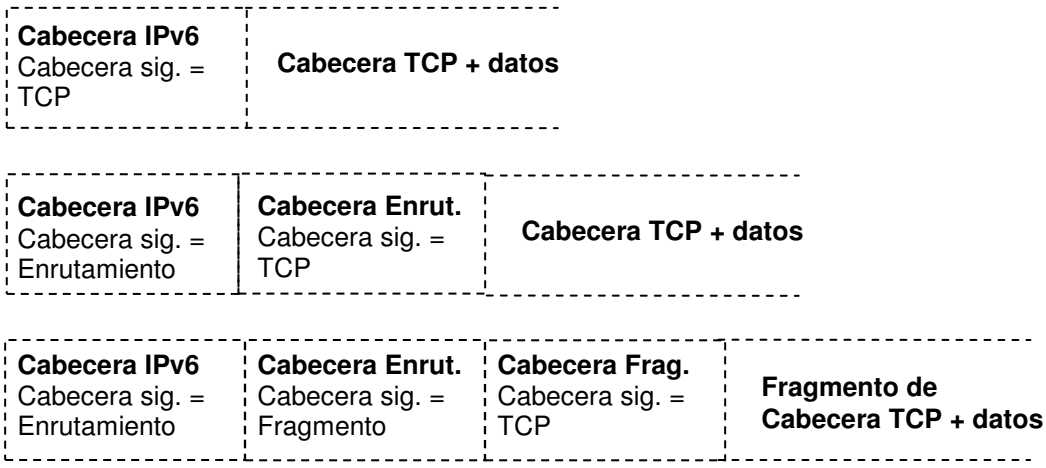

Figura 28 Uso del campo Next Header

En el primer caso no es solicitada ninguna cabecera de extensión y Next Header = TCP, al cual le sigue el encabezado TCP y cualquier protocolo de capa superior. En el segundo caso es solicitada una cabecera de enrutamiento, la cual no solicita ningún encabezado de extensión adicional y Next Header = TCP. En el último caso tanto el encabezado de enrutamiento como el de fragmento son solicitados con el campo Next Header identificado acordemente.

1.6 EL CAMPO LÍMITE DE SALTOS

El campo Hop Limit tiene una longitud de 8 bits, se decrementa en 1 por cada host que reenvía el paquete. El paquete es descartado si el Limite de Saltos es disminuido hasta cero. Se diferencia del campo Time to Live (TTL) de IPv4 en que el TTL puede ser medido en saltos o en segundos, en IPv6 el Limite de Saltos no dispone la opción del manejo temporal.

1.7 EL CAMPO DIRECCIÓN FUENTE

Dirección de 128 bits de longitud que identifica al nodo originador del paquete.

1.8 EL CAMPO DIRECCIÓN DE DESTINO

Dirección de 128 bits de longitud que identifica al nodo que tiene la intención de recibir el paquete, aunque no sea el nodo final sino cualquier nodo intermedio en la ruta.

2. ENCABEZADOS DE EXTENSIÓN

En IPv6 la información opcional de la capa Internet es codificada en cabeceras independientes que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Cada cabecera de extensión es identificada por un valor en el campo Siguiente Cabecera. Según lo ilustrado en la figura 28, un paquete IPv6 puede llevar desde cero, una o más cabeceras de extensión.

Las cabeceras de extensión sólo deben ser examinadas por el nodo final de la ruta, con una excepción, la cabecera de Opciones de Salto a Salto, la cual lleva información que debe ser procesada por cada nodo a lo largo de la ruta de entrega de un paquete, incluyendo los nodos origen y de destino.

Sólo cuando el paquete alcanza el nodo identificado en el campo Dirección de Destino de la cabecera IPv6, ocurre el demultiplexaje normal en el campo Siguiente cabecera de la cabecera IPv6, el cual invoca al módulo indicado para procesar la primera cabecera de extensión, o la cabecera de capa superior si no hay cabecera de extensión presente.

El contenido y la semántica de cada cabecera de extensión determinan si se procede o no a la cabecera siguiente. Por lo tanto, las cabeceras de extensión se deben procesar estrictamente en el orden que aparecen en el paquete. Un nodo intermedio no debe examinar a través de un paquete buscando un tipo en particular de cabecera de extensión y procesar esa cabecera antes de procesar todas las precedentes.

Si al procesar una cabecera un nodo necesita proceder a la siguiente cabecera, pero el valor Cabecera Siguiente en la cabecera actual es desconocido por el nodo, este debe descartar el paquete y enviar un mensaje ICMP de problema de parámetro al origen del paquete, con un valor código ICMP de 1 ("encontrado tipo de Cabecera Siguiente desconocido"). La misma acción se debería tomar si un nodo encuentra un valor Cabecera Siguiente de cero en cualquier cabecera con excepción de una cabecera IPv6.

Cada cabecera de extensión es un múltiplo de 8 bytes de largo, con el fin de conservar la alineación de 8 bytes para las cabeceras subsiguientes. Los campos multi-octeto dentro de cada cabecera de extensión se alinean en sus límites naturales, es decir, los campos de ancho de n bytes son colocados en un entero múltiplo de n bytes desde el inicio de la cabecera, para n = 1, 2, 4, o 8.

Una implementación completa del IPv6 debe incluir la implementación de las siguientes cabeceras de extensión:

- Opciones de Salto a Salto
- Enrutamiento (Tipo 0)
- Fragmento
- Opciones de Destino
- Autenticación
- Seguridad del Encapsulado de la Carga Útil

Las primeras cuatro están especificadas en [RFC 2460], las últimas dos están especificadas en la [RFC 2402] y [RFC 2406], respectivamente.

2.1 ORDEN DE LAS CABECERAS DE EXTENSIÓN

Cuando más de una cabecera de extensión se usa en un mismo paquete, se recomienda que esas cabeceras aparezcan en el siguiente orden:

1. Cabecera IPv6
2. Cabecera Opciones de Salto a Salto
3. Cabecera Opciones de Destino
4. Cabecera Enrutamiento
5. Cabecera Fragmento
6. Cabecera Autentificación
7. Cabecera Seguridad del Encapsulado de la Carga Útil
8. Cabecera de Capa Superior

Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la cabecera Opciones de Destino la cual debe de ocurrir a lo sumo dos veces (una vez antes de una cabecera Enrutamiento y la otra vez antes de una cabecera de capa superior).

Se aconseja que los nodos originadores de paquetes IPv6 se apeguen al orden recomendado arriba hasta y a menos que especificaciones subsiguientes corrijan esta recomendación.

2.2 OPCIONES

Las cabeceras de Salto a Salto y de Destino llevan un número variable de opciones codificadas Tipo-Longitud-Valor (TLV), tal y como se aprecia en la siguiente grafica:

Figura 29 Formato TLV

Donde:

- **Tipo de Opción:** identificador de 8 bits del tipo de opción.
- **Longitud de Datos Opcionales:** entero sin signo de 8 bits. Longitud del campo Datos de la Opción de esta opción, en bytes.
- **Datos de la Opción:** Campo de longitud variable. Datos específicos del Tipo de Opción.

El identificador Tipo de Opción se codifica tal que sus 2 bits de más alto orden especifican la acción que se debe tomar si el nodo IPv6 en proceso no reconoce el Tipo de Opción:

Valor	Acción
00	No tomar en cuenta esta opción y continuar procesando la cabecera
01	Descartar el paquete
10	Descartar el paquete y enviar un mensaje ICMP Problema de Parámetro a la fuente, señalando Tipo de Opción desconocido

11	Descartar el paquete y enviar un mensaje ICMP Problema de Parámetro a la fuente, señalando Tipo de Opción desconocido. Lo anterior solo si la dirección de destino no es Multicast

Tabla 7 Codificación de acciones del campo Tipo de Opción en una cabecera TLV

El tercer bit de orden mayor especifica si los Datos de la Opción de esa opción pueden modificar el enrutado hacia el destino final del paquete. La codificación es la siguiente:

0 -> Los datos de la Opción no modifican el enrutado.

1 -> Los datos de la Opción pueden modificar el enrutado.

Además, existen 2 opciones que se utilizan para rellenar las opciones de forma que el encabezado de extensión contenga un múltiplo de 8 bytes. La opción Pad1 es utilizada para insertar un byte de relleno, si se requiere más de un byte de relleno, la opción PadN se debe usar, en lugar de varias opciones Pad1.

2.3 CABECERA DE EXTENSIÓN: OPCIONES SALTO A SALTO

La cabecera de Opciones de Salto a Salto se usa para llevar información opcional que deba ser examinada por cada nodo a lo largo de la trayectoria de entrega de un paquete. La cabecera de Opciones de Salto a Salto se identifica por un valor de cero en el campo de Siguiente Cabecera de la cabecera IPv6, su formato se puede observar en la siguiente grafica:

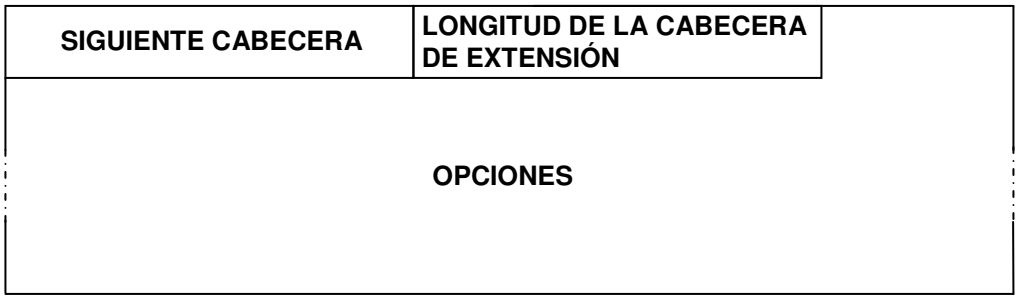

Figura 30 Formato de la cabecera de extensión Salto a Salto

Donde:

- **Siguiente Cabecera:** Su tamaño es de 8 bits, identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Salto a Salto. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC 3232].
- **Longitud de la Cabecera de Extensión:** Entero sin signo de 8 bits, indica la Longitud de la cabecera Opciones de Salto a Salto en unidades de 8 bytes, no incluye los primeros 8 bytes.
- **Opciones:** Campo de longitud variable, de longitud tal que la cabecera Opciones de Salto a Salto completa es un entero múltiplo de 8 bytes de largo. Contiene una o más opciones codificadas TLV, como se describe en el Anexo A - sección 2.2.

Se ha definido una opción *Jumbo Payload*, que se usa para enviar paquetes entre 65.536 y 4.294.967.296 bytes de longitud. La opción *Jumbo Payload* es definida por el campo Tipo de Opción de TLV = 194 (C2H en hex.), con el campo Longitud de Datos Opcionales = 4 bytes y un campo de 4 bytes que identifica la longitud del paquete jumbo en bytes (sin incluir la cabecera IPv6, pero incluyendo el encabezado de Opciones Salto a Salto). Otra opción de Salto a Salto se ha propuesto para alertar a los routers a examinar un determinado paquete IPv6, esta opción se denomina Router Alert Option [RFC 2711].

2.4 CABECERA DE EXTENSIÓN: OPCIONES DE DESTINO

La cabecera de extensión de Opciones de Destino tiene un formato idéntico al de la cabecera de extensión de Opciones de Salto a Salto Figura 30, el cual incluye los siguientes campos:

- **Siguiente Cabecera:** Su tamaño es de 8 bits, identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Destino. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC 3232].
- **Longitud de la Cabecera de Extensión:** Entero sin signo de 8 bits, indica la Longitud de la cabecera Opciones de Destino en unidades de 8 bytes, no incluye los primeros 8 bytes.
- **Opciones:** Campo de longitud variable, de longitud tal que la cabecera Opciones de Destino completa es un entero múltiplo de 8 bytes de largo. Contiene una o más opciones codificadas TLV, como se describe en el Anexo A - sección 2.2.

Las únicas opciones de Destino definidas en [RFC 2460] son Pad1 y PadN tratadas en el Anexo A - sección 2.2.

Existe dos maneras de codificar información de destino opcional en un paquete IPv6: como una opción en la cabecera Opciones de Destino, o como una cabecera de extensión separada. La cabecera Fragmento y la cabecera Autenticación son ejemplos de la más reciente propuesta. Qué propuesta puede ser usada depende de qué acción es deseada de un nodo destino que no entiende la información opcional:

1. Si la acción deseada es que el nodo destino descarte el paquete y, sólo si la Dirección Destino del paquete no es una dirección Multicast, debe enviar un mensaje ICMP Tipo No reconocido a la Dirección Origen del

paquete, luego la información puede ser codificada como una cabecera separada o como una opción en la cabecera Opciones de Destino cuyo Tipo de Opción tiene el valor 11 en sus dos bits de más alto orden. La elección puede depender de factores tales como cual toma menos bytes, o cual rinde mejor alineación o un análisis más eficiente.

2. Si alguna otra acción es deseada, la información debe ser codificada como una opción en la cabecera Opciones de Destino cuyo Tipo de Opción tiene el valor 00, 01, o 10 en sus dos bits de más alto orden, especificando la acción deseada (ver sección 2.2).

2.5 CABECERA DE EXTENSIÓN: ENRUTAMIENTO

Es utilizada por el nodo origen del paquete IPv6 para listar uno o más nodos intermedios a ser "visitados" en el camino hacia el nodo destino del paquete. La cabecera de Enrutamiento se identifica por un valor de 43 en el campo de Siguiente Cabecera de la cabecera inmediatamente precedente. En la figura 31 se observa el formato de la cabecera de Enrutamiento:

SIGUIENTE CABECERA	LONGITUD DE LA CABECERA DE EXTENSIÓN
TIPO DE ENRUTAMIENTO	SEGMENTOS DEJADOS
DATOS ESPECIFICOS DEL TIPO	

Figura 31 Formato de la cabecera de extensión de Enrutamiento

Donde:

- **Siguiente Cabecera:** su tamaño es de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC 3232].
- **Longitud de la Cabecera de Extensión:** entero sin signo de 8 bits, indica la Longitud de la cabecera Enrutamiento en unidades de 8 bytes, no incluye los primeros 8 bytes.
- **Tipo de Enrutamiento:** identificador de 8 bits de una variante en particular de cabecera Enrutamiento.
- **Segmentos Dejados:** entero sin signo de 8 bits, que indica el número de segmentos de ruta restantes, es decir, el número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.
- **Datos específicos del tipo:** campo de longitud variable, de formato determinado por el Tipo de Enrutamiento, y de longitud tal que la cabecera Enrutamiento completa es un entero múltiplo de 8 bytes de largo.

Si, al procesar un paquete recibido, un nodo encuentra una cabecera de Enrutamiento con un valor Tipo de Enrutamiento desconocido, el comportamiento requerido por el nodo depende del valor del campo Segmentos Dejados, como sigue:

- Si el valor del campo Segmentos Dejados es cero, el nodo debe ignorar la cabecera de Enrutamiento y proceder a procesar la siguiente cabecera en el paquete, cuyo tipo se identifica por el campo Siguiente Cabecera en la cabecera Enrutamiento.

- Si el valor del campo Segmentos Dejados es diferente de cero, el nodo debe descartar el paquete y enviar un mensaje ICMP Problema de

Parámetro, Código 0, a la Dirección Origen del paquete, apuntando al Tipo de Enrutamiento desconocido.

Si, después de procesar una cabecera Enrutamiento de un paquete recibido, un nodo intermedio determina que el paquete será remitido hacia un enlace cuya MTU de enlace es menor que el tamaño del paquete, el nodo debe descartar el paquete y enviar un mensaje ICMP Paquete Demasiado Grande a la Dirección Origen del paquete.

2.6 CABECERA DE EXTENSIÓN: FRAGMENTO

La cabecera Fragmento es utilizada por un origen IPv6 para enviar un paquete más grande de lo que cabría en la MTU de la ruta hacia su destino. La cabecera Fragmento se identifica por un valor Cabecera Siguiente de 44 en la cabecera inmediatamente precedente, y tiene el siguiente formato:

<table>
<tr><td colspan="2">SIGUIENTE CABECERA</td><td colspan="2">RESERVADO</td></tr>
<tr><td colspan="2">DESPLAZAMIENTO DEL FRAGMENTO</td><td>RES</td><td>M</td></tr>
<tr><td colspan="4">IDENTIFICACIÓN</td></tr>
</table>

Figura 32 Formato de la cabecera de extensión de Fragmento

Donde:

- **Siguiente Cabecera:** Su tamaño es de 8 bits. Identifica el tipo de cabecera inicial de la Parte Fragmentable del paquete original. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC 3232].
- **Reservado:** Campo reservado de 8 bits. Inicializado a cero para la transmisión, ignorado en la recepción.

- **Desplazamiento del Fragmento:** Entero sin signo de 13 bits. Indica el desplazamiento, en unidades de 8 bytes, de los datos que siguen a esta cabecera, con respecto al comienzo de la Parte Fragmentable del paquete original.
- **Res:** Campo reservado de 2 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
- **Bandera M:** Bit que indica si continúan más fragmentos (M = 1), o si es el último fragmento (M = 0).
- **Identificación:** Campo de 32 bits, su descripción a continuación.

Para enviar un paquete que es demasiado grande para caber en la MTU de la ruta hacia su destino, un nodo origen puede dividir el paquete en fragmentos y enviar cada fragmento como un paquete separado, para al final poder ser reensamblado en el nodo receptor.

Por cada paquete que será fragmentado, el nodo origen genera un valor Identificación, el cual debe ser diferente que el de cualquier otro paquete fragmentado enviado recientemente, con la misma Dirección Origen y Dirección Destino. Si una cabecera Enrutamiento está presente, la Dirección Destino de interés es la del destino final.

El paquete original, es decir el de gran tamaño, está constituido por dos partes: una parte que no se puede fragmentar (consiste en la cabecera IPv6 más cualquiera de las cabeceras de extensión que debe procesarse por nodos en la ruta hacia el destino) y una segunda parte que contiene información fragmentable (consiste en el resto del paquete, es decir, cualquiera de las cabeceras de extensión que necesitan ser procesadas solamente por el nodo destino final, más la cabecera de capa superior y los datos).

