UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS SOBRE LA MIGRACIÓN AL PROTOCOLO IPV6 EN EL PERÚ

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

CARLOS EFRÉN BARRIOS VILLACORTA

PROMOCIÓN
2005 - II

LIMA – PERÚ
2010

ANÁLISIS SOBRE LA MIGRACIÓN AL PROTOCOLO IPV6 EN EL PERÚ

Dedicatoria

A mis padres,

A mis abuelos,

A mis hermanos,

A Nafrith,

Y a mis amigos de toda una vida.

SUMARIO

El presente trabajo describe los métodos usados para llevar a cabo una migración adecuada hacia redes de nueva generación. Mediante este informe, se pretende documentar la planificación que se realizaría en un departamento IT con el fin de implementar el protocolo de red IPv6 en las redes de datos, de tal manera que, durante el tiempo que sea necesario, pueda convivir con el protocolo de Internet actual IPv4. Para ayudar en la tarea de decidir cómo diseñar y construir la nueva red, cómo protegerla y qué tipos de servicios has de ser creados al principio, se proveen de los instrumentos básicos para usar el nuevo protocolo tales como las diversas tecnologías de transición que se detallan para un buen entendimiento. Finalmente, haciendo un análisis de la integración de las redes avanzadas, se pretende dar un alcance sobre los logros obtenidos por nuestro país acerca de la conectividad global a Internet IPv6 siendo parte de la red CLARA latinoamericana y desarrollando proyectos en la actual Red Académica Peruana RAAP que nos hace miembros partícipes de los avances de redes actuales y su tendencia a migrar hacia nuevas tecnologías.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La migración de las redes actuales al protocolo IPv6 es un proceso por etapas y abarca todo un conjunto de tecnologías que establecen reglas de funcionamiento permitiendo la coexistencia de ambos protocolos siendo de alguna manera compatibles para ciertas aplicaciones. Las principales fuentes de este proceso son los trabajos y proyectos realizados en las redes avanzadas, que han venido implementándolo desde las pruebas de inicio hasta la implementación final.

Buscando mejorar el entendimiento y el uso adecuado de una red que soporte IPv6, es que se hace un análisis sobre las diversas tecnologías y la situación actual en el Perú sobre el soporte hacia redes avanzadas IPv6.

El presente informe se encuentra dividido para el análisis del tema en cuatro capítulos.

El capítulo uno, muestra un enfoque de lo que está aconteciendo con las redes IPv4, las razones de uso del nuevo protocolo y su repercusión con el crecimiento inesperado de Internet.

El capítulo dos, describe ambos protocolos desde la estructura básica de los encabezados IP hasta las formas de representación de direcciones y los mecanismos de direccionamiento y enrutamiento de paquetes durante el intercambio de información.

El capítulo tres, detalla las diferentes tecnologías de transición las que permiten implementar redes avanzadas conectadas a Internet IPv6 como aquellas que soporten ambos protocolos o que sean sólo de IPv6.

El capítulo cuatro, resume la situación actual de la interconectividad de nodos en el Perú con soporte para redes IPv6 y con acceso a redes avanzadas en el mundo.

CAPÍTULO I

MIGRACIÓN Y ADAPTABILIDAD AL CAMBIO

La necesidad de usar redes de comunicaciones mucho más potentes que utilicen mejor el ancho de banda asignado y con mejores servicios ha permitido que surjan nuevas tecnologías sobre las que se puedan integrar diversas y nuevas aplicaciones, las que requieren en muchos casos, mayor velocidad en la transferencia de datos y mejor seguridad, lo cual no es posible con las redes actuales.

En este capítulo se revisarán por qué es necesario implementar una red que soporte al protocolo IPv6, cuáles son las razones esenciales con respecto al tradicional protocolo IPv4 y enfrentarnos al inminente crecimiento global de la red de Internet.

1.1 Necesidad del cambio

Cambiar a otra forma de tecnología no es tan simple, surgen diversos factores que impiden adaptar todo un sistema de comunicaciones a corto plazo; tal es así que algunos optan por mantener aún la tecnología que han venido usando por varios años, lo cual no está mal sino que tarde o temprano será necesario realizar un cambio el cual, en muchos casos es inevitable. Esto está referido al uso actual que se le ha venido dando al protocolo IPv4 y a las diversas aplicaciones que lo soportan y que se ha convertido en uno de los protocolos más utilizados en las grandes redes como Internet y otras redes similares. El protocolo IP forma parte de la suite de protocolos de la familia TCP/IP muy importante por la cantidad de aplicaciones que permite utilizar durante la transferencia e intercambio de información. La necesidad surge por los diversos problemas que empiezan a notarse en IPv4 debido al crecimiento de las grandes redes como Internet y otros factores que se resuelven con la tecnología ofrecida en IPv6.

