Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACIÓN

Fernando Augusto Espinoza Estévez
Asesorado por el Ing. Rodolfo Estuardo Arriaga Herrera

Guatemala, septiembre de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

FERNANDO AUGUSTO ESPINOZA ESTÉVEZ
ASESORADO POR EL ING. RODOLFO ESTUARDO ARRIAGA HERRERA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, SEPTIEMBRE DE 2013

NIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. César Augusto Fernández Cáceres
EXAMINADORA	Inga. Vivian Damaris Campos González
EXAMINADOR	Ing. Edgar René Ornelis Hoíl
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACIÓN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha febrero de 2013.

Fernando Augusto Espinoza Estévez

Ing. Marlon Antonio Pérez Turk
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Guatemala, 2 de Agosto de 2013

Estimado Ingeniero Pérez Turk.

Por este medio hago de su conocimiento de que eh terminado con la revisión del trabajo de tesis para aplicar a proceso de graduación del estudiante **FERNANDO AUGUSTO ESPINOZA ESTEVEZ**, titulado **"IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACION"**, que a mi criterio el mismo cumple con todos los objetivos propuestos para su desarrollo, según su protocolo inicial.

Sin otro particular, me es grato suscribirme.

Atentamente,

Ing.
Rodolfo Estuardo Arriaga Herrera
Colegiado 7030

Ing. Rodolfo Estuardo Arriaga Herrera

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 14 de Agosto de 2013

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **FERNANDO AUGUSTO ESPINOZA ESTÉVEZ** carné **1998-10807,** titulado: **"IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACIÓN"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUAT. - FACULTAD DE INGENIERIA EN CIENCIAS Y SISTEMAS - COORDINACION

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACIÓN"****, realizado por el estudiante FERNANDO AUGUSTO ESPINOZA ESTÉVEZ, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Türk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 20 de septiembre 2013

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.641.2013

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ciencias y Sistemas, al trabajo de graduación titulado: **IP V.6 SOBRE NUEVOS PROTOCOLOS DE TELECOMUNICACIÓN,** presentado por el estudiante universitario: **Fernando Augusto Espinoza Estévez,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, septiembre de 2013

/cc

ACTO QUE DEDICO A:

Dios padre	Por estar siempre presente de una u otra forma en mi vida, sin tí nada soy, contigo seré lo que me proponga.
Mi padre	Luis Fernando Espinoza, por su apoyo incondicional y ser siempre mi fuente de inspiración.
Mi madre	Mayra Palacios, por demostrarme siempre el verdadero amor no importando las adversidades de la vida.
Mi hijo	Diego Sebastián Espinoza, eres sin duda la parte más importante de mi vida, razón de mis esfuerzos y logros, gracias por existir.
Mi hermano	Luis Estuardo Espinoza, por todos los momentos vividos que llevaré siempre conmigo.

AGRADECIMIENTOS A:

La Universidad San Carlos de Guatemala	Por proporcionar las herramientas y oportunidades que apoyaron mi carrera.
Mis asesores	Ing. Rodolfo Estuardo Arriaga, por su ayuda y apoyo constante en la finalización de mi trabajo. Ing. Victor Quan, por su valioso tiempo, dedicación y apoyo incondicional al iniciar mi trabajo.
Mis amigos y compañeros	Por permitirme ser parte de sus vidas, compartir muchas experiencias, por su apoyo en tiempos difíciles y por todos esos momentos de alegría que jamás olvidaré.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ATM — *Asynchronous Transfer Mode*. El estándar de CCITT para transporte de células que transportan múltiples tipos de información tales como: voz, video, datos.

Backbone — Infraestructura que constituye la base del internet. Nivel más alto en la jerarquía de ISPs que brindan conexión a internet.

CHAP — *Challenge Handshake Authentication Protocol*, tipo de autenticación en el cual el agente autenticador envía al cliente un valor aleatorio que es utilizado solamente una vez.

CNAME — *Canonical Name* campo de una base de datos de un DNS, indica el verdadero o canónico nombre de una computadora.

Desencapsulamiento — Proceso por el cual se remueve una cabecera que fue agregada previamente a un paquete.

Dirección privada — Dirección utilizada por un nodo para la comunicación interna dentro de la red.

Dirección pública — Dirección única asignada por InterNIC utilizada para comunicarse a través de internet.

Ethernet Especificación de LAN inventada por Xerox Corporation y desarrollada posteriormente por las compañías Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y corren sobre una variedad de cables a 10Mbps. Ethernet es similar al estándar IEEE 802.3.

Encapsular Proceso por el cual se agrega una cabecera extra a la que contiene un paquete que brinda conexión a internet.

Enrutador Dispositivo de capa 3 del ISO/OSI que determina la ruta óptima para enviar el tráfico de red basado en métricas.

Extranet Red externa e interconectada a la red corporativa de una organización.

Fast Ethernet Cualquier especificación de Ethernet a 100-Mbps. Ofrece un incremento de velocidad diez veces mayor que la especificación 10BaseT Ethernet, Conserva sus características en cuanto al formato de trama, los mecanismos de MAC y MTU.

FDDI *Fiber Distributed Data Interface*. Un estándar de ANSI (X3T9.5) que especifica una red de 100 Mbps usando fibra óptica.

Frame Relay Estándar industrial, protocolo de capa de enlace del ISO/OSI que maneja múltiples circuitos virtuales utilizando encapsulamiento HDLC entre dispositivos interconectados. Frame Relay es más eficiente que X.25.

Gigabit Ethernet Tecnología que incrementa diez veces la velocidad de Fast Ethernet, 1 gigabit por segundo (Gbps) o 1000 Mbps. Toma ventaja de la alta velocidad de la tecnología de interface física de ANSI X3T11 Fiber Channel mientras que mantiene el mismo formato que IEEE 802.3.

HDLC *High-Level Data Link Control*. Es un protocolo de capa de enlace del estándar ISO/OSI orientado a bit, esta derivado del SDLC. HDLC especifica un método de encapsulamiento de información sobre enlaces de datos sincrónicos seriales.

IGRP *Internal Gateway Routing Protocol*. Protocolo de enrutamiento desarrollado por Cisco Sytems para ofrecer a sus clientes una alternativa de mayor escalabilidad que RIP. Direcciona los beneficios asociados con el enrutamiento en redes extensas y heterogéneas.

Internet Término utilizado para hacer referencia a la red de mayores dimensiones del mundo, conectando miles de redes en todo el mundo. El internet surgió del ARPANET.

Intranet Red corporativa y privada de una compañía, término conocido tradicionalmente como sistema autónomo.

IPsec Familia de protocolos y servicios que se utilizan para proporcionar seguridad adicional a los data gramas de IP.

IPX *Internetwork Packet Exchange*. Protocolo de nivel 3 de Novell similar al XNS y al IP que se utilizan en redes NetWare.

ISDN *Integrated Services Digital Network*. Protocolos de comunicación propuesta por compañías telefónicas para permitirá redes telefónicas transportar datos, voz, y otro tipo de material.

ISP Compañía que provee acceso a internet a otras compañías.

LAN *Local Área Network*. Red de datos de alta velocidad y baja tasa de errores, cubre un área geográfica relativamente pequeña. Interconecta estaciones de trabajo, equipo periférico, terminales y otros dispositivos en un mismo edificio u otra área geográficamente limitada.

LAPB *Link Access Procedure Balanced*. Protocolo de capa de enlace relativa a los niveles de X.25. Es también un protocolo orientado a bit derivado de HDLC.

Netware Un sistema operativo de red de área local desarrollado por Novell Corporation. Es un programa que corre en una variedad de tipos de redes. Provee una interfaz para transmisión de mensajes.

Nodos Término genérico utilizado para hacer referencia a una entidad que puede tener acceso a una red. También conocido como dispositivo.

OSPF *Open Shortest Path First*. Protocolo de enrutamiento avanzado y escalable basado en el algoritmo Link State de Dijkstra

PABX Private Automatic Branch Exchange

Paquete Unidad de transmisión de la capa de red del modelo OSI.

PPP *Point-to-Point Protocol*. Sucesor de SLIP este protocolo ofrece conexiones de enrutador a enrutador y de host a red empleando circuitos sincrónicos y asincrónicos. Fue diseñado para trabajar con varios protocolos de capa 3 como IP, IPX y ARA. Presenta mecanismos de seguridad como CHAP y PAP.

RIP *Routing Information Protocol*. Protocolo de enrutamiento basado en el algoritmo vector de distancias de Bellman y Ford.

RIPE *Reseaux Ip Europeens Network Coordination Center*, administra y provee de direcciones IP.

Router Dispositivo encargado de reenviar paquetes que no están dirigidos a él.

SLIP *Serial Line internet Protocol*, un protocolo para la conexión por medio de un MODEM (Dial-Up).

SMDS *Switched Multimegabit Data Services*, un servicio de comunicación de datos de alta velocidad, ofrecido por compañías telefónicas para conectar redes de área local.

SNIFFER Es un programa o dispositivo que monitorea el tráfico de datos sobre una red.

Switch Dispositivo de Red que filtra y envía las tramas basado en la dirección destino de cada trama. Opera en la capa 2 del modelo OSI.

Túnel Conexión lógica sobre la cual viaja la información encapsulada.

TCP/IP *Transport Control Protocol/ Internet Protocol*. Los dos protocolos de internet más conocidos que erróneamente suelen confundirse con uno solo. TCP, corresponde a la capa 4 (capa de transporte) del modelo OSI y ofrece transmisión confiable de datos, IP corresponde a la capa 3 (capa de red) del modelo OSI y ofrece servicios de datagramas sin conexión.

Token Ring Tecnología de LAN basada en la transmisión de estafeta y soportada por IBM. Corre a 4 o 16 Mbps sobre una topología de anillo. Es similar a IEEE 802.5.

VLAN Virtual LAN. Grupo de dispositivos en una o más LANs que son configurados (utilizando software de administración) de tal manera que se pueden comunicar como si ellos estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN.

VoFR *Voice Over Frame Relay*. Permite a un Enrutador transportar el tráfico de voz (por ejemplo llamadas telefónicas y Fax) sobre una red de *Frame Relay*. Cuando se envía el tráfico de voz sobre *Frame Relay* el tráfico de voz es segmentado y encapsulado para su tránsito a través de la red utilizando FRF.12 como encapsulamiento.

WAN Red de comunicaciones de datos que da servicio a los usuarios a través de un área geográfica muy amplia. *Frame Relay*, SMDS y X.25 son ejemplos de WAN.

WWW *World Wide Web*, Telaraña mundial de información en formato de Hipertexto. El formato más popular de obtención de información en internet en la actualidad.

X.25 Protocolo de telecomunicación Internacional y estandarización de sector para comunicaciones de una red WAN, para la comunicación entre usuarios y dispositivos del mismo usuario.

RESUMEN

El presente trabajo presenta la evaluación del Protocolo de internet versión 6 (IPv6) en relación a su interoperabilidad con las diferentes plataformas existentes, se pretende demostrar el funcionamiento, las ventajas, desventajas y posibilidades que ofrece el nuevo protocolo Ipv6, así como su implementación sobre diferentes plataformas. Se mostrará también, los distintos mecanismos de transición de Ipv4 a Ipv6 y diversidad de formas de configurar una o varias interfaces de red con este protocolo en diferentes plataformas, los nuevos protocolos y mecanismos para la utilización del nuevo protocolo Ipv6, también se pretende mostrar todas las oportunidades que se pueden y que están siendo utilizadas por empresas, gobiernos, etc.

Asimismo, como nuevo protocolo se comporta con los medios de transmisión, tales como: redes Ethernet, redes ATM, entre otros. Además de su comportamiento y sus mecanismos de transición como los Túneles *6to4*, el doble *Stack* y el *Tunnel-broker*. Además se proporciona un escenario global de cómo este nuevo protocolo esta impactando en el desarrollo de nueva tecnología que demanda por direccionamiento IP dentro de una red global internet.

Lo principal es que se mostrará cómo los protocolos actuales pueden ser modificados, actualizados, o en su caso reemplazado para poder dar acceso a esta nueva versión, la cual tiene como base principal la misma que la versión actual Ipv4, pero se modificaron y mejoraron para traer esta nueva versión en forma eficiente, versión 6 Ipv6.

Con esta nueva versión Ipv6 se tendrán beneficios y ventajas sobre la versión actual, de las cuales se pueden mencionar:

- Ipv6 retiene la mayoría de los conceptos básicos de Ipv4.
- Al igual que Ipv4, Ipv6 es un servicio de entrega de datagramas no confiables y sin conexión.
- Provee nuevas funcionalidades como autentificación y seguridad.
- Los encabezados de extensión son opcionales; Ipv6 los usa para codificar la mayoría de las opciones de Ipv4.
- Las direcciones en Ipv6 son de 128 bits.
- Las direcciones están divididas en tipos, de manera análoga a las clases en Ipv4.
- El beneficio es mayor a un largo plazo versus el costo que conlleva.

OBJETIVOS

General

Evaluar todos los aspectos técnicos y no técnicos para poder realizar la identificación de los protocolos compatibles con Ipv6, así como la definición de herramientas que deban utilizarse para la utilización de los nuevos protocolos de telecomunicación, como nuevas tecnologías de desarrollo para la utilización de protocolos sobre sistemas ipv6.

Específicos

1. Presentar el nuevo direccionamiento Ipv6.

2. Reconocer los nuevos protocolos de telecomunicación sobre los cuales se utilizará el nuevo direccionamiento Ipv6.

3. Determinar el impacto que tendrá el nuevo direccionamiento sobre las tecnologías de comunicación actual y futura.

4. Presentar las nuevas tecnologías que se están desarrollando para la utilización del nuevo direccionamiento Ipv6.

5. Establecer lo necesario para implementar el nuevo direccionamiento en diferentes plataformas.

INTRODUCCIÓN

Actualmente, la tecnología cambia de una manera acelerada y en la rama de las telecomunicaciones, también se ha visto un desarrollo importante. Lo primordial es poder trasportar la información de una manera más eficiente y segura, lo cual permitirá aumentar el tráfico de información. Con la entrada del nuevo protocolo ipv6, lo que se trata de realizar es aumentar el número de direcciones posibles para internet, y la tecnología forma parte importante, ya que está convergiendo hacia este nuevo protocolo, y lo está utilizando para el desarrollo de nuevos protocolos y nuevos productos que utilicen este nuevo protocolo de comunicación ipv6.

Desde los inicios del internet, todas aquellas empresas, personas, universidades, etc. que utilizan la misma, se han visto beneficiados por esta, pero el principal problema es que cada vez que se agrega algún computador a la inmensa red de internet, esta debe de ser identificada, y la única forma de lograr hacerlo es asignarle un número de IP, el cual con el ingreso de más y más computadores a la internet, se ha visto mermado debido a su poca capacidad en el rango definido para la versión de IP versión 4.

Actualmente, internet funciona gracias a un protocolo general para redes de ordenadores llamado TCP/IP (*Transfer Control Protocol/Internet Protocol*), en concreto la versión 4, o Ipv4. IP define la manera que se enrutan los paquetes entre las redes. Cada nodo en cada una de las redes tiene una dirección IP diferente para garantizar un correcto enrutamiento.

Pero el mayor problema que existe con la actual versión de IP, es su estructura de direccionamiento y en el sistema de asignación de direcciones. Las direcciones Ipv4 están encapsuladas en 32 bits. Esto permite 4,000 millones de direcciones, lo que parecía suficiente, cuando lo más común era que hubiese un ordenador por universidad. Con el paso del tiempo, la cantidad de ordenadores personales conectados y la aparición de otros dispositivos (teléfonos móviles, televisores conectados a internet, electrodomésticos también conectados en el futuro), han hecho que este número sea demasiado corto. Se calcula que la asignación actual de espacio ha bloqueado casi un 75 por ciento de estas direcciones. Como consecuencia, las compañías que solicitan direcciones IP hoy, deben arreglárselas con una fracción de las direcciones restantes.

Lo que busca este trabajo de investigación es demostrar o dar una introducción de cómo los fabricantes de productos, ya sean de hardware ó software, ya están tomando en cuenta el nuevo protocolo para el desarrollo del mismo, también quiere mostrar que no existen grandes dificultades para migrar de un protocolo antiguo de comunicación ipv4 hacia un nuevo protocolo de comunicación ipv6.

También se tiene como objetivo poder demostrar cuáles son los cambios que se están realizando a los actuales protocolos de telecomunicación, sus cambios, nuevas características y sobre todo comprender cómo se pueden utilizar con la nueva tecnología de direccionamiento de internet Ipv6.

1. INTRODUCCION A IPV6

IP son las siglas de *Internet Protocol*. El protocolo fue diseñado en los años 70 con el fin de interconectar ordenadores que estuviesen en redes separadas. Hasta entonces los equipos informáticos se conectaban entre sí mediante redes locales (LAN), pero éstas estaban separadas entre sí formando islas de información.

1.1. ¿Qué es el protocolo IP?

El nombre internet para designar el protocolo y posteriormente la red mundial de información, significa justamente *INTERRED*, es decir, conexión entre redes. Al principio el protocolo tuvo un uso exclusivamente militar pero rápidamente se fueron añadiendo ordenadores de universidades y posteriormente usuarios particulares y empresas.

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

1.2. ¿Qué son las direcciones IP?

La dirección IP es un identificador único que se aplica a cada dispositivo que esté conectado a una red IP. De esa forma los distintos elementos participantes de la red (servidores, routers, ordenadores de usuarios, etc.) se comunican entre sí utilizando su dirección IP como identificación. En la versión 4 del protocolo IP (la usada actualmente) las direcciones están formadas por 4

números de 8 bits (un número de 8 bits puede valer desde 0 hasta 255) que se suelen representar separados por puntos, por ejemplo: 217.76.128.63. En total, una dirección IP versión 4 tiene 32 bits, lo que equivale a 2^{32} direcciones IP diferentes.

1.3. ¿Qué es el Ipv6?

Ipv6 es la nomenclatura abreviada de *Internet Protocol* versión 6. Ipv6 es el protocolo de la próxima generación de internet, por lo que a veces también se denomina IPng que viene de *Internet Protocol Next Generation*. Ipv6, es por tanto la actualización del protocolo de red de datos en el que se fundamenta internet. El *IETF* (*Internet Engineering Task Force*) desarrolló las especificaciones básicas durante los años 90 para sustituir la versión actual del protocolo de internet, IP versión 4 (Ipv4), que vio la luz a finales de los 70.

Ipv4 ha demostrado por su duración un diseño flexible y poderoso, pero está empezando a tener problemas, siendo el más importante el crecimiento en poco tiempo de la necesidad de direcciones IP.

Nuevos usuarios en países tan poblados como China o la India, nuevas tecnologías con dispositivos conectados de forma permanente (xDSL, cable, PDA, teléfonos móviles, UMTS, etc.) están provocando la rápida desaparición de las direcciones IP disponibles en la versión 4. Ipv6 resuelve este problema creando un nuevo formato de dirección IP con muchísimas más variaciones, de forma que el número de direcciones IP no se agote, incluso contando con que cada dispositivo que se pueda imaginar (incluyendo electrodomésticos) se termine conectando a la red internet.

Ipv6 añade también muchas mejoras en áreas como el *routing* y el auto configuración de red. Los nuevos dispositivos que se incorporen a la red serán *Plug&Play*. Simplemente habrá que enchufar el equipo a la red y este obtendrá de la misma todos los datos de configuración necesarios. Se espera que Ipv6 reemplace gradualmente a Ipv4, coexistiendo las dos un determinado número de años durante la transición.

1.4. ¿Por qué surge Ipv6?

El motivo básico para crear un nuevo protocolo, fue la falta de direcciones. Ipv4 tiene un espacio de direcciones de 32 bits, en cambio Ipv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de Ipv4, junto al hecho de falta de coordinación para su asignación durante la década de los años 80, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Debido a la multitud de nuevas aplicaciones en las que Ipv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de Ipv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la calidad de servicio (QoS), seguridad (IPsec) y movilidad.

1.5. Características principales de Ipv6

- Mayor espacio de direcciones: el tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Simplificación del formato del *header*: algunos campos del *header* Ipv4 se quitan o se hacen opcionales.

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los *routers*, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del *router*.

- Posibilidad de paquetes con carga útil (datos) de más de 65,355 bytes.

- Seguridad en el núcleo del protocolo (IPsec): el soporte de IPsec es un requerimiento del protocolo Ipv6.

- Capacidad de etiquetas de flujo: puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (*flow*) de tráfico particular, que requieren manejo especial por los *routers* Ipv6, tal como calidad de servicio no por defecto o servicios de tiempo real.

- Auto configuración: la auto configuración de direcciones es más simple; especialmente en direcciones *Aggregatable Global Unicast*, los 64 bits superiores son configurados por un mensaje desde el *router* (*Router Advertisement*) y los 64 bits más bajos son configurados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red.

- Renumeración y *multihoming*: facilitando el cambio de proveedor de servicios.

- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.

- Calidad de servicio (QoS) y clase de servicio (CoS).

- Capacidades de autenticación y privacidad.

1.6. ¿Qué tan grande es el espacio de direcciones de 128 bits?

Habrían 2 ^ 128 direcciones IP diferentes, significa que si la población mundial fuera de 10 billones habría 3.4 * 10 ^ 27 direcciones por persona. O visto de otra forma habría un promedio de 2.2 * 10 ^ 20 direcciones por centímetro cuadrado. Siendo así muy pequeña la posibilidad de que se agoten las nuevas direcciones.

1.7. ¿Cuándo se agotará el espacio de direcciones Ipv4?

No hay una fecha concreta, pero se estima que con el crecimiento actual el número de direcciones IP versión 4 disponibles se agotará antes de que termine la presente década. Teniendo en cuenta que se necesitan varios años de coexistencia entre ambas versiones para preparar la migración, no es difícil imaginar que el paso a la nueva generación de internet se realizará muy pronto.

NAT es un sistema que permite que una red local se pueda conectar a internet teniendo una única dirección IP real, por ejemplo, la dirección IP asignada a una conexión ADSL o cable. Casi todas las redes locales actuales se implementan asignando a cada ordenador direcciones IP privadas del rango 192.168.X.X. Estas direcciones se pueden asignar libremente dentro de una red local, pero a cambio no pueden utilizarse en la red internet.

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

El NAT se encarga de gestionar todas estas conversiones entre IPs privadas internas y la IP real. La existencia del NAT ha sido un auténtico salvavidas para el protocolo IP actual (versión 4). Sin el NAT hace mucho tiempo que las direcciones IP se hubieran agotado, pues no hay suficientes como para asignar una dirección única para cada equipo susceptible de conectarse a internet. Entonces cabría preguntarse, ¿no sería posible seguir soportando con el esquema de direccionamiento IP actual a base de utilizar más y más NAT?. La respuesta es que las direcciones IP versión 4 se están agotando, incluso contando con un uso masivo del NAT. Si además se toma en cuenta que en un futuro cercano, multitud de dispositivos como teléfonos móviles, UMTS o electrodomésticos estarán conectados a internet de forma permanente (con dirección IP fija), queda claro que el uso del NAT sería insuficiente para satisfacer tal demanda de conectividad.