La Parte Fragmentable del paquete original es dividida en fragmentos, cada uno con longitud igual a un entero múltiplo de 8 bytes. Los fragmentos se transmiten en "paquetes fragmento", donde cada paquete debe contener la parte no Fragmentable, la cabecera de fragmento y el fragmento del paquete original.
Deben escogerse las longitudes de los fragmentos tal que los paquetes de fragmento resultantes quepan dentro de la MTU de la ruta hacia el destino final del paquete. En el destino, se reensamblan los paquetes fragmento en su forma original (no fragmentada) teniendo en cuenta las siguientes reglas:

- Un paquete original sólo se reensambla a partir de paquetes fragmento que tienen la misma Dirección Origen, Dirección Destino, e Identificación del Fragmento.
- La Parte No Fragmentable del paquete reensamblado consiste en todas las cabeceras, pero sin incluir, la cabecera Fragmento del primer paquete fragmento (es decir, el paquete cuyo Desplazamiento del Fragmento es 0).

2.7 CABECERA DE EXTENSIÓN: AUTENTIFICACIÓN

La cabecera de extensión de Autentificación AH (*Authentication Header* [RFC 2402]) se usa para proporcionar integridad sin conexión y autenticación del origen de datos para datagramas IP y para proporcionar protección contra reenvíos. Aporta autentificación a las partes de la cabecera IP que se les pueda brindar este servicio, así como también a los datos de los protocolos de las capas superiores. Sin embargo, algunos campos de la cabecera IP pueden cambiar durante el transporte, así los valores de tales campos no pueden ser protegidos por AH. Entonces la protección proporcionada a la cabecera IP por AH se proporciona a fragmentos.

La cabecera de extensión de Autentificación es identificada en la cabecera IPv6 o alguna cabecera de extensión, por un valor de Siguiente Cabecera = 51 y posee el siguiente formato:

SIGUIENTE CABECERA	LONGITUD DE LA CARGA	RESERVADO
INDICE DE PARAMETROS DE SEGURIDAD SPI		
NUMERO DE SECUENCIA		
DATOS DE AUTENTICACIÓN		

Figura 33 Formato de la cabecera de extensión de Autentificación

Donde:

- **Siguiente Cabecera:** Su tamaño es de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de Autenticación. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC 3232].
- **Longitud de la carga:** Sus 8 bits de longitud proveen la longitud del encabezado de Autentificación en palabras de 32 bits menos 2 (los primeros 8 bytes del encabezado de Autentificación no son incluidos).
- **Reservado:** Campo reservado de 16 bits. Inicializado a cero para la transmisión, ignorado en la recepción.
- **Índice de parámetros de seguridad:** El SPI es un valor arbitrario de 32 bits que, conjuntamente con la dirección de destino IP y el protocolo de seguridad (AH), identifican unívocamente a la Asociación de Seguridad (SA) para este datagrama.
- **Numero de secuencia:** Campo de 32 bits sin signo que contiene un valor reciente y único del contador (de número de secuencia). Es obligatorio y

debe estar siempre presente incluso si el receptor elige no habilitar el servicio contra envíos para una SA específica.

- **Datos de autenticación:** Este campo es de longitud variable y contiene el Valor de Comprobación de Integridad (ICV) para este paquete. Este campo debe contener un múltiplo entero de 32 bits de longitud. El algoritmo de autentificación debe especificar la longitud ICV y las reglas de comparación y los pasos de procesamiento para la validación.

En el contexto IPv6, el AH se ve como carga extremo a extremo y debe aparecer después de las cabeceras de extensión: salto a salto, de enrutamiento, y de fragmentación.

2.8 CABECERA DE EXTENSIÓN: SEGURIDAD DEL ENCAPSULADO DE LA CARGA ÚTIL

La cabecera de extensión para la Seguridad del Encapsulado de la Carga Útil ESP (Encapsulating Security Payload [RFC 2406]) está diseñada para proveer una mezcla de servicios de seguridad para IPv4 e IPv6. ESP puede ser usada sola o en combinación con AH. Los servicios de seguridad se pueden proveer entre pares de host, entre pasarelas de seguridad o entre un host y una pasarela de seguridad.

ESP es usada para proveer confidencialidad, autentificación del origen de datos y un servicio contra reenvió y un flujo limitado de trafico confidencial. El conjunto de servicios a proveer depende de las opciones seleccionadas en el momento de establecer las SA y la implementación.
La cabecera de extensión de Seguridad del Encapsulado de la Carga Útil es identificada en la cabecera IPv6 o alguna cabecera de extensión, por un valor de Siguiente Cabecera = 50 y posee el siguiente formato:

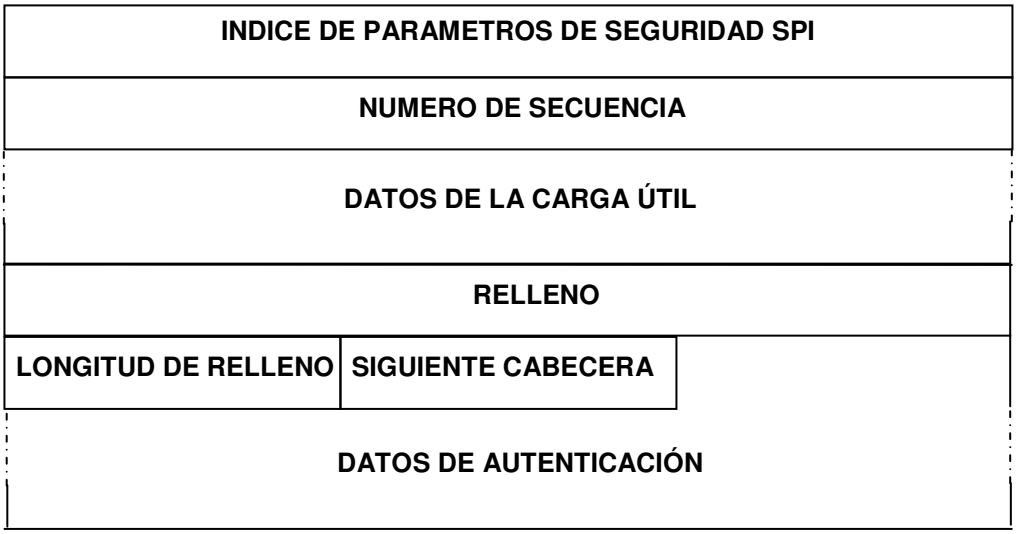

Figura 34 Formato de la cabecera de extensión de Seguridad del Encapsulado de la Carga Útil

Donde:

- **Índice de parámetros de seguridad:** El SPI es un valor arbitrario de 32 bits que, conjuntamente con la dirección de destino IP y el protocolo de seguridad (AH), identifican unívocamente a la Asociación de Seguridad (SA) para este datagrama.
- **Numero de secuencia:** Campo de 32 bits sin signo que contiene un valor reciente y único del contador (de número de secuencia). Es obligatorio y debe estar siempre presente incluso si el receptor elige no habilitar el servicio contra envíos para una SA específica.
- **Datos de la Carga Útil:** Es un campo de longitud variable y contiene los datos descritos por el campo Siguiente Cabecera. Este campo es obligatorio y es un número entero de bytes de longitud.
- **Relleno:** Contiene opcionalmente entre 0 y 255 bytes de relleno usados como requisito para la encriptación de la carga útil (puede ser necesitado para alinear la carga útil a múltiplos de 4 bytes, aunque este aumento de tamaño puede perjudicar el rendimiento de ancho de banda).

- **Longitud de relleno:** Sus 8 bits se usan para indicar el número de bytes de relleno que lo preceden. El rango de valores válidos es de 0 a 255, un valor de cero indica que no hay presentes bytes de relleno. El uso del campo de longitud de relleno es obligatorio.
- **Siguiente Cabecera:** Su tamaño es de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de Autenticación. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC 3232].
- **Datos de autenticación:** Este campo es de longitud variable y contiene el Valor de Comprobación de Integridad (ICV) para este paquete. Este campo debe contener un múltiplo entero de 32 bits de longitud. El algoritmo de autentificación debe especificar la longitud ICV y las reglas de comparación y los pasos de procesamiento para la validación.

2.9 CABECERA DE EXTENSIÓN: NO HAY SIGUIENTE

El valor 59 en el campo Cabecera Siguiente de una cabecera IPv6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo Longitud de la Carga Útil de la cabecera IPv6 indica la presencia de octetos más allá del final de una cabecera cuyo campo Cabecera Siguiente contiene 59, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

ANEXO B. ARQUITECTURA DE DIRECCIONAMIENTO EN IPV6[38]

Los 32 bits de las direcciones IPv4 se han tornado insuficientes para las demandas actuales de Internet; ahora con IPv6 y sus 128 bits de longitud, ¿Es posible que en algunos años se esté pensando en el diseño de IPv7? Es muy poco probable y nadie lo sabe, lo que cabe resaltar es que 2^{128} es una cifra enorme y difícil de pronunciar, equivale exactamente a 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones posibles, es decir aproximadamente $6.6*10^{23}$ (665.570.793.348.866.943.898.599) direcciones por metro cuadrado de la superficie terrestre.

Indudablemente con IPv6 hay espacio para todos los dispositivos existentes y los que faltan por venir. Este espacio de direcciones abre nuevas oportunidades para el desarrollo de las denominadas *redes sin redes*, es decir redes donde todos sus dispositivos son móviles.

1. DIRECCIONES IPV6

Las direcciones en IPv6 son números de 128 bits de longitud, las cuales se usan para identificar interfaces ó grupos de interfaces. Existen 3 tipos de direcciones IPv6:

- **Direcciones Unicast:** Las direcciones Unicast o de única difusión son usadas para identificar a una sola interfaz. Un paquete enviado a una dirección Unicast es entregado a la interfaz identificada con esa dirección.

[38] Anexo basado en [RFC 3513]

- **Direcciones Anycast:** Las direcciones Anycast o de cualquier difusión son usadas para identificar un grupo de interfaces (generalmente ubicadas en distintos nodos). Un paquete enviado a una dirección Anycast es entregado a una de las interfaces identificadas con esa dirección (la más cercana de acuerdo con la medida de distancias del protocolo de enrutamiento).

- **Direcciones Multicast:** Las direcciones Multicast o de difusión múltiple son usadas para identificar un grupo de interfaces (generalmente ubicadas en distintos nodos). Un paquete enviado a una dirección Multicast es entregado a todas las interfaces identificadas con esa dirección.

Las funciones de las direcciones Broadcast en IPv4 han sido reemplazadas por las direcciones Multicast en IPv6. Todos los tipos de direcciones IPv6 son asignadas a interfaces, no a nodos. Una dirección Unicast IPv6 es referida a una sola interfaz, siempre y cuando esta interfaz pertenezca solo a un nodo, cualquiera de las direcciones Unicast asignadas a ese nodo puede ser usada para referirse al nodo.

Todas las interfaces requieren tener por lo menos una dirección Unicast de Enlace Local (sección 4.6). Una sola interfaz también puede ser asignada a múltiples direcciones IPv6 de cualquier tipo (Unicast, Anycast y Multicast) o ámbito. Direcciones Unicast con ámbito mayor que el del enlace no son necesarias para interfaces que no sean usadas como origen y destino de paquetes IPv6 hacia o desde nodos no vecinos, es decir para comunicarnos internamente en el campus no van a ser necesarias direcciones IPv6 globales.

2. REPRESENTACIÓN TEXTUAL DE LAS DIRECCIONES IPV6

Dado el gran tamaño de una dirección IPv6 (128 bits), es necesario para nuestra comodidad representarlas de una manera resumida y más fácil de recordar. A continuación se encuentran las 3 formas convencionales de representar textualmente una dirección IPv6:

1. La forma preferida es **x:x:x:x:x:x:x:x**, donde cada "x" representa un valor hexadecimal de 16 bits de largo. Ejemplos:

   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
   1080:0:0:0:8:800:200C:417A

   Nótese que no es necesario escribir los ceros a la izquierda de una cifra en un campo cualquiera, pero debe al menos haber un número en cada campo (excepto en el caso descrito a continuación).

2. Debido a la longitud de una dirección IPv6 y la poca cantidad de direcciones asignadas, es común encontrar direcciones que contengan largas cadenas de bits en cero. Para permitir una escritura más ágil de estos campos en cero, se ha diseñado una sintaxis especial para comprimir ceros. El uso de "**::**" indica la existencia de grupos adyacentes de 16 bits en cero. El "**::**" sólo puede aparecer una vez por dirección. Por ejemplo las siguientes direcciones:

1080:0:0:0:8:800:200C:417A	una dirección Unicast
FF01:0:0:0:0:0:0:101	una dirección Multicast
0:0:0:0.0:0:0:1	una dirección *loopback* o de retorno
0:0:0:0.0:0:0:0	una dirección no especificada

Pueden ser representadas así:

1080::8:800:200C:417A	una dirección Unicast
FF01::101	una dirección Multicast
::1	una dirección *loopback* o de retorno
::	una dirección no especificada

3. Una forma conveniente de asignar direcciones IPv6 durante la transición, en el cual el funcionamiento de la red involucra tanto a hosts IPv4 como host IPv6, es x:x:x:x:x:x:d:d:d:d, donde cada "x" representa los valores en hexadecimal de los 6 campos de mayor orden de la dirección, y cada "d" representa los valores en decimal de 8 bits de los cuatro campos de menor orden en la dirección (representación estándar de IPv4). Ejemplos:

0:0:0:0:0:0:200.50.87.11	**->**	**::200.50.87.11**
0:0:0:0:0:FFFF:192.168.65.17	**->**	
::FFFF:192.168.65.17		

3. PREFIJOS DE DIRECCIONES IPV6

La representación textual de un prefijo de dirección IPv6 es semejante a la forma de representar en IPv4 los prefijos en notación CIDR (*Classless Inter-Domain Routing*, reemplaza la generación de direcciones IPv4 con clases). En IPv6 un prefijo de dirección se representa de la siguiente manera:

Dirección IPv6 / **Longitud del prefijo**

Donde:

- **Dirección IPv6:** es una dirección IPv6 expresada en cualquier notación descrita en la sección 3.3.2.
- **Longitud del prefijo**: es un valor decimal que especifica cuantos de los bits a la izquierda de la dirección IPv6 comprenden el identificador de red (identificador de un tipo específico de dirección).

Por ejemplo, las siguientes son representaciones validas de un prefijo de 60 bits (12AB00000000CD3 en hexadecimal):

12AB:0000:0000:CD30:0000:0000:0000:0000 / 60
12AB::CD30:0:0:0:0 / 60
12AB:0:0:CD30:: / 60

Cuando se escribe una dirección de host y un prefijo de ese nodo (Ej. El prefijo de la subred a la cual pertenece el nodo), las dos posibles combinaciones son las siguientes:

La dirección del nodo:	**12AB:0:0:CD30:123:4567:89AB:CDEF**
Y su prefijo de subred:	**12AB:0:0:CD30:: / 60**
Pueden ser abreviados así:	**12AB:0:0:CD30:123:4567:89AB:CDEF / 60**

Las siguientes NO son representaciones validas del anterior prefijo:

- **12AB:0:0:CD3 / 60** en los campos 2 y 3 de mayor orden se truncaron los ceros a la izquierda de cada campo cuidando dejar al menos un numero por campo, pero en el campo 4 se trunco el cero a la

derecha del campo lo cual es un error. Los últimos 4 campos fueron truncados totalmente sin usar "::" como se debía.

- **12AB::CD30 / 60** al no tener cuidado de usar "::" y evitar dejar al menos un numero en cada campo donde se eliminen los ceros a la izquierda, la dirección expandida a la izquierda de "/" es: 12AB:0000:0000:0000:0000:0000:0000:CD30

- **12AB::CD3 / 60** al no tener cuidado de usar "::" y truncar los ceros a la derecha de un campo, la dirección expandida a la izquierda de "/" es: 12AB:0000:0000:0000:0000:0000:0000:0CD3

3.1 ASIGNACIÓN DE PREFIJOS IPV6

El tipo específico de una dirección IPv6 es indicado por los bits de mayor orden en las direcciones. Este campo de longitud variable es llamado Formato de Prefijo (FP *Format Prefix*). La asignación inicial de estos prefijos se encuentra a en la tabla 5.

PREFIJO (BINARIO)	ASIGNACIÓN	FRACCIÓN
0000 0000	No asignado	1 / 256
0000 0001	No asignado	1 / 256
0000 001	Reservado para asignaciones NSAP[39]	1 / 128
0000 01	No asignado	1 / 64

[39] NSAP (*Network Service Access Point*) Punto de acceso a servicios de red, es el punto donde los proveedores de servicio de Internet pueden conectarse entre si, por lo tanto son los puntos de mayor congestión de la red.

0000 1	No asignado	1 / 32
0001	No asignado	1 / 16
001	Direcciones Unicast Globales	1 / 8
010	No asignado	1 / 8
011	No asignado	1 / 8
100	No asignado	1 / 8
101	No asignado	1 / 8
110	No asignado	1 / 8
1110	No asignado	1 / 16
1111 0	No asignado	1 / 32
1111 10	No asignado	1 / 64
1111 110	No asignado	1 / 128
1111 1110 0	No asignado	1 / 512
1111 1110 10	Direcciones Unicast Locales de Enlace	1 / 1024
1111 1110 11	Direcciones Unicast Locales de Sitio	1 / 1024
1111 1111	Direcciones Multicast	1 / 256

Tabla 8 Prefijos de dirección IPv6 asignados

La dirección no especificada, la dirección loopback y las direcciones IPv6 con una IPv4 incluida son asignadas fuera del espacio del prefijo binario 0000 0000.

Una dirección Multicast se identifica por comenzar por el valor binario 1111 1111 o FF en hexadecimal, cualquier otro prefijo identifica una dirección Unicast. Las direcciones Anycast han sido tomadas del espacio Unicast, por lo tanto son sintácticamente semejantes.