1.2 El Problema de IPv4

Los problemas más resaltantes con IPv4 para los cuales IPv6 puede considerarse una solución son:

El crecimiento inevitable e inesperado del espacio de direcciones en IPv4.

El colapso inminente de la estructura de enrutamiento debido al crecimiento explosivo de las tablas de enrutamiento.

El problema de la interoperatividad a través de los dominios de enrutamiento en los cuales las direcciones IP pueden no ser globales únicas.

Básicamente la principal limitación de IPv4 es el espacio de direcciones que ofrece debido a que utiliza 32 bits para asignar direcciones IP. Este reducido espacio, a pesar de tener más de cuatro mil millones de direcciones disponibles se está saturando por completo lo cual fue insospechado hace 20 años.

IPv4 ha probado tener un diseño flexible y potente, pero presenta algunas limitaciones en el funcionamiento de las redes actuales y futuras, así por ejemplo:

Escasez de direcciones IP, menos direcciones disponibles lo cual limita el crecimiento de Internet.

Impide el uso de internet a nuevos usuarios.

El enrutamiento es ineficiente en la actualidad.

Ocasiona que los usuarios utilicen NAT.

Es complicado adecuarlo para soportar nuevas aplicaciones como IPv6 en tiempo real.

IPv4 no fue diseñado para ser un protocolo seguro, sólo para enrutamiento.

Ante el reducido espacio de direcciones en IPv4, existe una solución que se podría considerar que es la renumeración y reasignación de dicho espacio de direccionamiento, pero, no es tan simple y quizás imposible en algunas redes, ya que para esto se requiere coordinar varios aspectos a nivel global lo cual es algo complejo.

Es más, uno de los problemas de IPv4 sería el gran tamaño de las tablas de enrutamiento en la troncal (*backbone*) de Internet que lo hace ineficiente y perjudica enormemente los tiempos de respuesta durante la transmisión de información.

La utilización de direcciones IP de parte de los usuarios está cambiando en la razón de 10 a 1 y en poco tiempo será de 1 a 1. Más aún en unos años más, cada usuario podrá tener hasta 50 direcciones IP e incluso 100 (razón de 1 a 50 ó 1 a 100) con lo que se estaría invirtiendo la proporción inicial usando tecnologías con dispositivos que estarán "siempre conectados".

En muchos casos, los proveedores de servicios de internet ISP (*Internet Services Provider*), se ven obligados a proporcionar a sus clientes direcciones IP privadas usando mecanismos NAT (*Network Address Table*) el cual permite traducir direcciones usando una sola IP pública para toda una red privada. Con esto, la mayoría de ISP's sólo han

podido otorgar un números reducido de direcciones IP públicas para la mayoría de sus clientes empresariales.

Como es de notar, con IPv4 la solución temporal sería usar mecanismos NAT lo cual implica la imposibilidad de usar algunas aplicaciones que no soportan este tipo de tecnología de traslación, debido a que muchos protocolos no pueden atravesar los dispositivos NAT.

1.3 Las razones de uso del protocolo IPv6

La razón principal por la que surge la necesidad de crear un nuevo protocolo fue notar la falta de direcciones IP en las redes. Esto surgió en la IETF (*Internet Engineering Task Force*) que permitió crear el proyecto denominado IPng (*IP Next Generation*).

Además, es bueno mencionar que los creadores de IPv4 en los años 70, no predijeron en ningún momento, el éxito que este protocolo iba a tener en tan poco tiempo no sólo en la ciencia y educación, sino también en las innumerables facetas de la vida cotidiana. A partir de ese instante y debido a la creación de muchas aplicaciones con soporte para IPv4, ha sido conveniente crear "agregados" al protocolo básico, entre los "parches" más conocidos se puede mencionar: medidas para mejorar la Calidad de Servicio (QoS), Seguridad (IPSec) y Movilidad principalmente.

El inconveniente más resaltante de estas mejoras de IPv4 es que utilizar cada uno de ellos en forma individual es sencillo, el problema está cuando queremos utilizar dos "agregados" al mismo tiempo o quizás tres, lo cual se hace un poco más complejo.

1.4 El crecimiento de Internet

Ha sido inesperado e inevitable el crecimiento de internet a nivel global, las cifras de navegadores o denominados "internautas" esperadas en los próximos años corroboran lo mencionado anteriormente:

África: *800'000,000* (sólo *3'000,000* sin NAT).