Además, NAT añade complejidad de mantenimiento y uso de recursos de computación en los *routers*. Los *routers* que realizan NAT tienen que reasignar las direcciones IP de cada uno de los paquetes entrantes o salientes a la red, lo cual es una sobrecarga grande de CPU respecto a su misión original, que es simplemente enrutar los paquetes. Además se ha de tener en cuenta que Ipv6 no solamente incrementa el espacio de direccione; es más que eso, Ipv4 se ha utilizado durante más de veinte años y existen agujeros y limitaciones en sus especificaciones para el uso actual. Ipv6 intenta incluir tecnologías que están utilizándose actualmente e intenta ser un protocolo preparado para el siglo XXI.

1.8. Direccionamiento en el Ipv6

Las direcciones son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en Ipv4 en los nodos se asignan a interfaces. Se clasifican en tres tipos:

- Unicast: identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada con dicha dirección.

- Anycast: identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast.

- Multicast: identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección. En el Ipv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

1.9. Representación de las direcciones Ipv6

Existen tres formas de representar las direcciones Ipv6 como *strings* de texto.

- x:x:x:x:x:x:x:x : donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo. Por ejemplo:

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

- Será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de utilizar sintácticamente dos puntos continuos ::. El uso de :: indica múltiples grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección. Por ejemplo:

1080:0:0:0:8:800:200C:417A	*unicast address*
FF01:0:0:0:0:0:0:101	*multicast address*
0:0:0:0:0:0:0:1	*loopback address*
0:0:0:0:0:0:0:0	*unspecified addresses*

Podrán ser representadas como:

1080::8:800:200C:417A	*unicast address*
FF01::101	*multicast address*
::1	*loopback address*
::	*unspecified addresses*

- Para escenarios con nodos Ipv4 e Ipv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:x:d.d.d.d, donde x representa valores hexa-decimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones Ipv4. Ejemplos:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

1.10. ¿Cómo se asignarán las nuevas direcciones Ipv6 a los usuarios?

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

Existe una diferencia muy grande entre las recomendaciones para la asignación de las direcciones IP versión 4, que busca ante todo la economía de direcciones y las de la versión 6 que busca la flexibilidad. RIPE recomienda a los ISP y operadores que asignen a cada cliente de Ipv6 una subred del tipo /48 con el fin de que el cliente pueda gestionar sus propias subredes sin tener que utilizar NAT (el NAT desaparece en Ipv6).

Con el protocolo IP versión 4 un cliente de conectividad (por ejemplo, con una conexión RDSI) de arsys.es podría tener como mucho, una única dirección IP fija para su red. Las direcciones IP de los equipos de su red local deberían ser privadas (192.168.X.X) y utilizar NAT para dar salida a internet a su red local. Sin embargo, con Ipv6 el cliente recibiría una subclase como la siguiente:

2001:0ba0:1c01::/48

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

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

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

1.11. ¿Por qué Ipv6 y no Ipv5?

La información que circula por una red IP como internet está distribuida en paquetes. Cada paquete incluye no solo los datos a transmitir sino también un envoltorio que, entre otras cosas, tiene el número de versión del protocolo IP que se está utilizando. IANA decidió asignar el número de versión 5 para un protocolo experimental que nunca llegó a utilizarse en la práctica llamado ST-II *Stream Protocol versión 2*. Si el número es 4 entonces se trata de un paquete normal, si es 5 entonces es un paquete del *Stream Protocol*. Por ese motivo el número 5 no se puede utilizar para designar a la versión del protocolo IP que sigue a la 4. Por tanto no hay un salto de versión, simplemente la versión 6 es la que sigue a la 4 porque el número 5 se reservó para otro protocolo.

1.12. ¿Dónde conseguir una implementación de Ipv6 para un sistema operativo?

Para utilizar Ipv6 en su ordenador necesita tener instalado como protocolo de red el software IP versión 6, el cual está disponible para, prácticamente todos los sistemas operativos.

En el caso de Windows XP y Windows 2003, el software viene incorporado con el sistema operativo, aunque es necesario instalarlo, ya que no viene instalado como protocolo de red por defecto. Para los restantes sistemas operativos deberá descargar el software correspondiente para la pila TCP/IP en versión 6 e instalarlo en su equipo.

1.13. DNS e Ipv6

El almacenamiento actual de direcciones de internet en el *Domain Name System* (DNS) de Ipv4 no se puede extender fácilmente para que soporte direcciones Ipv6 de 128 bits, ya que las aplicaciones asumen que a las consultas de direcciones se retornan solamente direcciones Ipv4 de 32 bits. Inicialmente, para resolver este problema, se definieron las siguientes extensiones:

- Un nuevo tipo de registro: el registro AAAA se usa para almacenar direcciones Ipv6, porque las extensiones están diseñadas para ser compatibles con implementaciones de DNS existentes.

- Un nuevo dominio para soportar búsquedas basadas en direcciones Ipv6: este dominio es IP6.INT.

- Redefinición de las consultas existentes: que localizan direcciones Ipv4, para que puedan también procesar direcciones Ipv6.

Posteriormente, para soportar el concepto de *aggregation* de direcciones, renumeración y *multihoming*, se incluyeron las siguientes extensiones:

- Un nuevo tipo de registro: A6 para almacenar las direcciones Ipv6, y facilitar la renumeración y *multihoming* de redes.

- Un nuevo dominio IP6.ARPA: definido para soportar búsquedas basadas en direcciones Ipv6, que en el futuro sustituirá al dominio IP6.INT. Para ejecutar las búsquedas de reverso, asociadas al dominio IP6.ARPA, definió un nuevo formato llamado *Binary Labels*.

- Redefiniciones a consultas existentes que localizan direcciones Ipv4, para que procesen direcciones Ipv4 e Ipv6.

- Un método de delegación de prefijo, basado en un nuevo registro DNAME: este provee la capacidad de relacionar (*MAP*) un subárbol entero del DNS con otro dominio. Se diferencia del registro *CNAME* que relaciona solamente un nodo del DNS.

1.14. Mecanismos de transición básicos

Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en *hosts* y *routers*, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de internet al Ipv6 con la menor interrupción posible.

Existen dos mecanismos básicos:

- *Dual Stack*: provee soporte completo para Ipv4 e Ipv6 en *host* y *routers*.

- *Tunneling*: encapsula paquetes Ipv6 dentro de *headers* Ipv4 siendo transportados a través de infraestructura de ruteo Ipv4.

Están diseñados para ser usados por hosts y *routers* Ipv6 que necesitan ínter operar con hosts Ipv4 y utilizar infraestructuras de ruteo Ipv4. Se espera que muchos nodos necesitarán compatibilidad por mucho tiempo y quizás indefinidamente. No obstante, Ipv6 también puede ser usado en ambientes donde no se requiere interoperabilidad con Ipv4. Nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

1.15. *Dual Stack*

La forma más directa para los nodos Ipv6 de ser compatibles con nodos Ipv4-only es proveyendo una implementación completa de Ipv4. Los nodos Ipv6 que proveen una implementación completa de Ipv4 son llamados nodos Ipv6/Ipv4. Estos nodos tienen la habilidad de enviar y recibir paquetes Ipv6 e Ipv4, pudiendo así ínter operar directamente con nodos Ipv4 usando paquetes Ipv4, y también operar con nodos Ipv6 usando paquetes Ipv6.

1.15.1. Tunneling

Los nodos o redes Ipv6 que se encuentran separadas por infraestructuras Ipv4 pueden construir un enlace virtual, configurando un túnel. Paquetes Ipv6 que van hacia un dominio Ipv6 serán encapsulados dentro de paquetes Ipv4. Los extremos del túnel son dos direcciones Ipv4 y dos Ipv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual. Un ejemplo de redes conteniendo túneles configurados es el 6bone. Los túneles automáticos no necesitan configuración manual.

1.15.2. ¿Qué es el 6bone?

El 6bone es el *backbone* de Ipv6, su función es asistir en la evolución y desarrollo del Ipv6. Su creación se formalizó en marzo de 1996 en una reunión del IETF en Los Ángeles. Es una red experimental, informal y cooperativa de alcance mundial. Está supervisada por el grupo *Next Generation Transition* (*ngtrans*) del IETF y opera bajo Ipv6 *Testing Address Allocation*.

Está formada por varios 6bones regionales. Aunque la mayoría de los 6bones utilizan túneles, lentamente algunos de ellos están migrando a links nativos Ipv6. Uno de ellos es el *WIDE 6bone* del proyecto *WIDE* de Japón.

Actualmente existen otros *backbones* académicos y comerciales que ofrecen servicios Ipv6. El objetivo inicial del 6Bone era validar los estándares e implementaciones del Ipv6, Su objetivo es validar los procedimientos de transición.

2. IPV6 SOBRE DIFERENTES MEDIOS

2.1. Método de transmisión de paquetes Ipv6 sobre redes *Ethernet*

Las redes *Ethernet* fueron diseñadas como un protocolo destinado a cubrir las necesidades de las redes *LAN*. A partir de 2001 Ethernet alcanzó los 10 Gbit/s, lo que dio mucha más popularidad a la tecnología, se ha situado en una buena posición para extenderse al nivel *WAN.*

2.1.1. El tamaño máximo de transmisión MTU

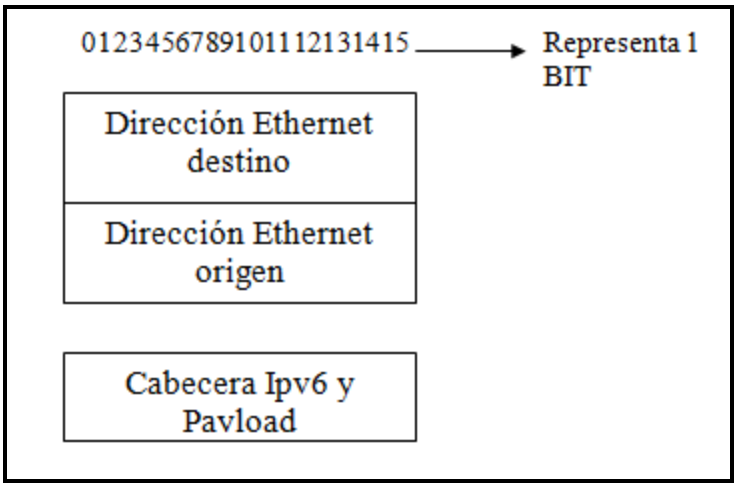
Para el protocolo Ipv6 el tamaño máximo de transferencia de paquetes sobre redes Ethernet es de 1 500 octetos, el cual puede ser más pequeño dependiendo del aparato de hardware que se utilice. El tamaño puede ser reducido por un *Router*, el cual debe de contener una opción MTU que especifique o que se pueda especificar un tamaño o un MTU más pequeño, el cual puede ser configurado manualmente o automáticamente. Si un *Router* poseyera un MTU mayor a 1,500 la configuración, ya sea manualmente o automáticamente debe de ser ignorada.

2.1.2. El formato de la cabecera

Los paquetes que son transmitidos sobre redes Ethernet son estándares. Están los campos cabecera y datos. Como las cabeceras estándares, estas poseen en la cabecera la información de la dirección destino, la dirección origen y el código de tipo de red *Ethernet*, el cual debe contener el valor 86DD hexadecimal.

En el campo de datos contiene la cabecera Ipv6 seguida de los datos *PayLoad*, y tal vez haya más datos para poder llenar el tamaño mínimo para una red Ethernet.

Figura 1. **Campos de cabecera**



Fuente: elaboración propia.

2.1.3. Estado de auto configuración

El identificador de la interface para una red Ethernet está basado en la EUI-64 derivado de las interfaces de 48-BIT de la IEEE 802 de direccionamiento.

El EUI-64 está conformado como se describe a continuación: los primeros 3 octetos componen del ID de la empresa de EUI-64, el cuarto y el quinto son asignados para un valor de FFFE hexadecimal. Los últimos 3 octetos de la dirección de red Ethernet se convierten en los últimos 3 octetos de EUI-64.

El identificador es convertido de la EUI-64 complementando con Universal/local (U/L) BIT, el cual es el siguiente valor bajo de significancia (BIT) del primer octeto de la EUI-64. Este BIT puede después cambiar a 0 para describir valores de la IEEE 802 o de EUI-64, sin embargo, para la dirección global de Ipv6 es con valor 1. Por ejemplo, el identificador de interface para una interface Ethernet la cual éste construido sobre una dirección hexadecimal:

34-56-78-9A-BC-DE

Puede volverse

36-56-78-FF-FE-9A-BC-DE.

Una dirección MAC que sea manipulada manualmente no debe de ser usada para un identificador de interface, pero si esta dirección MAC debe de ser utilizada, entonces esta dirección MAC debe poseer un valor en el BIT U/L. Un prefijo de una dirección Ipv6 usada para un estado de auto configuración de una interface Ethernet, debe de poseer una longitud de 64 bits.

2.1.4. Establecimiento de direcciones locales

El direccionamiento de Ipv6 de una interface Ethernet es formado por el identificador de la interface como es definida a continuación:

Figura 2. **Prefijo FE80::/64**

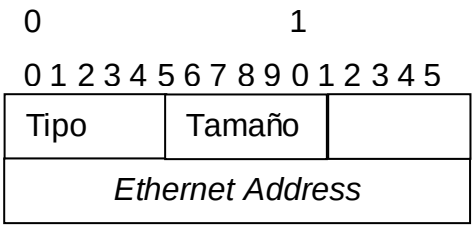
10 bits	54 bits	64 bits
111111	(Ceros)	Identificador

Fuente: elaboración propia.

2.1.5. Mapeo de direccionamiento Unicast

El procedimiento de mapear una dirección Unicast hacia una capa de direccionamiento Ethernet, tiene una opción cuando la capa de red es Ethernet como se describe a continuación:

Figura 3. **Mapeo de direccionamiento Unicast Ethernet**



Tipo 1:	para dirección capa de red origen
Tipo 2:	para dirección capa de red destino
Tamaño:	1 (en unidades de 8 bits)
Ethernet Address:	La dirección Ethernet de 48 BIT, en orden canónica. Esta es la dirección a la que normalmente responde y hace la diferencia de la dirección del identificador de interface.

Fuente: elaboración propia.

2.1.6. Mapeo de direccionamiento Multicast

Un paquete de Ipv6 con un destino multicast DST, consiste en los 16 BIT desde DST(1) hasta DST(16), es transmitido hacia la dirección de multicast de Ethernet, la cual los primeros 2 octetos son el valor 3333 hexadecimal y de los cuales los últimos 4 octetos son los últimos 4 octetos de la DST.

2.2. Método de transmisión de paquetes ipv6 sobre FDDI

Conjunto de estándares OSI y ANSI para la transmisión de datos en redes de área extendida WAN o local LAN mediante cable de fibra óptica.

2.2.1. El tamaño máximo de transmisión MTU

El tamaño de las FDI permite octetos de 4500 (9000 símbolos), incluyendo, por lo menos 22 octetos (44 símbolos) de encapsulación de datos cuando se utilizan direcciones de formatos largos. Sustrayendo 8 octetos de la cabecera LLC/SNAP, esto permitirá que el paquete de ipv6 en el campo de información pueda tener un máximo de 4470 octetos. Es deseable permitir que el tamaño sea variable y que futuras posibles extensiones para el encabezado MAC y campos de status del marco. Por lo anterior, el tamaño default de la MTU para un paquete de Ipv6 sobre redes FDDI es de 4,352 octetos. El tamaño puede ser reducido por un *Router* conteniendo una opción para MTU que especifica una menor, o manualmente configurar cada *Router*.

Si un *router* posee una interface de FDDI y tiene una opción de MTU 4,352 octetos o más grande de un valor configurada manualmente, puede ser que este *Router* esté conectado a un sistema de mantenimiento, pero este debe de ser ignorado

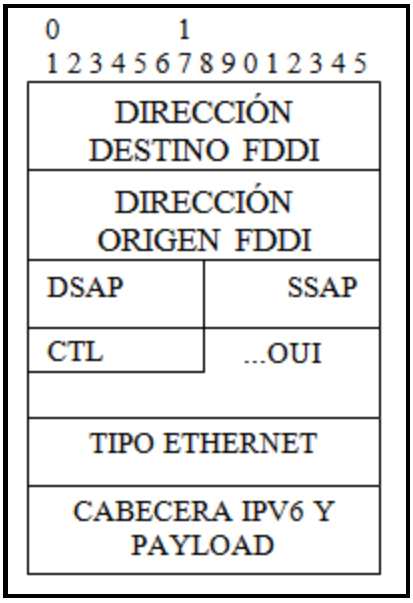
.

2.2.2. El formato de la cabecera

FDDI provee transmisiones, tanto asíncronas como síncronas. Únicamente transmisiones asíncronas con *Tokens* no restringidos son requeridas para la intemporalidad FDDI. En contraste, paquetes de ipv6 deben ser enviados asincrónicamente utilizando *Tokens* no restringidos.

El principio de robustez, dicta que los nodos deben recibir tanto marcos asíncronos como marcos síncronos, utilizando por su puesto *Tokens* no restringidos. Los paquetes Ipv6 son transmitidos en marcos LLC/SNAP, usando direccionamiento largo de 48 BIT. El campo de datos contiene la cabecera de Ipv6 y el cuerpo *PayLoad*, el cual es seguido por el marco de chequeo de secuencia de FDI, terminando con símbolos de delimitación y de estado para el marco.

Figura 4. **Campos de cabecera FDDI**



Fuente: elaboración propia.

Campos de cabecera FDDI:

- FC: el código de marco *Frame Code* tiene que estar en el rango de 50 a 57 hexadecimal, con los tres menores bits de prioridad del marco.

- DSAP, SSAP: ambos campos deben de contener el valor AA hexadecimal, indicando encapsulación SNAP.

- CTL: el campo de control *Control Field* tiene que tener un valor de 03 hexadecimales.

- OUI: el identificador organizacional tiene que estar el valor puesto a 000000 hexadecimal.

- Tipo de Ethernet: el protocolo de tipo de *Ethernet Type*, debe contener el valor 86DD hexadecimal.

2.2.3. Interacción de FDDI con Bridges

El protocolo 802.1d de direcciones MAC para Bridges que conecta diferentes medios, por ejemplo: el Ethernet y el FDI se han vuelto muy amplio. Algunas de estas realizan la fragmentación de Ipv4 y soportan el MTU para Ipv4, otras no lo soportan, o lo soportan de forma incorrecta. El uso de diferentes medios de *Bridges* que utilizan Ipv6, no debe depender de MAC Bridges, a no ser que los *Bridges* sean específicamente utilizados para que puedan utilizar los protocolos de Ipv6.

Para la correcta operación de diferentes medios de Bridges, utilizando unos que si soportan Ipv6 MTU y otros que no lo soportan, los de menor MTU son los que deben configurar la comunicación. Si de casualidad no existiera ningún r*outer*, la MTU debe de ser configurada manualmente en cada nodo el cual está conectado al medio, configurando el MTU más pequeño.

2.2.4. Estado de auto configuración

El identificador de interface, de una interface FDI está basado en un identificador EUI-64 derivado de las interfaces de 48-BIT del direccionamiento de IEEE 802. El OUI de la dirección MAD de FDI, los primeros 3 octetos, se convierten en los identificadores de compañía de la EUI-64. El cuarto y el quinto octeto de la EUI son asignados con el valor de FFFE hexadecimal.

Los últimos 3 octetos del direccionamiento MAC de FDI se convierten en los 3 últimos octetos de la EUI-64. El identificador de interface es formado de la EUI-64 complementando el BIT U/L (universal/local), el cual es el primer BIT de significancia baja que utiliza eui-64. Por ejemplo: el identificador de interface para una interface FDI cuya dirección en hexadecimal es:

34-56-78-9A-BC-DE

Se vuelve

36-56-78-FF-FE-9A-BC-DE

Una diferente dirección MAC que sea puesta manualmente o por medio de algún tipo de software no debe derivarse en el identificador de interface. Si esta dirección MAC tiene que ser utilizada, su propiedad única debe verse reflejada en el valor del BIT U/L. Un prefijo utilizado por el estado de auto configuración de una interface FDDI debe de tener una longitud de 64 bits.

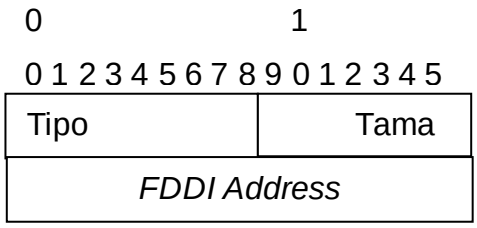
2.2.5. Establecimiento de direcciones locales

El direccionamiento local para una interface FDI es formada por el identificador de interface, como se define a continuación, por el prefijo FE80::/64, el cual podemos visualizar en la Figura 2.

2.2.6. Mapeo de direcciones Unicast

El procedimiento de mapear una dirección Unicast hacia una capa de red FDDI de direcciones es descrito en (disc). El origen / blanco de la capa red de la opción de dirección tiene el siguiente formato cuando la capa es FDDI:

Figura 5. **Mapeo direcciones Unicast FDDI**



Tipo 1: para dirección capa de red origen

Tipo 2: para dirección capa de red destino

Tamaño: 1 (en unidades de 8 bits)

FDDI *Address*:

1. El 48 BIT FDDI IEEE 802 direccionamiento, en orden de BIT canónico.
2. Esta la dirección a la que usualmente responde.
3. Tal vez sea diferente de la dirección del identificador de interface.

Fuente: elaboración propia.

2.2.7. Mapeo de direcciones Multicast

Un paquete de Ipv6 con un destino multicast DST consiste en los 16 BIT desde DST(1) hasta DST(16), es transmitido hacia la dirección de multicast de FDDI, de los primeros 2 octetos son el valor 3333 hexadecimal de los cuales los últimos 4 octetos son los últimos 4 octetos de la DST.

2.3. Transmisión de paquetes Ipv6 sobre dominios Ipv4 sin túneles explícitos

Un nodo que solo trabaje con Ipv4 no puede recibir un paquete Ipv6.

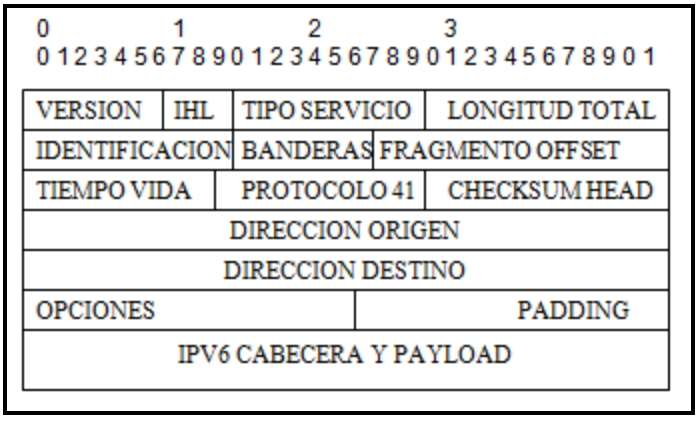
2.3.1. Tamaño máximo de transmisión

El tamaño máximo de transmisión de un paquete Ipv6 sobre un dominio de Ipv4 es 1480 octetos. Este tamaño puede ser variado dependiendo de un *Router* conteniendo una MTU con opción que especifica una diferente MTU, o por una configuración manual de cada nodo.