Por ahora, la IANA[40] debe limitar la asignación del espacio de direccionamiento Unicast al rango de direcciones que empiecen por el valor en binario 001. El resto del espacio de direcciones Unicast Globales (aproximadamente el 85% del espacio de direccionamiento IPv6) es reservado para una futura definición y uso, y no será asignado por la IANA en este momento.

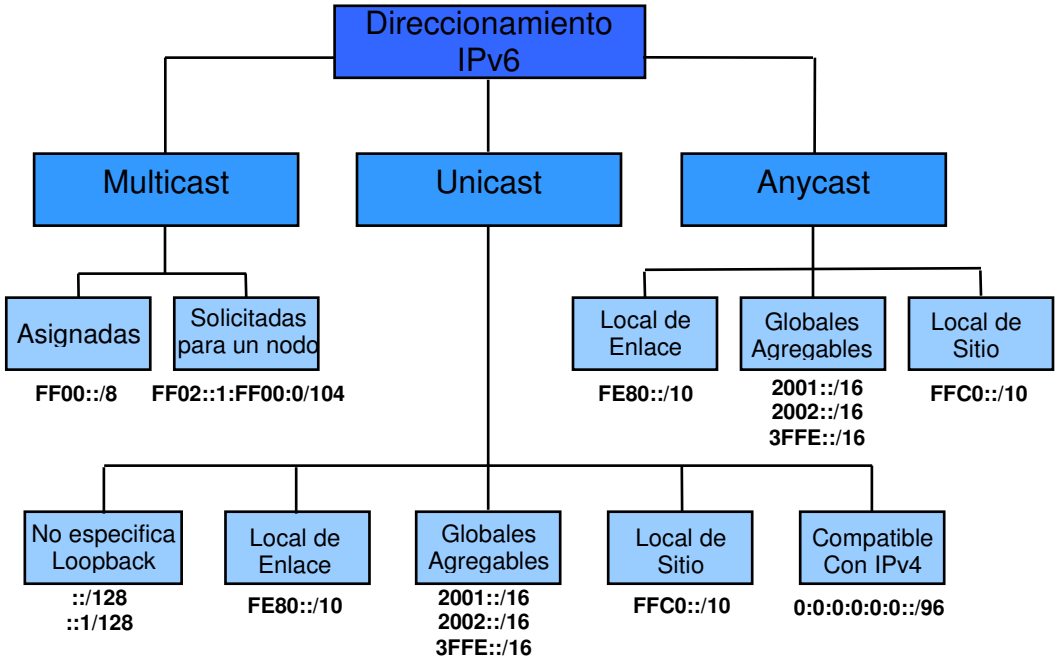

Figura 35 Arquitectura de direccionamiento IPv6

4. DIRECCIONES UNICAST [RFC 3513 - 2374]

Las direcciones Unicast IPv6 son asignadas con prefijos de tamaño variable, de manera similar a las direcciones IPv4 representadas con CIDR. Hay varias formas de asignación de direcciones Unicast en IPv6, incluyendo las

[40] IANA – *Internet Assigned Number Authority*, entidad que asignó inicialmente el espacio global de direcciones IPv6, aunque posteriormente fue reemplazada por la ICANN - *Internet Corporation for Assigned Names and Numbers,* si bien la IANA no existe sus asignaciones aún permanecen vigentes, ver anexo C

direcciones Globales Agregables, las direcciones NSAP, las direcciones IPX jerárquicas, las direcciones Locales de Sitio, las direcciones Locales de Enlace y las direcciones que puedan ser definidas en el futuro.

Algunos nodos IPv6 pueden tener algún conocimiento sobre la estructura interna de las direcciones IPv6, todo depende del rol del host. Como mínimo un host puede considerar que una dirección Unicast tiene una estructura interna en la cual los 128 bits de la dirección corresponden a la dirección del nodo, es decir no considera la existencia de subredes ni prefijos. Un equipo de red un poco más sofisticado puede considerar que de los 128 bits de la dirección, un numero n de bits pueden representar a la subred y que (128 – n) bits representan el identificador de un nodo o interfaz. Algunos equipos aun más sofisticados pueden ser concientes de los límites jerárquicos que rodean una dirección Unicast, los límites conocidos diferirán de un router a otro, dependiendo de qué posición tiene el router en la jerarquía de asignación de rutas.

4.1 IDENTIFICADORES PARA UNA INTERFAZ

Los identificadores de interfaz en las direcciones Unicast IPv6 son usados para identificar interfaces en un enlace (por ejemplo en la LAN UIS). Estos identificadores requieren ser únicos dentro de un prefijo de subred, esto no implica que vayan a ser únicos en un ámbito mayor al del enlace. El mismo identificador de interfaz puede ser usado por múltiples interfaces en el mismo nodo. Por consiguiente un identificador de interfaz NO debe ser usado como dirección pública global, el ámbito de estas direcciones debe ser solamente la red interna.

Para todas las direcciones Unicast, excepto las que empiezan con un valor binario de 000, se requiere de un Id de interfaz de 64 bits de longitud

construidos en base a la norma EUI-64 y su formato modificado. Dichos identificadores pueden ser globales en el caso en el cual un *token* global este disponible por ejemplo los 48 bits de la dirección MAC, o locales en casos como el de un enlace por puerto paralelo o los extremos de un túnel. Ahora que las direcciones Unicast agregadas a interfaces requieren manejar de manera implícita la dirección MAC (la cual se caracteriza por ser diferente en cada host), no es permitido asignar un mismo identificador de interfaz a diferentes máquinas en una subred, tal como lo recomienda el [RFC 3513 apéndice B] como corrección del [RFC 2373].

4.1.1 NORMA EUI - 64[41]

Las direcciones EUI-64 de 64 bits han sido definidas por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos). A continuación se observa el proceso que establece la dirección MAC de un equipo como su identificador de interfaz para una dirección IPv6:

Dirección MAC= **00-AA-00-3F-2A-1C**

1- Se convierte la dirección MAC a EUI-64 insertando FF-FE entre el tercer y cuarto byte = **00-AA-00-FF-FE-3F-2A-1C**

2- Se hace el bit 7 del primer byte = 1(dirección Local) ó 0 (dirección Global Agregable). En este caso el primer byte es 00000000 se convierte en 00000010 (0x02) = **02-AA-00-FF-FE-3F-2A-1C** ó en notación hexadecimal con dos puntos = **2AA:FF:FE3F:2A1C** que es el identificador de interfaz.

[41] Una completa descripción del nuevo formato EUI-64 se encuentra en el [RFC 3513 Apéndice A]

3- La dirección local de enlace correspondiente a la tarjeta de red con dirección física 00-AA-00-3F-2A-1C es **FE80::2AA:FF:FE3F:2A1C**.

4.2 LA DIRECCIÓN NO ESPECIFICADA

La dirección **0000:0000:0000:0000:0000:0000:0000:0000** o **::** es llamada la dirección no especificada y nunca debe ser asignada a ningún nodo. Dicha dirección indica la ausencia de una dirección. Esta dirección puede usarse en un inicio en el campo Dirección de Origen cuando un nodo todavía no tiene una dirección asignada. La dirección no especificada no debe usarse en el campo Dirección de Destino de paquetes IPv6 o en encabezados de enrutamiento.

4.3 LA DIRECCIÓN DE RETORNO

La dirección **0000:0000:0000:0000:0000:0000:0000:0001** ó **::1** es llamada la dirección *Loopback* o dirección de retorno, ella puede usarse para que un nodo IPv6 pueda enviarse paquetes a sí mismo. Esta dirección nunca debe ser asignada a una interfaz física.

La dirección de retorno no debe ser usada como dirección de origen en un paquete IPv6 que vaya a ser enviado fuera de un simple nodo, ni tampoco deben ser reenviadas por ningún router IPv6.

4.4 DIRECCIONES IPV6 CON UNA DIRECCIÓN IPV4 INCLUIDA

Este tipo de dirección de compatibilidad con IPv4 es usada por nodos que posean soporte para IPv4 e IPv6, que desean comunicarse con IPv6 sobre una infraestructura de IPv4. Cuando se utiliza una dirección IPv4 embebida en una

dirección IPv6 como destino IPv6, el tráfico de IPv6 se encapsula automáticamente con un encabezado IPv4 y es enviado al destino a través de la infraestructura IPv4, este proceso es llamado Túnel Automático. Este tipo de dirección es llamada "dirección IPv4 compatible con IPv6" y posee el siguiente formato:

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

Figura 36 Formato de una dirección IPv4 compatible con IPv6

Como corrección del [RFC 2373], a partir de [RFC 3513] queda definido que la dirección IPv4 usada en una dirección compatible con IPv6 debe ser una dirección IPv4 única y global (pública).

Un segundo tipo de dirección IPv6 que contiene una dirección IPv4 incluida es la denominada "dirección IPv4 *mapeada* en una dirección IPv6". Esta dirección es usada para representar la dirección de un nodo que es sólo IPv4 ante un nodo IPv6. La dirección IPv4 mapeada en una dirección IPv6 nunca debe ser utilizada como dirección origen o de destino de un paquete IPv6, y posee el siguiente formato:

80 bits	16 bits	32 bits
0000……...0000	**FFFF**	**Dirección IPv4**

Figura 37 Formato de una dirección IPv4 mapeada en una dirección IPv6

Las anteriores direcciones especiales IPv6, han sido diseñadas para ayudar a la migración de IPv4 a IPv6 y a la coexistencia de ambos tipos de hosts.

4.5 DIRECCIONES UNICAST GLOBALES

El formato general de una dirección Unicast global es el siguiente:

n bits	m bits	128 – n - m bits
Prefijo global de enrutamiento	**Id. de subred**	**Id. de Interfaz**

Figura 38 Formato de una dirección Unicast global

Donde el prefijo global de enrutamiento es un valor (generalmente estructurado jerárquicamente) asignado a un sitio (conjunto de subredes / enlaces), el Id. de subred es un identificador de un enlace dentro de un sitio, y el Id. de interfaz está definido en la sección 3.4.1.

Un ejemplo de direcciones Unicast globales llamado direcciones Unicast Globales Agregables está descrito en el [RFC 2374]. Este formato de direcciones esta diseñado para soportar el tipo de agregación basados en proveedores que se emplea actualmente y uno nuevo basado en intercambios. La combinación permitirá la agregación eficiente de rutas para sitios que se conectan directamente a los proveedores y para sitios que se conectan a los intercambios.

Las direcciones Unicast Globales Agregables son equivalentes a las direcciones IPv4 públicas, es decir son accesibles globalmente en la parte IPv6 de Internet (6Bone red troncal de IPv6) o enrutables globalmente. El termino “agregables” indica que este tipo de direcciones son diseñadas para ser agregadas basadas en *intercambios* de modo que se obtenga una infraestructura de enrutamiento eficiente.

Las direcciones Agregables están organizadas en tres niveles de jerarquía:

- **Topología pública:** es una colección de proveedores e intercambios que proveen el servicio de transito en Internet público.
- **Topología de sitio:** es local a un sitio específico u organización que no provee servicios de transito público a nodos fuera de la organización.
- **Identificadores de interfaz:** identifican interfaces unívocamente en un enlace específico.

Así, una arquitectura de red basada en agregación incluye a los proveedores intercontinentales, los intercambios y los suscriptores. Los intercambios se encargan de asignar direcciones IPv6, en algunos casos los suscriptores se pueden conectar directamente a un intercambio. Este modelo de asignación de rutas provee acceso a múltiples proveedores intercontinentales y permitirá realizar un cambio de proveedor sin tener que reenumerar todos los host de nuestra red.

En la siguiente gráfica se observa la estructura de una dirección Unicast Global Agregable:

	13 bits	8 bits	24 bits	16 bits	64 bits
001	**Id. TLA**	**Res**	**Id. NLA**	**Id. SLA**	**Id. De interfaz**

Figura 39 Formato de una dirección Unicast Global Agregable

Donde:

- **Id. TLA:** Indica el Agregador de nivel superior (TLA, *Top Level Aggregator*) para la dirección. Identifica el nivel superior de jerarquía de enrutamiento.

- **Res:** Bits reservados para uso futuro al expandir el tamaño del Id. de TLA o del Id. de NLA.
- **Id. NLA:** Indica el Agregador de nivel siguiente (NLA, *Next-Level Aggregator*) para la dirección.
- **Id. SLA:** Indica el Agregador de nivel de sitio (SLA, *Site-Level Aggregator*) para la dirección, puede servir a una organización para identificar subredes dentro de su sitio.
- **Id. de Interfaz:** Indica la interfaz de una subred específica.

4.6 DIRECCIONES UNICAST DE USO LOCAL

Las direcciones IPv6 locales [RFC 4193], tienen las siguientes características:

- Prefijo global único (con probabilidad alta de ser único[42]).
- El prefijo es muy conocido para permitir así una fácil filtración de tráfico a los límites de la subred.
- Permite combinar sitios (interconectarlos privadamente) sin crear conflictos de direcciones o requerir una nueva numeración de las interfaces que usen estos prefijos.
- Independencia del Proveedor de Servicios de Internet y puede ser usado para comunicaciones dentro de un sitio sin tener una conexión permanente a Internet.
- Sí accidentalmente se *fuga* tráfico vía router o DNS, no hay ningún conflicto posible con cualquier otra dirección.
- En la práctica, aplicaciones pueden tratar estas direcciones como direcciones de alcance global (siendo únicas no hay inconveniente)

[42] En [RFC 4193 - sección 3.2.2] es propuesto un algoritmo para asignar un Id. global a un grupo de direcciones locales Unicast pertenecientes a una subred, con una muy remota probabilidad de ser repetido gracias al gran numero de combinaciones posibles.

Por ahora se recomienda no instalar direcciones de uso local en el servidor DNS global. Se encuentran definidos dos tipos de direcciones Unicast para uso local. Estas son las direcciones locales de enlace (*Link – Local*) y las locales de sitio (*Site – Local*).

Las direcciones locales de enlace han sido diseñadas para ser usadas en un simple enlace con propósitos tales como la auto-configuración de direcciones, descubrimiento del vecino o cuando ningún enrutador se encuentra presente. El formato de las direcciones Unicast de enlace local es el siguiente:

10 bits	54 bits	64 bits
1111111010	**0000……0000**	**Id. de Interfaz**

Figura 40 Formato de una dirección Unicast local de enlace

Los routers no deben reenviar hacia otros enlaces ningún paquete que contenga una dirección local de enlace como dirección de origen o destino.

Las direcciones locales de sitio tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111011	**Id. de Subred**	**Id. De Interfaz**

Figura 41 Formato de una dirección Unicast local de sitio

Las direcciones locales de sitio fueron diseñadas para ser usadas para el direccionamiento dentro de un sitio que no necesita de un prefijo global, equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/12

y 192.168.0.0/16). No se puede tener acceso a las direcciones locales de sitio desde otros sitios y los enrutadores no deben reenviar el tráfico local fuera del sitio. A diferencia de las direcciones locales de enlace, las direcciones locales de sitio no se configuran automáticamente y deben asignarse a través de procesos de configuración de direcciones sin estado y con estado.

Aunque un Id. de subred depende de los 54 bits, se espera que los sitios conectados globalmente usen el mismo

5. DIRECCIONES ANYCAST [RFC 3513 - 2526]

Una dirección Anycast en IPv6 es asignada a más de una interfaz (generalmente localizadas en nodos diferentes), con la propiedad de que un paquete enviado a una dirección Anycast es enrutado hacia la interfaz mas *cercana* que tenga asignada esa dirección Anycast, la definición de cual es la interfaz mas cercana depende de la apreciación de distancia del protocolo de enrutamiento.

Las direcciones Anycast son asignadas del espacio de direccionamiento de las direcciones Unicast, por lo tanto las direcciones Anycast y Unicast son sintácticamente indistinguibles. Cuando una dirección Unicast es asignada a más de una interfaz, esta dirección se convierte automáticamente en una dirección Anycast. Los nodos a los cuales se les asigna una dirección Anycast deben configurarse para conocer que son y como se procesan las direcciones Anycast.

Para la correcta asignación de direcciones Anycast, se debe definir un prefijo de gran extensión P, el cual identifica la región topológica que reúne a todas las interfaces que pertenecen a la dirección Anycast. Dentro de la región identificada por P, cada miembro del grupo Anycast es identificado como una

entrada separada en el sistema de enrutamiento. Fuera de la región identificada por P, la dirección Anycast debe ser agregada en el anuncio de asignación de ruta para el prefijo P.

Se espera que las direcciones Anycast sean usadas para identificar un grupo de routers que pertenecen a una organización que proporcione servicios de Internet (ISP), con el fin de forzar que el enrutamiento hacia un determinado ISP no se haga limitando el acceso por un solo router. Tales direcciones pueden tambien ser usadas como direcciones intermedias IPv6 en el encabezado de extensión de Enrutamiento.

A su vez una dirección Anycast puede ser usada para identificar un grupo de routers *atados* a una subred en particular, o el grupo de routers que provean la entrada a un dominio particular de enrutamiento, por ejemplo para que un host pueda acceder a un servidor de una colección de servidores identificados con una dirección Anycast, los cuales ofrezcan un servicio muy conocido. Todo lo anterior evitando la configuración manual de cada servidor de la lista, por definición del Anycast sólo el mas cercano de los servidores proveerá el servicio.

Actualmente existe poca experiencia en el uso de Anycast de manera extendida, su uso arbitrario en Internet y los consecuentes riesgos y complicaciones que ha traído un uso inadecuado de las mismas, han impulsado a la imposición de las siguientes restricciones para las direcciones IPv6:

- Una dirección Anycast no debe usarse como dirección de origen de un paquete IPv6.
- Una dirección Anycast no debe asignarse a hosts IPv6, es decir solo deben ser asignadas a routers IPv6.

Se pretende que las anteriores restricciones permanezcan vigentes solo mientras se adquiere la suficiente experiencia y práctica en el manejo de las direcciones Anycast.