América Central y del Sur: *500'000,000* (sólo *10'000,000* sin NAT).

América del Norte: *500'000,000* (sólo *125'000,000* sin NAT).

Asia: *2500'000,000* (sólo *50'000,000* sin NAT).

Europa Occidental: *250'000,000* (sólo *50'000,000* sin NAT).

Además, lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas y globales, válidas para conexiones de extremo a extremo que sean enrutables como videoconferencia, VoIP, seguridad e incluso, juegos en línea.

En 1997, el mercado de dispositivos con aplicaciones capaces de conectarse a Internet (sin incluir terminales ni computadoras personales, tan sólo WebTV, agendas electrónicas, teléfonos con acceso a internet y consolas de videojuegos), era de tres millones. En el año 1998, esta cifra se duplicó hasta llegar a seis millones. En el año 2010, según IDC esta cifra superará fácilmente los mil millones de dispositivos conectados.

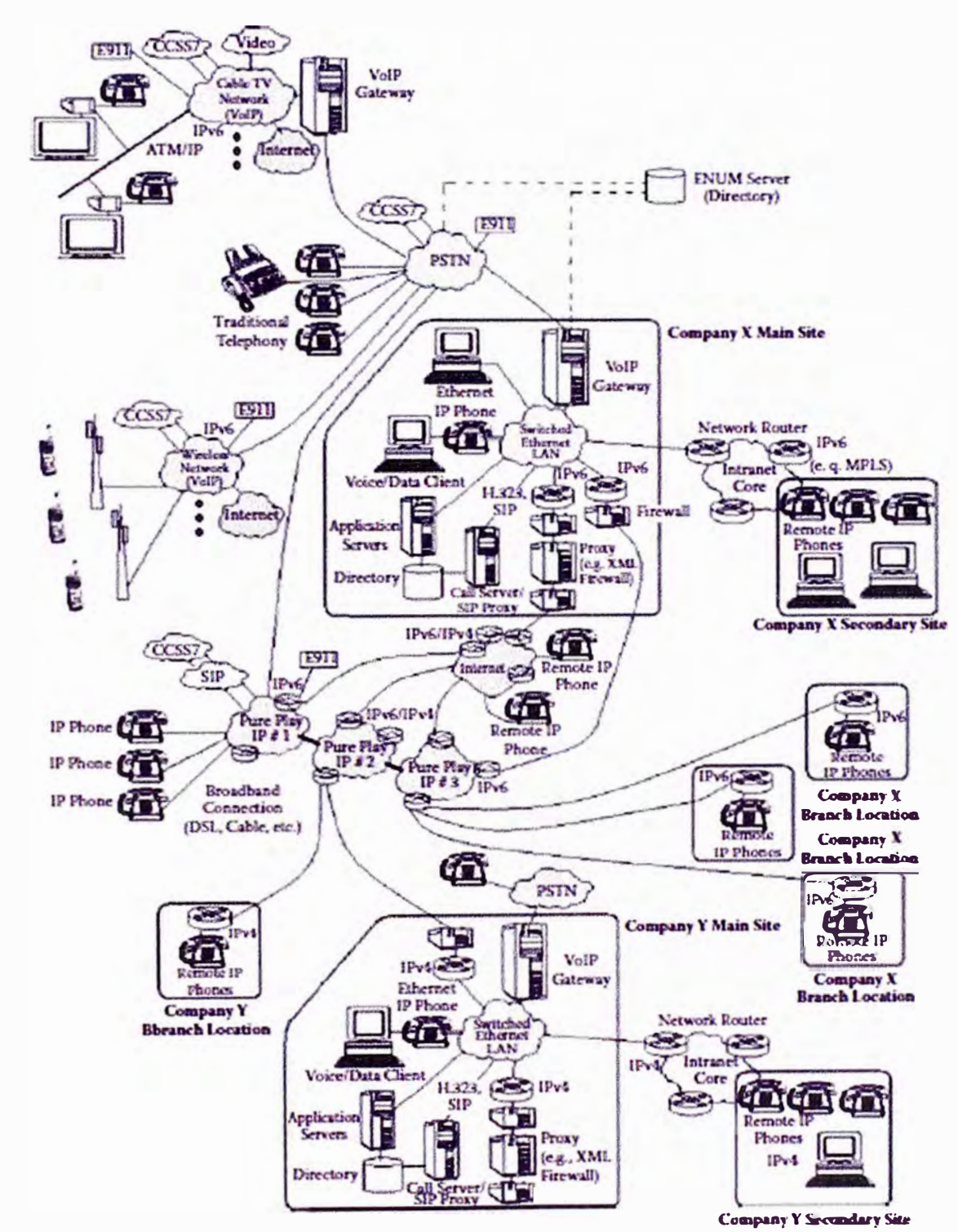

Fig. 1.1 Elementos de una Red IPv6

Según el foro de la UMTS/GSM se prevé unas necesidades de direcciones IP para los dispositivos de la red que interfieren en el crecimiento de nodos que ya no serán soportados con una red IPv4.