2.3.2. Formato de la cabecera

Paquetes Ipv6 son transmitidos sobre paquetes Ipv4 con un protocolo Ipv4 de tipo 41(proto-41), el mismo que ha sido asignado por los paquetes Ipv6 que son enviados sobre marcos de Ipv4. La cabecera del Ipv4 contiene las direcciones origen y destino. El cuerpo del paquete de un Ipv4 contiene la cabecera de Ipv6 seguidamente del *PayLoad*.

Figura 6. **Formato cabecera sin túneles explícitos**



Fuente: elaboración propia.

Si hay opciones de Ipv4, entonces el campo PADDING deberá ser agregado a la cabecera para que la cabecera de Ipv6 empiece en un límite de 32 BIT Offset del final de la cabecera de datos. El campo de tiempo vida *TimeToLive* debe de estar puesto con un valor bajo, para prevenir que los paquetes de Ipv4 se salgan del dominio de Ipv4. Este debe ser un parámetro de configuración, con un valor *Default* recomendado de 8.

2.3.3. Auto configuración sin estado y las direcciones locales

El identificador de interface de una red Ipv4 es de 32-bit, para Ipv6 los octetos en el mismo orden que en la cabecera de un paquete Ipv4, añadiendo hacia la izquierda ceros para completar un total de 64-bit. Hay que hacer notar que el bit local universal es cero, indicando que el identificador de la interface no es globalmente único.

Cuando el cliente (HOST) tiene más de una dirección Ipv4 en uso en la interface física involucrada, una opción administrativa de una de estas direcciones Ipv4 se hace. Un prefijo Ipv6 de dirección usado para auto configuración sin estado de una interface Ipv4, debe tener una longitud de 64-bit salvo un caso especial.

La dirección Ipv6 local para una interface virtual Ipv4 es formada añadiendo el identificador de interface, se utiliza el prefijo FE80::/64.

Figura 7. **Prefijo FE80::/64**

FE	80	00	00	00	00	00	00
00	00	00	00	DIRECCIÓN Ipv4			

Fuente: elaboración propia.

2.3.4. Mapeo de direcciones Unicast

Las direcciones Origen y Destino de la capa de red tienen el siguiente formato. Dado que el campo de longitud esta dado en unidades de 8 bytes, el valor utilizado es de 1.

Figura 8. **Mapeo direcciones Unicast sin túneles explícitos**

TIPO	LONGITUD	DEBE SER CERO	DIRECCIÓN Ipv4

Tipo 1:	para dirección capa de red origen
Tipo 2:	para dirección capa de red destino
Longitud:	1 (en unidades de 8 bits)
Dirección Ipv4:	La dirección de 32-bit de Ipv4, en orden de byte de red. Esta es la dirección de la interface a la que responde, y puede ser diferente del identificador de interface de auto configuración sin estado.

Fuente: elaboración propia.

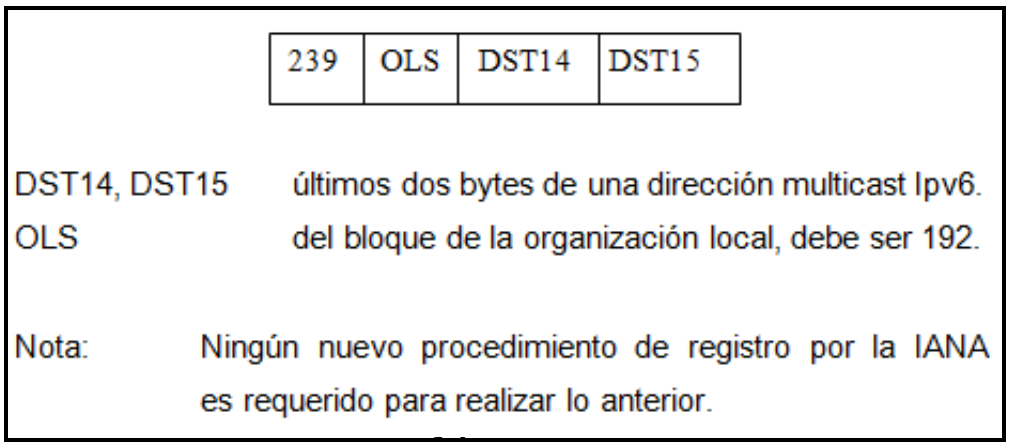
2.3.5. Mapeo de direcciones *Multicast*

Un paquete Ipv6 con una dirección destino *multicast* DST debe transmitirse a las direcciones de *multicast* de la Organización local utilizando el siguiente mapeo:

- Estas direcciones *multicast* Ipv4 deben ser tomadas del bloque 239.192.0.0/16, un subbloque de la direcciones de la organización local o si todos aquellos no están disponibles, de la expansión, los bloques definidos como expansión.

Cuando se utilizan los bloques de expansión, estos bloques solo utilizan un bloque /16 de tamaño.

Figura 9. **Bloque de expansión de tamaño 16**



Fuente: elaboración propia.

El mecanismo del *multicast* descrito parece tener esencialmente las mismas propiedades de un Ipv6 nativo sobre medios de comunicación, salvo la reducción ligera en MTU que se traduce en una reducción de traspaso de volumen.

Un escenario puede escoger empezar su transición a Ipv6 configurando un *Router* Ipv6 para apoyar 6over4 en una interface conectada al dominio del escenario Ipv4, y otro formato de interface Ipv6 conectado a internet Ipv6. Cualquier cliente habilitado para 6over4 en el dominio Ipv4 podrá entonces comunicarse con los dos, con el *Router* y con la internet Ipv6, sin configuración manual de un túnel y sin la necesidad para una dirección compatible Ipv4 - Ipv6.

Durante la transición, los *Routers* necesitaran por lo menos dos prefijos Ipv6, uno para el LAN nativo (ej. Ethernet) y uno para 6over4.

Como con cualquier prefijo Ipv6 asignado a una subred Ipv6, el último debe ser único dentro de su alcance, no importando si son direcciones locales o direcciones globales.

2.3.7. Consideraciones de seguridad

Los impulsores deben ser conscientes que, además de los ataques posibles contra Ipv6, la seguridad contra Ipv4, también debe ser considerado. Uso de seguridad IP a ambos niveles Ipv4 e Ipv6 debe ser tomado en cuenta, por las razones de eficacia. Por ejemplo, si en Ipv6 están corriendo datos encriptados, los datos encriptados de Ipv4 serían redundantes excepto si el tráfico llegara ser una amenaza.

Si Ipv6 está corriendo de modo autenticado, entonces la autenticación de Ipv4 agregará un poco. Recíprocamente, la seguridad de Ipv4 protegerá el tráfico de Ipv6 una vez deje los dominios Ipv6-over-Ipv4, por consiguiente, implementar seguridad con Ipv6 es requerido que la seguridad de Ipv4 esté disponible.

La autenticación está disponible, la técnica utilizada para esto es configurar el r*outer* externo a la red para que acepte solo paquetes de tipo protocolo 41(proto-41) de direcciones orígenes con un rango confiable o rangos confiables de direcciones.

2.4. Transmisión de paquetes Ipv6 sobre redes *Frame Relay*

Es un tipo de comunicación mediante la retransmisión de tramas de una variedad de tamaños para datos, perfecto para la transmisión de grandes cantidades de datos.

2.4.1. Unidad máxima de transmisión MTU

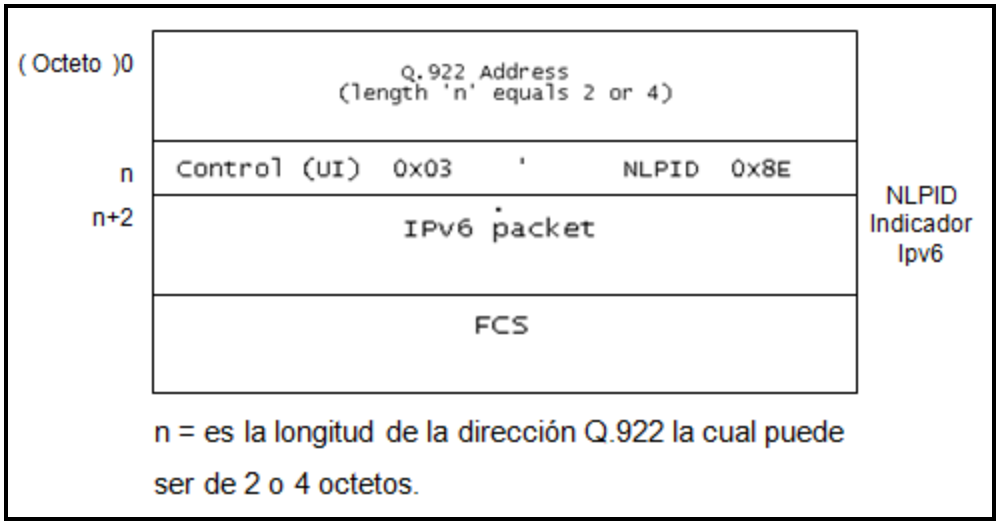
Los dispositivos *Frame Relay* están configurados para tener un máximo de MTU de 1,600 octetos. Por lo tanto, el MTU para una interface de Frame Relay de IPv6 es de 1592. Un tamaño más pequeño puede ser configurado, pero claramente no más pequeño que el mínimo MTU de IPv6. Un tamaño adecuado más grande puede utilizarse para la MTU de Ipv6, para poder así evitar la fragmentación. En general, si capas superiores pueden proporcionar mecanismos adecuados para detección y protección de errores, un MTU de un Frame Relay puede tener un valor mucho más grande, pero para IPv6 no es aconsejable.

La configuración del MTU es posible, puede haber problemas para la transmisión si se definen parámetros de envío y recepción en los cuales la MTU es diferente, por lo consiguiente y por simplificación se asume que son simétricamente iguales.

2.4.2. Formato de la cabecera

El marco de encapsulación para la red Frame Relay sigue lo que estipula el ENCAPS, el cual permite que VC lleve paquetes Ipv6 junto con otros paquetes de otros protocolos. El formato de marco NLPID es usado, en el cual el Ipv6 tiene un valor de 0x8E.

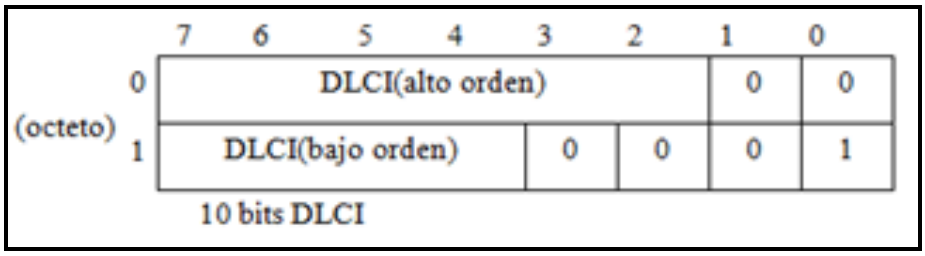
Figura 10. **Formato cabecera *Frame Relay***



Fuente: elaboración propia.

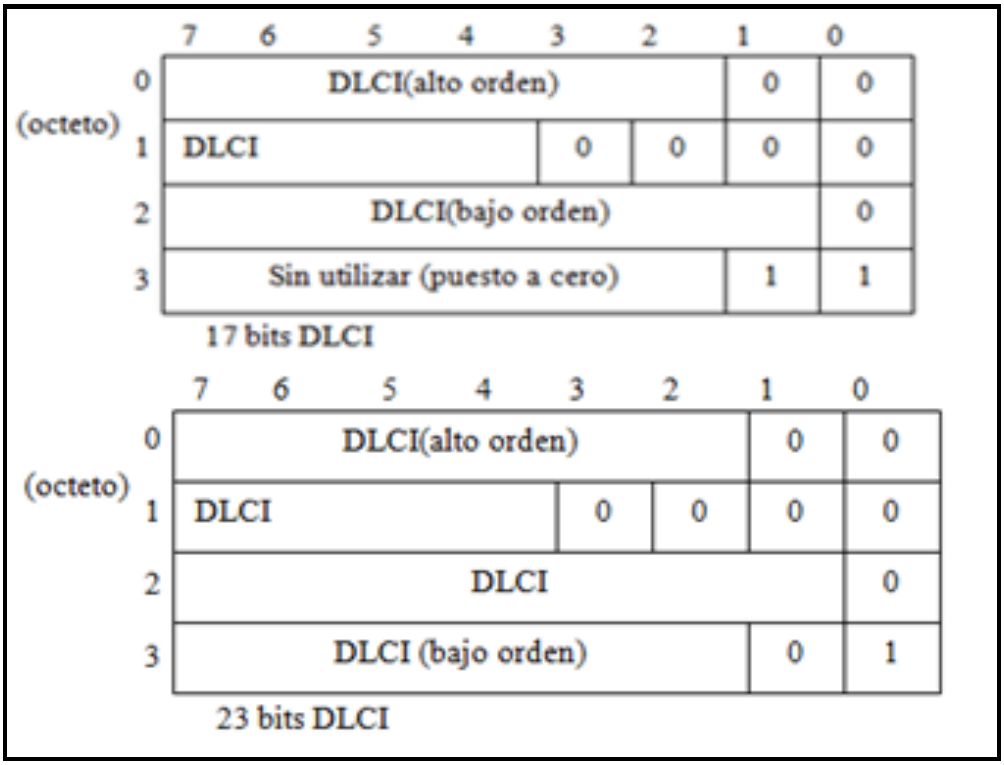
La representación del Q.922 de un DLCI (en orden canónico, el primer BIT es guardado en el menos significativo) es el siguiente:

Figura 11. **Representación Q.922 de un DLCI**



Fuente: elaboración propia.

Continuación de la figura 11.



Fuente: elaboración propia.

2.4.3. Estado de auto configuración

Un identificador de la interface para una red *Frame Relay* debe ser único y también en las redes virtuales representado por el VCs terminado en la interface. La interface para una red *Frame Relay* es generada localmente por el módulo de Ipv6.

Cada circuito virtual en una red *Frame Relay* es identificado como único en una interface DLCI. Además, un DLCI puede verse como una identificación del punto extremo de un circuito virtual en una interface de *Frame Relay*.

2.4.4. Dirección de red local

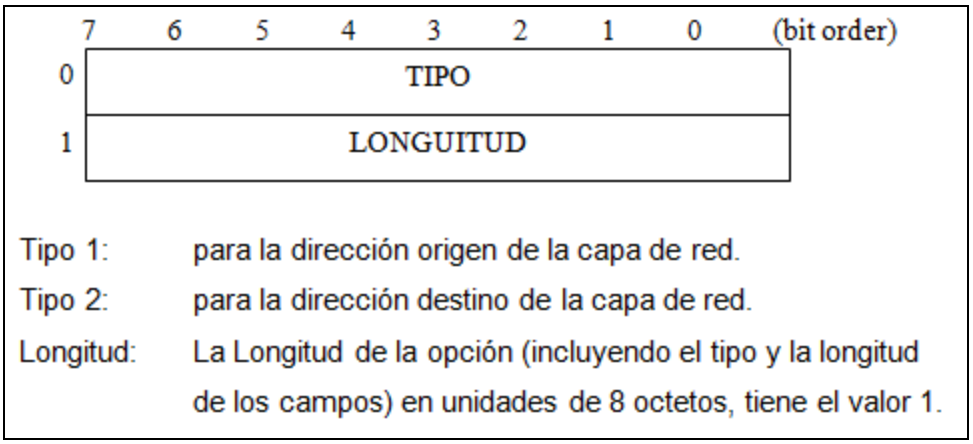
La dirección de red local para una interface *Frame Relay* para Ipv6, es formado por la adición del identificador de interface, el prefijo es FE80::/64, visualizar figura # 2.

2.4.5. Mapeo de direcciones Unicast y Multicast

Las direcciones Ipv6 para un *Frame Relay* pueden ser mapeadas de 2 formas, por DLCIs y por direcciones de *Frame Relay* las cuales son las siguientes:

- FLCI: utiliza él envió de mensajes de descubrimiento de vecinos o descubrimiento inverso de vecino en un VCs(*Virtual Circuit*) que fue establecido antes del envío de mensajes.

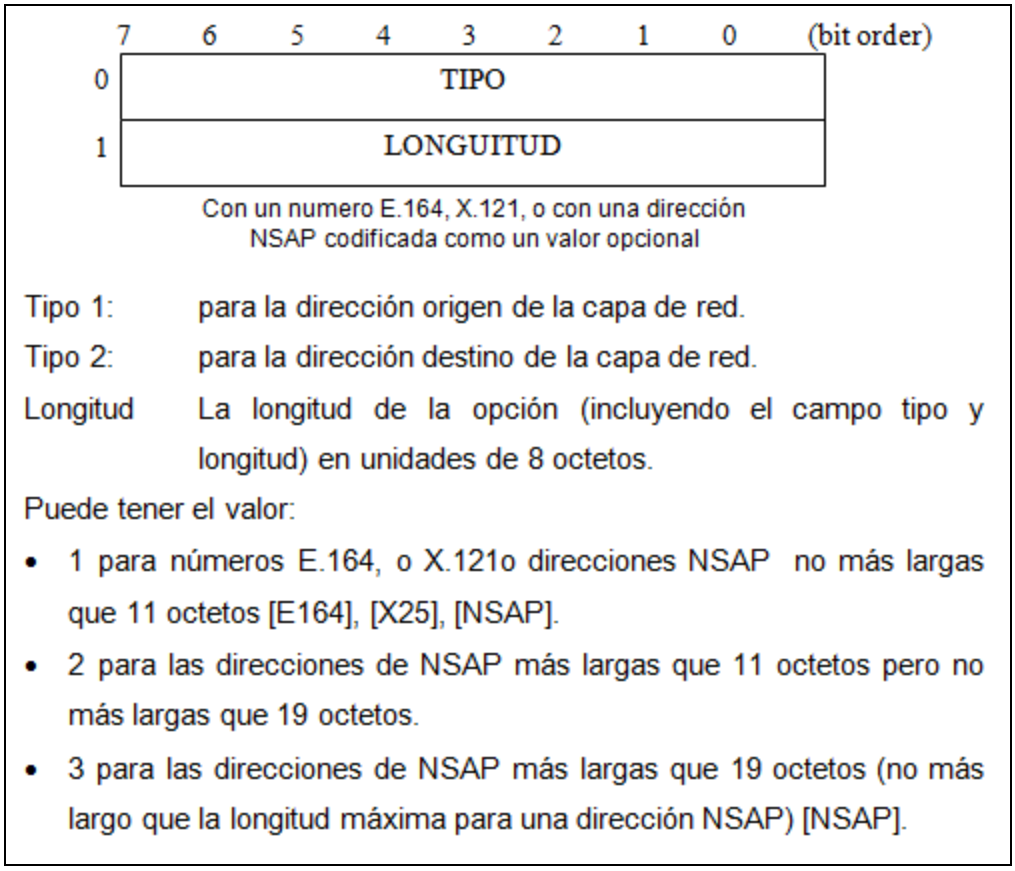
Figura 12. **Mapeo direcciones Unicast y Multicast FLCI**



Fuente: elaboración propia.

- Direcciones *Frame Relay*: utilizadas con más frecuencia antes de establecer una nueva SVC, para obtener el mapeo del identificador del nodo remoto del *Frame Relay* para poder mapearlo a cierta dirección Ipv6.

Figura 13. **Mapeo direcciones Unicast y Multicast Frame Relay**



Fuente: elaboración propia.

2.5. Método de transmisión de paquetes Ipv6 sobre PPP

Protocolo de comunicación, también llamado *Point-to-Point*.

2.5.1. Tamaño máximo de transmisión

El tamaño máximo de transmisión de un paquete Ipv6 sobre un protocolo de capa de red PPP es el mismo al del máximo tamaño del campo de información de un marco del protocolo PPP. Protocolos PPP que soporten Ipv6 deben permitir, por lo menos, el tamaño mínimo para el campo de información del tamaño de MTU mínimo requerido por la Ipv6.

2.5.2. Protocolo de control de red PPP para Ipv6

El protocolo de control de Ipv6 (Ipv6cp) es responsable de configurar, habilitar y deshabilitar los módulos del protocolo Ipv6 en los dos extremos de una conexión o red punto a punto *Point-to-Point*. IPV6CP utiliza el mismo intercambio de paquetes como el protocolo de control de red *Link Control Protocol LCP*. Los paquetes de IPV6CP tal vez no sean intercambiados hasta que el protocolo PPP haya alcanzado la fase de la capa de red, los paquetes que son recibidos antes de que el protocolo PPP alcance esta fase serán descartados.

El protocolo de control de IPV6 es exactamente el mismo que el protocolo de control de red, excepto de las siguientes excepciones:

- Campo de datos del protocolo capa red: un paquete es encapsulado en el campo de información del marco el cual indica que el tipo es 8057 hexadecimal (protocolo de control Ipv6).

- Campo código: únicamente códigos entre 1 y 7 son utilizados (*Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack and Code-Reject*), otros códigos deben ser

tratados como códigos no reconocidos y deben de ser tratados como códigos rechazados.

- Tiempos fuera *TimeOuts*: Los paquetes de IPV6CP tal vez no sean intercambiados hasta que el protocolo PPP haya alcanzado la fase de la capa de red, una implementación debe ser preparada para esperar por autenticación y buena determinación de calidad de red antes de terminar el tiempo de espera de respuesta.

2.5.3. Opciones de configuración para IPV6CP

Las opciones de IPV6CP permiten la negociación de los parámetros de Ipv6. IPV6CP utiliza el mismo formato de opción de configuración definido en el LCP, con una lista separada de opciones. Si una opción de configuración no es incluida en el paquete, se utilizará el valor default para la configuración del mismo. Los valores presentes son los siguientes:

2.5.3.1. Identificador de interface

Provee un método para negociar 64 bits únicos de identificador de interface para ser utilizados en el direccionamiento del auto configuración en la parte final de la red. El identificador de interface debe ser único para la capa de red PPP y también sobre toda la red. Asumiendo que los bits del identificador de interface sean numerados del 0 hasta el 63 en forma canónica y con un orden cuando el más significante BIT es el de numero 0 y el de menos significativo es el de 63, hay que decir que el valor 6 es el llamado BIT u (*universal/local BIT en IEEE EUI-64 TERMINOLOGY*), la cual indica está basado en un único valor global de la IEEE de identificadores.

Este valor es puesto a 1 si un el identificador de IEEE es globalmente único, el valor es puesto a cero si lo anterior no se cumple. Los siguientes métodos son una opción para escoger el identificador de interface en el orden de preferencia:

- Un identificador global de la IEEE está disponible en cualquier lado en el nodo y debe ser utilizado para construir el identificador de interface con sus propiedades únicas. Si se trata de extraer un identificador global de la IEEE de cualquier otro aparato o dispositivo en el nodo, debe tenerse el respectivo cuidado de que el identificador sea ordenado de forma canónica.

- Si un identificador global de la IEEE no está disponible, otra forma de que sea único deberá ser utilizada. Se puede tomar direcciones de la capa de red, series de las maquinas, etc.

- Si no se puede encontrar una forma de ser único, se recomienda que un número sea generado de forma aleatoria. De lo contrario identificador de interface debe de ser puesto a cero.

2.5.3.2. Protocolo de compresión de Ipv6

Esta opción de configuración provee una forma de negociar el uso de un paquete específico de Ipv6 con protocolo de compresión. El protocolo de compresión de Ipv6, la opción de configuración es utilizada para indicar si está habilitado para recibir paquetes comprimidos.