5.1 DIRECCIONES ANYCAST REQUERIDAS

La dirección Anycast *Subnet – Router* (o dirección asignada a los routers atados a una subred) ya ha sido definida y posee el siguiente formato:

n bits	128 – n bits
Prefijo de la subred	**0000……..….0000**

Figura 42 Formato de una dirección Anycast

El prefijo de subred en una dirección Anycast es el prefijo que identifica a un enlace específico. Este tipo de dirección Anycast es sintácticamente igual a una dirección Unicast asignada a una interfaz perteneciente a un enlace, con el campo de identificador de interfaz en cero.

Paquetes enviados a una dirección Anycast Subnet – Router será entregado a un router en la subred. Todos los routers deben tener soporte para las direcciones Subnet – Router, para las subredes para los que ellos tengan una interfaz asignada. En IPv4 una dirección con un identificador de host igual a cero, es asignada como dirección de subred y no puede ser usada por ningún host de esta red, en esta caso se acostumbra asignar la primera dirección del espacio de host al router.

6. DIRECCIONES MULTICAST [RFC 3513 - 2375]

Una dirección Multicast IPv6 es un identificador para un grupo de nodos. Un nodo puede pertenecer a varios grupos Multicast. Una dirección Multicast tiene el siguiente formato:

8 bits	4 bits	4 bits	112 bits
11111111	**Banderas**	**Alcance**	**Id. de Grupo**

Figura 43 Formato de una dirección Multicast

Donde:

- **11111111:** todas las direcciones Multicast comienzan con esta cifra.
- **Banderas:** es un grupo de cuatro bits (**0 0 0 T**). Los 3 bits de orden mayor son reservados para usos futuros y deben ser inicializados en cero. El cuarto bit T con un valor de T = 0 indica que esa dirección se encuentra asignada permanentemente por la IANA, cuando T = 1 indica una dirección no asignada permanentemente o dirección Multicast transitoria.
- **Alcance:** sus 4 bits son usados para limitar el alcance de un grupo Multicast. Los valores en hexadecimal son:

VALOR	ASIGNACIÓN
0	Reservado
1	Alcance de interfaz local
2	Alcance de enlace local
3	Reservado
4	Alcance de administración local

5	Alcance de sitio local
6	No asignado
7	No asignado
8	Alcance de organización local
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Alcance global
F	Reservado

Tabla 9 Valores del campo Alcance en una dirección Multicast

El alcance de interfaz local abarca solo a una simple interfaz en un nodo, y es muy útil para el retorno de una transmisión Multicast. El alcance de enlace local y de sitio local, abarca la misma región topológica que el alcance de las direcciones Unicast de enlace local y de sitio local respectivamente. El alcance de administración local es el alcance más pequeño que debe ser configurado por un administrador. El alcance de organización local comprende múltiples sitios pertenecientes a una misma organización. Los alcances no asignados están disponibles para que administradores puedan definir nuevas regiones Multicast.

- **Id. de grupo:** identifica al grupo Multicast, puede ser temporal o permanente dentro del alcance dado.

El significado de una dirección Multicast asignada permanentemente es independiente del valor del Alcance. Por ejemplo si al grupo de universidades pertenecientes a la red RENATA se les asigna una dirección Multicast permanente con un identificador de grupo de 101 (hexadecimal), entonces:

- FF0**1**:0:0:0:0:0:0:101 significa que todas las universidades en la misma interfaz son el remitente.

- FF0**2**:0:0:0:0:0:0:101 significa que todas las universidades en este enlace son el remitente.

- FF0**5**:0:0:0:0:0:0:101 significa que todas las universidades en este sitio son el remitente.

- FF0**E**:0:0:0:0:0:0:101 significa que todas las universidades en Internet son el remitente.

Las direcciones Multicast no deben ser usadas como dirección origen para paquetes IPv6 o incluidas en un encabezado de Enrutamiento.Los routers no deben reenviar ningún paquete Multicast más allá del alcance indicado en el campo de alcance en la dirección de destino Multicast.

Los nodos no deben originar un paquete a una dirección Multicast cuyo campo de alcance contenga el valor reservado de 0; si alguno de estos paquetes es recibido, este debe ser detenido sin generar mensaje de aviso alguno. Los nodos no deben originar un paquete a una dirección Multicast cuyo campo de alcance contenga el valor reservado F; si alguno de estos paquetes es enviado o recibido, debe ser tratado igual que un paquete con dirección Multicast con un campo de alcance global E.

6.1 DIRECCIONES MULTICAST PREDEFINIDAS

El grupo de direcciones **FF0X::** para X = 0,1,2,3,4,5,6,7,8,9,A ,B ,C ,D ,E están reservadas y nunca deben ser asignadas a un grupo Multicast.

Las siguientes direcciones Multicast se denominan *All Nodes,* identifican al grupo de todos los nodos IPv6, con un Alcance de nodo local (1) y de enlace local (2) respectivamente:

FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

Las siguientes direcciones Multicast se denominan *All Routers,* identifican al grupo de todos los enrutadores IPv6, con un alcance de nodo local (1), de enlace local (2) y de sitio local (5) respectivamente:

FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:2

Cuando un nodo IPv6 (Unicast o Anycast) solicita una dirección Multicast, esta dirección se denomina *Solicited – Node Address* y es hallada teniendo en cuenta los 24 bits de menor orden de la dirección IPv6 del nodo y el prefijo **FF02:0:0:0:0:1:FF00::** / **104.** Por ejemplo la solicitud de una dirección Multicast correspondiente a una dirección IPv6 **4037::01:800:200E:8C6C** es **FF02::1:FF0E:8C6C**.

7. DIRECCIONES IPV6 PARA UN HOST

Por defecto un host IPv4 con una sola tarjeta de red tiene una única dirección IPv4 asignada a la tarjeta. Sin embargo, un host IPv6 suele tener varias direcciones IPv6, incluso con una sola interfaz.

De un host IPv6 se requiere que reconozca las siguientes direcciones mientras se identifican a si mismos:

- Su dirección de Enlace Local para cada interfaz.
- Alguna dirección adicional Unicast y Anycast que haya sido configurada para las interfaces de un nodo (manualmente o automáticamente).
- Su dirección de retorno.
- Su dirección Multicast *All Nodes* definidas en la sección 3.6.1.
- La dirección *Solicited – Node* para cada una de sus direcciones Unicast y Anycast
- Su dirección Multicast para todos los grupos a los que pertenezca.

Además, si el nodo es un router se requiere que reconozca todas las direcciones que a un host se le exigen reconocer, más las siguientes direcciones que lo identifican:

- Las direcciones Anycast *Subnet – router* de cada subred para la cual está configurado para operar como router.
- Todas las otras direcciones Anycast con que el router ha sido configurado.
- Su dirección Multicast *All Routers* definidas en la sección 6.1 – Anexo B.

Los únicos prefijos de direcciones que deben ser predefinidos en una implementación son los siguientes:

- La dirección no especificada.
- La dirección de retorno.
- El prefijo Multicast 11111111 (FF).
- Los prefijos locales de enlace y locales de sitio.
- Las direcciones Multicast predefinidas.
- Los prefijos compatibles con IPv4.

Las aplicaciones deben asumir que todas las direcciones diferentes a las anteriores son Unicast a menos que se encuentren configuradas específicamente, por ejemplo las direcciones Anycast.

8. IPV6 Y EL SERVIDOR DE NOMBRES DE DOMINIO DNS

El soporte actual para el almacenamiento de direcciones Internet en el Sistema de Nombres de Dominio DNS no puede ser fácilmente extendido para dar soporte a direcciones IPv6 ya que las aplicaciones asumen que las consultas de dirección retornan solamente direcciones IPv4 de 32 bits, razón por la cual se definieron las siguientes extensiones:

8.1 REGISTRO DE RECURSOS AAAA [RFC 1886]

El tipo de registro de recurso AAAA (derivado del registro A de IPv4) es un nuevo registro específico a la clase Internet que almacena una sola dirección IPv6. Una dirección IPv6 de 128 bits se codifica en la parte de datos de un

registro de recurso AAAA en orden byte de red (primero el byte de mayor orden).

Una consulta AAAA para un nombre de dominio especificado en la clase Internet retorna todos los registros de recurso AAAA asociados en la sección de respuesta de una contestación. Una consulta de tipo AAAA no lleva a cabo procesamiento de sección adicional.

El manejo de registros AAAA es elemental (de igual manera a como IPv4 utiliza los registros A), se asocia el nombre de la máquina con la dirección IPv6 de la siguiente manera:

<NOMBREMAQUINA> IN AAAA <DIRECCIÓNIPV6MAQUINA>

Aunque el uso de los registros AAAA es relativamente sencillo, existía un problema previsible, ¿Qué pasará cuando se cambie de proveedor de servicios de Internet y los prefijos de red tambien cambien? La idea de actualizar todos y cada uno de los registros se tornaba tediosa, en gran parte por el formato en general de las direcciones IPv6. Surgió entonces una propuesta que permitiera de forma eficaz realizar las traducciones, además de ser un sistema dinámico de traducción, dicha propuesta son los registros A6 [RFC 2874].

En el [RFC 3363] es recomendado utilizar los registros AAAA hasta tanto se pruebe y estudie exhaustivamente el uso de registros A6.

8.2 REGISTRO DE RECURSOS A6

Los registros A6 han sido definidos para permitir la concordancia entre un nombre de dominio y una dirección IPv6. Esta forma de almacenamiento tiene

como principal característica agilizar los procesos de reenumeración en la red y el de multi – proveedor. Los registros A6 permiten que una consulta se haga en forma recursiva, de tal forma en que la respuesta a una petición no sea proporcionada por un solo servidor, sino que la consulta sea dividida en subconsultas y así, recursivamente ir solicitando las distintas respuestas a los servidores correspondientes.

Las direcciones IPv6 son almacenadas en uno o varios registros A6. Un simple registro A6 puede incluir una dirección IPv6, o una porción de una dirección e información que llevan uno o más prefijos. La información del prefijo comprende una longitud de prefijo y un nombre DNS que es a su vez *poseedor* de uno o más registros A6 que definen el prefijo o prefijos que son necesarios para formar una o varias direcciones IPv6. Cuando la longitud de prefijo es cero, ningún nombre de DNS es presentado y todos los bits de la dirección son considerados significantes.

Una aplicación que busque una dirección IPv6 generalmente originará una petición al DNS para acceder a varios registros A6, y múltiples direcciones IPv6 pueden ser retornadas aun cuando el nombre requerido solo poseía un registro A6.

Un registro A6 posee dos o tres campos y tiene el siguiente formato:

1 byte	0 a 16 bytes	0 a 255bytes
Long. Prefijo	**Sufijo de la dirección**	**Id. De Interfaz**

Figura 44 Formato de registro A6

Donde:

- **Longitud del prefijo:** la longitud del prefijo de la dirección IPv6 debe ser codificada en estos 8 bits, es un entero sin signo entre 0 y 128.
- **Sufijo de la dirección:** codificado a nivel de red en el primer octeto de mayor orden. Debe haber en este campo exactamente un numero de bits igual a 128 bits menos la longitud del prefijo, con de 0 a 7 bits de relleno con el fin de hacer a este campo un número entero de bytes. Sí es necesario incluir bits de relleno, estos deben tener un valor de cero y ser ignorados al cargar el archivo en el destino.
- **Id. de interfaz:** el nombre del prefijo codificado, es un nombre de dominio. Debido a las especificaciones de dominio incluidos en el [RFC 1035], este nombre no debe ser comprimido.

El componente de nombre de dominio no estará presente si la longitud del prefijo es cero, así mismo, el componente del sufijo de dirección no estará presente si la longitud del prefijo es 128. Se sugiere que un registro A6 pueda ser usado como prefijo para otro registro A6, teniendo en cuenta que todo el grupo de bits del campo de Sufijo de Dirección deben estar fijados a cero.

Mientras que la idea de los registros AAAA es una simple adaptación del DNS IPv4, la idea de A6 es una revisión y puesta a punto del DNS para ser más genérico, y de ahí su complejidad, sin embargo la IETF ha declarado que los registros A6 y CNAME[43] son solo registros de uso experimental y por ahora solo los registros AAAA son un estándar. En el [RFC 3364] se encuentra una completa descripción comparativa de las ventajas y desventajas de cada tipo de registro.

[43] Formato definido en [RFC 2874], cuya característica principal es re-usar zonas de nombres de dominio en el caso de un cambio de proveedor.

8.2.1 REPRESENTACIÓN TEXTUAL DE UN REGISTRO A6

La representación textual de un registro A6 en un archivo de zona comprende dos o tres campos separados por un espacio en blanco:

- Una longitud de prefijo, representada por un numero decimal entre 0 y 128.
- El sufijo de la dirección, es la parte de la dirección que se resuelve con este registro A6
- Un nombre de dominio, sí la longitud del prefijo es diferente de cero.

El nombre de dominio debe ser retirado sí la longitud del prefijo es cero. La dirección IPv6 debe ser retirada sí la longitud del prefijo es 128.

Nombre a resolver A6 <Longitud del prefijo> <Sufijo de la Dirección> <Nombre>

Por ejemplo, supongamos que queremos resolver la dirección cormoran.ipv6.uis.edu.co. En el archivo de zona ipv6.uis.edu.co, podemos encontrar por ejemplo la siguiente declaración:

cormoran IN A6 56 :22 prueba.subdom.ipv6.uis.edu.co

Esta declaración se interpreta así: este dominio sólo resuelve 72 bits (128-56), y esa resolución se traduce a ::22, mientras que los 56 bits restantes serán resueltos en el registro prueba.subdom.ipv6.uis.edu.co. Ahora veamos cómo debe ser la declaración de prueba.subdom.ipv6.uis.edu.co, en el dominio subdom.ipv6.uis.edu.co:

prueba.subdom.ipv6.uis.edu.co IN A6 0 3ffe:8070:1019:200::

Lo que significa que los 56 bits que faltaban se traducen a 3ffe:8070:1019:200:: y que ya no hay nada que resolver, lo denota el 0 del campo Longitud del prefijo.

La característica principal de estas consultas es la recursividad evidenciada en que ambas consultas son hechas por el mismo cliente, sólo que a servidores distintos, algo así como una consulta dividida en dos subconsultas. Como resultado obtenemos dos respuestas referidas a la misma dirección solo que en partes diferentes de la misma, ahora le corresponde al cliente reensamblar las respuestas para conseguir la traducción correcta.

8.3 EL DOMINIO IP6.INT

Un dominio especial es definido para buscar un registro dada una dirección. La intención de este dominio es para proporcionar una manera de relacionar una dirección IPv6 a un nombre de host, aunque puede ser usado para otros propósitos también. El dominio está enraizado a IP6.INT.

Una dirección IPv6 se representa como un nombre en el dominio IP6.INT por una secuencia de nibbles (un nibble esta formado por 4 bits) separados por puntos con el sufijo ".IP6.INT". La secuencia de nibbles se codifican en orden inverso, es decir el nibble de menor orden se codifica primero, seguido por el siguiente nibble de menor orden y así sucesivamente. Cada nibble se representa por un dígito hexadecimal. Por ejemplo, el nombre de dominio de búsqueda inversa correspondiente a la dirección:

4321:0:1:2:3:4:567:89ab es:

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT.

9. CONFIGURACIÓN DE DIRECCIONES

El método usado en IPv6 para la auto-configuración de direcciones sin estado se denomina *Stateless Address Autoconfiguration* y se encuentra definido en [RFC 2462]. La autoconfiguración sin estado no requiere configuración manual de servidores, configuración mínima de routers y ninguna de servidores adicionales. El mecanismo sin estado permite que una máquina genere su propia dirección mediante una combinación de información disponible localmente y anunciada por los routers. Los routers anuncian prefijos que identifican la(s) subred(es) asociada(s) a un enlace y los hosts generan identificadores de interfaz que identifican unívocamente a una interfaz en una subred. La dirección se forma combinando ambos. Si no hay routers, una máquina tan sólo puede generar direcciones de enlace local. Sin embargo, las direcciones de enlace local son bastante para permitir la comunicación entre nodos conectados al mismo enlace.

En el modelo de configuración con estado, las máquinas obtienen direcciones de interfaz y/o información de configuración y parámetros de un servidor. Los servidores mantienen una base de datos que lleva un registro de qué direcciones han sido asignadas y a qué host. El protocolo de configuración con estado permite a los hosts obtener direcciones, información de configuración o ambas de un servidor. La configuración automática con estado y sin estado son complementarias. Por ejemplo, un host puede usar configuración sin estado para configurar sus direcciones y usar configuración con estado para obtener el resto de información.

9.1 STATELESS ADDRESS AUTOCONFIGURATION

La autoconfiguración se ejecuta sólo en enlaces con capacidad de multicast, y comienza cuando una interfaz con capacidad multicast se activa, por ejemplo, en el arranque. Los nodos (tanto hosts como routers) comienzan el proceso de

autoconfiguración generando una dirección de enlace local para la interfaz. Una dirección de enlace local se forma añadiendo el identificador de interfaz al prefijo del enlace local ya conocido.

Antes de que puedan asignarse direcciones de enlace local a una interfaz y sean usadas, un nodo debe intentar verificar que esta dirección *tentativa* no está ya en uso por otro nodo del enlace. Específicamente, envía un mensaje de Solicitud de Vecino conteniendo la dirección tentativa como el destino. Si otro nodo ya está usando esa dirección, devolverá un Anuncio de Vecino diciéndolo. Si otro nodo está intentando usar esa dirección, enviara una Solicitud de Vecino para el destino también. El número exacto de veces que se (re)transmite la Solicitud de Vecino y el tiempo de retraso entre solicitudes consecutivas es específico del enlace y puede ser fijado mediante la gestión del sistema.

Una vez que un nodo asegura que su dirección de enlace local tentativa es única, la asigna a la interfaz. En este momento, el nodo tiene conectividad a nivel IPv6 con los nodos vecinos. Los pasos restantes de la autoconfiguración son ejecutados sólo por los hosts.

La siguiente fase de la autoconfiguración implica obtener un Anuncio de Router o concluir que no hay routers alrededor. Si hay routers, enviarán un Anuncio de Router que especifica qué tipo de autoconfiguración debería hacer una máquina. Si no hay routers, debe invocarse la autoconfiguración con estado.