Ante todo esto, hay que sumar los diversos dispositivos que se van creando o los ya existentes a los que les damos nuevas y mejores aplicaciones, mediante su conexión a Internet, así tenemos:

Telefonía, por la tendencia de utilizar en las nuevas tecnologías, voz sobre IP (VoIP).

Radio y Televisión, basados también en tecnologías IP.

Sistemas de seguridad, control y televigilancia.

Dispositivos MP3, que conectados a la red, nos permiten recuperar y almacenar creaciones musicales.

También, las nuevas tecnologías emergentes, como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc., hacen que esta necesidad siga creciendo, al menos en lo que se refiere al número de direcciones IP.

La última tendencia, por ejemplo, es de permitir a cualquier dispositivo serie, estar conectado a una LAN o WAN y mejor aún, a Internet. Este tipo de convertidores, denominados UDS (*Universal Device Server*) o Servidor de Dispositivos Universal, permite que aplicaciones impensables por la limitaciones de los cableados serie, se realicen remotamente a través de redes, o inclusive, que un sistema de alarmas, que antes requería de un módem dedicado para la conexión con la central de recepción de alarmas, pueda ahora enviar un e-mail, con todos los detalles posibles. Así se podría mencionar, sobre cualquier dispositivo industrial o doméstico, integrado a la gran red, así como también sobre dispositivos de control médico, marcapasos, entre otros.

En algunos artículos, se menciona que esta tendencia de las nuevas tecnologías es inevitable y que, debemos estar preparados para adaptarse al gran cambio y que de seguro, será sólo el inicio del uso de nuevas tecnologías que con el transcurrir de los años serán cada vez mejores.

Algunos afirman lo siguiente, con respecto a IPv6:

"La verdadera cuestión no es si necesitamos y creemos en IPv6, sino ¿estamos interesados en una red que permita a cualquier dispositivo electrónico IP comunicarse transparentemente con otros, independientemente de su localización, en la red global?" de una importante compañía de ingeniería y consultoría canadiense denominada "*Viagénie*".

"El camino de IPv4 a IPv6 no es una cuestión de transición ni de migración sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora, y al mismo tiempo necesaria. IPv6 nos permitirá un crecimiento escalable y simple, principales hándicaps actuales de IPv4. Preparemos y mejoremos nuestras redes, las de nuestros clientes, las de nueva implantación, con dispositivos, sistemas operativos y aplicaciones que estén realmente listos o en camino de cumplir las especificaciones de IPv6, sin por ello dejar de ser válidos en IPv4. Hay que asegurar el futuro, no hipotecarlo, frente al inevitable comercio electrónico móvil (*m-commerce*), por la salud de la red global. Seamos y estemos ¡*IPv6 READY*!", de CONSULINTEL (*Consultores Integrales en Telecomunicaciones*) de España, que es parte del fórum de desarrollo e implementación de IPv6. Además, se puede afirmar lo siguiente: "Ante todo cambio habrá siempre consecuencias que de alguna manera afecten la vida cotidiana y si IPv6 y toda su tecnología significan algo bueno para un usuario común, bienvenido sea. Es por ello que debemos estar preparados para adaptarse a este gran cambio."

CAPÍTULO II

ARQUITECTURA IPV6 FRENTE A IPV4

Cada nueva tecnología presenta mejoras en cuanto a su estructura y es por esto que en este capítulo se hace referencia de las características más relevantes del protocolo IPv6 con respecto a IPv4, las características de los encabezados en cada protocolo, las formas de representación de direccionamiento y los mecanismos de enrutamiento para la transmisión de datos dentro de una red corporativa y organizada.

2.1 Modelo de Referencia OSI

Durante los años 1970's, aproximadamente doce años después del desarrollo de varios protocolos de comunicación incluyendo TCP/IP, la Organización de Estándares Internacional ISO (*International Standards Organization*), estableció un modelo para estandarizar los sistemas de comunicaciones. Este modelo es conocido como Modelo de Referencia de Interconexión de Sistema Abierto OSI (*Open System Interconnection*) y define una arquitectura cuyas funciones de comunicación están divididas en siete capas o niveles cada una con funciones específicas.