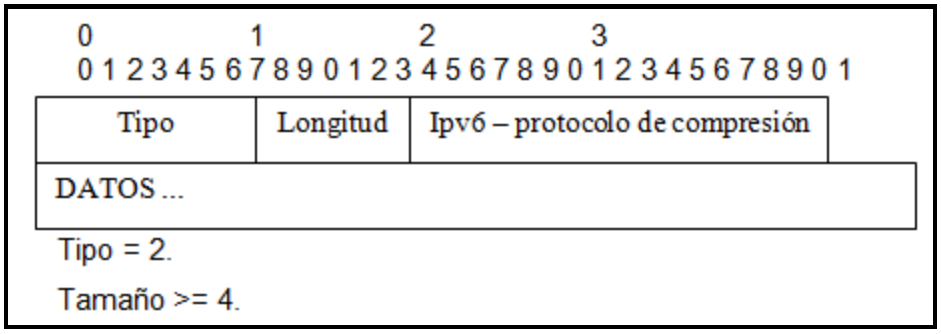
Cada lado de la red, cada *Host* debe separadamente configurar esta opción si se está utilizando una transmisión bidireccional, la cual utilice el

protocolo de compresión de Ipv6, por default el protocolo de compresión no está habilitado.

La compresión de Ipv6 negocia con las opciones específicas de los data gramas de Ipv6 y no debe de confundirse con el protocolo de control de compresión de data gramas CCP.

En la siguiente figura se puede visualizar el marco que utiliza este protocolo de compresión:

Figura 14. **Protocolo compresión Ipv6**



Fuente: elaboración propia.

Los tipos de compresión pueden ser los siguientes:

- Ipv6: tiene un campo de dos octetos e indica el protocolo de compresión deseado. Valores de este campo son los mismos del campo del protocolo de capa de red de datos de PPP, valores del mismo protocolo de compresión. Normalmente no son asignados los valores del campo del protocolo de compresión.

- Datos: el valor de campo es cero o más octetos y contiene datos adicionales que son determinados por un protocolo de compresión particular

- Default: cuando este está presente, quiere decir que el protocolo de compresión no está habilitado.

2.6. Método de transmisión de paquetes Ipv6 sobre redes ATM

La utilización del protocolo IP sobre redes ATM es ciertamente compleja, debido a las importantes diferencias de diseño que existen entre ambos. La naturaleza orientada a conexión de las redes ATM no constituye el entorno ideal para un protocolo no orientado a conexión como IP.

La configuración de las redes ATM tanto en entornos WAN como en redes de acceso basadas en tecnologías xDSL (sus dos ámbitos tradicionales) es estática, basada en el uso exclusivo de circuitos permanentes (PVC) preconfigurados.

El uso de PVC simplifica significativamente la utilización conjunta de IP y ATM. Sin embargo, tiene importantes inconvenientes a la hora de aplicarse a un entorno como el planteado en BTI, ya que no permite la realización de reservas de QoS dinámicas que deben traducirse en el establecimiento dinámico de circuitos ATM (SVC), ni el aprovechamiento del servicio multipunto ATM para soportar tráfico multicast IP, ambos requisitos fundamentales a la hora de soportar las aplicaciones multimedia seleccionadas en BTI.

2.6.1. Solución de Ipv6 sobre ATM

La solución inicial planteada para llevar datagramas IP sobre SVC se especificó siguiendo el modelo clásico de IP, que se basa en definir cómo un datagrama IP viaja sobre una determinada subred. Dicha solución, denominada CLIP (*Classical IP over ATM*), engloba dos entidades: el servidor de ATMARP y el servidor MARS (*Multicast Address Resolution Server*).

El primero se encarga de la resolución de direcciones IP a ATM. Esta función que se resuelve de una forma sencilla en las redes locales utilizando sus mecanismos de difusión, ha de realizarse de forma centralizada en ATM. Todos los clientes mantienen una conexión con el servidor y hacia el dirigen sus preguntas cuando necesitan obtener la dirección ATM que corresponde a una determinada dirección IP. El segundo se encarga de la gestión de los grupos multicast. A diferencia de lo que sucede en las redes locales, la correspondencia directa entre direcciones IP multicast y direcciones ATM no es posible, puesto que en ATM no existen direcciones multicast dinámicamente.

La solución pasa por gestionar la correspondencia entre direcciones IP multicast y el conjunto de las direcciones ATM de los clientes que en cada momento desean recibir el tráfico dirigido a dicha dirección de grupo. Esta es precisamente la función del servidor de MARS. A la hora de enviar tráfico multicast, el estándar MARS define dos posibles escenarios:

- El centralizado está basado en la existencia de un servidor de multicast (*MultiCast Server,* MCS), todos los emisores que envían tráfico a un grupo multicast establecen una conexión con una misma máquina, que es raíz de un único circuito multipunto compartido hacia los miembros del grupo.

- El segundo escenario es el distribuido (VC *mesh*), donde cada emisor realiza una consulta al servidor de MARS, para obtener las direcciones ATM de los miembros del grupo, abriendo posteriormente un circuito multipunto directamente con ellos.

Esta última opción fue la escogida para el desarrollo realizado, ya que, a pesar de presentar más problemas de escalabilidad, es la única que soporta de una manera estandarizada la especificación del soporte de QoS. En el caso de la nueva versión del protocolo Ipv6, la solución planteada para su funcionamiento sobre ATM es similar. Sin embargo, existen algunos cambios de importancia.

El modelo empleado para la resolución de direcciones en Ipv6 basado en el protocolo *Neighbour Discovery (ND)* se ha definido de forma genérica, independiente de subred y se ha obligado a que toda subred ofrezca servicio de multicast. La consecuencia es que en Ipv6 no es necesaria la existencia del servidor de ATMARP utilizando un solo protocolo ND para resolver direcciones de cualquier tipo de subred (a diferencia de lo que sucede en Ipv4 con la utilización de dos protocolos: ARP para redes locales y ATMARP para ATM). Sin embargo, esta solución implica la obligatoriedad de soportar multicast que se plantea como opcional en Ipv4.

2.6.2. Servicios integrados sobre ATM

Dentro del modelo de internet de servicios integrados (*IntServ*) propuesto para dotar a las redes IP de soporte de QoS, se propone la utilización del protocolo RSVP (*Resource ReSerVation Protocol*) como protocolo de señalización que permita a los sistemas finales realizar peticiones de reserva de recursos para sus flujos de datos. RSVP se basa principalmente en dos tipos de

mensajes denominados: PATH, cuyo objetivo es informar acerca de las características de los flujos de datos enviados; y RESV, para realizar las reservas de recursos.

Sin embargo, la aplicación del modelo *IntServ* a escenarios ATM no es sencilla, debido a las sustanciales diferencias entre ambos modelos de soporte de QoS. Cabe mencionar, como aspectos más relevantes a este respecto, los siguientes:

- RSVP establece peticiones de reserva iniciadas en el receptor, mientras que la señalización ATM relacionada con la apertura de circuitos es iniciada en el emisor. La solución requiere comunicar al emisor la necesidad de apertura de un circuito ATM, junto con la QoS requerida, para que sea él mismo el que realice la apertura.

- RSVP: permite cambios dinámicos en los parámetros de QoS en una sesión, sin embargo los parámetros en un circuito ATM son estáticos: para cambiarlos, es necesario cerrar el circuito y abrir otro.

- La reserva de recursos que se define en RSVP es unidireccional: en el caso de circuitos ATM, esta reserva es bidireccional si el circuito es Unicast, y unidireccional si es *multicast* (aunque se permiten reservas asimétricas, e incluso una reserva nula en uno de los sentidos).

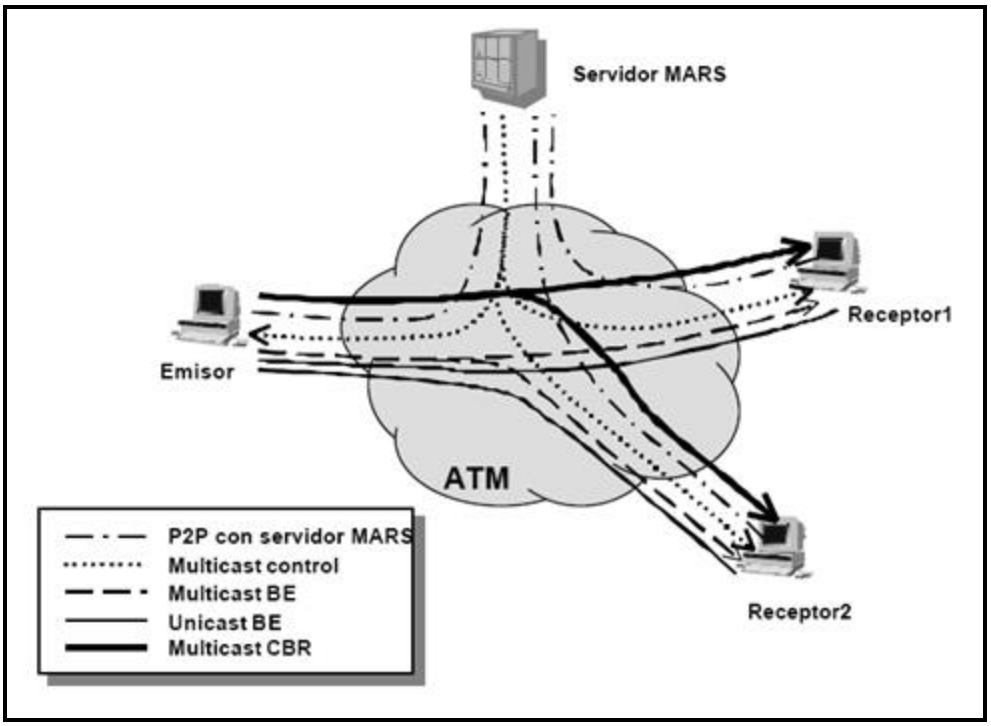
- RSVP: permite heterogeneidad en las reservas hechas por los diferentes miembros de una sesión *multicast*. Pero un circuito ATM *multicast* proporciona la misma calidad de servicio a todos los receptores.

A pesar de la dificultad que entraña la implementación de *IntServ* sobre ATM, el esfuerzo invertido en los últimos años ha dado como resultado una serie de estándares que especifican de forma detallada cómo debe realizarse.

2.6.3. Complejidad de los escenarios

Tras el repaso a las distintas tecnologías que participan en el desarrollo realizado, y como ejemplo de la complejidad de los escenarios que las aplicaciones imponen, se puede mencionar el caso de un audio conferencia con garantías de calidad de servicio en la que se tienen un emisor y dos receptores que pertenecen a un grupo *multicast*.

Figura 15. **Audio conferencia con un emisor y dos receptores**



Fuente: GARCÍA, Ana B. *Soporte de calidad de servicio en internet sobre redes ATM*, *http://www.it.uc3m.es/azcorra/papers/atm_qos_telecom00.pdf*. Consulta: 20 de marzo de 2013.

Como se puede observar, en este caso cada cliente debe gestionar entre cinco y seis circuitos ATM (de entrada y/o salida) que transportan tráfico de distinta naturaleza:

- El servidor de MARS establece un circuito multipunto con todos los clientes, con el propósito de difundir información sobre las pertenencias a los grupos multicast IP.

- Cada uno de los clientes (emisor y receptores) establece un circuito punto a punto de control con el servidor de MARS para solicitar las direcciones de los miembros de un determinado grupo.

- El emisor establece un circuito multicast BE con los dos receptores, por el que se envían los mensajes RSVP de PATH.

- Cada receptor establece un circuito Unicast BE con el emisor por el que se envían los mensajes RSVP de RESV (solicitud de reserva de recursos).

- El emisor establece un circuito multicast con QoS con los dos receptores, por el que se envían los datos de la aplicación.

Este elevado número de circuitos da una idea de lo complejo de la implementación de la torre de protocolos integrada, así como de los problemas de escalabilidad que se vislumbran al aplicar esta solución a redes con un gran número de nodos.

2.6.4. Torre de protocolos integrada

Uno de los principales problemas es proporcionar una torre de protocolos capaz de proporcionar calidad de servicio según el modelo *IntServ* sobre redes Ipv6/ATM, con soporte completo para multicast, y bajo el entorno elegido para las aplicaciones de usuario (Windows NT). Fue por tanto que se realizó una integración de dicha torre de protocolos, partiendo de software cuyo código fuente está disponible (principalmente Ipv6 y RSVP), al que se añadió soporte completo para ATM, entre otras características.

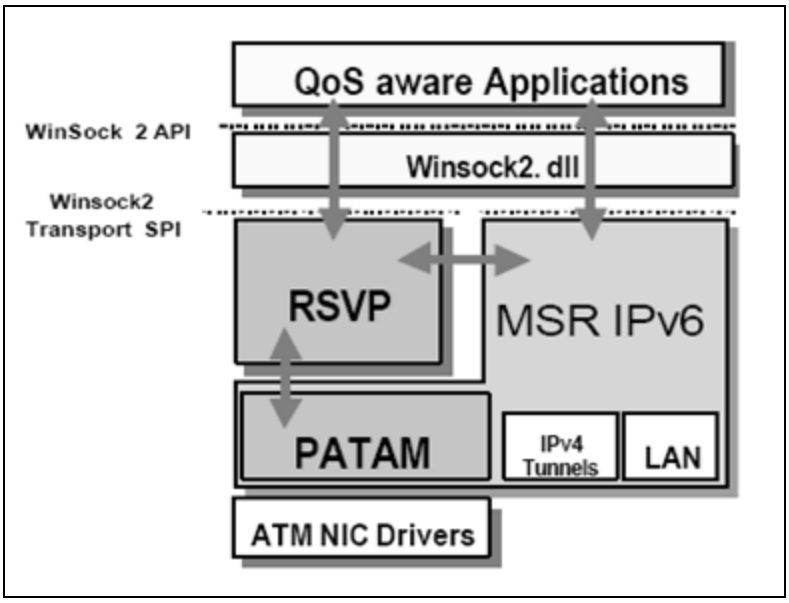
A continuación se describen las principales características. Se ha desarrollado una torre de protocolos (Figura 2) para entornos NT compatible con el estándar Winsock2 que incluye:

- Ipv6 sobre ATM, con soporte completo para multicast a través del protocolo MARS.

- RSVP sobre Ipv6.

- Reserva de recursos (control de tráfico) sobre subredes ATM. Este control de tráfico está integrado con RSVP de manera que se soporta el servicio predictivo (*Controlled Load*) de *IntServ* sobre circuitos CBR y el servicio *besteffort(mejor esfuerzo)* sobre circuitos UBR. Esta QoS se proporciona tanto para flujos Unicast como multicast.

Figura 16. **Arquitectura de protocolos**



Fuente: GARCÍA, Ana B. *Soporte de calidad de servicio en internet sobre redes ATM*, *http://www.it.uc3m.es/azcorra/papers/atm_qos_telecom00.pdf.* Consulta: 20 de marzo de 2013.

Como se puede observar, a las aplicaciones se ofrece el API estándar Winsock2 tanto para acceder a Ipv6 como a RSVP. Los dos principales bloques que se han desarrollado PATAM (el *controlador* Ipv6/ATM) y el módulo de RSVP. Ambos son descritos más adelante.

2.6.5. PATAM, controlador Ipv6/ATM

PATAM (*Ipv6 over ATm Adaptation Module with RSVP support*) es un controlador de Ipv6 sobre ATM desarrollado a partir de una implementación de Ipv6 para Windows NT de Microsoft Research (que sólo soportaba interfaces Ethernet). En concreto, se trata de un controlador que se ejecuta en modo usuario, y que implementa Ipv6/ATM utilizando circuitos virtuales conmutados (SVCs). Incluye soporte para multicast mediante un cliente de MARS. Los principales módulos que componen PATAM son:

- Base de datos de flujos: en ella se almacena toda la información sobre los flujos Ipv6 de tipos BE (*Best Effort*) y CL (*Controlled Load*), Unicast o Multicast, que están activos.

- Módulo de acceso a Ipv6: se encarga de la comunicación con Ipv6, de manera que los paquetes destinados al interfaz ATM son dirigidos por este módulo hacia el de envío/recepción análogamente, cada vez que se recibe un paquete Ipv6 por un circuito ATM, es entregado a la torre Ipv6 por este módulo.

- Módulo de envío/recepción de paquetes: este integra las funciones necesarias para el envío y recepción de paquetes Ipv6 sobre ATM. Incluye el clasificador y el planificador, encargados en conjunto de, conforme a los flujos registrados en la base de datos de flujos, enviar cada paquete Ipv6 por el circuito ATM que corresponda (en definitiva, asegurar que los paquetes de cada flujo recibirán la calidad de servicio adecuada).

- Módulo de acceso a ATM: permite la apertura y cierre de SVCs y de hojas de los mismos (si son multipunto), así como la notificación de eventos relacionados con los circuitos ATM a otros módulos.

- Cliente de MARS: se encarga de la comunicación con el servidor de MARS de la LIS para la gestión referente a los grupos multicast. Para su desarrollo se partió de una implementación de NIST para Linux.

- Módulo de control de tráfico: realiza la comunicación con el demonio de RSVP para la creación y liberación de flujos CL y sus correspondientes circuitos ATM multipunto de tipo CBR. Se describe con más detalle en el siguiente apartado.

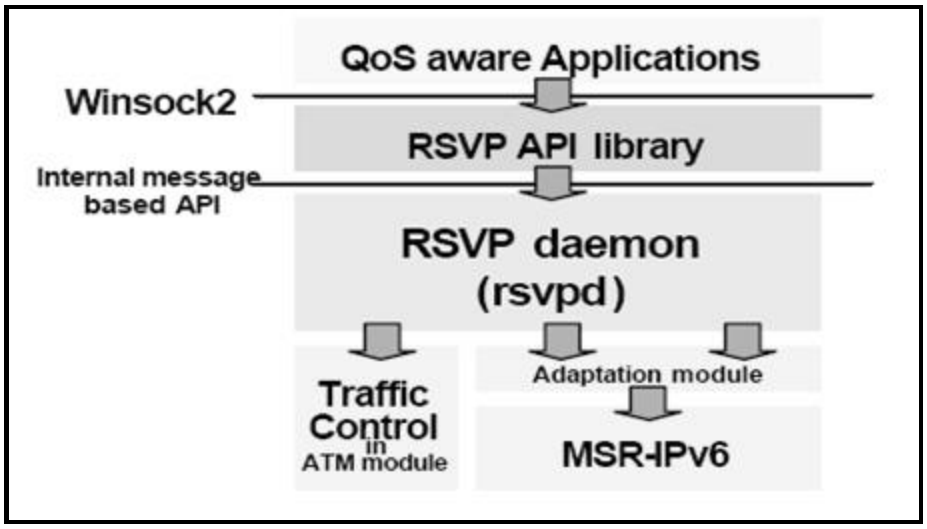
2.6.6. RSVP

El demonio RSVP desarrollado conforme a los estándares actuales e incluye la siguiente funcionalidad:

- API de acuerdo al estándar Winsock2.
- Funcionamiento sobre Ipv6 nativo (sin encapsulación sobre UDP).
- Implementación de sistema final (*host*).
- Soporte para interfaces tanto Ethernet como ATM.
- Interacción con PATAM *controlador Ipv6/ATM* para proporcionar control de tráfico real sobre subredes ATM. Se soportan los estilos de reservas FF (*Fixed-Filter*) y SE (*Shared- Explicit*), y el servicio de carga controlada (*Controlled Load*) de *IntServ*.

Para el desarrollo del demonio de RSVP se partió de una implementación de referencia, esta implementación, que funciona en diversas plataformas Unix, fue migrada para su utilización en entornos Windows NT y completada de manera que se dispusiese de control de tráfico sobre subredes ATM. La figura 3 muestra la arquitectura modular relacionada con el soporte para RSVP que se implementó.

Figura 17. **Arquitectura RSVP**



Fuente: GARCÍA, Ana B. *Soporte de calidad de servicio en internet sobre redes ATM*, *http://www.it.uc3m.es/azcorra/papers/atm_qos_telecom00.pdf.* Consulta: 20 de marzo de 2013.

Los principales cometidos que se llevaron a cabo a la hora de realizar la migración fueron:

- Desarrollo de una biblioteca de enlace dinámico que ofrece a las aplicaciones el API estándar de Winsock2 y se comunica con el procesamiento central de RSVP a través de una interfaz interna (que se ha conservado como en la implementación de ISI).

- Modificación de la torre Ipv6 de MSR para soportar la funcionalidad avanzada que el demonio de RSVP necesita respecto a entrada/salida y encaminamiento. una capa intermedia para encapsular las llamadas de bajo nivel que se solicitan al Ipv6, ofreciendo al procesamiento central de RSVP interfaces genéricas de más alto nivel.

- Desarrollo, dentro del controlador PATAM, de un módulo de Control de Tráfico sobre ATM.

Este módulo ofrece una interfaz que permite la apertura (y cierre) de circuitos y hojas de circuitos ATM de tipo CBR, asociados a reservas de QoS realizadas (o terminadas). La implementación de RSVP de ISI proporcionaba un *control de tráfico* casi vacío, apropiado para interfaces de tipo Ethernet. La inclusión de control de tráfico sobre ATM se ha realizado aprovechando la posibilidad que la estructuración modular del código de ISI ofrecía para añadir, en lugar de sustituir, nuevos módulos de control de tráfico apropiados para distintos tipos de interfaces.

3. NUEVAS OPORTUNIDADES PARA LAS REDES

3.1. Plug and Play, sueño de los administradores de redes

Conjunto de protocolos de comunicación que permite a los periféricos en red descubrir de manera transparente la presencia de otros en la red.

3.1.1. IPv6 Plug and Play con prefijos

Cuando se habla de la migración de una red IPv4 hacia una nueva red Ipv6, no solo se refiere al aumento de números de IP's, sino también a la puesta en práctica de mecanismos, procedimientos, etc., para poder configurar de manera automática la nueva dirección Ipv6 con la información de la red. Cuando existe cualquier nodo en la red, un nodo Ipv6, se desea que este se auto configurara automáticamente con la nueva dirección IP. La configuración automática de la dirección IP se ha considerado especialmente importante, y ha sido punto de discusión debido a la importancia que esta toma en la estandarización hacia el Ipv6. Para poder visualizar las diferencias, se explicará la forma de auto configuración de la actualidad con el IPv4 y la nueva forma de auto configuración del Ipv6.

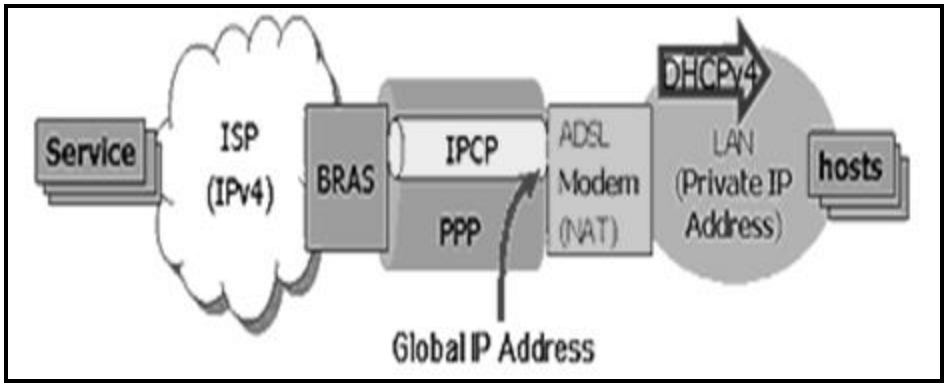
3.1.1.1. Asignación dinámica de la Dirección IPv4

Actualmente en IPv4, la configuración automática de la dirección se realiza principalmente en con tres métodos: Dirección automática del PPP (*Point to Point Protocol*), de DHCP (*Dynamic Host Configuration Protocol*) y de APIPA (*Automatic Private IP Addressing*).