Los Anuncios de Routers también contienen cero o más opciones de Información de Prefijo que contienen información usada por la autoconfiguración de dirección sin estado para generar direcciones de enlace local y global. Debe notarse que los campos de la autoconfiguración con y sin estado en los Anuncios de Router son procesados independientemente uno del otro, pudiendo una máquina usar tanto autoconfiguración con estado como sin estado simultáneamente.

9.1.1 CREACIÓN DE DIRECCIONES LOCALES DE ENLACE

Un nodo forma una dirección de enlace local cuando una interfaz se activa. Un interfaz puede pasar a estar activado después de cualquiera de los siguientes eventos:

- La interfaz se inicializa en el momento arranque del sistema.
- La interfaz se re-inicializa después de un fallo temporal o después de ser temporalmente desactivado por la gestión del sistema.
- La interfaz se conecta a un enlace por primera vez.
- La interfaz se activa por la gestión del sistema después de ser administrativamente desactivado.

Una dirección de enlace local se forma precediendo el prefijo de enlace local FE80::0 al identificador del interfaz. Si el identificador del interfaz tiene una longitud de N bits, el identificador de la interfaz reemplaza los N bits 0 más a la derecha del prefijo de enlace local. Si el identificador de interfaz tiene más de 118 bits, la autoconfiguración falla y se requiere configuración manual. Note que los identificadores de interfaz serán típicamente de 64 bits y basados en identificadores EUI-64 como se describe en el Anexo B - sección 4.1.1.

9.1.2 CREACIÓN DE DIRECCIONES GLOBALES Y LOCALES

Las direcciones globales y locales a la instalación se forman añadiendo un identificador de interfaz a un prefijo de longitud apropiada. Los prefijos se obtienen de opciones de Información de Prefijo contenidas en Anuncios de Router. La creación de direcciones globales y locales a la instalación y la configuración de otros parámetros debería ser configurable localmente.

Solicitando Anuncios de Router

Los Anuncios de router se envían periódicamente a la dirección de multicast de todos los nodos (sección 6.1 – Anexo B). Para obtener anuncios rápidamente, las máquinas envían Solicitudes de Router, como se discute en [RFC 2461].

9.2 DHCPv6 [RFC 3315]

La configuración dinámica de direcciones IPv6 debe ser usada en caso que se haya encontrado una dirección duplicada o cuando no existen routers presentes. El protocolo DHCPv6 consiste de dos elementos:

- Un protocolo que envía información específica a cada host desde un servidor DHCPv6.
- Un mecanismo que permita la asignación direcciones de red y otros parámetros a host IPv6.

DHCPv6 está diseñado en un modelo cliente-servidor, que usa 6 mensajes *Request* y *Reply* (petición y respuesta) para la comunicación de los parámetros de configuración. Además se han definido *roles* que deben cumplir ciertos hosts para permitir el correcto funcionamiento DHCPv6:

- Cliente DHCPv6, es el nodo encargado de iniciar las solicitudes en un enlace para obtener los parámetros necesarios para la configuración.
- Servidor DHCPv6, es el nodo encargado de responder las solicitudes de los clientes para proveer los parámetros de configuración. El servidor puede o no estar en el mismo enlace que el cliente.

- Agente relevo DHCP, es un nodo que funciona como intermediario para enviar mensajes entre clientes y servidores DHCPv6, a diferencia del servidor, este nodo si debe estar obligatoriamente en el mismo enlace que el nodo cliente.

La comunicación entre agentes DHCPv6 usa las siguientes direcciones multicast:

- **FF02:0:0:0:0:0:1:2** grupo multicast de ámbito local para todos los agentes DHCPv6.
- **FF05:0:0:0:0:0:1:3** grupo multicast de ámbito de sitio para todos los servidores DHCPv6.
- **FF05:0:0:0:0:0:1:4** grupo multicast de ámbito de sitio para todos los agentes de relevo DHCPv6.

Todos los mensajes DHCPv6 intercambiados por los nodos poseen un formato semejante, el cual empieza con un campo Tipo de Mensaje (*Msg Type*), el cual indica la función específica. Además se encuentran las Extensiones, que sirven para especificar los parámetros de configuración tales como: direcciones IP, horarios de uso, DNS, directorio de agentes, un servidor de tiempo de red, parámetros TCP, autenticación cliente – servidor, entre otros.

ANEXO C. SOPORTE PARA LA MOVILIDAD EN IPV6[44]

Con IPv6 cada nodo móvil (MN) tendrá una dirección de *casa* (*Home Address* - HA), la cual será su dirección origen en su red. Esta dirección permanecerá invariable aunque el MN cambie de red. Los paquetes enviados al nodo móvil serán encaminados normalmente siempre y cuando se encuentre en su red de origen.

Cuando el nodo móvil pase a una red que no sea la de origen, el nodo obtendrá una nueva dirección de *invitado* (*Care of Address* – CoA). Con esto el nodo también podrá ser alcanzado a través de la CoA. A continuación el nodo móvil contactará el router de su red origen informándole cual es su CoA actual. De esta forma cuando un paquete sea enviado a su dirección de casa, el router sabrá que tendrá que reenviarlo con dirección de destino CoA al nodo móvil.

Este mecanismo funciona básicamente mediante el envío de un mensaje BU (*Binding Update*) por parte del nodo móvil, luego de cambiar de red. El BU asocia la CoA con la dirección de casa del nodo móvil durante un tiempo determinado administrativamente.

Cuando un nodo móvil se comunica con un nodo correspondiente (CN), el nodo móvil usa la dirección de invitado para enviar paquetes al CN. Por su parte, el CN envía los paquetes a la dirección de casa del nodo móvil, que serán interceptados por el router de casa y reenviados a la CoA del nodo móvil.

Tendríamos aquí un caso de ruta triangular, que aunque no sea problemático, si es ineficiente. Para resolver esto, MobileIPv6 [RFC 3775] presenta el concepto

[44] Anexo basado en [RFC 3775]

de optimización de ruta. Este mecanismo permite al nodo móvil avisar al CN que puede enviarle paquetes directamente a su CoA utilizando para ello mensajes BU.

1. CABECERAS ADICIONALES

MobileIPv6 logra la optimización de la ruta, utilizando las cabeceras de Opción de Destino (sección 2.4 – Anexo A). Esto permite enviar información de señalización en los mismos datos del paquete. Las nuevas opciones diseñadas para soportar movilidad son:

- **Home Address Option:** indica cual es la dirección de casa del nodo móvil cuando este se encuentra fuera de su red origen.

- **Binding Update Option:** sirve para crear, actualizar y eliminar entradas en las asociaciones que se mantienen entre el nodo móvil y su dirección de invitado. Un paquete con esta opción hará que se produzca una asociación en el CN o en el HA entre la dirección origen del paquete y la dirección contenida en el campo Home Address Option.

- **Binding Acknowledgement Option:** es enviada por el HA y por el CN como respuesta a los BU enviados por el nodo móvil.

- **Binding Request Option:** es enviada por el CN para solicitar al nodo móvil que refresque su entrada en la lista de asociaciones actual del nodo móvil.

2. SEGURIDAD EN MOBILEIPV6

Tanto los Binding Updates como los Binding Acknowledgements provocan un cambio de estado en los nodos, por lo que necesitan ser autenticados. MobileIPv6 usa la cabecera de autenticación AH (sección 2.8 – Anexo A) para evitar cualquier ataque.

Sin embargo la autenticación no es el único problema, el control en la autorización también debe ser establecido, la cual consiste en que el nodo cliente pueda alterar las asociaciones en la tabla de un nodo móvil (lo cual afecta las tablas de enrutamiento). Una forma posible de solucionar esto es utilizando IKE (Internet Key Exchange) junto a DNSSEC, asumiendo que tanto el nodo móvil como el CN utilizan la misma infraestructura de llave pública.

ANEXO D. SEGURIDAD EN IPV6 - IPSEC[45]

Acerca de la seguridad en IPv6, ya hemos tratado los encabezados de extensión AH (Autentificación) y ESP (Seguridad del Encapsulado de la Carga Útil), los cuales son necesarios para una completa implementación de IPv6. Las funciones de autentificación (AH) y cifrado (ESP) pueden ser usadas conjuntamente o de manera individual, todo depende de las necesidades de las aplicaciones de capas superiores.

1. ARQUITECTURA DE SEGURIDAD

IPsec está diseñado para proporcionar seguridad ínter-operable de alta calidad, basada en criptografía tanto para IPv4 como para IPv6. El conjunto de servicios de seguridad ofrecidos incluye: control de acceso, integridad sin conexión, autenticación del origen de los datos, protección anti-*replay* (una forma de integrabilidad parcial de la secuencia), confidencialidad (encriptación), y confidencialidad limitada del flujo de tráfico. Estos servicios se implementan en la capa IP, y ofrecen protección para este nivel y/o los niveles superiores.

Estos objetivos se llevan a cabo haciendo uso de dos protocolos de seguridad, la Cabecera de Autentificación (AH) y Carga de Seguridad Encapsulada (ESP), a través de procedimientos de manejo de claves criptográficas y protocolos. El conjunto de protocolos IPsec empleados en cualquier conexión, y la forma en que se emplean, serán determinados por la seguridad, y los requerimientos del sistema del usuario, aplicaciones y/o sitios u organizaciones.

[45] Anexo basado en [RFC 2401]

Cuando estos mecanismos se implementan correctamente y se ejecutan, no afectan negativamente a los usuarios, hosts, y otros componentes de Internet que no empleen estos mecanismos de seguridad para la protección de su tráfico.

Estos mecanismos están diseñados para ser independientes del algoritmo. Esta modularidad permite seleccionar diferentes conjuntos de algoritmos sin afectar a las otras partes de la implementación. Por ejemplo, grupos diferentes de usuarios pueden seleccionar grupos diferentes de algoritmos si se necesita.

Un conjunto de algoritmos se especifica para facilitar la interoperabilidad en la Internet global. El uso de estos algoritmos, en conjunto con la protección del tráfico de IPsec, y los protocolos de manejo de claves, están constituidos para permitir el desarrollo de aplicaciones, sistemas y tecnología de seguridad criptográfica de alta calidad en la capa IP.

El grupo de protocolos IPsec y demás algoritmos asociados permiten proporcionar seguridad de alta calidad para el flujo de tráfico de Internet. Sin embargo, la seguridad ofrecida por estos protocolos depende en última instancia de la calidad de su implementación, que esta fuera del alcance de estos estándares. Además, la seguridad de un sistema informático o en una red es una función de muchos factores. IPsec solo es una parte de un sistema global de seguridad.

Una implementación de IPsec funciona en un host o en un *security gateway* (SG[46]), proporcionando protección al tráfico IP. La protección ofrecida se basa en requerimientos definidos en el establecimiento de una Base de Datos de Políticas de Seguridad (SPD) y mantenidas por un usuario o administrador del sistema o por una aplicación funcionando dentro de las restricciones ya

[46] Sistema intermedio que implementa los protocolos IPsec (router o firewall)

establecidas. En general, los paquetes se seleccionan para uno de tres modos de procesamiento basados en IP y la información de la cabecera de la capa de transporte comparándolas con las entradas en la SPD. Cada paquete es un servicio de seguridad, descartado, desviado, o procesado, de acuerdo con las políticas aplicables en la base de datos identificadas por los selectores.

2. FUNCIONAMIENTO DE IPSEC

IPsec se puede utilizar para proteger una o más *trayectorias* entre un par de hosts, o entre un par de security gateway, o entre un security gateway y un host. IPsec utiliza las cabeceras AH y ESP de la siguiente forma:

- La Cabecera de Autentificación (AH): Proporciona integridad sin conexión, autentificación del origen de datos, y un servicio opcional de protección anti-*replay*.
- La Carga de Seguridad Encapsulada (ESP): Puede proporcionar confidencialidad (encriptación), y confidencialidad limitada de flujo de tráfico. También puede proporcionar integridad sin conexión, autentificación del origen de datos, y un servicio de protección anti-*replay*. (Uno u otro de estos servicios de seguridad debe ser aplicado siempre que se use ESP.)
- AH y ESP son instrumentos para el control de acceso, basados en la distribución de claves criptográficas y en el manejo de flujo de tráfico concerniente a estos protocolos de seguridad.

Estos protocolos pueden aplicarse solos o en conjunto con otros para proporcionar un conjunto de servicios de seguridad en IPv4 e IPv6. Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En modo transporte los protocolos proporcionan protección sobre todo a los protocolos de

capa superiores; en modo túnel, los protocolos son aplicados a paquetes (a los que se hizo un túnel a través de IP).

IPsec permite que el usuario (o el administrador de sistema) controle la "granularidad" (grado de modularidad de un sistema, cuanto mayor sea la granularidad, más personalizable o flexible será el sistema) en la cual un servicio de seguridad es ofrecido. Por ejemplo, uno puede crear un único túnel encriptado y llevar todo el tráfico entre dos security gateway, o se puede crear un túnel encriptado separado para cada conexión TCP entre cada par de hosts que se comunican a través de un gateway. La gestión de IPsec debe incorporar facilidades para especificar:

- Que servicios de seguridad se utilizan y en que combinaciones.
- La granularidad con la que se debe aplicar una determinada protección de seguridad.
- Los algoritmos usados para efectuar la seguridad basada en criptografía.

Debido a que estos servicios de seguridad usan valores secretos compartidos (claves criptográficas), IPsec se basa en un conjunto de mecanismos separados para que pongan estas claves en su sitio (las claves se utilizan para autentificación / integrabilidad y los servicios de encriptación). Este documento requiere soporte para la distribución manual y automática de claves. Específica un acercamiento basado en clave pública (IKE - MSST97, Orm97, HC98) para la gestión automática de claves, pero otras técnicas de distribución automatizada de claves pueden ser utilizadas. Por ejemplo, los sistemas basados en KDC tales como *Kerberos* y otros sistemas de clave pública tales como SKIP podrían ser empleados.

Hay varias formas en las cuales se puede implementar IPsec, en un host o en conjunto con un router o un firewall (creando un security gateway). Algunos ejemplos frecuentes son:

1. Integrar IPsec en una implementación nativa IP. Requiere tener acceso al código fuente IP, y se puede aplicar tanto a host como a un security gateway.
2. Puesto en la Pila (BITS), IPsec se implementa "por debajo" de una implementación existente de una pila IP, entre el IP nativo y los drivers locales de la red. El acceso al código fuente para la pila IP no es requerido en este contexto, este contexto es apropiado para los sistemas antiguos. Este método, cuando se adopta, se emplea generalmente en hosts.
3. El uso de un procesador criptográfico externo es una característica de diseño común de los sistemas de seguridad de red usados por los militares, y en algunos sistemas comerciales. A estos sistemas algunas veces se los refiere como implementaciones Puesto en el cable (BITW). Tales implementaciones se pueden diseñar para asistir a un host o un gateway (o a ambos). El dispositivo BITW generalmente tiene una IP direccionable. Cuando asiste a un único host, puede resultar análogo a una implementación BITS, pero en un router o en un firewall debe funcionar como un security gateway.

3. ASOCIACIONES DE SEGURIDAD – SA

Esta sección define los requisitos para administrar Asociaciones de Seguridad (SAs) para toda implementación IPv6 y para implementaciones IPv4 que implemente AH, ESP, o ambos. El concepto de Asociación de Seguridad (SA) es fundamental para IPsec. AH y ESP hacen uso de SAs y una función importante

de IKE es el establecimiento y el mantenimiento de SAs. Toda implementación de AH o ESP debe soportar el concepto de SA como se describe a continuación.

3.1 DEFINICIONES Y ÁMBITO

Una Asociación de Seguridad (SA) es una conexión unidireccional (simplex) que ofrece servicios de seguridad al tráfico transportado por este. Los servicios de seguridad ofrecidos en una SA son usados por AH o ESP, pero no por ambos. Si ambos (AH y ESP) se aplican a un flujo de tráfico, dos (o más) SAs se crearán para generar la protección de flujo de tráfico. Para asegurar la comunicación bidireccional entre dos hosts, o entre dos security gateway, se requieren dos Asociaciones de Seguridad (uno en cada sentido).

Una SA es identificada unívocamente por un trío que consiste en: un Índice de Parámetros de Seguridad (SPI), una Dirección IP de Destino, y un identificador de protocolo de seguridad (AH o ESP). En principio, la Dirección de Destino puede ser una dirección unicast, una dirección de difusión IP, o una dirección de grupo multicast. Sin embargo, los mecanismos IPsec para la gestión de SA se definen solamente para unicast. Por lo tanto, publicaciones siguientes, describirán el contexto de comunicaciones punto-a-punto, aun cuando el concepto también es aplicable a conexiones punto-a-multipuntos.

Según lo descrito con anterioridad, se definen dos tipos de SAs: modo transporte y modo túnel. Una SA en modo trasporte es una SA entre dos hosts. En IPv4, una cabecera de protocolo de seguridad en modo transporte aparece inmediatamente después de la cabecera IP y de algunas opciones, y antes que cualquier protocolo de capas superior (por ejemplo, TCP o UDP). En IPv6 las cabeceras del protocolo de seguridad se situarán después de la cabecera IP y de extensiones pero deben aparecer antes o después de la cabecera de opciones de dirección y antes de los protocolos de capas superiores. En el caso

de ESP, una SA en modo transporte proporciona servicios de seguridad solamente para los protocolos de las capas superiores, no para la cabecera IP o cualquier cabecera de extensión precedente a la cabecera ESP. En el caso de AH la protección se extiende a las partes seleccionadas de la cabecera IP, a las partes seleccionadas de las cabeceras de extensión y a las opciones seleccionadas (contenidas en la cabecera de IPv4, la cabecera de extensión Salto-por-Salto de IPv6, o la cabecera de extensión de destino de IPv6).