2.1.1 Nivel Físico

Es el nivel más bajo del Modelo de Referencia OSI. Este nivel implica la conexión de un sistema de comunicaciones al medio de comunicación. Además, es el encargado de especificar la conexión física y eléctrica entre los dispositivos de comunicaciones que permiten conectar a los diferentes tipos de medios de comunicación. En esta nivel se especifican las conexiones de cable y las reglas eléctricas necesarias para el intercambio de datos entre dispositivos.

2.1.2 Nivel de Enlace

Este nivel es responsable de definir la forma en que un dispositivo tiene acceso al medio especificado en la capa física. También es responsable de definir los procedimientos para el control de errores.

El Instituto de Ingenieros Electricistas y Electrónicos IEEE, responsable del desarrollo de estándares para una LAN, subdivide la capa de enlace en dos sub niveles: LLC (*Control*

de Enlace Lógico LLC) y MAC (*Control de Acceso al Medio*). La capa LLC es responsable de generar e interpretar los comandos que controlan el flujo de datos y realiza las operaciones de recuperación en los errores detectados. Asimismo, la capa o nivel MAC es responsable de proveer el acceso a la red local, que permite a una estación en la red poder transmitir información. La Fig.2.1, muestra la relación entre Ethernet y el modelo OSI.

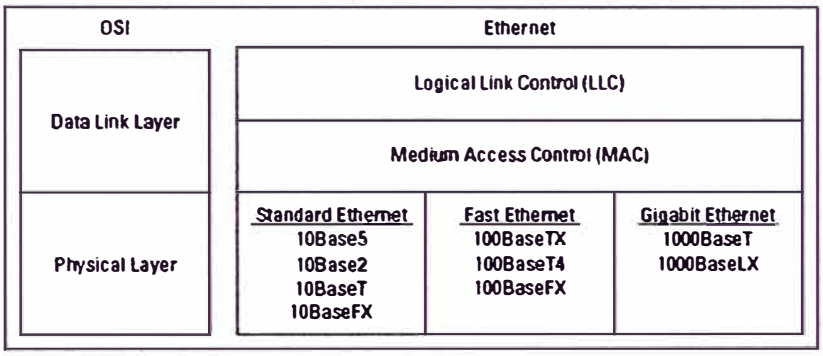

Fig.2.1 Ethernet y el Modelo OSI

2.1.3 Nivel de Red

Esta capa es responsable de arreglar una conexión lógica entre el origen y destino en la red, seleccionar y elegir una ruta adecuada para el flujo de información entre el origen y destino basándose en caminos disponibles (enrutamiento).

En la capa de red, las unidades de información son colocadas en paquetes que tienen un encabezado. Así, un paquete contendrá la información de direccionamiento así como un campo que facilite la detección y corrección de errores.

2.1.4 Nivel de Transporte

Es responsable de la transferencia de información luego de haberse establecido el enrutamiento en el nivel de red. En general, existen dos tipos de protocolos de nivel de transporte, uno orientado a conexión y otro a sin conexión. Un protocolo orientado a conexión requiere primero que se establezca una prioridad en la conexión para que ocurra la transferencia de datos. Este tipo de protocolo realiza el control de errores, chequeo de secuencias y otros tipos de funciones de fiabilidad. El otro tipo de protocolo opera en modo de sin conexión y depende de los niveles más altos para la detección de errores.

2.1.5 Nivel de Sesión

Este nivel es responsable de proveer un conjunto de reglas que permiten el establecimiento y finalización del flujo de datos que fluyen entre los nodos de una red. Los

servicios que este nivel puede proveer incluyen el establecimiento y terminación de conexiones a los nodos, control del flujo de mensajes y control de diálogo. La Fig.2.2, muestra el esquema del Modelo de Referencia OSI y algunos ejemplos de protocolos en cada nivel.