Un ejemplo PPP es una conexión del internet con el módem análogo. IPCP en la secuencia del PPP fija una dirección IP a la interfaz del PPP de un anfitrión. El método de DHCP se utiliza, por ejemplo, en conectar los equipos Ipv4 en una red LAN con un servidor que provea el servicio de DHCP. En este caso, la dirección IP se configura en la interfaz de la red LAN de un equipo, trata aleatoriamente de configurar en su propia interfaz de la red LAN, cuando el anfitrión no puede encontrar un servidor de DHCP. Esto más que todo se pone en ejecución en los sistemas de Windows y de Macintosh.

Los proveedores de servicios de ADSL utilizan el método PPP o DHCP, aunque los detalles de la puesta en práctica pueden diferenciar a partir de un proveedor a otro. Máquinas conectadas con este módem del ADSL consiguen la dirección privada IPv4 del módem. Los módems del ADSL tienen función nacional. La interfaz de la red LAN del módem del ADSL puede dar una dirección tal como 192,168,0,1/24, y puede asignar direcciones a los dispositivos que estén conectados en la red LAN, tal como 192,168,0,2. Las direcciones de los proveedores de redes LAN que estén unidos siguen cambiando, incluso cuando se cambia la dirección PPP de la red WAN.

Figura 18. **Direccionamiento dinámico en Ipv4**



Fuente: http://www.ipv6forum.com/Ipv6_news.htm. Consulta: 20 de febrero de 2013.

3.1.1.2. Asignación dinámica de la Dirección Ipv6

Con Ipv6, la configuración automática la Dirección IP de un nodo se realiza con un auto configuración manual o con un Dhcpv6.

Ipv6 se considera capaz de fácilmente ofrecer los servicios que requieren una dirección global en cada anfitrión, pues no requiere de servicios NAT en los sitios del usuario, ya que tienen bastante número de direcciones. Dos modelos están actualmente disponibles para el establecimiento de una red global Ipv6 entre dos equipos. Uno es el modelo de *multilink* subred *Router* y el otro es modelo de es un *Router* de capa 3.

3.1.1.2.1. Modelo de múltiples subredes *Router*

El modelo de múltiples subredes *Router* considera acoplamientos múltiples, tales como un acoplamiento del ADSL y acoplamiento de Ethernet en el sitio del usuario, todo como una subred.

Varios métodos se proponen, incluyendo uno que tiende un puente sobre simplemente marcos de Ethernet, y uno que provee el descubrimiento del vecino como este sea necesario (ND Proxy). El ND Proxy no tiene ninguna puesta en práctica real todavía. Estos métodos serán utilizados para asignar /64 prefijos a cada sitio del usuario, conectando un anfitrión.

3.1.1.2.2. Modelo de *Router* capa 3

El modelo de *Router* de capa 3, toma el modelo del servicio ADSL de PPP para conexiones IPv4 y los aplican al servicio Ipv6.

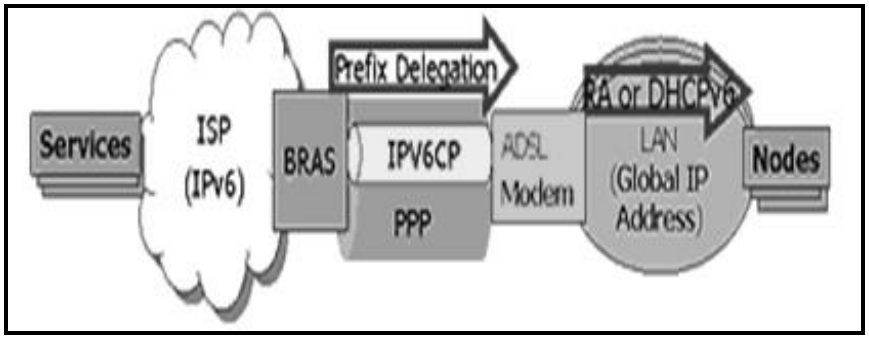
En este modelo, el acoplamiento del PPP y el acoplamiento de Ethernet se consideran subredes separadas. Este modelo incluye los servicios del ADSL que no utilizan el PPP si tratan acoplamiento del ADSL y acoplamiento de Ethernet como subredes separadas.

3.1.1.2.3. Configuración de direcciones a través de diversas redes

Ipv6 PPP posee el IPV6CP, que es equivalente a IPCP en IPv4. En IPv4, IPCP se puede utilizar para configurar la dirección global del interfaz del PPP, y el NAT permite a los nodos de una red LAN comunicarse con los anfitriones del internet. Pero IPV6CP configura solamente la identificación del interfaz de un nodo. La dirección local del acoplamiento puede ser generada configurando la identificación del interfaz, pero el ADSL todavía no conoce el prefijo para asignar para la red LAN. Por lo tanto, nodos en la red LAN no pueden comunicarse con los nodos en una red WAN. La pregunta es, qué se puede hacer para que se puedan comunicar automáticamente y se configuren automáticamente las direcciones globales Ipv6 para una red LAN ?. una de las posibles respuestas seria el prefijo, la delegación del prefijo. La delegación del prefijo es un mecanismo para asignar un prefijo a un sitio del usuario, configurando el *Router* de una LAN con el prefijo necesario. Varios métodos de delegación de prefijos han sido propuestos, y todos estos métodos pueden dar un prefijo /48 al sitio del usuario. El *Router* de la red LAN se encargará de configurar el prefijo /64 de cada nodo en la red interna LAN.

Una vez que el prefijo /64 esté disponible para todos los nodos de la red LAN, las direcciones globales se pueden configurar con el método antes mencionado, configuración manual de la dirección Ipv6 o Dhcpv6.

Figura 19. **Modelo capa 3 para *Router* Ipv6**



Fuente: http://www.ipv6forum.com/Ipv6_news.htm, Consulta 20 febrero 2013

3.2. Auto configuración del DNS

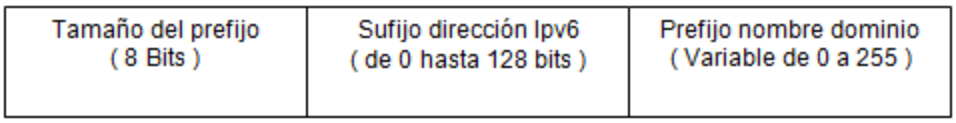
Para facilitar la interconexión entre el hombre y la máquina, las aplicaciones usualmente manejan, generalmente los nombres del dominio en vez de utilizar las direcciones numéricas de cada máquina IP. Una dirección es obtenida buscándola en el *Domain Name System* (DNS), la base de datos distribuida de los nombres de las máquinas para cada dominio del internet.

Las direcciones se almacenan en las estructuras de datos llamadas registros fuentes e identificado por el tipo. Las direcciones IPv4 se almacenan en los registros fuentes del tipo A, que por lo tanto contienen direcciones 32-bit. Para IPv6, los nuevos registros de tipo AAAA o A al cuadrado (A squad), se definió que contienen direcciones de 128-bit.

Actualizar las listas de un DNS es una operación muy costosa en lo que a tiempo se refiere, pues es necesario procesar cada registro que su contenido deba ser cambiado o haya sido cambiado y después propagar esta información desde el servidor primario a los otros servidores de la red. Con IPv6, esta operación es aún más laboriosa debido al tamaño de las direcciones y que se

debe de renumerar con más frecuencia. Por tanto es esencial que un mecanismo esté desarrollado para el DNS automático que se actualice y se configure.

Figura 20. **Formato del registro A6**



Fuente: elaboración propia.

Aunque no hay protocolo disponible en el momento que permite la auto configuración del DNS, un nuevo tipo de registro llamado A6 se ha definido que substituye el registro AAAA y facilitará la adopción de un mecanismo automático para el manejo del DNS. El nuevo registro A6 se muestra en el cuadro anterior. El registro A6 contiene tres campos: la longitud del prefijo, un sufijo de la dirección IPv6 y el nombre del dominio del prefijo. Para entender, tomar el caso de una máquina que pertenece al sitio X y servido por el servidor A. Si registros de tipo AAAA son utilizados, es necesario almacenar el nombre, dirección y mapearlo de la siguiente manera:

hostIPv6.site-X.providerA.net<-> 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0

Usando un registro simple. Con los registros A6, se debe de realizar el siguiente mapeo:

p> hostIPv6 <-> 64 :: 1234:5678:9ABC:DEF0 site-X

site-X <-> 48 : 00C1:CA11:0001:: providerA.net

providerA.net <-> 0 2345

Para obtener esta máquina con dirección IPv6, un cliente DNS deber adquirir por completo la cadena de tres registros A6. El último registro en la cadena es identificado por un prefijo de longitud de cero. La ventaja de utilizar un sistema como este, es la simplicidad con que se puede actualizar, ya que solo se debe de modificar la información del sitio mientras los demás registros no tienen que ser modificados.

3.3. Telefónica conecta Europa y Latinoamérica con tecnología IPv6

Telefónica ha sido una de las empresas que más importancia le ha dado a la nueva tecnología de Ipv6, porque ya está proporcionando conectividad directa IPv6 entre Madrid y Sao Paulo el cual es llamado IPv6 *Global Launch Event* organizado por la Comisión Europea Euro6ix y Net e incorpora estos servicios en su catálogo comercial Telefónica.

Telefónica ha presentado los primeros servicios basados en tecnología Ipv6, durante la celebración del *IPv6 Global Launch Event* organizado por la Comisión Europea. Este congreso, de amplia proyección internacional, va a reunir a los principales responsables sobre el despliegue de la nueva internet, basada en IPv6. El objetivo del encuentro es impulsar el despliegue de IPv6 en Europa y dar a conocer los últimos avances en servicios, terminales y aplicaciones, generados gracias a dos importantes proyectos financiados por la Unión Europea: Euro6ix, que lidera Telefónica I+D y 6net.

La experiencia pionera de Telefónica en la retransmisión de eventos en TV de alta definición (HDTV) bajo este protocolo, permitirá la conectividad IPv6 entre Madrid y Sao Paulo durante el evento. La Red IP Global de Telefónica, con más 20 millones de clientes finales y conexión directa a los puntos de intercambio de tráfico más importantes del mundo, tiene sus nodos

completamente preparados para dar servicio de acceso internacional a internet IPv6, facilitando la integración de servicios de comunicación en IPv6 entre Europa y América Latina.

Telefónica, además ha incorporado el nuevo protocolo en su catálogo de servicios para empresas en España y para operadoras internacionales. Data internet es el primer servicio disponible que incorpora el nuevo protocolo, una solución gestionada de acceso dedicado a internet para empresas, a la que se irán agregando progresivamente otros servicios.

3.4. La internet planetaria podría llegar a ser una realidad

Uno de los padres de internet, *Vinton Cerf*, ha asegurado en la sesión plenaria de inauguración del internet *Global Congress* (IGC) de Barcelona, que se está trabajando en un proyecto que podría materializar una red interplanetaria. Así, *Cerf* ha explicado que en la actualidad, internet funciona en Marte, pero que no es posible realizar conexiones entre planetas, algo en lo que se está trabajando para hacer posible esta interrelación en un futuro próximo.

El padre del protocolo TCP/IP, también se ha referido a la llegada de la Red de nueva generación y la implantación de IPv6. *Cerf* señala al respecto que el actual protocolo, la versión 4, está agotado y es necesario adoptar el nuevo.

En este sentido insta a trabajar para que el nuevo protocolo funcione, ya que el actual no alcanza a cubrir todas las necesidades, al tiempo que indica que habrá un tiempo en que ambos sistemas deberán coexistir. En la actualidad, las redes de nueva generación como Gean o internet 2, ya usan el nuevo protocolo que ofrece más ancho de banda y mayores garantías de seguridad.

Cerf, también ha hecho un repaso de la evolución de las nuevas tecnologías en la sociedad desde que hace 30 años publicara, junto a Robert Kahn, el primer monográfico de internet. *Cerf* ha declarado que en 1997 había 50 millones de usuarios en el mundo, frente a los actuales 745 millones centrados en Estados Unidos (dos de cada tres) y Europa (27 por ciento).

Los países con una mayor penetración son Suecia, con el 78,8 por ciento; Estados Unidos, con el 67 por ciento, y Australia, con el 66 por ciento. Bajo esta óptica, *Cerf* ha alertado de que Asia se convertirá en una nueva potencia en este ámbito si internet consigue tener la misma penetración por el mayor número de habitantes de este continente.

4. NUEVAS TECNOLOGÍAS QUE UTILIZAN IPV6

4.1. Especificaciones para el software IOS de Cisco

Las especificaciones y nuevos beneficios que provee la nueva tecnología de IPv6, son soportadas por únicamente en 12.0 ST y 12.2 T del software IOS de Cisco, empezando en el software de IOS de Cisco 12.0(21) ST y versión 12.2(2)T específicamente. Nuevas versiones del 12.0 ST y 12.2 T del software IOS de Cisco soportarán cualquier especificación de IPv6 y nuevas especificaciones.

4.1.1. Versiones de software soportadas por Cisco para IPv6

En la tabla I se puede apreciar cuáles son las versiones del software de Cisco que soportarán IPv6:

Tabla I. **Versiones soportadas por Cisco software**

Data link layer protocols:	ATM PVC and ATM LANE	12.0(21)ST[4]	12.2(2)T
	CDP IPv6 address support for neighbor information	—	12.2(8)T
	Ethernet, Fast Ethernet, and Gigabit Ethernet	12.0(21)ST	12.2(2)T
	FDDI	—	12.2(2)T
	Frame Relay PVC	12.0(21)ST	12.2(2)T
	Cisco High-Level Data Link Control	12.0(21)ST	12.2(2)T
	PPP over Packet-Over-SONET, ISDN, and serial (synchronous and asynchronous) interface types	12.0(21)ST	12.2(2)T
	Use of the first MAC address as the IPv6 interface identifier for point-to-point links	12.0(21)ST	12.2(4)T
	VLANs using Inter-Switch Link and IEEE 802.1Q encapsulation	12.0(21)ST	12.2(2)T

Continuación de la tabla I

Feature		12.0 ST Release	12.2 T Release
IPv6 unicast routing		12.0(21)ST	12.2(2)T
Services:	DNS lookups over an IPv4 transport	12.0(21)ST	12.2(2)T
	DNS lookups over an IPv6 transport	12.0(21)ST	12.2(8)T
	TFTP	12.0(21)ST	12.2(2)T
	Automatic IPv6 tunnels	12.0(21)ST	12.2(2)T
	Manual IPv6 tunnels	12.0(21)ST[1]	12.2(2)T
	Manual IPv6 tunnels using GRE	—[2 3]	12.2(4)T
	6to4 tunnels	12.0(21)ST[1]	12.2(2)T
	Path MTU discovery	12.0(21)ST	12.2(2)T
	Neighbor discovery	12.0(21)ST	12.2(2)T
	Static cache entry for IPv6 neighbor discovery	12.0(21)ST	12.2(8)T
	Packet internet groper (ping)	12.0(21)ST	12.2(2)T
	SSH over an IPv6 transport	—	12.2(8)T
	Standard access lists	12.0(21)ST	12.2(2)T
	Stateless autoconfiguration	12.0(21)ST	12.2(2)T
	Telnet	12.0(21)ST	12.2(2)T
	Traceroute	12.0(21)ST	12.2(2)T
Feature		**12.0 ST Release**	**12.2 T Release**
Routing protocols:	Integrated IS-IS for IPv6	12.0(21)ST	12.2(8)T
	Link-local address peering in multiprotocol BGP extensions for IPv6	12.0(21)ST	12.2(4)T
	Multiprotocol BGP extensions for IPv6	12.0(21)ST	12.2(2)T
	RIP for IPv6	12.0(21)ST	12.2(2)T
	Static routes	12.0(21)ST	12.2(2)T
	Route redistribution	12.0(21)ST	12.2(2)T
Switching services:	Distributed CEF switching for IPv6	12.0(21)ST	—

Fuente: *Cisco IOS software Release for Ipv6.*

http://www.cisco.com/web/LA/LATAM/cs/ic/index.html. Consulta: 25 de marzo de 2013.

4.1.2. Versiones de plataformas soportadas por Cisco para Ipv6

En la tabla II se puede apreciar cuáles son las versiones de las plataformas de Cisco que soportarán IPv6:

Tabla II. **Plataformas soportadas por Cisco software**

Platform	12.0 ST Release	12.2 T Release
Cisco 800 series[1]	—[2]	12.2(2)T
Cisco 1400 series	—	12.2(2)T
Cisco 1600 series	—	12.2(2)T
Cisco 1700 series	—	12.2(2)T
Cisco 2500 series[3]	—	12.2(4)T
Cisco 2600 series	—	12.2(2)T
Cisco 3600 series	—	12.2(2)T
Cisco 3700 series	—	12.2(8)T
Cisco 4000 series (4700 and 4700-M)	—	12.2(2)T[4]
Cisco 7100 series	—	12.2(2)T
Cisco 7200 series	—	12.2(2)T
Platform	**12.0 ST Release**	**12.2 T Release**
Cisco 7500 series	—	12.2(2)T[5]
Cisco 12000 series	12.0(21)ST	—

Fuente: *Cisco IOS software Release for Ipv6.*
http://www.cisco.com/web/LA/LATAM/cs/ic/index.html. Consulta: 25 de marzo de 2013.

4.2. Ipv6 en las redes móviles 3G

Las ventajas de IPv6, que es compatible con IPv4, son ampliamente reconocidas por la industria, por lo que se está empezando a introducir en los distintos sistemas (los fabricantes más grandes de equipos de

telecomunicaciones, como Cisco, Ericsson, Nortel, etc., incluyen soporte para IPv6 en sus productos).

La IETF (*internet Engineering Task Force*) ha estandarizado IPv6 con un conjunto básico de recomendaciones finalizadas en 1998 (el trabajo empezó mucho antes, en 1993), que ya está listo para ser empleado y el Proyecto de Asociación para la 3G (3GPP/3G Partnership Project) ha especificado IPv6 como el protocolo IP obligatorio en la prestación de servicios multimedia en redes de telefonía móvil, ya que no hay suficientes direcciones públicas IPv4 disponibles para todos los terminales móviles (PDA´s, teléfonos GPRS/WAP, módulos, etc.) conectados a internet.

4.2.1. Características y ventajas de IPv6 relacionadas con la movilidad

Las características más relevantes se describen con detalle en la documentación de especificación del protocolo IPv6 elaborada por el IETF, que ha sido adoptada por el grupo 3GPP. Se describen solamente las relacionadas con la movilidad.

El protocolo IPv4 tiene dificultades en gestionar ordenadores móviles, por varios motivos, de los cuales se mencionan los siguientes:

- Los ordenadores móviles (cualquier clase de producto con una dirección IP) necesitan usar una dirección en cada punto de conexión nuevo a internet, y con IPv4 no siempre es posible obtenerla, debido a su poco espacio de direcciones.

- Se necesitan buenos procedimientos de autenticación, que por lo general no se instalan en los nodos IPv4, para informar a cualquier elemento en la infraestructura de enrutamiento sobre la nueva localización del nodo móvil.

- En Ipv4 puede ser difícil para los nodos móviles determinar si están o no conectados a la misma red, pero en el nuevo IPv6 es más sencillo, ya que la misma dirección contiene la información de la red o subred a la que pertenece esa dirección.

- Los nodos móviles en IPv4 no pueden, por lo general, informar sobre un cambio de localización, véase un cambio de red sobre la cual trabajan, ejemplo, teléfonos celulares de un país hacia otro.

En Mipv6 (Móvil Ipv6), como se le ha designado, que provee mayor flexibilidad para nuevas funciones y servicios, cada nodo móvil (Terminal) se identifica mediante una dirección local independiente de su actual punto de conexión a internet (en las redes fijas existe una cierta relación entre dirección IP de red y la localización geográfica). Cuando el nodo móvil se sitúa fuera de su red propia (Home Network), puede ser asociado a una dirección anfitriona (dependiendo de la región) que proporciona información acerca de la localización actual del nodo móvil.

Para los paquetes que envía el nodo móvil, mientras se encuentra fuera de su red propia, la dirección anfitriona se usa como la dirección de origen en el encabezado del paquete. La opción de dirección local de destino se usa, en un paquete enviado por un nodo móvil mientras está lejos de su red propia, para informar al destinatario del paquete de la dirección local del nodo.

Incluyendo una opción de dirección local de destino en el paquete, el correspondiente nodo que lo recibe es capaz de sustituir la dirección local del nodo por esta dirección anfitriona cuando esté procesando el paquete; así, los paquetes IPv6 que son direccionados al nodo móvil se enrutan transparentemente hacia la dirección anfitriona del nodo.

De esta manera se optimiza la ruta entre el nodo móvil y esta dirección, el resultado de esto es un uso más efectivo de la red. Es lo que se llama *Direct Routing*; los paquetes no necesitan pasar por la red propia del nodo y se puede mantener una sesión activa mientras el móvil cambia de red (R*oaming*).

4.2.2. Prueba de la importancia del IPv6 en las redes móviles 3G

Una prueba de la importancia que tiene IP en el ámbito europeo ha sido la celebración realizada, Global Ipv6 Summit en Madrid, con presencia de las más importantes compañías de telecomunicación, y apoyado por la Comisión Europea, este evento tuvo o es de carácter anual, ya que asistieron más de 500 delegados y donde se han expuesto los últimos avances y noticias relacionados con esta nueva versión del protocolo IP que ya empieza a adquirir cierta notoriedad, y como los desarrolladores de productos móviles están implementando ya este protocolo para sus nuevos productos.

4.2.3. Transición suave de la tecnología 3G de IPv4 hacia IPv6

Los diseñadores del protocolo eran conscientes de que era clave asegurar una transición suave durante la cual convivirán ambos mundos. Es probable que los dispositivos finales operen en redes que tengan algunas

capacidades v6 y otras v4, por lo que será necesario el uso de una pila de protocolo dual.

Un ejemplo son los *Hadsets* móviles que pueden utilizar algunos servicios sobre v4 (como acceso internet general a sitios convencionales) y otros sobre v6 (servicios IP multimedia). La infraestructura que soporte este tipo de operación también, tendrá soporte de pila de protocolo dual.

Además, deben instalarse *Gateways* que transporten los paquetes IPv6 e IPv4 en función del tipo de usuarios. Un *Gateways* termina ambos contextos y envía el tráfico v4 a través de sus interfaces v4. El tráfico IPv6 es dirigido a través de túneles v4 a *Routers* con capacidades v6 que tienen acceso a plataformas de servicio IPv6.

Una red de este tipo permite capacidades de servicio IPv6 significativas al y desde el usuario de *Hadsets*, incluida una identidad de usuario estable y única capaz de empujar servicios al dispositivo móvil. En el estado final, es posible imaginar interfaces IPv6 sobre todos los elementos de red y la utilización del nuevo protocolo para conectar todos los elementos.