Una SA en modo túnel es en esencia una SA aplicada a un túnel IP. Siempre que un extremo de la SA sea un security gateway, la SA debe estar en modo túnel. Una SA entre dos security gateway, es siempre una SA en modo túnel, al igual que una SA entre un host y un security gateway. Nótese que para el caso donde el tráfico es destinado para el security gateway, por ejemplo, comandos SNMP, la security gateway actúa como un host y el modo trasporte es permitido. Pero en este caso, la security gateway, no esta actuando como un gateway, es decir, no esta trasportando tráfico. Dos host pueden establecer una SA en modo túnel entre ellos. El requisito para cualquier SA que involucre a una security gateway (trasporte de tráfico) es un túnel SA debido a la necesidad de evitar problemas potenciales con la fragmentación y reensamblaje de paquetes IPsec y en circunstancias donde existan múltiples trayectorias (por ejemplo vía diferentes security gateway) para el mismo destino detrás de un security gateway.

Para una SA en modo túnel, hay una cabecera IP "externa" que especifica el destinatario del proceso IPsec, más una cabecera IP "interna" que especifica el último destinatario (aparente) del paquete. La cabecera del protocolo de seguridad aparece después de otras cabeceras IP externas y antes de las cabeceras IP internas. Si se emplea AH en modo túnel, a otras partes de la cabecera IP se les ofrecen protección así como también a todo el paquete IP al cual se le hizo el túnel (es decir, toda la cabecera IP interna es protegida, como así también protocolos de capas superiores). Si se emplea ESP, la protección es

proporcionada únicamente al paquete IP al cual se le hizo el túnel (al paquete entunelizado), no a las cabeceras externas.

Resumiendo:

a. Un host debe soportar modo trasporte y túnel.
b. Una security gateway solo debe soportar el modo túnel. Si soporta modo trasporte este debería ser usado únicamente cuando la security gateway actúa como host, por ejemplo para la administración de la red.

3.2 FUNCIONALIDAD DE LAS ASOCIACIONES DE SEGURIDAD

El conjunto de servicios de seguridad ofrecido por una SA depende del protocolo de seguridad seleccionado, del modo de la SA, de los extremos de la SA, y de la elección de los servicios opcionales seleccionados dentro del protocolo. Por ejemplo, AH proporciona autentificación del origen de los datos e integridad sin conexión para datagramas IP (a partir de ahora equivale a "autentificación"). La precisión de estos servicios de autentificación estará en función de la granularidad de la SA con la que se emplea AH.

AH ofrece además un servicio de anti-replay (integridad parcial de la secuencia) según el deseo del receptor, esto ayudará a prevenir ataques contra denegación de servicios. AH es un protocolo apropiado para emplearse cuando la confidencialidad no es requerida (o no se permite, por ejemplo, debido a las restricciones gubernamentales en el uso criptográfico). AH también proporciona autentificación para las partes seleccionadas de la cabecera IP, que puede ser necesaria en algunos contextos. Por ejemplo, si la integridad de una opción de IPv4 o una cabecera de extensión de IPv6 se debe proteger en el camino entre el emisor y el receptor, AH puede proporcionar este servicio (a excepción de las partes mutables no predecibles de la cabecera IP).

ESP proporciona de forma opcional confidencialidad para el tráfico. (La robustez del servicio de confidencialidad depende en parte, del algoritmo de encriptación utilizado). ESP también proporciona de forma opcional, autenticación como en el caso anterior. Si la autentificación es negociada por una SA ESP, el receptor también puede elegir implementar el servicio de anti-replay con las mismas características que el servicio de anti-replay de AH. La autentificación ofrecida por ESP abarca menos que la ofrecida por AH, es decir las cabeceras que quedan por fuera de la cabecera ESP no están protegidas. Si solo los protocolos de capas superiores necesitan ser autentificados, entonces la autentificación de ESP es una elección apropiada y es más eficiente en tamaño que usar ESP encapsulado con AH. Note que aunque la confidencialidad y la autenticación son opcionales, no se pueden omitir ambas, al menos una debe ser escogida.

Si se elige el servicio de confidencialidad, entonces una SA ESP (en modo túnel) entre dos security gateway pueden ofrecer confidencialidad parcial al flujo de tráfico. El uso del modo túnel permite encriptar las cabeceras IP internas, ocultando las identidades del origen del tráfico y del (último) destino. También, se puede usar el relleno en la carga útil (*payload padding*) de ESP para ocultar el tamaño de los paquetes, consiguiendo ocultar las características externas del tráfico. Similares servicios de confidencialidad del flujo de tráfico pueden ser ofrecidos cuando un usuario móvil está asignado a una dirección IP dinámica en un contexto de *dial-up* (conexión por línea conmutada), y establecer una SA ESP (en modo túnel) en un firewall corporativo (actuando como un security gateway).

4. BASES DE DATOS DE ASOCIACIONES DE SEGURIDAD - SAD

Muchos de los detalles relacionados al procesamiento de tráfico IP en una implementación IPsec son en gran parte tema local, no sujetos a estandarización. Sin embargo algunos aspectos externos del proceso deben ser estandarizados para asegurar interoperabilidad y proporcionar una capacidad de gestión mínima

que es esencial para el uso productivo de IPsec. Esta sección describe un modelo general para procesar el tráfico IP referente a asociaciones de seguridad, el soporte de esta interoperabilidad y el funcionamiento global. El modelo descrito debajo es nominal; las implementaciones obtenidas no necesitan igualar los detalles de este modelo según lo presentado, pero el comportamiento externo de tales implementaciones debe ser manejado por las características externas observadas de este modelo.

Hay 2 bases de datos nominales en este modelo: la Base de Datos de Políticas de Seguridad (SPD) y la Base de Datos de Asociaciones de seguridad (SAD).
SPD especifica las políticas que determinan el tratamiento de todo el tráfico IP entrante o saliente en un host, security gateway, o en implementaciones IPsec BITS o BITW.

SAD contiene los parámetros que se asocian con cada SA (activa). Esta sección también define el concepto de Selector, que es un conjunto de campos con valores de protocolos de capas superiores y de la capa IP que son usados por la SPD para asignar el tráfico a una política, es decir, a una SA (o grupo de SA).

Cada interfaz para la cual se habilite IPsec normalmente requiere, entradas y salidas de la base de datos separadas (SAD y SPD), debido a que la direccionalidad de varios de los campos son usados como selectores. Típicamente hay solo una interfaz, para un host o security gateway. Observe que un security gateway podría tener 2 interfaces, pero una red corporativa interna, usualmente no tendría habilitado IPsec y tan sólo un par de SADs y un par de SPDs serían necesarios. Por otra parte, si un host tiene múltiples interfaces o un security gateway tiene múltiples interfaces externas, puede que sea necesario tener una SAD y una SPD separadas para cada interfase.

4.1 BASE DE DATOS DE POLÍTICAS DE SEGURIDAD - SPD

En última instancia, una SA es generada por la gestión usada para implementar una política de seguridad en el ambiente IPsec. De esta manera un elemento esencial del proceso de la SA es una SPD subyacente que especifica qué servicios deben ser ofrecidos a los datagramas IP y de qué forma. La forma de la base de datos y su interfaz están fuera del alcance de esta especificación. Sin embargo, esta sección especifica ciertas funciones mínimas de gestión que deben ser proporcionadas, para permitir que un usuario o administrador del sistema controle cómo se aplica IPsec al tráfico enviado o recibido por un host o una transmisión a un security gateway.

El SPD se debe consultar durante todo el procesamiento del tráfico (entrante y saliente), incluyendo tráfico no IPsec. Para soportar esto, la SPD requiere entradas distintas para el tráfico de entrada y de salida. Uno puede pensar en esto como SPDs separadas (una de entrada y otra de salida). Una SPD nominal separada se debe proporcionar para cada interfaz IPsec habilitada.

Una SPD debe diferenciar entre el tráfico al que debe ofrecer protección IPsec de al que le esta permitido evitar IPsec. Esto implica que la protección IPsec a ser empleada debe estar presente tanto en el receptor como en el emisor. Para cualquier datagrama de entrada o de salida, hay tres opciones de procesamiento posibles: descartar, evitar IPsec (no IPsec), y que se aplique IPsec. La primera opción se refiere al tráfico que no se permite salir del host, atravesar una security gateway, o que se entregue a una aplicación. La segunda opción se refiere al tráfico que se le permite pasar sin la protección de IPsec. La tercera opción se refiere al tráfico que es protección producida por IPsec, y para tal tráfico la SPD debe especificar los servicios de seguridad que se proporcionarán, los protocolos que se emplearán, los algoritmos que se utilizarán, etc.

Para cada implementación IPsec, debe haber una interfaz administrativa que permita a un usuario o administrador del sistema manejar la SPD. Específicamente, cada paquete de entrada o de salida esta sujeto al procesamiento de IPsec, SPD debe especificar qué acción será tomada en cada caso. La interfaz administrativa debe permitir que el usuario (o el administrador del sistema) especifique que proceso de seguridad a de ser aplicado a cualquier paquete entrante o saliente del sistema, o a un paquete por paquete básico. (En una implementación IPsec el host utiliza una interfaz socket, la SPD puede no necesitar ser consultado sobre bases de paquetes, pero el efecto sigue siendo igual.) La interfaz de gestión para el SPD debe permitir la creación de entradas consistentes con los selectores, y debe soportar el ordenamiento (total) de esas entradas. Se espera que con el uso de comodines en varios campos del selector, y puesto que todos los paquetes en una sola conexión UDP o TCP tenderán correspondencia con una sola entrada SPD, este requisito no impondrá un nivel irracionalmente detallado de la especificación de SPD. Los selectores son análogos a los que se encuentran en un firewall o en un filtrado de router los cuáles son actualmente manejados de esa forma.

En un sistema host, las aplicaciones se pueden permitir seleccionar que proceso de seguridad debe ser aplicado al tráfico que generan y consumen. (Los medios para señalar tales peticiones para la implementación IPsec están fuera del alcance de este estándar.) Sin embargo, el administrador de sistema DEBE poder especificar si una aplicación puede o no reemplazar la política del sistema (por defecto). Observe que la aplicación especificó políticas que pueden satisfacer requisitos del sistema, de modo que el sistema puede no necesitar un proceso IPsec adicional que procese más allá de este para resolver los requisitos de una aplicación. La forma de la interfaz administrativa no es especificada por este documento y puede diferir entre un host y un security gateway, y en interior del host la interfaz puede diferir entre socket-base o implementación BITS. Sin embargo, este documento especifica un conjunto de estándares de SPD, elemento que toda implementación de IPsec debe soportar.

El SPD contiene una lista ordenada de políticas de entrada. Cada política de entrada es introducida por uno o más selectores que definen el conjunto de tráfico IP comprendido por esta política de entrada. Estos definen la granularidad de las políticas o SAs. Cada entrada incluye un indicador para el tráfico coincidente con esta política, si será desviado, desechado, o procesado por IPsec. Si el procesamiento IPsec es aplicado, la entrada incluirá una especificación de SA (o grupo de SA), listado de Protocolos IPsec, los modos, y algoritmos que se emplearán, y incluirán cualquier requisito relacionado.

4.2 SELECTORES

Una SA (o grupo de SA) puede tener mayor o menor modularidad dependiendo de los selectores usados para definir el grupo de tráfico para la SA. Por ejemplo todo el tráfico entre dos host puede ser trasportado por una SA simple, y ofrecer un conjunto uniforme de servicios de seguridad. Alternativamente, el tráfico entre un par de host puede ser extendido a múltiples SAs, dependiendo de la aplicación donde será usada (definido por el campos Siguiente Protocolo y el Puerto), cuando diferentes servicios de seguridad se ofrecen por diferentes SAs. Similarmente, todo el tráfico entre un par de security gateway puede ser trasportado por una SA simple, o una SA podría ser asignada para cada par de host que se comunican. Los siguientes parámetros del selector deben ser soportados por la gestión de SA para facilitar el control de la granularidad de SA.

- Dirección IP de Destino (IPv4 o IPv6)
- Dirección IP de Origen (IPv4 o IPv6)
- Nombre (de host, security gateway o ID de usuario)
- Nivel de sensibilidad de los datos (Requerido por los sistemas que proporcionan información de flujo de seguridad [RFC 2401])
  Protocolo de la Capa de Trasporte
- Puertos de Origen y Destino (por ejemplo, puertos TCP o UDP)

Nótese que en el caso de recibir un paquete con una cabecera ESP, por ejemplo en un security gateway o en una implementación BITW, el protocolo de la capa de trasporte, puerto de origen/destino y nombres (si están presente) pueden estar "ocultos", es decir inaccesibles debido a la encriptación o fragmentación. Note también que la Dirección de Origen y de Destino deben ser IPv4 o IPv6.

El contexto de una implementación IPsec determinará que selector se debe utilizar. Por ejemplo una implementación integrada en un host dentro de la pila puede hacer uso de una interfaz socket. Cuando una nueva conexión es establecida la SPD puede ser consultada y una SA (o grupo de SA) unirá al socket. Así el tráfico enviado vía ese socket no necesitará operaciones de búsqueda adicionales en la SPD/SAD. En contraste implementaciones, BITS, BITW o security gateway necesitan mirar cada paquete y realizar operaciones de búsqueda en SPD/SAD basados en los selectores. Los valores permitidos para los campos del selector difieren entre el flujo de tráfico, la SA y la política de seguridad.

ANEXO E. POLITICAS DE ASIGNACIÓN Y DELEGACIÓN DE DIRECCIONES IPV6[47]

En este capítulo se definen las políticas de registro y asignación de direcciones IPv6 globalmente únicas a los ISPs y otras organizaciones.

En [RFC 2373] se designa el bloque 2000::/3 como el espacio global de direcciones Unicast que la IANA puede adjudicar a los RIRs. Las primeras asignaciones hechas de este espacio de direcciones a los RIRs pertenecen al bloque de direcciones 2001::/16.

1. DEFINICIONES

Internet Registry – IR

Un Registro de Internet (IR) es una organización responsable de la distribución de espacios de direcciones IP a sus miembros o clientes y del registro de esa distribución. Los IRs están clasificados de acuerdo a su función principal y alcance territorial dentro de la estructura jerárquica delineada en la figura 45.

Regional Internet Registry – RIR

Los Registros Regionales de Internet (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir el espacio de direcciones público de Internet dentro de las

[47] Anexo tomado de http://www.lacnic.net/sp/politicas/ipv6.html

respectivas regiones. El RIR que representa a nuestra región ante la IANA es LACNIC (Registro Regional de Internet para América Latina y el Caribe).

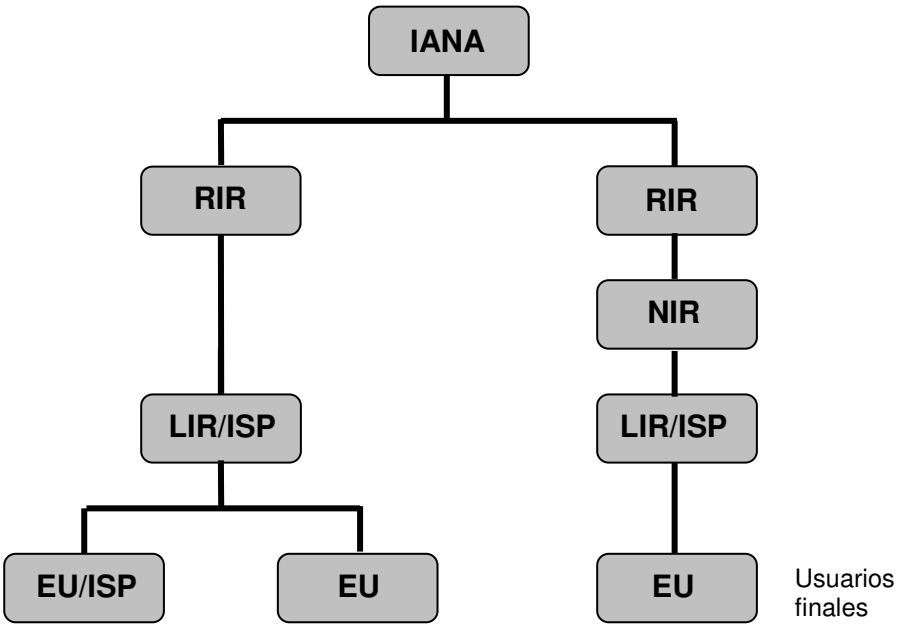

Figura 45 Estructura jerárquica para la asignación de direcciones IPv6

National Internet Registry - NIR

Un Registro Nacional de Internet (NIR) adjudica principalmente, espacios de direcciones a sus miembros o constituyentes, los cuales son generalmente LIRs a un nivel nacional. Los NIRs existen mayormente en la región de Asia Pacífico

Local Internet Registry – LIR

Un Registro Local de Internet (LIR) es un IR que asigna, principalmente, espacios de direcciones a los usuarios de los servicios de red que éste provee.

Los LIRs son generalmente ISPs, cuyos clientes son principalmente usuarios finales y posiblemente otros ISPs.

Adjudicar

Adjudicar significa distribuir el espacio de direcciones a los IRs con el propósito de que ellos realicen la subsiguiente distribución.

Asignar

Asignar significa delegar espacio de direcciones a un ISP o usuario final, para su uso específico dentro de la infraestructura de Internet que ellos operan. Las asignaciones deben ser realizadas solamente para los propósitos específicos documentados por organizaciones específicas y no para ser sub-asignadas a otras partes.

Utilización

A diferencia de IPv4, IPv6 es generalmente asignado a sitios finales (*end sites*) en cantidades fijas (/48). La utilización real de direcciones dentro de cada asignación será bastante baja comparada con las asignaciones de IPv4. En IPv6, "utilización" es medida en términos de los bits a la izquierda del límite /48. En otras palabras, la utilización se refiere a la asignación de /48s a los end sites, y no al número de direcciones asignadas dentro de /48s individuales en esos end sites. El término utilización se refiere a la adjudicación de /48s a los end sites, y no al número de direcciones asignadas dentro de los /48s individuales en esos sites.

HD Radio

El HD Ratio es un modo de medir la eficiencia de asignación de direcciones [RFC 3194]. Es una adaptación del H Ratio, originalmente definido en [RFC1715], y es expresado de la siguiente manera:

$$HD = \frac{\text{Log (numero de objetos adjudicados)}}{\text{Log (número máximo de objetos adjudicables)}}$$

Donde los objetos son direcciones IPv6 de sites (/48s) asignadas desde un prefijo IPv6 de un tamaño dado.