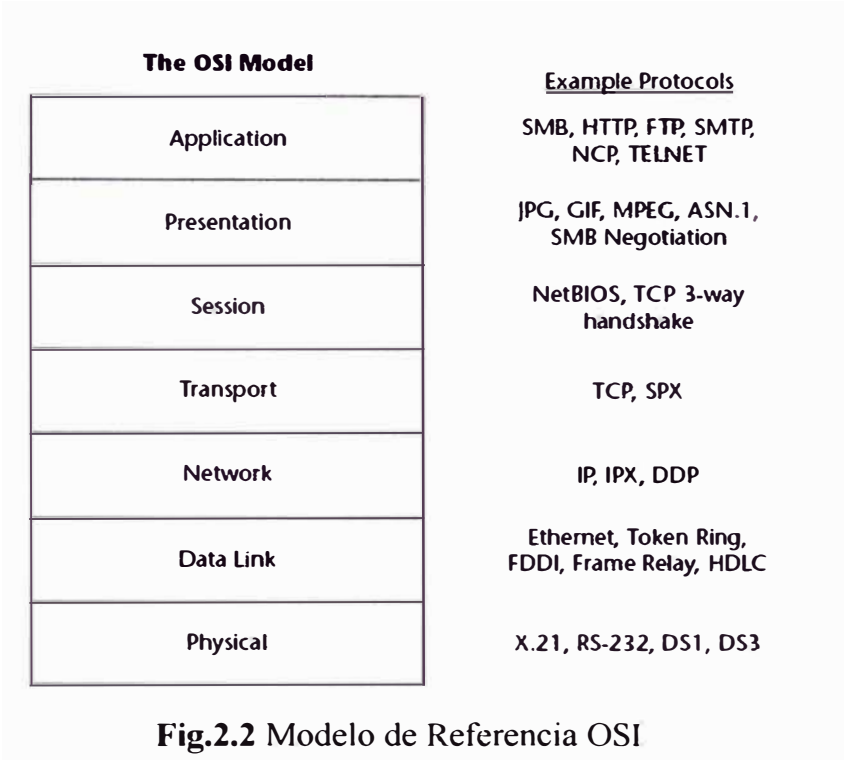

Fig.2.2 Modelo de Referencia OSI

2.1.6 Nivel de Presentación

Este nivel se encarga de la conversión de datos transmitidos en un formato adecuado para ser mostrado en el dispositivo receptor. Como funciones que se realizan en este nivel pueden incluir la compresión y descompresión de información, así como la encriptación y desencriptación.

2.1.7 Nivel 7: Aplicación

Este nivel permite el acceso a todos los servicios proporcionados en el modelo OSI. Ejemplos de estos servicios son: correo electrónico, transferencia de archivos, compartición de recursos y acceso a base de datos.

2.2 La suite de Protocolos TCP/IP

El protocolo de red TCP/IP se ha convertido en el protocolo más importante en los últimos años desde su creación en los años 1960's (adoptado recién en los años 1980's como estándar). En realidad se trata de un conjunto o suite de protocolos cada uno con una función específica. Nació como un proyecto y se consolidó con el surgimiento y crecimiento de Internet a nivel mundial.

El flujo de datos en cada nivel OSI se da como lo mostrado en la Fig.2.3.

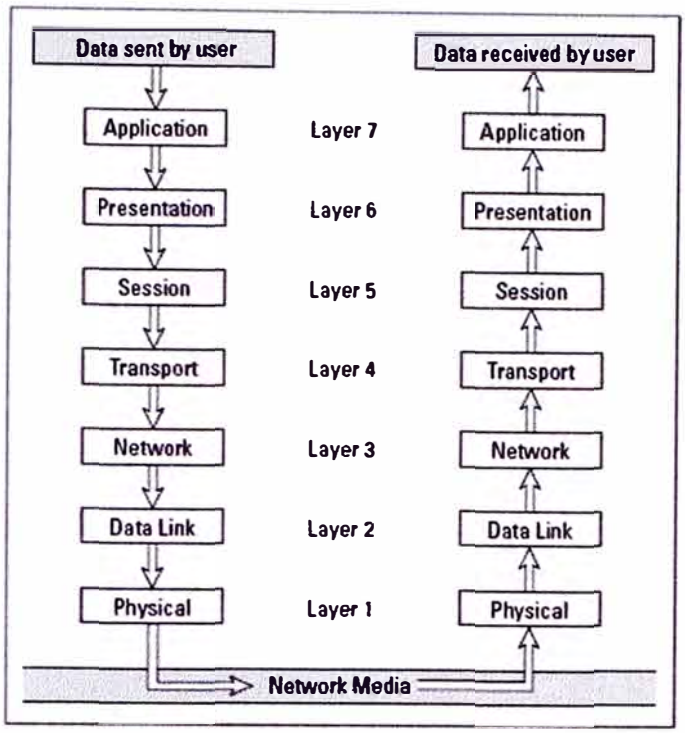

Fig.2.3 Flujo de Datos a través de los Niveles OSI

El protocolo TCP/IP, actualmente representa dos protocolos distintos. La mayor parte del tráfico en una red es transferido usando ambos protocolos, pero el conjunto de protocolos que incluye a TCP e IP es conocido como suite TCP/IP.