4.3. Pruebas de interoperabilidad 3G de Ericsson

En las instalaciones de Ericsson se realizaron las primeras pruebas de interoperabilidad de sistemas de telefonía de tercera generación (3G) (UMTS), en las cuales participaron 16 empresas, este anuncio fue proporcionado por la compañía de Ericsson. Desde hace algún tiempo, Ericsson ha venido realizando estas pruebas, en las cuales se ha probado la interoperabilidad de uno de los protocolos, en este caso es el protocolo de comunicación IPv6, en

los que según la compañía Ericsson se basará la arquitectura de transmisión de las nuevas redes de tercera generación.

Estas pruebas han permitido que múltiples equipos de diferentes suministradores pudieran trabajar conjuntamente en una red. La compañía Ericsson ha proporcionado las facilidades de la infraestructura de la red, ha definido los casos a los cuales se le realizaron las pruebas y ha dirigido las pruebas.

4.4. Telia es el primer operador con el protocolo IPv6

La compañía telefónica sueca Telia, mediante su subsidiaria Skanova, es la primera operadora de Europa que lanza una red de telecomunicaciones basada en la última versión del Protocolo internet (IPv6) para uso comercial.

Los principales responsables de la operadora de telefonía sueca presentaron, en rueda de prensa, el plan de instalación, diseño y ventas de capacidad en la nueva red internet IP de telecomunicaciones de Telia, que es la primera en uso comercial en el continente europeo. La red internet de última generación IPv6 permite a la operadora disponer de un muy elevado número de direcciones IP (abonados) y ofrecer servicios de banda ancha, voz y telefonía móvil de alta calidad. La nueva red de Telia unirá a varias capitales europeas: Estocolmo, Londres, Oslo y Copenhague, y también a las ciudades suecas de Malmoe y Goeteborg, así como a la ciudad finlandesa de Vasa para un inicio.

Es de dar a conocer que esta es la primera fase, la red IPv6 de Telia ofrecerá servicios mayoristas de transmisión ultra rápida de datos a un reducido grupo de compañías multinacionales.

La versión 6 del protocolo internet resuelve el problema de las direcciones IP utilizando un espacio para direcciones de 128 bites de capacidad, el cual provee un potencial que supera con creces el actual protocolo IPv4, de 32 bites. Mattias Lignell[1] (2006), director del S-Lab (laboratorio de pruebas de Skanova) señaló que, "con esta nueva versión IPv6, prácticamente cada hogar en el planeta podría tener acceso a varias direcciones IP".

La nueva red de internet IPv6 de Telia está preparada para ofrecer servicios sofisticados de telecomunicaciones, especialmente en telefonía móvil y se dice que próximamente, internet de bolsillo, gracias a los sistemas de tercera generación de telefonía móvil (UMTS).

4.5. Google, migrar hacia IPv6

Google, lograr la actualización, migración y utilización del nuevo protocolo de internet IPv6 es relativamente barato económicamente y solo se necesitaría de un grupo de trabajadores. Los ingenieros y desarrolladores de Google hablan que no fue caro, ya que solo se necesitó actualizar o migrar las aplicaciones existentes para que soporten el nuevo protocolo de IPv6, futuro camino del internet.

Google confirma que puede ofrecer todos los servicios que ellos prestan en el nuevo protocolo IPv6, les tomó cerca de 18 meses tomar un grupo de desarrolladores pequeño grupo base para desarrollar una plataforma *Google IPv6* disponible para el público. Los ingenieros que desarrollaron este proyecto, trabajaron en él un 20 por ciento de su tiempo, por lo que indica que no era su

[1] LIGNELL. Mattias, First in Europe with Ipv6 in Commercial Network. http://www.thefreelibrary.com/Telia+to+build+Europe%27s+first+commercial+IPv6+network.-a075351404. Consulta: 10 de marzo de 2013.

principal objetivo de trabajo, la creación de una red principal que corriera sobre el protocolo IPv6 se realizó por etapas, en las se recalcaba que en IPv6 no hay nada poco fiable. La experiencia de Google en la implementación de esta nueva red que utiliza el protocolo IPv6 es importante porque solo unas cuantas empresas de USA han adoptado el nuevo protocolo de internet. Se predice que para el 2012 las direcciones IPv4 se habrán agotado, en ese momento, todas las agencias, agencias gubernamentales, proveedores de servicios de internet y empresas que tendrán que soportar IPv6 en sus redes.

Google ha adoptado IPv6 como algo necesario que cualquier empresa tendrá que realizar si desea seguir funcionando. Los servicios que Google ya presenta en este nuevo protocolo son:

- Google Search Engine
- Google News
- Google Docs
- Google Calendar
- Google Maps

Hay tres puntos para Google para el desarrollo de Ipv6:

- Infraestructura de una red en producción, es decir, el mirar con importancia el tránsito de paquetes, por el que IPv6 esté proporcionando transferencia de datos entre varios centros.

- Despliegue a nivel corporativo, para que todas las redes y personal internos de Google migren a la utilización de IPv6.

- Aplicar el IPv6 a todos los servicios y software que pueda tener Google incluyendo gmail, búsquedas, o las correspondencias de Google en calidad de la producción.

Todos estos servicios ya están disponibles en su versión IPv6, y Google estima que el tráfico sobre las redes IPv6 aparecerá de la noche a la mañana reportando ya un tráfico de 150,000 usuarios en su versión Google en IPv6.

4.6. Ipv6 en la nueva red 4G

4G son las siglas de la cuarta generación de tecnologías de telefonía móvil, conocida como 4-G. La 4G está basada totalmente en IP lo que se conoce como un sistema de sistemas y una red de redes. Esta nueva red se está probando gracias a la convergencia de redes de cables, inalámbricas así como en ordenadores, dispositivos eléctricos y en tecnologías de la información, todo esto para poder lograr ofrecer velocidades de 100 Mbps en movimiento y 1 Gbps en reposo, manteniendo una calidad de servicio (QoS), conexión de punta a punta (*End-to-End*) , alta seguridad, ofrecer servicios de cualquier clase con el mínimo coste posible.

Esta generación utiliza el protocolo TCP/IP, el cual es el mismo protocolo de internet, pero para esta generación se estará utilizando el Protocolo de internet versión 6, protocolo internet IPv6. Se espera que este protocolo actúe como elemento concentrador de las diferentes tecnologías radio, debido a que las mejoras de IPv6 en comparación con el protocolo que aún se sigue utilizando (IPv4) son notables, entre ellas la movilidad, direccionamiento y la

seguridad. Debido a esto, la IETF (*internet Engineering Task Force*) ha empezado a definir el Protocolo Mobile IP. Uno de los problemas que se encuentra para esta generación es que con este protocolo aún no saben cómo añadir el *Paging* ya que este protocolo no lo proporciona. El *Paging* es cuando un nodo móvil informa su posición a la red.

El WWRF (*Wireless World Research Forum*) define 4G como una red que funcione en la tecnología de internet, combinándola con otros usos y tecnologías tales como: Wi-Fi y WiMAX.

Para evitar este problema, se tiene un proyecto, que se llama *Geopaging*, el cual es un protocolo multicast diseñado para realizar un transporte de los mensajes de *Paging* sobre una red celular basada en IPv6. A este proyecto se le conoce como Mcast.

4G, el futuro de la telefonía móvil ante la actual dependencia cada día más de los aparatos móviles, es el claro remedio para las necesidades actuales, de nada serviría tener que usar un aparato móvil solamente para hablar por teléfono si se puede tener el mismo aparato móvil para realizar un sin fin de actividades con solo presionar un botón y una conexión a internet mediante el protocolo de IPv6.

4.7. Ipv6 en la ciudad del futuro

La ciudad del futuro es un modelo donde todos los equipos pueden estar conectados a una infraestructura de red de comunicación.

4.7.1. Juegos en línea

El protocolo internet actual IPv4, no proporciona la infraestructura requerida para el juego en línea (punto a punto), principalmente debido al agotamiento del direccionamiento, ya que el actual protocolo de IPv4 necesita pasar por muchos saltos para lograr conectividad entre 2 puntos. Para el desarrollo de un juego en línea necesita utilizar al máximo el beneficio del (punto a punto) del protocolo TCP/IP. Los productos en línea y los servicios como los juegos deben escalar a muchos puntos geográficamente distribuidos y también proporcionar la seguridad para la autentificación, aislamiento y realización de pagos. Además, los productos como los juegos en línea y los servicios se prevé que tendrán que utilizar redes establecidas fijas y redes móviles.

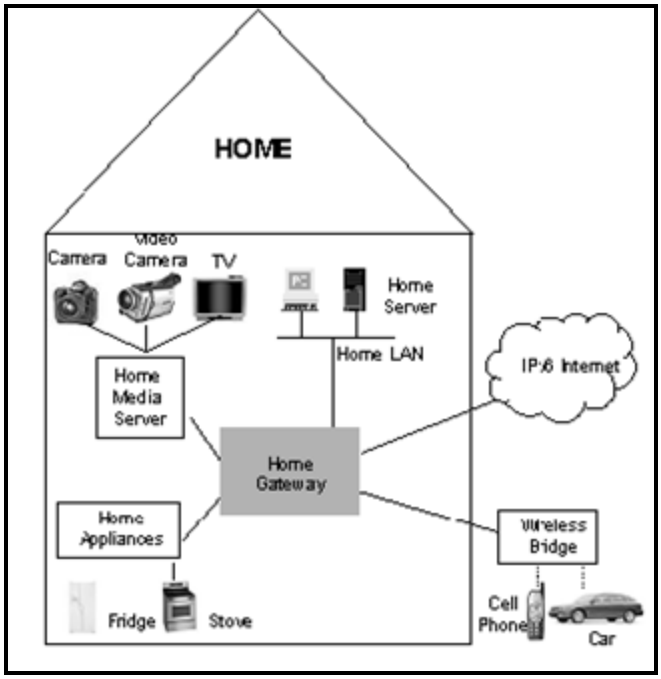
Debido a estos requisitos técnicos y del negocio mismo, los juegos en línea realmente no pueden tener éxito sin usar el establecimiento formal de una red con el protocolo de internet IPv6. Es un punto importante, ya que técnicamente no está lejos de ser verdad que los juegos en línea o la demanda de estos mismos crecerán rápidamente en los próximos años... Esta misma demanda conducirá a un rápido establecimiento y evolución de una red con protocolo de internet IPv6.

Actualmente, se observa al mercado, el potencial es enorme. Por ejemplo. en Japón a partir de agosto 2008 a enero de 2009, 4 millones de copias vendidas de un juego X. El número de unidades vendidas por todo el mundo es gigantesco y está en crecimiento.

4.7.2. Interconexiones en casa

Como la tecnología avanza creando nuevos dispositivos en la industria de electrónica, más y más dispositivos contienen microchips y micro-procesadores, tales como: los automóviles, celulares, equipos de video, televisores, aparatos electrodomésticos y juegos. Es un hecho que el número de las unidades o aparatos caseros está en crecimiento constante, cada uno de estos con la opción de tener una conexión a una red, acá se ve la necesidad de cada uno de estos aparatos de tener un direccionamiento único. El crecimiento del equipo que provee banda ancha y del DSL (basado-hogar) está ayudando al crecimiento del mercado para el establecimiento de redes de tipo casero, para acceder a muchas herramientas por medio de una red de telecomunicación.

Figura 21. **Interconexiones en casa**



Fuente: HEMMINGER. Gary, *Ipv6 Market Drivers*, http://www.ciscoknowledgenetwork.com/files/223_IPv6Economics.pdf. Consulta: 20 de marzo de 2013.

La nueva tecnología tal WIMAX, y Bluetooth, WI-FI, etc., para el uso en aparatos móviles y el uso casero se está desarrollando cada día más y nuevos productos con necesidad de un direccionamiento salen al mercado. Cada vez más los microprocesadores son utilizados en los aparatos electrónicos, ya muchos de estos están listos para una conexión a una red IPv6. Por ejemplo ya podemos interconectarnos con un dispositivo como una refrigeradora o una cámara de vigilancia en casa, a los cuales podemos acceder mediante la Web y tener reportes o estados de los mismos. Debido a esta creciente en el desarrollo de productos, los mismos ya vienen configurados con una dirección IP fija para conexión, ya que para muchos consumidores es más complicada la configuración manual de estos para su conexión a la red.

La solución para esta nueva demanda de direcciones es la nueva red o protocolo IPv6 para los nuevos depositos. Las nuevas consolas de juegos ya vienen preparadas para una conexión Ipv6, tal como *Wii, Play Station*, etc. El nuevo direccionamiento de Ipv6 ofrece un espacio tan grande que los dispositivos y las aplicaciones contendrán microprocesadores con direccionamiento de la nueva red Ipv6 que actúan como números de serie para accesos libres o directos. Hay que considerar las posibilidades para la seguridad, si todos los dispositivos tienen un direccionamiento establecido de Ipv6, podría fácilmente recuperar aparatos robados que se conectaran a la red y capturar a los criminales. El nuevo protocolo Ipv6 establecerá el crecimiento de las redes caseras para dispositivos, aplicaciones residenciales, etc.

4.7.3. Ipv6 en dispositivos móviles

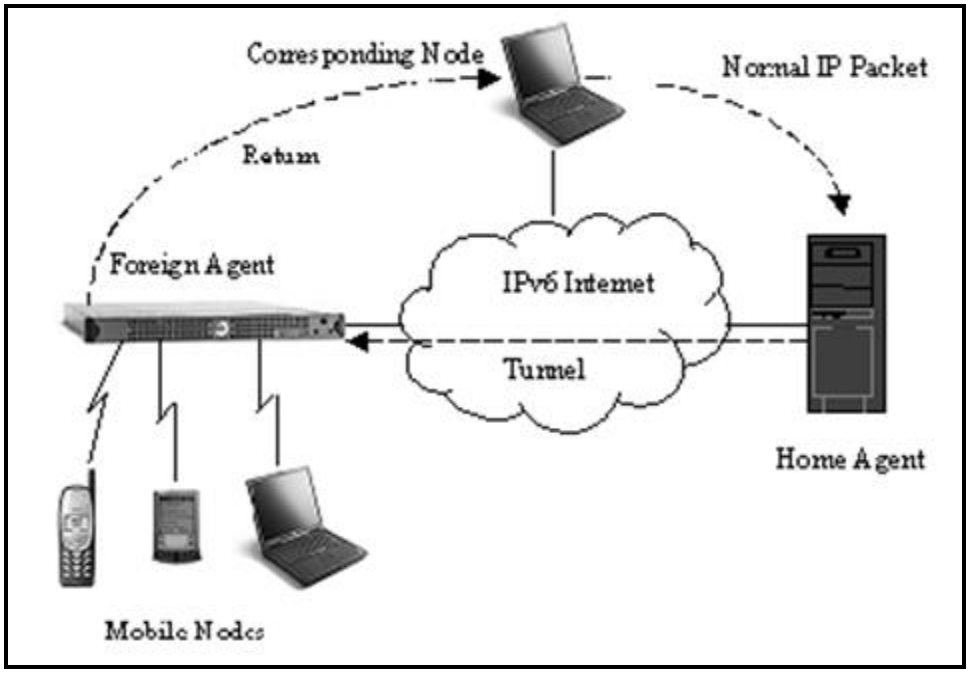
Una de las tecnologías que más auge está teniendo es la telefonía móvil, con el gran crecimiento y desarrollo de aparatos móviles que cada día necesitan conexión a redes, es imprescindible que los protocolos que estos aparatos

utilicen estén desarrollados para la conectividad de este vía IP sin importar la localización física del dispositivo.

El problema es que el protocolo IP no fue diseñado para dispositivos que utilizan *Roaming*.

La respuesta a este problema es el desarrollo por parte de la IETF del protocolo IP móvil estándar. Este estándar definió el concepto de un agente casero (HomeAgent) y del agente foráneo (ForeignAgent), junto a esto el desarrollo de un nodo móvil (MovilNode), y seguridad con (CareOfAddress).

Figura 22. **Ipv6 en dispositivos móviles**



Fuente: HEMMINGER. Gary, *Ipv6 Market Drivers*, http://www.ciscoknowledgenetwork.com/files/223_IPv6Economics.pdf. Consulta: 20 de marzo de 2013.

El concepto básico según lo mostrado en la figura, es que cada MovilNode tiene un HomeAgent. Cuando un MovilNode se mueve lejos de un HomeAgent, su conexión la realiza o se registra con un ForeignAgent. Luego este ForeignAgent se comunica con el HomeAgent del MovilNode. Cuando un nodo correspondiente (CorrespondingNode) desea entrar en contacto con un MovilNode, él le envía los paquetes al HomeAgent, luego el HomeAgent realiza un túnel y manda los paquetes al ForeignNode quien entrega los paquetes al MovilNode. El proceso de descubrimiento y del registro se define en RFC 2002.

Debido a que estos protocolos son relativamente nuevos y generaran el incremento enormemente en el direccionamiento en dispositivos móviles, es muy probable que el protocolo móvil IP Standard sea completamente desplegado o desarrollado sobre el protocolo IPv6. El protocolo de descubrimiento de vecinos en IPv6 simplifica grandemente el proceso de encontrar un agente foráneo (ForeignAgent).

4.8. Ipv6 en la industria de aviación

El IPv6 y sus características de movilidad ejercerán un enorme impacto sobre la industria aeronáutica y de los viajes. El IPv6 es un factor crítico para alcanzar mayores velocidades y precisión en el desempeño de operaciones que se centran en torno a la red global en el área de comunicaciones terrestres y aéreas. La integración oportuna a los requisitos IPv6 dentro de los planes de desarrollo de la industria aeronáutica disminuirán la complejidad, así como los costos de transición al asegurarse de que las aplicaciones actuales operen dentro de un ambiente libre de problemas de interoperabilidad y de costos adicionales.

Algunos casos concretos en los que el IPv6 puede convertirse en un capacitador empresarial clave para la industria aeronáutica son los siguientes:

- Servicios durante vuelo: las aerolíneas buscan mejorar la disponibilidad de opciones electrónicas en los aviones. Los servicios de internet durante el vuelo precisan de movilidad, características de conexión de punto-a-punto, así como medidas de seguridad que estén fácilmente disponibles al integrar características IPv6 como parte de los sistemas ICT medulares disponibles para la aviación. Las aerolíneas ya se encuentran ofreciendo servicios tales como e-mail, Web, internet inalámbrico, telefonía.

- Sistemas de mensajes: información crítica sobre vuelos, equipaje y las necesidades de distribución de bienes y productos para dispositivos inalámbricos y portátiles tales como un celular, PDAs y laptops para personal de aerolíneas y aeropuerto. Los mensajes más críticos precisarán de mejores y mayores características de seguridad.

- Proceso para el manejo de equipaje: se están colocando tarjetas con chips en el equipaje, que se activan a través de distintos procesos. Una combinación de Bluetooth o RFID (Identificación de radio frecuencia) o dispositivos inalámbricos de corto alcance y tecnologías IP facilitarán el que los pasajeros rastreen su equipaje en aeropuertos tales como Hong-Kong, uno de los aeropuertos más ajetreados del mundo que recientemente anunció una infraestructura de RFID para realizar el rastreo de equipaje.

- Sistemas de reconciliación: las aerolíneas precisan que cada maleta sea acompañada por su propietario durante un vuelo. Los sistemas de

reconciliación precisan un cotejamiento de la maleta con su dueño, por motivos de seguridad.

- Sistemas de rastreo: las aerolíneas y aeropuertos pueden fácilmente realizar el seguimiento y monitorear la información sobre el avión al convertirse este en una dirección IP, mediante sensores y cámaras.

- Comunicaciones en tierra: el IPv6 facilita la accesibilidad de la gente y máquinas y afianza comunicaciones que son fundamentales para que los aeropuertos logren alcanzar un eficiente manejo de recursos.

Estos son claros indicios de cómo la tecnología y la industria aeronáutica está ya utilizando y desarrollando contemplando la utilización del nuevo protocolo de internet IPv6.

5. IPV6 HOY Y SU FUTURO

5.1. Despliegue de Ipv6

Ipv6 está destinado a suplir Ipv4 proporcionando un direccionamiento mucho más amplio, permitiendo a dispositivos direcciones propias y permanentes.

5.1.1. Ventajas y desventajas

- Ventajas

El Ipv6 tiene ventajas con respecto al Ipv4 tanto para los operadores de la red como para los usuarios finales. El nuevo protocolo permite la conexión de millones de dispositivos con capacidad IP, Algunos operadores se han adaptado a esta limitación de direcciones utilizando la NAT (Network Address Translation) o Conversión de la Dirección de Red. La NAT proporciona una solución a las aplicaciones cliente/servidor con base en el internet, pero resulta menos apropiada para aplicaciones de *Point-to-Point* en cuando a comunicaciones móviles, lo que siempre limita en gran manera el despliegue de servicios innovadores en la Red.

Los beneficios más notables que ofrece el Ipv6 tienen que ver con el enorme espacio y capacidad para direcciones IP, seguridad incorporada y características de movilidad, Plug&Play (conecte y haga funcionar) hasta auto-configuración de direcciones, redes y servicios de fácil re-diseño. Estas

características inherentes al Ipv6 ayudarán a reducir gastos de ejecución y minimizarán la carga administrativa para las empresas.

- Desventajas

  La necesidad de extender un soporte permanente para Ipv6 a través de todo internet y de los dispositivos conectados a ella. Para estar enlazada al universo Ipv6 durante la fase de transición, todavía se necesita una dirección Ipv4 o algún tipo de NAT (compartición de direcciones IP) en los *Routers* (Ipv6<-->Ipv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.

Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de Ipv6 caseros múltiples. Las direcciones Ipv6 son mucho más largas que las direcciones Ipv4 y, por lo tanto, más difíciles de memorizar. Una preocupación real radica en el riesgo de crear “islas Ipv6” debido a la ausencia del compromiso de desplegar el Ipv6 de manera que abarque enteramente la industria. A pesar de ello un plan de transición bien establecido y que comprenda a toda la industria ayudará a eliminar estos riesgos, poniendo en lugar mecanismos de transición apropiados y permitiendo que exista una completa interoperabilidad con los demás servicios que todavía no se adaptan al Ipv6.

5.1.2. América más lenta que Europa

Actualmente se visualiza que los esfuerzos por parte de América han sido pocos a comparación de sus similares de Europa y hacia, para el desarrollo del nuevo protocolo de internet Ipv6, América menciona que sin un

mayor liderazgo gubernamental en la transición al Protocolo de internet versión 6 (Ipv6) el comercio americano podría enfrentarse a una competencia devastadora desde Europa y Asia, ya que quienes adopten las tecnologías Ipv6 durante una etapa temprana cuentan con la oportunidad única de obtener conocimiento y experiencia, que a su vez se traducirán en una ventaja competitiva y un manejo fácil y de bajo costo de la transición hacia el Ipv6, a la vez que se aseguran nuevos negocios.

Quienes adopten las tecnologías Ipv6 en fase temprana precisarán manejar ambos protocolos Ipv6 e Ipv4 dentro de sus organizaciones y entre sus clientes y proveedores. Esto es importante y no puede subestimarse; sin embargo, a menudo se exagera.