End site

Un end site es definido como un usuario final (suscriptor) que tiene una relación de negocios con un proveedor de servicios que involucra:

- Al proveedor de servicios asignando un espacio de direcciones al usuario final.
- Al proveedor de servicios otorgando un servicio de tránsito para el usuario final hacia otros sites.
- Al proveedor de servicios transportando el tráfico del usuario final.
- Al proveedor de servicios anunciando un prefijo de ruta agregado que contiene la asignación del usuario final.

2 ADJUDICACIÓN INICIAL DE DIRECCIONES

2.1 CRITERIO PARA LA ADJUDICACIÓN

Para calificar para la adjudicación inicial de un espacio de direcciones IPv6, una organización debe:

a) Ser un LIR o ISP
b) No ser un sitio final (usuario final)
c) Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones (clientes)
d) Anunciar en el sistema de rutas entre dominios de Internet un único bloque, que agregue toda la asignación de direcciones IPv6 recibida, en un plazo no mayor de 12 meses
e) Ofrecer servicios en IPv6 a clientes localizados físicamente en la región del LACNIC en un plazo no mayor de 24 meses

2.2 TAMAÑO DE LA ADJUDICACIÓN INICIAL

Las organizaciones que cumplan con el criterio de adjudicación inicial pueden recibir un mínimo de adjudicaciones de /32. Las organizaciones podrían calificar para una adjudicación inicial más grande que /32 entregando documentación que justifique razonablemente el pedido. Si así lo hicieran, el tamaño de adjudicación estará basado en el número de usuarios existentes y en la extensión de la infraestructura de la organización.

3. ADJUDICACIÓN SUBSIGUIENTE

Las organizaciones que ya tengan una adjudicación IPv6 pueden recibir adjudicaciones subsiguientes de acuerdo a las siguientes políticas.

3.1 CRITERIO PARA LA ADJUDICACIÓN SUBSIGUIENTE

La adjudicación subsiguiente será provista cuando una organización (ISP/LIR) satisfaga el umbral de evaluación de utilización histórica de direcciones en términos del número de sites en unidades de asignaciones de /48. El HD Ratio [RFC 3194] es usado para determinar los umbrales de utilización que justifican la adjudicación de direcciones adicionales como se describe a continuación.

3.2 HD RADIO APLICADO

El HD Ratio no tiene el fin de reemplazar las mediciones tradicionales de uso que los ISPs tienen actualmente con IPv4. De hecho, el HD Ratio aún requiere el conteo de objetos asignados. El principal valor del HD Ratio es su utilidad al determinar los rangos razonables de utilización para un espacio de direcciones de un tamaño dado. Este documento utiliza el HD Ratio para determinar los rangos en los cuales una asignación dada ha alcanzado un nivel aceptable de utilización y se justifica la asignación de espacio adicional.

El valor HD Ratio de 0.8 es adoptado como una aceptable utilización de direcciones para justificar la adjudicación de espacio de dirección adicional.

3.3 TAMAÑO DE LA ADJUDICACIÓN SUBSIGUIENTE

Cuando una organización ha logrado una aceptable utilización de su espacio de direcciones adjudicado, está inmediatamente calificada para obtener una adjudicación adicional que resulte en una duplicación de su espacio de direcciones adjudicado. Cuando sea posible, la adjudicación será realizada de bloques de direcciones adyacentes, es decir que su adjudicación existente es extendida un bit hacia la izquierda. Si una organización necesita más espacio de direcciones, debe proveer documentación justificando sus requerimientos para un período de 2 años. La adjudicación se basará en este requerimiento.

4. ADJUDICACIÓN DE LIR A ISP

No hay una política específica para la adjudicación de espacio de direcciones de una organización (LIR) a los ISPs subordinados. Cada LIR podría desarrollar su propia política para ISPs subordinados para alentar una utilización óptima del bloque de direcciones total adjudicado al LIR. Sin embargo, todas las asignaciones de /48 a *end sites* deben ser registradas por el LIR o por sus ISPs subordinados de modo que el RIR/NIR puede evaluar apropiadamente el HD Ratio cuando es necesaria una adjudicación subsiguiente.

Las asignaciones deben ser realizadas de acuerdo con las recomendaciones existentes [RFC3177], las cuales resumimos aquí como:

- /48 en el caso general, excepto para suscriptores muy grandes
- /64 cuando se conoce por diseño que una y solo una subred es necesaria
- /128 cuando se conoce absolutamente que uno y solo un dispositivo se está conectando.

A los RIRs/NIRs no les concierne el tamaño de direcciones que los LIR/ISP realmente asignan. Por lo tanto, los RIRs/NIRs no pedirán información detallada sobre redes de usuarios IPv6 como lo hicieron en IPv4, excepto para los casos que se describen en la sección 2.1 y para los propósitos de medir la utilización como se define en este anexo.

4.1 ASIGNACIÓN DE MULTIPLES /48S A UN SOLO SITIO

Cuando un solo end site requiere un bloque de direcciones de /48 adicional, debe pedir la asignación con documentación o materiales que justifiquen el pedido. Los pedidos de bloques múltiples o adicionales de /48s serán procesados y revisados (Ej.: evaluación de la justificación) al nivel de los RIR/NIR.

4.2 ASIGNACIÓN A LA INFRAESTRUCTURA DEL OPERADOR

Una organización (ISP/LIR) puede asignar un /48 por PoP como un servicio de infraestructura de un operador de servicio IPv6. Cada asignación a un PoP es considerada como una asignación sin tener en cuenta el número de usuarios que usen el PoP. Puede obtenerse una asignación separada para operaciones propias del operador.

5. MICRO-ASIGNACIONES EN IPV6

LACNIC podrá realizar micro-asignaciones en casos de proyectos e infraestructuras de redes claves o críticas para el funcionamiento, y desarrollo de IPv6 en la región como son IXP (Internet Exchange Point), NAP (Network Access Point), RIR, proveedores de DNS, entre otros. Dichas asignaciones se

realizarán en bloques menores o igual a un /32 pero siempre mayores o iguales a un /48.

En el caso de los IXP o NAP para poder solicitar este tipo de asignaciones las organizaciones deberán cumplir los siguientes requisitos:

1. Documentar adecuadamente los siguientes aspectos:
   1.1. Demostrar a través de sus estatutos su calidad de IXP o NAP. Deberá poseer al menos tres miembros y una política abierta para la asociación de nuevos miembros.
   1.2. Enviar un diagrama de la estructura de red de la organización.
   1.3. Documentar el plan de numeración a instrumentar.

2. Proveer un plan de utilización para los próximos tres y seis meses.

El resto de las solicitudes se estudiarán basadas en el análisis de documentación que justifique los aspectos críticos y/o claves del proyecto. Todas las micro-asignaciones se asignarán de bloques de direcciones específicamente reservados para este tipo de asignaciones. LACNIC hará pública la lista de dichos bloques y las micro-asignaciones realizadas.

La organización que reciba una micro-asignación no podrá realizar sub-asignaciones con estas direcciones IP.

6. REGISTRO

Cuando una organización que posee una adjudicación de espacio IPv6, hace asignaciones de sub-espacios IPv6, debe registrar la información de asignaciones en una base de datos accesible a los RIRs como corresponde (la información registrada por un RIR/NIR puede ser cambiada en el futuro por una

base de datos para registrar manejo de direcciones). La información es registrada en unidades de redes /48 asignadas. Cuando a una organización se le asigna más de una /48 la organización que la asigna es responsable de asegurar que el espacio de direcciones esté registrado en una base de datos RIR/NIR.

Los RIR/NIRs usarán los datos registrados para calcular el HD Ratio en el momento de la solicitud, para subsecuentes adjudicaciones y para verificar eventuales cambios en las asignaciones.

Los IRs deben mantener sistemas y prácticas que protejan la seguridad de la información personal y comercial que es usada en la evaluación de solicitudes, pero que no es requerida para el registro público.

7. POSEEDORES DE IPV6 YA EXISTENTES

Las organizaciones que hayan recibido adjudicaciones de IPv6 /35 bajo la política previa de IPv6 (http://www.arin.net/policy/ipv6.html) están inmediatamente autorizadas a expandir su asignación a un bloque de direcciones /32 sin necesidad de justificación, siempre y cuando satisfagan los criterios del anexo B sección 2.1.

El bloque de direcciones /32 contendrá el bloque más pequeño ya adjudicado (uno o múltiples /35 bloques en muchos casos) que ya ha sido reservado por el RIR para una posterior asignación a la organización. Las solicitudes de espacio adicional más allá del mínimo tamaño /32 serán evaluadas de manera similar a los /48 (Anexo E - sección 4.1).

ANEXO F. INSTALACIÓN DE IPV6 EN PLATAFORMAS WINDOWS[48]

Las plataformas de Microsoft disponen de soporte para IPv6 a partir de la versión del sistema operativo Windows XP. Todo el soporte de Microsoft para IPv6 se encuentra en http://www.microsoft.com/ipv6.

1. WINDOWS SERVER 2003

Para esta versión de Windows, IPv6 ya está instalado, solo hace falta habilitarlo. Para ello es necesario ejecutar, con privilegios de administrador, el siguiente comando (Menú de inicio – Ejecutar – CMD – Enter):

prompt>netsh interface ipv6 install

Un mensaje nos indicará que IPv6 se ha configurado correctamente.

Otra forma de hacerlo es utilizando la interfaz gráfica, seleccionando Propiedades sobre la interfaz LAN en la que se desea habilitar IPv6, luego -> Instalar, Protocolo, IPv6.

Para comprobar que IPv6 ha sido instalado correctamente, use:

prompt>netsh interface ipv6 show address

Como resultado se mostrará la configuración y las direcciones IPv6 asignadas automáticamente para cada interfaz de red existente.

[48] Tomado de www.6sos.org

Con **prompt>netsh interface ipv6** obtenemos todos los comandos que junto a esta sentencia permiten comprobar y configurar manualmente interfaces, direcciones y rutas.

Para comprobar el correcto funcionamiento de la pila IPv6, podemos usar un comando ping a la dirección de retorno:

prompt>ping ::1

Para desinstalar IPv6 se usa **prompt>netsh interface ipv6 uninstall**

Mayor información en:

http://www.microsoft.com/windowsserver2003/technologies/ipv6/default.mspx

2. WINDOWS XP

Para versiones de Windows XP con Service Pack 1 o posterior, las instrucciones son idénticas a las anteriormente descritas (Windows 2003). La versión del XP se puede comprobar en Mi PC, Propiedades, Sistema, General.

Sin importar que versión del XP usemos, todas traen por defecto los comandos del IPV6.EXE los cuales sustituyen a los comandos Netsh de versiones anteriores. Para habilitar IPv6 vamos a Menú de inicio – Ejecutar – CMD – Enter:

prompt>ipv6 install

Podemos comprobar si ha sido correctamente instalado con:

prompt>ipv6 if

Como resultado se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

El comando **prompt>ipv6 help** nos muestra la lista de comandos usados junto a "ipv6" que nos permiten comprobar y configurar manualmente interfaces, direcciones y rutas.

Tambien podemos usar **prompt>ping6 ::1** para comprobar que la pila IPv6 está correctamente instalada. Adicionalmente existen otros comandos útiles como "tracer6", "telnet6", "ftp", "ipsec6", "tlntserver" y "6to4-cfg".

Mayor información en:

http://www.microsoft.com/windowsxp/pro/techinfo/administration/ipv6/default.asp

3. WINDOWS 2000

3.1 WINDOWS 2000 SERVICE PACK 1

En el caso en que se necesite utilizar este sistema para navegar por sitios Web IPv6, es necesario usar Internet Explorer versión 5 o posteriores (ver Tabla 9).

Esta instalación es válida en cualquier versión comercial de Windows 2000, siempre que tenga instalado service pack 1.

Ejecute el archivo tpipv6-001205.exe desde:
http://msdn.microsoft.com/downloads/sdks/plattform/tpipv6/download.asp

Luego hay que descomprimir el archivo en una carpeta local, por ejemplo C:/IPv6TP. Ejecute desde esta carpeta el archivo setup.exe. Probablemente sea necesario reiniciar el equipo.

Ahora desde el escritorio, Entorno de Red, Propiedades, seleccionar la tarjeta de red en la que se quiere instalar IPv6, Propiedades, Instalar, Protocolo, Añadir, IPv6, OK. Para comprobar que ha sido instalado correctamente usar:

prompt>ipv6 if

Como resultado se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

El comando **prompt>ipv6 help** nos muestra la lista de comandos usados junto a "ipv6" que nos permiten comprobar y configurar manualmente interfaces, direcciones y rutas.

Tambien podemos usar **prompt>ping6 ::1** para comprobar que la pila IPv6 está correctamente instalada. Adicionalmente existen otros comandos útiles como "tracer6", "telnet6", "ftp", "ipsec6", "tlntserver" y "6to4-cfg".

Mayor información en:

http://www.msdn.microsoft.com/downloads/sdks/plattform/tpipv6.asp
http://www.msdn.microsoft.com/downloads/sdks/plattform/tpipv6/faq.asp

3.2 WINDOWS 2000 CON SP2, SP3 O SP4

En el caso en que se necesite utilizar este sistema para navegar por sitios Web IPv6, es necesario usar Internet Explorer versión 5 o posteriores (ver Tabla 9). Esta instalación es válida en cualquier versión comercial de Windows 2000, siempre que tenga instalado service pack 2,3 o 4.

Para SP2, descargar el archivo tpipv6-001205-SP2-IE6.zip desde:

http://www.ipng.nl/tpipv6-001205-SP2-IE6.zip

Para SP3 o SP4, descargar el archivo tpipv6-001205-SP3-IE6.zip desde:

http://www.ipng.nl/tpipv6-001205-SP3-IE6.zip

Descomprimirlo en una carpeta local, por ejemplo C:/IPv6TP. Luego ejecute desde esta carpeta el archivo setup.exe, probablemente se necesite reiniciar el equipo.

Ahora desde el escritorio, Entorno de Red, Propiedades, seleccionar la tarjeta de red en la que se quiere instalar IPv6, Propiedades, Instalar, Protocolo, Añadir, Microsoft IPv6, OK. Para comprobar que ha sido instalado correctamente usar:

prompt>ipv6 if

Como resultado se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

El comando **prompt>ipv6 help** nos muestra la lista de comandos usados junto a "ipv6" que nos permiten comprobar y configurar manualmente interfaces, direcciones y rutas.

Tambien podemos usar **prompt>ping6 ::1** para comprobar que la pila IPv6 está correctamente instalada. Adicionalmente existen otros comandos útiles como "tracer6", "telnet6", "ftp6", "ipsec6", "tlntserver" y "6to4-cfg".
Mayor información en:

http://www.msdn.microsoft.com/downloads/sdks/plattform/tpipv6.asp
http://www.msdn.microsoft.com/downloads/sdks/plattform/tpipv6/faq.asp

4. WINDOWS 95, 98 Y NT 4.0

Microsoft no soporta IPv6 en estas plataformas, sin embargo se han desarrollado *parches* que habilitan su uso:

a. Trumpet Software suministra una pila IPv6, con periodo de prueba de 30 días. Para descargarla desde:
   http://www.trumpet.com.au/downloads.html
b. Alternativamente, existe una implementación de Hitachi, de un protocolo denominado Toolnet6. El inconveniente es que sólo la soportan algunas tarjetas de red. Toda la información en:
   http://www.hitachi.co.jp/Prod/comp/network/pexv6-e.htm

5. WINDOWS CE.NET, POCKET PC, MOBILE 2003 Y SMARTPHONE

Las últimas versiones de Microsoft para PDAs, teléfonos móviles y dispositivos similares, ofrecen soporte de IPv6 de forma automática. Para mayor información dirigirse a:

http://www.microsoft.com/ipv6
http://www.microsoft.com/windowsmobile/default.mspx

ANEXO G. INSTALACIÓN DE IPV6 EN PLATAFORMAS LINUX[49]

En Linux IPv6 se implementa como un módulo del Kernel. Así, las distribuciones con Kernel 2.2.x y 2.4.x ya vienen con soporte. De todas formas hay que asegurarse que el módulo se carga al arrancar.

Este anexo se basa en la distribución Red Hat. Información detallada sobre el soporte IPv6 en las distribuciones más comunes se encuentra en:

http://www.bieringer.de/linux/IPv6/status/IPv6+Linux-status-distributions.html

1. SOPORTE IPV6

Para comprobar que el Kernel soporta IPv6, se necesita comprobar que existe la siguiente entrada:

/proc/net/if_inet6

Si no existe, se puede intentar cargar con:

#> modprobe ipv6

Si se ha cargado correctamente debe existir la entrada mencionada anteriormente.

Para que el modulo IPv6 cargue automáticamente cuando se demande, se añade al fichero /etc/modules.conf las siguientes lineas:

[49] Tomado de www.6sos.org

alias net-pf-10 ipv6

alias sit0 ipv6

alias sit1 ipv6

alias tun6to4 ipv6

Para deshabilitar la carga automática usar **alias net-pf-10 off**

Se necesitan herramientas para configurar IPv6:

- Paquete net-tools: usando ifconfig, route.
- Paquete iproute: debe existir el programa /sbin/ip, dado que este programa es una extensión del paquete anterior.

2. SCRIPTS DE CONFIGURACIÓN IPV6

Se utilizan scripts para inicializar todo lo relacionado con IPv6 y para configurar las direcciones v4/v6 de las interfaces. Conviene actualizar a la última versión de los mismos, dichas actualizaciones se encuentran en:

http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/scripts/current/index.html

Se descarga la última versión IPv6-initscripts-20020125.tar.gz y se descomprime.