ISO Reference Model Layer	TCP/IP Protocol Suite						
Application Presentation Session	FTP	HTTP	Telnet	SMTP	DNS	SNMP	Other Applications
Transport	TCP				UDP		
Network	ICMP IP ARP						
Data Link	Ethernet	Token Ring	X.25	Frame Relay	Other		
Physical	Physical Layer						

Fig.2.4 Comparación entre la suite TCP/IP y el Modelo de Referencia OSI

En la Fig.2.4, puede verse claramente una comparación general entre el modelo de referencia OSI y la suite de protocolos TCP/IP. El término "comparación general" está referido porque la suite de protocolos TCP/IP consiste en cientos de aplicaciones de las cuales sólo se han mostrado algunas. El modelo TCP/IP a diferencia del modelo OSI, muestra una división en niveles como se menciona:

Nivel 1: Interfaz de red. Que comprende los niveles Físico y Enlace del modelo OSI.

Nivel 2: Internet. Comprende el nivel de Red de OSI.

Nivel 3: Transporte. Comprende nivel Transporte de OSI.

Nivel 4: Aplicación. Comprende los niveles: Sesión, Presentación y Aplicación de OSI.

2.2.1 Protocolos de Red

El nivel de red de la suite de protocolos TCP/IP consiste en las características propias del protocolo de Internet IP. Este protocolo incluye un esquema de direccionamiento que identifica a las direcciones de origen y destino de los paquetes que son transportados. En términos de TCP/IP, la unidad de datos que son transmitidos al nivel de red está definida como un datagrama. Además, se debe considerar a dos protocolos muy importantes que permiten definir al nivel de red. Dichos protocolos son: ARP (*Protocolo de Resolución de Direcciones*) y el protocolo ICMP (*Protocolo de Control de Mensajes de Internet*).

2.2.1.a Protocolo IP

El protocolo de Internet IP provee la capacidad de direccionamiento que permite a un datagrama ser enrutado entre varias redes. La versión usada actualmente en nuestro país es la versión IPv4, que consiste en tener un espacio de 32 bits en el uso de direcciones IP. La tendencia y crecimiento de nuevas tecnologías ha hecho posible también que el uso de direcciones emerja notablemente, un ejemplo claro es el Protocolo de Internet versión 6, conocido como IPv6.

2.2.1.b Protocolo ARP

Una de las diferencias más resaltantes entre el nivel de enlace y el nivel de red es el método de direccionamiento usado en cada nivel. En el nivel de enlace, como en redes LAN Ethernet y Token Ring se usan direcciones MAC de 48 bits. Comparándolo con TCP/IP, la versión actual usa 32 bits y la de nueva generación IPv6, usa 128 bits. Entonces, la entrega de un paquete o el flujo de un datagrama en una red, requiere de una conversión de direcciones.

Esa conversión está representada por el protocolo ARP (*Protocolo de Resolución de Direcciones).*

2.2.1.c Protocolo ICMP

El Protocolo de Control de Mensajes de Internet ICMP, como su nombre indica, representa un protocolo usado para transportar mensajes de control. Los mensajes ICMP son transportados con el prefijo de un encabezado IP para el mensaje.

2.2.2 Protocolos de Transporte

Como se muestra en la Fig.2.4, hay dos protocolos en el nivel de transporte soportados por la suite TCP/IP: el Protocolo TCP y el Protocolo UDP.

2.2.2.a Protocolo TCP

El protocolo TCP es un protocolo orientado a conexión. Esto significa que la prioridad para transmitir data por TCP, el protocolo requiere el establecimiento de un camino entre origen y destino tanto como saber que el receptor esté listo a recibir la información. Una vez que el flujo de datos comienza, cada unidad que se define como un segmento TCP, es revisada en caso de errores por el receptor. Si se detecta un error en el proceso, el receptor solicitará la retransmisión del segmento enviado. En conclusión, TCP no es un protocolo seguro, sólo está orientado a conexión. Como se muestra en la Fig.2.5, ciertas aplicaciones usan TCP como su protocolo de transporte mientras que otras aplicaciones usan UDP.