Según un testimonio, Europa y Asia han invertido más de 800 millones de dólares en el nuevo protocolo IP de próxima generación, diseñado para disponer de más direcciones, más movilidad y más seguridad. Solo la NTT japonesa cuenta con más clientes de Ipv6 que todas las empresas americanas juntas. Una pérdida de confianza y reputación de las redes americanas que utilizan el actual y altamente vulnerable protocolo Ipv4, junto a un aumento de la confianza en las redes Ipv6 en Europa y Japón podría tener un efecto devastador sobre la economía de servicios Americanos.

5.1.3. China será el líder de desarrollo de Ipv6

China ha construido con éxito la red de su próxima generación de internet, siendo el líder en el mundo en el desarrollo de la red más grande, más rápida y segura de internet que dominará el futuro. La red, llamada CNGI-CERNET2/6IX. Los expertos apuntaron que la red alcanza el nivel de líder mundial por completo con las mayores innovaciones y le concederá a China voz

y voto dentro del ámbito. China lanzó la construcción de la próxima generación de internet en el 2003 y terminó en el 2005 su primera generación de internet, la CNGI-CERNET2.

El éxito de la red CNG liberó a China de la dependencia de una clave extranjera de tecnologías y productos internet asegurando la información nacional, explicaron los expertos. Propuesto a mediados de la década de los 90, se estima que la próxima generación de internet incremente la velocidad de transmisión de la información en más de mil veces a 40 giga bites por segundo. Además ofrecerá más seguridad, la gestión será más sencilla y dará una lista casi inagotable de direcciones de internet.

En la próxima generación de internet, el protocolo internet 6 (Ipv6) fue aplicada en vez del actual utilizado internet 4 (Ipv4). Los dos protocolos regulan el tráfico de información de internet en diferentes modos. En el desarrollo del CNGI, China ha construido la primera red única en el mundo Ipv6 y es la primera vez que utiliza rutas domésticas Ipv6, los componentes del núcleo en su nacional columna de red.

Los expertos afirman que es un progreso con importancia estratégica puesto que termina con la dependencia de las tecnologías extranjeras sobre la construcción de internet. Con un rango de velocidad de transmisión de 2,5 a 10 giga bites por segundo, la columna de red CNGI conectada a 25 nodos está distribuida en 20 ciudades del país.

China, también consiguió innovaciones en la creación de un nuevo esquema de transición entre dos versiones de protocolo de internet y un sistema de validez de fuentes de dirección Ipv6 para asegurar la seguridad de la red. A ambos se les concedieron patentes nacionales y llegaron a ser

referencias básicas para organizaciones de internet internacionales para hacer estándares internacionales, según el Centro de Investigación de Redes de la Universidad de Tsinghua, institución líder en la construcción de CNGI.

Reconocido como la dirección futura en el desarrollo de internet y un arma de acuerdo con las ventajas económicas, políticas y militares, la próxima generación de internet ha sido una tarea estratégica para la mayoría de los países desarrollados como Japón y Estados unidos. China ha escrito el desarrollo de la próxima generación de internet en su plan de desarrollo nacional económico y social para el período 2006-2010, y ha elaborado un proyecto clave en la construcción de un país basado en la información CIIC.

5.2. Futuro de internet con Ipv6

Ipv6 es el nuevo protocolo desarrollado para el futuro, permitiendo un mayor número de asignación de direcciones IP permanentes.

5.2.1. Nuevos desafíos y riesgos

Con la implementación del nuevo protocolo de transmisión de Ipv6, este hace frente a un nuevo número de desafíos, tales como:

- Los costos y riesgos de implementar Ipv6.

- La utilización de NAT que es necesario para desplegar de una forma incremental el protocolo Ipv6, pero con este parece eliminar la necesidad del todo del mismo Ipv6.

- La inhabilidad, realmente de utilizar las características Ipv6 con eficacia durante el despliegue incremental.

Una de las visiones es que Ipv6 debería ser primero desarrollado e implementado a nivel empresarial, redes corporativas. Sin embargo, desarrollar redes corporativas para Ipv6 significará que haya una traducción o manejo entre las redes Ipv6 y la red Ipv4, como la salida al exterior internet. Pero aun así, es un riesgo más bajo el desplegar una red Ipv6 que aumentar la red Ipv4 con un dominio privado para satisfacer las necesidades de accesos de la misma red de la empresa. Esta solución eliminaría los riesgos de interrumpir los usuarios finales, *Routers*, *Switches* de múltiples capas y sistemas de administración de uso de la red al actualizarlos al nuevo protocolo de Ipv6.

Las soluciones basadas en NAT están bastante desarrolladas en la actualidad y, a la vez bien entendidas, en cambio Ipv6 es un mayor porcentaje aún en proceso experimental, y por eso se ve algo lejano que a nivel empresarial se realice la implementación del nuevo protocolo Ipv6. Otra de las visiones es que el nuevo protocolo Ipv6 debería de empezar su desarrollo e implementación en la columna vertebral de internet.

Esto parece ser injusto para los proveedores de internet ISP's, a invertir, generar costos y riesgos. Esta columna vertebral del internet no tendría mucha demanda de direccionamiento de Ipv6, ya que posee pocos nodos. Los ISP tendrán que soportar los dos protocolos Ipv4 e Ipv6 a menos que todos los clientes de un ISP específico se trasladaran simultáneamente hacia Ipv6. Mecanismos de Dual-*Stack* y *Tunneling* consumen recursos extras de red y humanos para soportar el protocolo Ipv4, y finalmente los ISP tendrán que proveer de una columna de *Routers* o nodos con un funcionamiento adecuado y rápido. El mercado actualmente, para estos productos es aun baja la demanda

y la inversión porque no se tiene un tráfico significativo o demanda del mismo sobre el protocolo de internet Ipv6. No está claro cuándo, cómo y dónde los ISP obtendrán este equipo para decidirse implementar en el nuevo protocolo Ipv6.

Otra visión es que el protocolo Ipv6 será ampliamente desarrollado e implementado por servicios tales como: redes *Wireless* para la telefonía celular, portátiles y dispositivos que acceden a redes inalámbricas que tendrán direccionamiento Ipv6 para su acceso rápido y automático a internet. Esta posible utilización tiene la desventaja que presenta más tiempo en transmisión debido a que la cabecera del paquete Ipv6 es más grande, a menos que se logre una compresión del mismo que pueda ser efectiva, ya que las cabeceras de los paquetes de redes *Wireless* tienden a ser más pequeñas, por las tecnologías y porque la transmisión de voz utiliza paquetes pequeños.

Un desafió más importante es cómo se maneje este sistema *Wireless,* los múltiples dispositivos conectándose unos con otros, habiendo telefonía celular, algunas aplicaciones *Wireless* en casa y dispositivos móviles como agendas. Si la cabecera del paquete Ipv6 no puede ser comprimida o reducida, esto reducirá el número de dispositivos a los cuales se les pueda dar servicio en el peor caso, incrementando los costos.

Hasta que no se pueda utilizar de una mejor forma el envió del paquete Ipv6 por su cabecera, el desarrollo del mismo protocolo en los servicios *Wireless*, se ve complicado que aparezca pronto la utilización del mismo.

Una visión adicional a los riesgos mencionados anteriormente para el desarrollo e implementación de Ipv6 en diferentes escenarios, existen riesgos técnicos significativos para el despliegue de Ipv6, una parte debido a los cambios realizados comparados con el actual Ipv4, además del cambio del

tamaño del direccionamiento. A pesar de todo el trabajo que se ha realizado en Ipv6 y demostrado su admirable alojamiento, existen suficientes diferencias para tener una legitima preocupación hacia el cambio del actual Ipv4 por problemas inesperados que puedan surgir, debido a que muchas aplicaciones han sido diseñadas, compiladas y optimizadas para el uso sobre el protocolo Ipv4.

5.2.2. Implicaciones de seguridad en Ipv6

Los riesgos introducidos inicialmente por la transición al protocolo Ipv6 pueden ser mitigados y controlados utilizando existentes aplicaciones o técnicas. La utilización de aplicaciones que transfieran tráfico Ipv6 hacia Ipv4 y viceversa, deberán de ser bloqueados o desaparecer, ya que estas aplicaciones fueron creadas para nodos independientes individuales que necesitan conexión con la internet.

Las redes de gran amplitud en nodos o servicios, tendrán que proveer el ruteo para acceso a redes Ipv6 donde esta sea soportado, no habrá necesidad de aplicaciones que trasfieran el tráfico entre Ipv4 y Ipv6. Esto se debe a que sí no habrá sitios o no se soportara Ipv6, no hay necesidad de estas aplicaciones.

Si el protocolo Ipv6 es soportado, los túneles que proveerá la infraestructura de la red tendrán que ser proveídos por los *Routers* y *Gateway*, no importando si existe tráfico o no de Ipv6. La entrega de paquetes que viajaran por la red Ipv6 para nodos individuales o estaciones de trabajo tienen que ser proveídos vía Ipv6 nativo por los dispositivos. Si es soportado 6to4, este debe ser soportado por un número específico de dispositivos o Gateway. El procedimiento provee soporte a acceso directo por parte de nodos 6to4 individuales en redes externas mientras se controla el tráfico que circula en la

red interna. Las redes también tendrán que ser monitoreadas para la auto-configuración de paquetes Ipv6, *Routers* y descubrimiento de vecinos solicitud y aviso de paquetes. Si la red no soporta Ipv6 o un segmento de la misma, es una posible indicación de una mala configuración. Si es soportado Ipv6 por la red, esta debe ser monitoreada, cualquier modificación, dispositivo, ruta o actividad fuera del monitoreo, deberá ser bloqueada e investigada por posible actividad maliciosa.

El protocolo Ipv6 es relativamente nuevo, contiene un gran número de ventajas en funcionamiento y seguridad sobre las versiones antiguas como el Ipv4, sin embargo, estos mismos beneficios o ventajas que la hacen tan atractiva y funcional, trabajan como desventaja para los administradores de la red y a la vez ventaja para los ataques por medio de usuarios maliciosos de Ipv6.

Esto ocurre cuando los administradores de red no han desplegado completamente le protocolo de Ipv6 y/o no saben técnicas de seguridad apropiada, esto lleva a que tráfico Ipv6 pueda ser transmitido por sus redes sin poder ser detectado.

Como con la mayoría de casos en la actividad maliciosa en el internet, es solamente una cuestión de tiempo para que el conocimiento de estos filtros sea un conocimiento de la red entera de internet. Administradores de redes Ipv4 están normalmente atrás con el tema de protección del abuso de Ipv6. Sin embargo, prácticas fuertes de seguridad en Ipv6, tales como las que provee el internet Security System, sistemas de seguridad en internet, están disponibles para proteger las redes ante estas posibles amenazas.

El protocolo Ipv6 ofrece ventajas de seguridad para aquellos que sepan cómo utilizarlas bien, estas ventajas o beneficios pueden ser aprovechadas por el administrador o por un intruso. Por lo tanto, la época para no hacer caso del nuevo protocolo de internet Ipv6 ha llegado a su fin, es época de entender el protocolo, reconocerlo y desplegarlo con sus ventajas.

5.2.3. Preguntas acerca de Ipv6

- ¿Qué sucederá con máquinas más viejas y los sistemas operativos, cuales utilizan Ipv6? ¿Qué dispositivos utilizan Ipv6?

Para las maquinas más viejas, asumiendo que se habla de máquinas de escritorio, máquinas para trabajos como oficina, estudios o el hogar, estas dependerán del software de sistema operativo que la maquina pueda tener instalado, por ejemplo, una máquina con sistema operativo Windows ya esta soportado desde las versiones como Windows 95, Vista, NT, XP, Server 2000, Server 2003.

Sin embargo, el nivel de soporte o desarrollo en cada una de las versiones o de los sistemas operativos variara dependiendo del constructor. La tecnología avanza increíblemente y cada día hay nuevos productos en el mercado, los cuales deben examinarse por individual para ver si soportaran el nuevo protocolo de Ipv6.

- ¿Cuál es el significado de que Ipv4 e Ipv6 tendrán que coexistir?

El funcionamiento técnico del internet sigue siendo igual en ambas versiones tanto para Ipv4 como para Ipv6 y es probable casi seguro que ambos protocolos o versiones continuarán funcionando simultáneamente en redes para

el despliegue de Ipv6. Actualmente, las redes que soportan Ipv6 tienen como base el soporte de Ipv4. Es importante que todas las organizaciones consideren la implementación del protocolo Ipv6 para sus servicios de internet durante los siguientes años, pero es también importante tener claro que el protocolo Ipv4 no se está erradicando, seguirá funcionando para los dispositivos que lo necesiten.

La transición del protocolo Ipv4 al protocolo Ipv6 sucederá sobre el curso de muchos años, dentro de los cuales los ambos protocolos seguirán trabajando para los accesos a servicios u otros sobre la Interne. Mucha de la infraestructura desplegada con protocolo Ipv4 continuará trabajando sobre internet durante muchos años.

- ¿Qué pasará si se tiene direccionamiento interno Ipv4 y el direccionamiento externo es Ipv6?

El nivel de trabajo u esfuerzo para que un sitio Web, servicio de correo, y otros servicios de la comunicación estén disponibles vía IPv6 será diferente para cada organización. Dependerá grandemente de cómo se instala, configura y despliega la red y los servicios que esta provea. Entidades de negocio que manejen sus propios sitios y servicios de correo con sus propios recursos. Estas necesitarán poner al día o actualizar su direccionamiento público para la utilización de ambos protocolos. Esto implica trabajo interno y coordinación con sus proveedores ISP para conseguir la comunicación con IPv6.

Entidades de negocio que utilizan a un ISP o contratista de servicio HOST para recibir y manejar sus sitios Web y servicios de correo, necesitarán entrar en contacto con su ISP o contratista del servicio *Host* e indicar su requisito que sus servicios estén disponibles sobre IPv4 e IPv6. Entidades de negocio que sean proveedores ISP, estas compañías necesitarán actualizar su

infraestructura de modo que incluya conectividad a internet usando Ipv6. Usuarios individuales es bastante probable que no tengan sitios Web o de servicios, pero si tienen comunicación con internet y se comunican con servidores de correo, estos estarán sujetos 100 por ciento al servicio proporcionado por su proveedor de internet, para poder comunicarse con ambos protocolos.

- ¿Cómo trabaja el direccionamiento IPv6? ¿Cómo se lee el nuevo direccionamiento?

En general, un direccionamiento IPv6 se compone de ocho cuartetos hexadecimales, cada uno separado por dos puntos. Por ejemplo, 2001:0db8:0049:0000:ab00:0000:0000:0102 es una dirección completa de IPv6. Los primeros cuatro cuartetos (64 dígitos binarios) del direccionamiento identifican la porción de la red del direccionamiento, designada como prefijo de la red, porque los direccionamientos IPv6 son jerárquicos, el prefijo de la red identifica la organización, el proveedor de servicio y otros elementos de la distribución de los paquetes. Los cuatro cuartetos restantes (64 dígitos binarios) componen la identificación del interfaz u dispositivo, un identificador único que es creado, principalmente usando la dirección MAC de un dispositivo.

Los direccionamientos se pueden comprimir por medio de dos pasos de progresión fáciles: primero, todos los ceros principales dentro de un cuarteto dado pueden ser eliminados. Para el direccionamiento antes dicho esto reduciría el direccionamiento a 2001:db8:49:0:ab00:0:0:102. Además, una vez por dirección (solamente una vez, de lo contrario se corre el riesgo de direccionamiento ambiguo) los cuartetos que contengan solo cero 0 pueden ser sustituidos por dos puntos dobles, haciendo la forma más comprimida del direccionamiento, como se muestra 2001:db8:49:0:ab00::102.

- ¿Los cortafuegos o llamados FIREWALLS trabajan realmente?

Sí, hay cortafuegos de protocolo IPv6 capaces y trabajan justo como cualquier otro cortafuego. La clave cuando se busca un corta fuegos y se evalúa su compatibilidad, se debe tener en cuenta qué es lo que el corta fuegos puede o no puede realizar. Este puede decir que es compatible con IPv6, pero a qué nivel o qué puede realizar con el protocolo IPv6. El comando común de la prueba de la interoperabilidad (JITC) ofrece una prueba más amplia y rigurosa para certificación de cortafuegos. El NIST ofrecerá una certificación en el futuro, pero no tiene realmente laboratorios de prueba disponibles. Siempre que hablemos de cortafuegos, no importa el performance o fácil configuración, si este no está bajo reglas certificadas, será muy poco recomendable la utilización del mismo.

- ¿Las herramientas u comandos comunes del establecimiento de una red tales como PING funcionarán con IPv6?

Sí, dependiendo de su plataforma (sistema operativo), algunos se pudieron renombrar los demonios o comandos levemente (y/o utilizar un protocolo, puerto especifico), por ejemplo: *Ping6,* pero las herramientas como Ping, el Tracert y el Telnet, están listos para el protocolo Ipv6.

- ¿Cómo trabaja el nuevo DHCPv6? ¿cómo es diferente de DHCPv4?

La auto configuración fue originalmente diseñada para eliminar la necesidad de un servicio DHCP en IPv6, y es en efecto, el método por defecto para la asignación de direccionamiento en casi todos los sistemas operativos de los ordenadores. Algunas empresas sentirán la necesidad de controlar sus asignaciones del direccionamiento más ordenada y controladamente. DHCPv6

trabaja de un punto de vista funcional, muy semejante a DHCP v4. La función del protocolo es proporcionar el direccionamiento y alguna otra útil información, por ejemplo: el direccionamiento de un servidor del DNS. Desde un punto de vista de operatividad, DHCP tiene algunas diferencias, el uso del multicast en vez de la difusión (broadcast) y la capacidad de asignar direccionamientos múltiples para un cliente. DHCP V6, también tiene dos modos de operación aparte del *Statefull, Stateless* y *Prefix Delegation*.

- ¿Cómo trabaja el nuevo DNSv6? ¿Cómo es diferente de DNSv4?

No existe el DNSv6, el servicio de DNS continúa funcionando con el valor por defecto, resolución de nombres en la ancha banda de internet, simplemente con un nuevo tipo de registro y una nueva opción de transporte. El nuevo tipo de registro es AAAA (cuarteto A) y el nuevo tipo de transporte es por supuesto el de IPv6.

Del punto de vista de la logística, el servicio de DNS trabaja justo como siempre lo ha hecho. Si un ordenador principal utiliza solamente el protocolo IPv4, este trabaja como siempre, haciendo la petición del registro A solamente. Si un ordenador utiliza solamente el protocolo IPv6, hará la petición del registro AAA. Si un ordenador utiliza ambos protocolos y tiene ambas opciones de transporte, realiza las peticiones de ambos.

- ¿Cómo se realiza la fragmentación de los paquetes IPv6 y cómo esto se compara con el actual IPv4?

La fragmentación ha cambiado completamente con IPv6. Cuando diferentes redes fueron unidas al inicio del internet, el trabajo de la fragmentación fue delegado a que fuera manejado por los puntos de entrada,

los *Routers* que conectaron diferentes redes entre sí o segmentos de una misma red. Puesto que algunos *Routers* tenían unidades de transmisión máximas más pequeñas (MTUs) que otros, tuvo sentido que se pudieran romper los paquetes cuando alcanzaran puntos de entrada, porque la confiabilidad y el rendimiento de procesamiento de la red estaban en un punto máximo. Con el nuevo protocolo IPv6, el papel del nodo que envía los paquetes es realizar el trabajo de la fragmentación. Como este trabajo es realizada por el nodo que envía y no en el tránsito de los paquetes, la carga en los *Routers* se reduce y estos pueden realizar el trabajo para el que fueron diseñados y construidos, pasar los paquetes hacia el siguiente salto u *Routers*.

5.3. El futuro sin IPv6, ¿es posible?

IPv6 es la primera gran actualización de IP en dos décadas; su predecesor, IPv4 permitió que internet haya pasado de ser una curiosidad militar y científica a una plataforma que conduce todas las industrias, servicios públicos y usos privados

5.3.1. Sin protocolo IPv6

Hasta ahora se han creado formas para poder seguir con la comunicación en internet con el protocolo existente, ¿cómo sería el futuro si todos los esfuerzos por implementar el nuevo protocolo IPv6, y estos fueran abandonados para la transición hacia el mismo? Como la transición no está pasando, la transición no pasará, son algunas incógnitas que pueden volverse realidad. Se estaría viviendo con el actual protocolo IPv4 y utilizando NAT por el resto de la vida.

Muchas personas que son mencionadas como expertos en el tema, piensan que el nuevo protocolo IPv6 es una solución en busca de un problema. Pueden realizar argumentos en diferentes casos como:

- No existe la escasez de direccionamiento en IPv4, ya que con NAT es posible que más de 1 usuario pueda compartir una o más direcciones.

- Cuando el direccionamiento de IPv4 escasee o se termine, los registros regionales de internet, pueden convertirse en compañías y las direcciones volverse en materias de intercambio en el mercado.

- Los costos y beneficios de estar utilizando solamente NAT con IPv4 son predecibles y bien entendidos, pero los costos de implementar IPv6 son altos y poco predecibles como entendibles.

NAT es la principal razón por la cual el direccionamiento de IPv4 no se haya agotado hasta hoy. Fue creado, principalmente para que pequeñas empresas puedan tener redes múltiples internas. Claro está que el direccionamiento siempre sigue agotándose. Se está tratando de no agregar nuevos nodos al *Back-Bone* del internet, el despliegue de nuevos nodos está haciéndose mediante ruteos hacia redes privadas, es decir, un NAT detrás de otro NAT.

Existe un límite en la profundidad de configuración de NAT tras NAT que se desee realizar utilizando direccionamiento IPv4, no es un límite muy brillante definido, pero si existe un límite. Aplicaciones que corran en esos nodos se multiplexan hacia una sola dirección global de acceso de 16 bits. Los limites se muestran rápido en la capa de transporte, la cual se ve afectada a excepción del TCP, así que entre más profundo se haga esta red de NAT más se limita a

las aplicaciones para la utilización de protocolos de transporte a excepción del protocolo TCP. La realización de redes NAT una detrás de otra, convierte en la internet en solamente conexiones tipo TCP.

Si se sigue tratando de multiplexar muchas conexiones sobre una sola conexión TCP se descubrirá que esos túneles de transporte su perform es gravemente afectado, debido a cómo los mecanismos externos del control de la tarifa del TCP y de la evitación de la congestión interfieren con los mecanismos internos del transporte. Pronto se descubrirá lo que muchos usuarios hace años, intentaron hacer esto, de que multiplexación en excesivo sobre TCP, es un juego de tontos. Apenas habrá más de una conexión del TCP. Pero cuantas más conexiones TCP necesite el nodo principal, serán menos conexiones TCP que tendrán los nodos detrás de las NAT detrás NAT que se tengan. Cuántas se necesitaran ¿?, dependerá de cuántas conexiones TCP por segundo se espera atender en el nodo principal, la cual no se puede tener una idea de la demanda del servicio.

El direccionamiento de IPv4 restante será asignado con el pasar de los años, a más tardar un par de años y el IPv4 puede verse agotado, aun para los pensadores optimistas que pronostican que el direccionamiento pueda durar hasta mediados de la siguiente década, pero nadie ve el IPv4 quedándose para siempre.