Se copian los archivos de script a los directorios correspondientes:

/etc/sysconfig/network-scripts/network-functions-ipv6

/etc/sysconfig/network-scripts/init.ipv6-global

/etc/sysconfig/network-scripts/ifup-ipv6

/etc/sysconfig/network-scripts/ifdown-ipv6

/etc/sysconfig/network-scripts/ifup-sit
/etc/sysconfig/network-scripts/ifdown-sit
/etc/ppp/ip-up.ipv6to4
/etc/ppp/ip-down.ipv6to4
/etc/ppp/ipv6-up
/etc/ppp/ipv6-down

/usr/sbin/test-ipv6-installation
/etc/sysconfig/static-routes-ipv6

Aplicar *parches,* copiar archivo .diff al mismo directorio donde está el archivo a *parchear:*

#cat network.diff | patch (/etc/sysconfig/)
#cat ifup.diff | patch
#cat netwok.diff | patch

Se recomienda instalar ipv6calc para habilitar la detección de direcciones extendidas. Puede descargarse de:
http://www.bieringer.de/linux/IPv6/ipv6calc/index.html

El tar.gz (ipv6calc-0.39.tar.gz) incluye el fichero spec-file, de forma que se puede crear el RPM mediante:

root# cd /usr/src/redhat/RPMS/i386
root# rpm –i ipv6calc-versión.i386.rpm

Debe existir ahora /bin/ipv6calc. En el fichero sysconfig-ipv6.txt que viene con el paquete de scripts, se da información detallada de los parámetros que se pueden configurar en cada script.

Para configurar que la configuración es correcta, se puede ejecutar el script:

/usr/sbin/test-ipv6-installation

3. CONFIGURACIÓN DE RED

Para cambiar el nombre del host se incluye en /etc/sysconfig/network, la linea:

HOSTNAME=nombre_host

Conviene después de esto, añadirlo en el fichero /etc/hosts:

::1 nombre_host

Se deben añadir entradas en /etc/hosts para IPv6:

::1	**localhost ip6-localhost ip6-loopback**
fe00::0	**ip6-localnet**
ff00::0	**ip6-mcastprefix**
ff02::1	**ip6-allnodes**
ff02::2	**ip6-allrouters**
ff02::3	**ip6-allhosts**

Comprobar que en /etc/protocols/ aparecen:

ipv6	**41**	**IPv6**
ipv6-route	**43**	**IPv6-Route**
ipv6-frag	**44**	**IPv6-Frag**

ipv6-crypt 50 IPv6-Crypt
ipv6-auth 51 Ipv6-Auth
ipv6-icmp 58 IPv6-ICMP
ipv6-nonxt 59 IPv6-NoNxt
ipv6-opts 60 IPv6-Opts

Comprobar que el fichero /etc/nsswitch.conf es correcto:

hosts: files dns
networks: files dns

Configurar /etc/host.conf:

order hosts, bind
multi on

Con esto se logra que el *resolver* primero consulte el fichero /etc/hosts y luego al servidor de nombres.

Configurar /etc/resolv.conf, donde:

- domain: especifica el nombre del dominio local
- search: lista de nombres de dominio alternativo para búsqueda del nombre de un host.
- nameserver: dirección IP de servidores de nombre a los que se consulta, pueden ser varios, así que pueden ir varias líneas nameserver.

Para cada interfaz existirá un fichero con la configuración que se le asignará al arrancar. Supongamos que se tiene una interfaz hacia la red local (10.0.0.x/24). En /etc/sysconfig/network-scripts/ifcfg-eth0:

DEVICE=eth0

IPADDR=10.0.0.3

NETMASK=255.255.255.0

NETWORK=10.0.0.0

BROADCAST=10.0.0.255

GATEWAY=10.0.0.1

ONBOOT=yes

El fichero /etc/sysconfig/network tiene respecto a IPv4:

GATEWAYDEV=eth0

GATEWAY=10.0.0.1

Que añade la ruta por defecto a través de eth1 y la IP del switch de salida hacia el ISP. Para establecer rutas de manera estática al arrancar el equipo (o la configuración de red) se puede utilizar el fichero /etc/sysconfig/static-routes (para IPv4) o /etc/sysconfig/static-routes-ipv6 (para IPv6).

Para asignar a eth0 direcciones IPv6 se realiza lo siguiente:

En el directorio /etc/sysconfig/network-scripts/ habrá un fichero para cada interfaz (eth0). Se añade:
A ifcfg-eth0 (caso de autoconfiguración):

IPV6INIT=yes

IPV6AUTOCONF=yes

A ifcfg-eth0 (caso asignación estática):

IPV6INIT=yes

IPV6AUTOCONF=no

IPV6ADDR=3ffe:3328:6:2a03::3

Cuando se haga un cambio en la configuración de red, se puede reiniciar todo el sistema de red ejecutando el script: /etc/rc.d/init.d/network restart.

4. COMANDOS ÚTILES

4.1 MOSTRAR DIRECCIONES IPV6

Se puede hacer mediante el uso de ip o ifconfig:

#> /sbin/ip -6 addr show dev <interface>

#> /sbin/ifconfig <interface>

Donde <interface> puede ser eth0.

4.2 AÑADIR UNA DIRECCIÓN IPV6

Se puede hacer mediante el uso de ip o ifconfig:

#> /sbin/ip -6 addr add <ipv6address>/<prefixlenght> dev <interface>

#> /sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlenght>

4.3 ELIMINAR UNA DIRECCIÓN IPV6

Se puede hacer mediante el uso de ip o ifconfig:

#> /sbin/ip -6 addr del <ipv6address>/<prefixlenght> dev <interface>

#> /sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlenght>

4.4 MOSTRAR RUTAS IPV6

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route show [dev <device>]

#> /sbin/route –A inet 6

Donde <device> puede ser eth0.

4.5 AÑADIR UNA RUTA IPV6 A TRAVÉS DE UN GATEWAY

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route add <ipv6network>/<prefixlenght> via <ipv6address> [dev <device>]

#> /sbin/route –A inet6 add <ipv6network>/<prefixlenght> gw <ipv6address> [dev <device>]

Para eliminar una ruta a través de un gateway se pueden usar las dos sentencias anteriores, simplemente cambiando el comando add por el comando del.

4.6 AÑADIR UNA RUTA IPV6 A TRAVÉS DE UNA INTERFAZ

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route add <ipv6network>/<prefixlenght> dev <device> metric 1
#> /sbin/route –A inet6 add <ipv6network>/<prefixlenght> dev <device>

Para eliminar una ruta a través de una interfaz se pueden usar las dos sentencias anteriores, simplemente cambiando el comando add por el comando del.

4.7 PING6

Generalmente está incluido en el paquete iputils:

#> ping6 <hostwithipv6address>
#> ping6 <ipv6address>
#>ping6 [-i <device>] <link-local-ipv6address>

4.8 TRACEROUTE6

Generalmente está incluido en el paquete iputils:

#>traceroute6 www.kame.net

ANEXO H. INSTALACIÓN DE IPV6 EN PLATAFORMAS FREEBSD[50]

Este anexo se basa en la versión 4.5 de FreeBSD.

1. SOPORTE IPV6

Las opciones básicas que se activan en /etc/rc.conf son:

ipv6_enable="YES"
ipv6_ifconfig_r10="2001:618:10:4::4 prefixlen 64"

Con la primera opción se activa automáticamente la pila IPv6, incluida la autoconfiguración. Con la segunda se asigna una IPv6 fija.

1.1 ACTIVAR DEMONIO RAS

Si se requiere que FreeBSD envíe RAs se puede hacer de dos maneras: usando radvd o rtadvd. Se recomienda el uso de radvd. Éste se encuentra en /usr/local/sbin/radvd.

Para que se ejecute correctamente debe activarse el *forwarding* de IPv6. Esto se hace poniendo en /etc/rc.conf: ipv6_gateway_enable="YES".

El demonio rtadvd se puede activar en /etc/rc.conf mediante:

rtadvd_enable="YES"
rtadvd_interfaces="r10"

[50] Tomado de www.6sos.org

1.2 ACTIVAR EL SERVICIO DNS

Normalmente se encuentran disponibles dos servidores DNS. El primero se activa desde /etc/rc.conf mediante:

named_enable="YES"

Su fichero de configuración se encuentra en /etc/namedb/named.conf

Tambien se puede encontrar el servidor BIND cuyo binario se encuentra en /usr/obj/usr/src/usr.sbin/named. Para activarlo se puede usar un script que se ejecute al arrancar, por ejemplo /usr/local/etc/rc.d/lanza_DNS.sh.

En el directorio /etc, se encuentra el fichero de configuración principal: named.conf.

Ahora vamos a gestionar el dominio de pruebas rdlab.es, por lo que se coloca en /etc/resolv.conf la línea: **domain rdlab.es**.

Zonas IPv4:

```
zone "." {
        type hint;
        file "named.root";
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "localhost.rev"
};
zone "localhost" {
```

```
            type master;
        file "localhost.zone";
};
zone "rdlab.es" {
            type master;
            file "rdlab.es.zone" ;
} ;
zone "11.168.192.in-addr.arpa" {
            type master ;
            file "11.168.192.in-addr.arpa.zone" ;
```

Zonas IPv6:

```
zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6
.int" {
            type master;
            file "::.zone";
};
zone "3.0.2.a.2.6.0.0.0.8.2.3.e.f.f.3.ip6.int" {
            type master ;
            file "3ffe :3328 :0006 :2a03 .zone" ;
} ;
```

Las direcciones para las resoluciones directas de Ipv6 se encuentran en rdlab.es.zone.

2. APLICACIONES

Habrá que instalar aplicaciones con soporte IPv6. Se pueden usar los *ports* de FreeBSD:

#> cd /usr/ports
#> make search key="ipv6"

Aparecerá una lista de aplicaciones que soportan IPv6. Entre la información de cada aplicación se encuentra *path* que será el directorio a donde nos moveremos y desde donde podemos instalar la aplicación:

#> cd path
#> make install

Esto hará que se comience a buscar en una lista de servidores el código fuente, que se descargará, se compilará y se instalará. Se puede sólo descargar el código fuente, que se colocará en /usr/ports/distfiles, haciendo en vez de make install, make fetch.

3. COMANDOS ÚTILES

3.1 AÑADIR UNA DIRECCIÓN IPV6

Se puede hacer mediante el uso de ifconfig:

#> ifconfig <interface> inet6 add <addressIPv6>

Para eliminar una dirección IPv6, se utiliza la sentencia anterior, cambiando el comando add por del.

3.2 AÑADIR UNA RUTA POR DEFECTO

Se puede hacer mediante el uso de route:

#> route –n add –inet6 default <addressIPv6>

Para eliminarla se usa **#> route –n del –inet6 default**

ANEXO I. CONFIGURACIÓN DE IPV6 EN SWITCHES CISCO[51]

Este documento trae la configuración para el software Cisco en las versiones 12.0 ST y 12.2 T.

1. CONFIGURACIÓN DE DIRECCIONES IPV6 Y ACTIVAR EL ENRUTAMIENTO IPV6

Por defecto, el enrutamiento IPv6 está desactivado para el software Cisco IOS. Para habilitar el enrutamiento IPv6, se debe activar primero el tráfico global de IPv6 en el router y se deben asignar direcciones IPv6 individuales a las interfaces.

Para que una interfaz pueda reenviar trafico IPv6, es necesario configurar una dirección IPv6 en esta interfaz. Al configurar una dirección global IPv6 en una interfaz, automáticamente se configura una dirección de enlace local y se activa IPv6 para esta interfaz. La interfaz configurada automáticamente ingresa en los grupos multicast para este enlace.

Los siguientes son los pasos para asignar una dirección IPv6 a una interfaz capa 3 y habilitar el enrutamiento IPv6:

1. **configure terminal** (entrar a modo de configuración global).
2. **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** (para activar ACLs[52] y otras funciones)

[51] Tomado de www.cisco.com
[52] ACLs - Listas de Control de Acceso, restricciones que se programan en los routers para permitir o denegar cierto tipo de tráfico desde y hacia las redes conocidas.

3. **end** (retorna a modo privilegiado).
4. **reload** (reinicie el IOS)
5. **configure terminal** (entrar a modo de configuración global).
6. **interface *interface-id*** (para ingresar el modo de configuración de la internaza la cual estamos configurando)
7. **no switchport** (remueve la configuración de la interfaz para capa 2)
8. **ipv6 address *ipv6-address* link-local** o **ipv6 enable** (el primero especifica una dirección de enlace local para activar el enrutamiento en la interfaz, la segunda sentencia configura automáticamente una dirección de enlace local y habilita el enrutamiento en la interfaz, esta dirección sólo puede ser usada para comunicarse con nodos en el mismo enlace)
9. **exit**
10. **ip routing** (habilita el enrutamiento IPv6 en el router)
11. **ipv6 unicast-routing** (habilita el reenvio de paquetes unicast IPv6)
12. **end**
13. **show ip v6 interface *interface-id*** (verifica las entradas)
14. **copy running-config startup-config** (para salvar los cambios en la flash)

Para remover una dirección IPv6 de una interfaz, use no + el comando usado para asignarla (Ej.: **no ipv6 address ipv6-address link-local**).

Para remover todas las direcciones IPv6 asignadas manualmente use **no ipv6 address**.

Para deshabilitar los procesos IPv6 en una interfaz use **no ipv6 enable** dentro del modo de configuración de esta interfaz.

Para deshabilitar globalmente el enrutamiento IPv6, use **no ipv6 unicast-routing** en el modo de configuración global.

2. CONFIGURACIÓN DE LAS PILAS DE PROTOCOLOS IPV4 E IPV6

Cuando se configura una interfaz con direcciones IPv4 e IPv6, la interfaz está habilitada para reenviar los dos tipos de tráfico y puede enviar y recibir datos para redes IPv4 e IPv6. A continuación se encuentran los pasos:

1. **configure terminal** (entrar a modo de configuración global).
2. **ip routing** (habilita el enrutamiento IPv4 en el router)
3. **ipv6 unicast-routing** (habilita el reenvío de paquetes de datos IPv6 en el router)
4. **interface *interface-id*** (ingresa al modo de configuración de la interfaz)
5. **no switchport** (remueve la configuración capa 2 para la interfaz)
6. **ip address *ip-address mask* [secondary]** (especifica una dirección IPv4 primaria o secundaria para la interfaz)
7. **ipv6 address *ipv6-address* link-local** o **ipv6 enable** (el primero especifica una dirección de enlace local para activar el enrutamiento en la interfaz, la segunda sentencia configura automáticamente una dirección de enlace local y habilita el enrutamiento en la interfaz, esta dirección sólo puede ser usada para comunicarse con nodos en el mismo enlace)
8. **end**
9. **show interface *interface-id*,** show ip interface *interface-id*, show ip v6 interface *interface-id* (para verificar las entradas)
10. **copy running-config startup-config** (para salvar los cambios en la flash)

Para deshabilitar el enrutamiento IPv4, use **no ip routing** en modo de configuración global.

Para deshabilitar el enrutamiento IPv6, use **no ipv6 unicast-routing** en modo de configuración global.

Para remover una dirección IPv4 de una interfaz, use **no ip address *ip-address mask*** en el modo de configuración para la interfaz.

Para remover una dirección IPv6 de una interfaz, use **no ipv6 address *ipv6-address* link-local** en el modo de configuración para la interfaz.

Para deshabilitar los procesos IPv6 en una interfaz use **no ipv6 enable** dentro del modo de configuración de esta interfaz.

Para deshabilitar globalmente el enrutamiento IPv6, use **no ipv6 unicast-routing** en el modo de configuración global.

3. CONFIGURAR ENRUTAMIENTO ESTÁTICO PARA IPV6

Las rutas estáticas deben ser configuradas manualmente y definen una ruta explicita entre dos dispositivos de red. Los beneficios de las rutas estáticas es que aumentan la seguridad (al no intercambiar tablas con otros routers) y la eficiencia en el uso de recursos.

Antes de configurar una ruta estática IPv6, se debe tener habilitado el enrutamiento mediante el uso de **ip routing** en el modo de configuración global, además es necesario habilitar el reenvío de paquetes IPv6 mediante el

uso de **ipv6 unicast-routing** en el modo de configuración global. Los siguientes son los pasos para configurar una ruta IPv6 estática:

1. **configure terminal** (entrar al modo de configuración global)
2. **ipv6 route *ipv6-prefix/prefix lenght {ipv6-address | interface-id [ipv6-address]}[administrative distance]*** , donde:

   ipv6-prefix- prefijo de la red destino de la ruta estática

   prefix lenght- longitud del prefijo anterior

   ipv6-address- dirección IPv6 del siguiente salto que es usado para alcanzar la red especifica.

   Interface-id- especifica rutas estáticas directas para interfaces punto-a-punto y broadcast. Con interfaces punto-a-punto no es necesario especificar la dirección IPv6 para el siguiente salto.

   administrative distance- su uso es opcional y especifica la distancia administrativa que hay para poder alcanzar la red (Ej.; de 1 a 254 saltos).
3. **end**
4. **show ipv6 route [*ipv6-address* | *ipv6-prefix/prefix lenght*]** para verificar las entradas generadas por el contenido en la tabla de enrutamiento.
5. **copy running-config startup-config** (para salvar los cambios)

4. COMANDOS PARA VISUALIZAR OPCIONES Y CONFIGURACIONES IPV6

COMANDO	PROPÓSITO
show ipv6 access-list	Muestra las ACLs configuradas
show ipv6 cef	Muestra el reenvio CEF

show ipv6 interface *interface-id*	Muestra el estado y configuración de la interfaz
show ipv6 mtu	Muestra la MTU para los destinos en caché
show ipv6 neighbors	Muestra los routers vecinos
show ipv6 ospf	Muestra la información OSPF
show ipv6 prefix-list	Muestra la lista de prefijos de las redes conocidas
show ipv6 protocols	Muestra los protocolos de enrutamiento activos
show ipv6 rip	Muestra el estado de RIP IPv6
show ipv6 route	Muestra las entradas en la tabla de enrutamiento
show ipv6 routers	Muestra los routers IPv6 locales
show ipv6 static	Muestra las rutas estáticas IPv6
show ipv6 traffic	Muestra estadísticas de tráfico IPv6

Tabla 10 Comandos para visualizar opciones IPv6 en un router Cisco