5.3.2. Nadie utilizará Ipv6

Actualmente, la implementación de IPv6 se refleja como el problema de quien vino primero, la gallina o el huevo, ya que hay que contemplar que:

- Proveedores de internet ISP's no dan direccionamiento de internet IPv6 debido a que la mayoría de sus clientes o usuarios no pueden manejar este protocolo. Utilizando módems para sus sistemas operativos, la mayoría de conexiones actualmente son proporcionadas por *Routers* de banda ancha, que solo soportan IPv4, como resultado nadie puede usar Ipv6.

- Los vendedores y fabricantes de *Routers* y *Switches*, la mayoría no soportan el protocolo IPv6 para mantener los costos bajos y el perform alto. No es necesario, ya que la mayoría de ISP's no soportan el protocolo IPv6, y no se mira que esto cambie en un futuro cercano.

Existe unos pocos ISP's que si han experimentado con el protocolo IPv6. Otro problema es que muchos sitios Web, por no abarcar a todos, no utilizan IPv6, pero es algo fácil de solucionar. Como la mayoría de servidores de servicios están localizados en centros de datos con *Routers* muy costosos que pueden ser actualizados.

Entonces qué cambiará este paradigma ¿?, un empujón por parte de los gobiernos, una transición de la televisión a digital, se necesitará que se realice:

- Especificar una fecha en la cual todos los dispositivos de hardware o aplicaciones de software vendidas sean compatibles con Ipv6.

- Especificar una fecha en la cual todos los ISP's con un número mayor a X de usuarios o clientes, o cierto nivel de ancho de banda, deban soportar IPv6

A diferencia de la transición de la televisión a digital, no existe una razón fuerte o extrema para eliminar de tajo el IPv4, así que no será malo que este tenga una muerte lenta y que se vuelva anticuado. La televisión digital es un caso diferente, ya que el tiempo comprado de televisión puede ser un incentivo para desplegar el cambio y la inversión sobre el nuevo protocolo IPv6.

Será esto lo que sucederá, es muy pronto para afirmarlo. Las olimpiadas en China, Pekin 2008, fue un ejemplo para la utilización del protocolo de internet IPv6, al utilizarlo con sus dispositivos, y esto es por la misma necesidad de ellos de direccionamiento debido a su gran crecimiento poblacional.

Los gobiernos, en especial el estadounidense, se están moviendo para la utilización del mismo, pero hasta que no se realice un empuje verdadero en el sector privado, es muy posible que se siga trabajando con IPv4, configurando redes con NAT, que es algo complicado de realizar.

5.4. Movilidad del protocolo IPv6 (MIPV6)

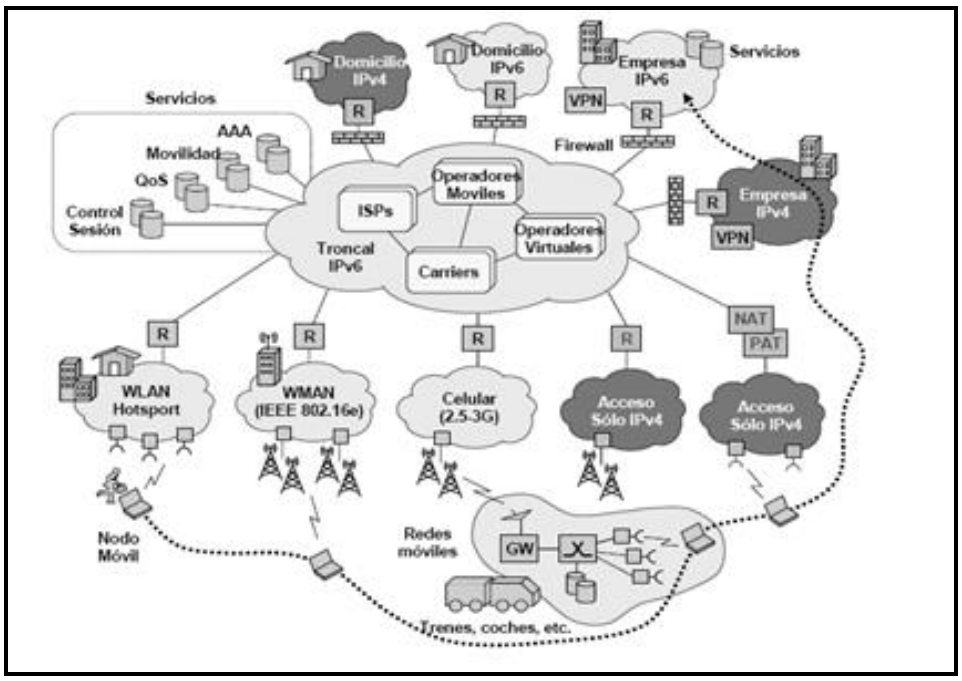
El modelo de conexión actual de internet, está basado o evolucionando rápidamente hacia un enfoque basado en la movilidad de los dispositivos gracias a la aparición de portátiles y a la cada vez más extensa cobertura de las redes de acceso.

Los operadores ven una fuente importante de ingresos en un servicio de movilidad basado en Ipv6 (MIPv6) que permita a sus dispositivos ser siempre alcanzables con independencia de la red en la que se encuentren. Aunque MIPv6 esta estandarizado, aún quedan algunos detalles que son necesarios resolver para permitir el despliegue a gran escala del servicio.

Actualmente, han empezado a aparecer todo tipo de dispositivos de red que permiten al usuario estar conectado a internet en cualquier lugar gracias a las tecnologías inalámbricas.

No solamente PCs portátiles sino también, PDAs, consolas de juegos, e incluso recientemente teléfonos móviles celulares y muchos más. Estos dispositivos van a empezar a cambiar el modelo de conectividad a internet.

Figura 23. **Escenario basado en movilidad IP**



Fuente: *Movilidad Ipv6*,
http://redesdecomputadores.umh.es/ipv6/Movilidad.html. Consulta: 25 de marzo de 2013.

Actualmente, cuando un dispositivo transita por distintas redes (*Roaming*), cada una de las nuevas redes le proporciona una dirección IP diferente por lo que el dispositivo no puede mantener una sesión de aplicación abierta.

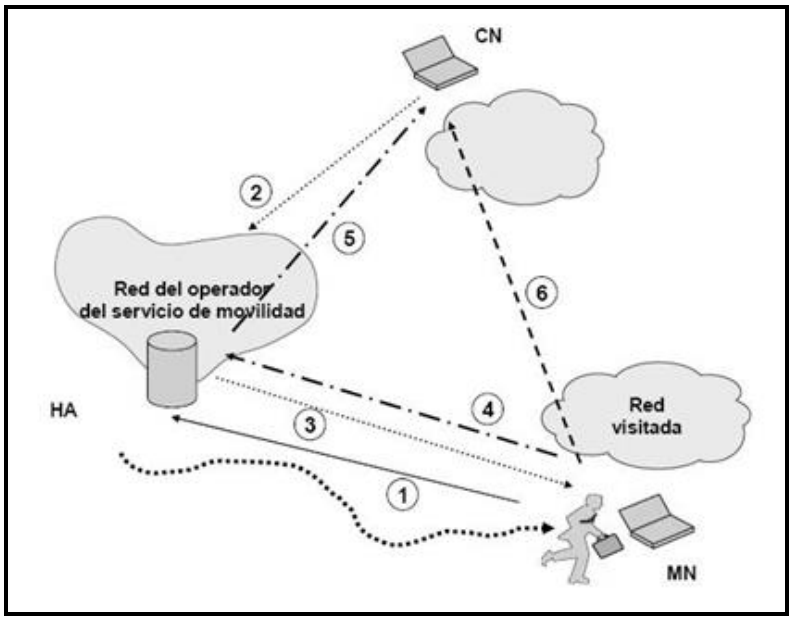
El modelo actual de conectividad impide la aparición de nuevos servicios basados en el escenario basado en movilidad IP, como la recepción en cualquier momento de mensajes multimedia, distribución de noticias, integración de comunicación vocal en aplicaciones; comunicaciones IP con servicios de seguridad, localización de flotas de autobuses, camiones, etc.

La IETF desarrolló un nuevo modelo de conectividad a internet que soluciona los problemas mencionados anteriormente. A esta tecnología se la conoce con el nombre de movilidad IP, la cual no es operativa sobre IPv4 por diversos motivos, pero gracias a IPv6 y sobre todo al protocolo de movilidad sobre IPv6 (MIPv6) la puesta en práctica de un modelo de conectividad con soporte de movilidad del usuario parece más cercana.

5.4.1. ¿Cómo funciona MIPv6?

En Mipv6 se definen tres agentes diferentes: *Home Agent* (HA), *Mobile Node* (MN) y *Correspondent Node* (CN). El HA es un agente que se despliega en la red del operador que despliega el servicio de movilidad. Es el encargado de tener registrada la verdadera posición del nodo móvil. Por su parte, el MN es el dispositivo del usuario que cuando se encuentra en la red de su operador tiene una dirección IPv6 denominada *Home of Address* (HoA) y cuando se desplaza y se encuentra en una red visitada adquiere una dirección diferente, denominada *Care of Address* (CoA). Por último, el CN es un nodo que pretende contactar con el MN y que en principio si no sabe cuál es su posición real trata de contactar usando la HoA del MN.

Figura 24. **Funcionamiento básico de MIPv6**



Fuente: *Movilidad Ipv6*, http://redesdecomputadores.umh.es/ipv6/Movilidad.html. Consulta: 25 de marzo de 2013.

Cuando el MN se encuentra en una red visitada, lo primero que hace es enviar a su HA un mensaje de señalización para notificar su verdadera posición (1), es decir, informa de la dirección IPv6 que tiene en ese momento (CoA). El HA actualiza su base de datos para ligar la dirección que tendría el MN en la red del operador (HoA) con la que realmente tiene en ese momento (CoA).

Cuando un CN quiere contactar con el MN (por ejemplo un usuario que quiere establecer una llamada de VoIP con el MN), lo que hace es intentar contactar con el MN a través de su HoA (2), ya que es la dirección fija conocida por el CN.

Los paquetes enviados a la red del operador y dirigidos a la HoA del MN son interceptados por él HA, encapsulados en un paquete MIPv6 y redirigidos hacia la nueva dirección CoA que el nodo móvil tiene en la red visitada (3). El MN contesta al CN encapsulando los paquetes de datos en un paquete MIPv6 y se lo envía al HA(4), el cual extrae el paquete original del paquete MIPv6 recibido y se lo envía al CN(5). Si el CN tiene soporte MIPv6, entonces es posible que el MN contacte con el CN para informarle que su dirección IPv6 en el momento de estar en la red visitada es la CoA y no la HoA, de manera que el CN envía los paquetes de datos directamente a la CoA del nodo móvil (6). A este procedimiento se le denominada *Route Optimization* y es una mejora en el camino seguido por los paquetes puesto que no tienen que pasar por él HA, lo cual introduce retardos innecesarios. Si el CN no posee soporte MIPv6 entonces no es posible que el CN y el MN puedan comunicarse directamente usando la función *Route Optimization*. Si el MN vuelve a cambiar de red, obtendrá una nueva CoA que deberá registrar en su HA con el fin de estar siempre alcanzable por cualquier CN que quiera comunicar con él.

5.4.2. Carencias de MIPv6

El mecanismo anteriormente descrito, corresponde al protocolo estandarizado y funciona de una manera efectiva y eficiente. Sin embargo, para que el despliegue de MIPv6 a gran escala en un operador sea realizable es necesario aún cierto trabajo para abordar diferentes aspectos de configuración de forma dinámica. En concreto, el protocolo de movilidad sobre IPv6 solo proporciona la definición de los agentes involucrados en el soporte de movilidad, su funcionamiento y sus interacciones, lo cual es suficiente si se piensa en un despliegue experimental o a baja escala en el que participen muy pocos usuarios y donde la configuración de los agentes implicados es predominantemente manual.

Si se piensa en movilidad como servicio de producción en un operador el marco de estandarización actual no es suficiente. Aún más escaso es el marco desarrollado para garantizar la seguridad en el servicio de movilidad. En el IETF se han desarrollado las pautas para integrar IPsec (concretamente el uso de la cabecera ESP de IPsec) en la señalización del servicio de movilidad (MIPv6), lo cual es beneficioso puesto que garantiza la confidencialidad y la integridad de las comunicaciones, pero es insuficiente puesto que no se menciona nada acerca de la distribución de las claves que serán utilizadas por el MN o por el HA para cifrar dichas comunicaciones sobre el protocolo IPv6.

Existen aún, por tanto algunos problemas relacionados con la configuración dinámica de los nodos que intervienen en el servicio de movilidad que requieren una solución cuando un proveedor de servicios pretende desplegar el servicio de movilidad a gran escala, con centeneras o millares de usuarios, puesto que el marco de estandarización actual no los contempla.

5.4.3. Problemas de MIPv6 en las redes visitadas

Los problemas descritos en la sección anterior están relacionados con el inicio del servicio de movilidad, pero no son los únicos con los que un usuario se puede encontrar cuando se desplaza por diferentes redes. En concreto existen dos obstáculos principales para que MIPv6 pueda funcionar: la presencia de firewalls que filtren los paquetes de tipo MIPv6 y la falta de soporte IPv6 en la red visitada por el usuario.

5.4.4. Funcionamiento en redes IPv4

Como su nombre indica, MIPv6 es un protocolo diseñado para funcionar sobre redes IPv6. Sin embargo, aunque un operador de servicios decida

realizar el despliegue de IPv6 en su red para proporcionar este tipo de conectividad a sus usuarios, no es garantía de que el servicio de movilidad sea operativo en cualquier escenario en el que se encuentre el usuario. Es muy probable que durante un período de tiempo existan otros operadores en los que no se realice el despliegue de IPv6 y por tanto sus redes sean solo IPv4.

Esto supone un problema cuando un usuario del servido de movilidad debido a su desplazamiento se encuentra en este tipo de redes, puesto que al tener solo conectividad IPv4 el MN no será capaz de contactar con el proveedor del servicio de movilidad, es decir, con él HA. Un despliegue real del servicio MIPv6 debe tener esta problemática solucionarla puesto que IPv6 hace ha dejado de ser un protocolo experimental y empieza a estar desplegado en las redes de los operadores más importantes.

5.5. Análisis de costo vr beneficio

El beneficio derivado de un nuevo protocolo, los cambios que este significa en la tecnología y principalmente en las arquitecturas de dispositivos para la transmisión de datos, debe ser balanceado por el costo asociado al realizar la transición del sistema actual.

El desarrollo de IPV6 se está llevando a cabo de una forma lenta pero constante, y se reconoce que no todos los sistemas actuales en la mayoría de países en desarrollo, podrán ser actualizados en muchos años, esto se debe a que muchas conexiones de redes son sistemas heterogéneos, con *Routers* de diferentes fabricantes los cuales les permiten tener acceso a una red externa la cual puede ser la misma internet, por otro lado se tiene la *World Wide Web* internet, la cual opera a través de 24 diferentes tipos de zonas.

Si se necesitara actualizar el protocolo Ipv4 hacia el nuevo protocolo Ipv6, este simple se complicaría, por consiguiente es necesario desarrollar estrategias para que el protocolo IPV4 coexista con el nuevo protocolo IPV6. El mecanismo que se utilizará para que el protocolo IPV4 y el protocolo IPV6 coexistan, es que el *Stack* de ambos protocolos sean implementados en un mismo dispositivo (*Router*, PC o servidor), el cual está referido como un nodo IPV6/IPV4. El nodo IPV6/IPV4 tiene la capacidad de enviar y recibir ambos tipos de paquetes IPV4 y IPV6 y puede ínter operar con un dispositivo de red con protocolo IPV4 usando paquetes IPV4 y con un dispositivo de red con protocolo IPV6 usando paquetes IPV6.

El nodo IPV6/IPV4 puede ser configurado con direcciones soportadas en ambos protocolos, como un protocolo de configuración dinámica (DHCP), conjuntamente con un protocolo de inicio y el sistema de nombre de dominio (DNS), los cuales deben ser involucrados en este proceso.

Cuando se piensa en una migración de un protocolo Ipv4 hacia el otro protocolo Ipv6, lo primero que se viene a la mente es el gran costo que esto conllevaría, en la gran inversión que se tendría que realizar para cambiar la infraestructura tecnológica de una empresa, organización, entidad educativa, etc. Pero hay que tener bien claro que la migración puede darse poco a poco, que no es necesario realizar la migración de un día para otro, ya que no está estipulada la fecha límite para la migración de los sistemas hacia Ipv6. La migración puede realizarse por fases y lo más conveniente es que se ejecute conforme las necesidades de la empresa, organización, entidad educativa, etc.

Un aspecto importante que hay que tomar en cuenta, es que el nuevo protocolo Ipv6, abre las puertas a que una cantidad enorme de dispositivos electrónicos tengan la posibilidad de poderse comunicar entre unos y otros, tal

es el caso de los celulares, agendas digitales, computadoras personales, hasta software hecho a la medida de cualquier otro medio que pueda trabajar debido al envío o recepción de datos.

El costo pronosticado es parecido al que actualmente se maneja, debido al cambio de tecnología tan acelerada. No se pueden indicar datos exactos de la inversión en migrar un sistema hacia el protocolo Ipv6, por las arquitecturas, dispositivos electrónicos y diferentes necesidades. Como cualquier inversión en I.T. se debe diseñar la combinación que maximice los beneficios de la empresa.

CONCLUSIONES

1. Debido a los avances que ha experimentado la tecnología últimamente, sobre todo el internet, se espera que los límites de capacidad de la red sean alcanzados en un corto plazo, lo cual permitirá usar nuevas formas de comunicación, esto será solucionado por el nuevo protocolo de comunicación Ipv6.

2. Las ventajas que ofrece este nuevo Ipv6 sobre el actual Ipv4 son: el número de direcciones posibles es cuatro veces más amplia, la seguridad, la configuración automática (plug and play) y rapidez.

3. La transición de internet hacia la nueva Ipv6 será un proceso lento a mediano plazo, ya que se deberán utilizar mecanismos para la transición, en los cuales se pueda tener la opción de poder trabajar con el nuevo Ipv6 y con el actual Ipv4.

4. Los encabezados de los nuevos y actuales protocolos sufren cambios de arquitectura, los cuales serán soportados por las nuevas generaciones de dispositivos de red, para que la utilización de estos nuevos protocolos sean transparentes para el usuario final.

5. La mayoría de sistemas operativos actuales, ya soportan el nuevo protocolo de comunicación Ipv6 o se pueden configurar para habilitar esta opción de soporte para este nuevo protocolo, algunos de estos sistemas operativos podrán seguir utilizando la actual Ipv4, además de poder utilizar la nueva Ipv6.

6. La magnitud e importancia de este nuevo protocolo de comunicación Ipv6, hace que muchas compañías alrededor del mundo, estén evolucionando y produciendo nuevos productos que utilicen este protocolo, por lo cual las nuevas tecnologías se ven beneficiadas con el mismo.

RECOMENDACIONES

1. Reforzar a las entidades que desarrollan software para internet, para que tomen las medidas preventivas sobre los nuevos programas, es decir que, estos puedan trabajar con la actual Ipv4 y que los mismos estén listos para trabajar con la Ipv6, ya que de lo contrario será necesario invertir en nuevos programas de software.

2. Explorar el impacto de Ipv6 para las organizaciones privadas o públicas, realizar proyectos o investigaciones que proporcionen información suficiente para entender y desarrollarse con el nuevo protocolo Ipv6.

3. Apoyar las iniciativas en la construcción y desarrollo de nuevas redes, servicios y aplicaciones por parte del sector privado. Dar a conocer los pasos necesarios para que se pueda realizar una transición lenta, pero segura hacia el nuevo protocolo de comunicación Ipv6.

4. Tomar en cuenta los cambios tecnológicos que se están realizando, adquirir información sobre los mismos y estar dispuestos o preparados para realizar un cambio en la forma de trabajar.

5. Fomentar la importancia que se debe tener sobre el nuevo protocolo Ipv6, ya que la tendencia de la tecnología es hacia este protocolo. Hay que estar conscientes de que el cambio se realizará como un proceso y no de forma acelerada.

BIBLIOGRAFÍA

1. ARMITAGE. G. *IPv6 over ATM Networks*. [en línea]. [Ref. diciembre de 1998] <http://www.ietf.org/rfc/rfc2492.txt.

2. CHANDER. Nav. *IPv6 Market Drivers and IPv6 Transition Strategies for Fixed Wireline Operators*. [en línea]. [Ref. mayo de 2013] <http:// www.ciscoknowledgenetwork.com/files/223_IPv6Economics.pdf.

3. CISCO SYSTEMS. *Cisco IOS Software Release Specifics for IPv6 Features*. [en línea]. [Ref. julio de 2011] <http://www.cisco.com/ en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-roadmap_xe.ht ml.

4. CONTA. A. *Generic Packet Tunneling in IPv6 Specification*. [en línea]. [Ref. diciembre de 1998] <http://www.ietf.org/rfc/rfc2473.txt.

5. CRAWFORD. M. *IP Version 6 over PPP*. [en línea]. [Ref. diciembre de 1998] <http://www.ietf.org/rfc/rfc2472.txt.

6. . *Transmission of IPv6 Packets over Ethernet Networks*. [en línea]. [Ref. diciembre de 1998] <http://www.ietf.org/ rfc/rfc2464.txt.

7. . *Transmission of IPv6 Packets over FDDI Networks*. [en línea]. [Ref. diciembre de 1998] <http://www.ietf.org/rfc/ rfc2467.txt.

8. DEERING. S. *Multicast Listener Discovery (MLD) for IPv6*. [en línea]. [Ref. octubre de 1999] <http://www.ietf.org/rfc/rfc2710.txt.

9. EVANS RED. K. *Transaction Internet Protocol - Requirements and Supplemental Information*. [en línea]. [Ref. julio de 1998] <http://tools.ietf.org/html/rfc2372.

10. GILLIGAN. R. *Transition Mechanisms for IPv6 Hosts and Routers*. [en línea]. [Ref. abril de 1996] <http://www.ietf.org/rfc/rfc1933.txt.

11. GONT. F. *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*. [en línea]. [Ref. marzo de 2013] <http://www.rfc-editor.org/rfc/rfc6980.txt.

12. HEMMINGER. Gary. *IPv6 Market Drivers*. [en línea]. [Ref. enero de 2004] <http://www.usipv6.com/CES_Presentations/CES_Gary_ Hemminger.pdf.

13. HINDEN. R. *Network Working Group IP Version 6 Addressing Architecture*. [en línea]. [Ref. febrero de 2006] <http:// tools.ietf.org/html/rfc4291.

14. JACOBSEN. J. *The Internet Protocol Journal*. [en línea]. [Ref. septiembre de 2010] <http://www.cisco.com/web/about/ac123/ ac147/archived_issues/ipj_13-3/ipj_13-3.pdf.

15. MCCANN. J. *Path MTU Discovery for IP version 6*. [en línea]. [Ref. agosto de 1996] <http://www.ietf.org/rfc/rfc1981.txt.

16. MCFARLAND. Shannon. etal *IPv6 for Enterprise Networks*. [en línea]. [Ref. abril de 2011] <http://my.safaribooksonline.com/book/ networking/ ip/9781587142291.

17. PERALTA. Luis. *IPv6*. [en línea]. [Ref. febrero de 2002] <http://www.uji.es/bin/docs/projectes/ipv6/ipv6p.pdf.