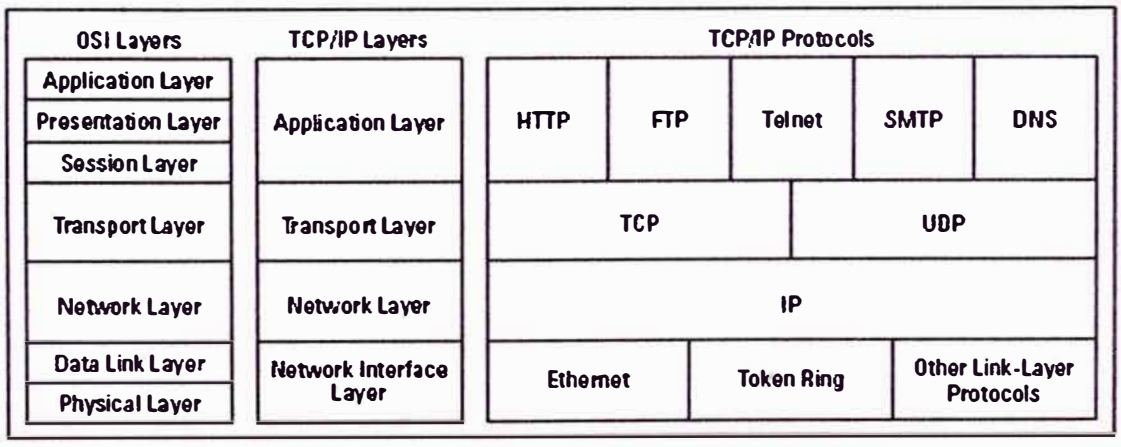

Fig.2.5 TCP/IP y el Modelo OSI

La característica "orientada a conexión" significa que esto requerirá de un periodo de tiempo en el origen y destino para intercambiar información durante la sesión de conexión. Además, al ser un protocolo no seguro, puede ser redundante en los niveles más altos de la suite de protocolos. Reconociendo los problemas mencionados anteriormente, los

desarrolladores de la suite de protocolos TCP/IP agregaron un segundo protocolo de transporte conocido como UDP.

2.2.2.b Protocolo UDP

El Protocolo de Datagramas de Usuario, fue desarrollado en reconocimiento de los factores que algunas aplicaciones pueden requerir pequeñas partes de información para ser transferidas y el uso de un protocolo orientado a conexión podría resultar en un gasto innecesario y significante para la transferencia de datos. Porque un nivel más alto en la suite de protocolos puede realizar un chequeo, detección y corrección de errores los cuales podrían ser eliminados desde UDP. La Fig.2.6, muestra el flujo de datos entre red TCP/IP para ser entregados a una red LAN.

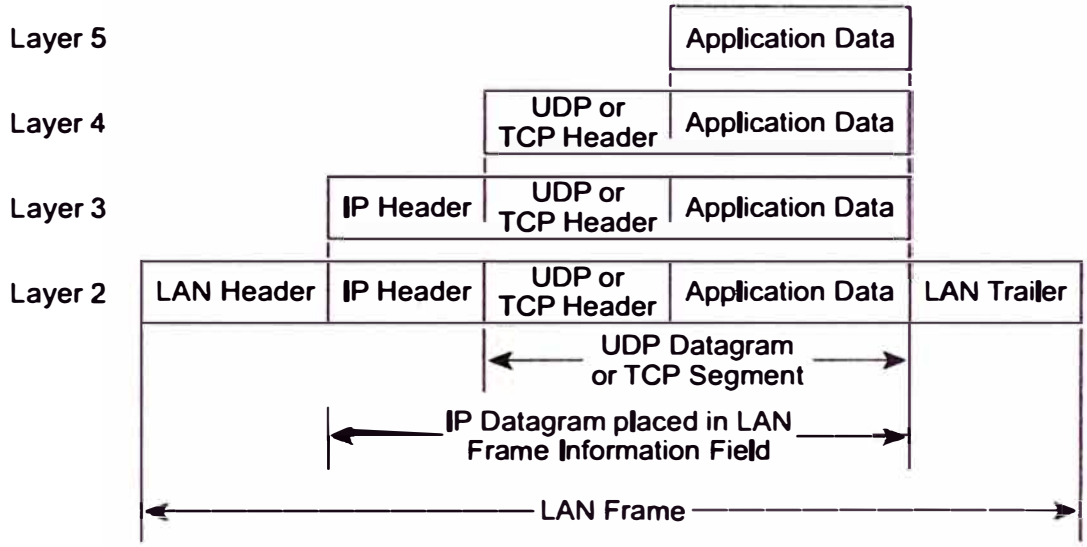

Fig.2.6 Flujo de datos dentro de una red TCP/IP para entregar datos en una LAN

La suite de protocolos TCP/IP, representa una colección de protocolos y aplicaciones metódicamente desarrollada y considerada. Como se ha notado, es una arquitectura abierta y muy flexible que permite el desarrollo de nuevos protocolos y aplicaciones; así como el desarrollo de IPv6 y sus notables ventajas sobre IPv4.

2.3 Características de IPv6

Las características principales del protocolo IPv6 pueden resumirse como:

Nuevo Formato de Encabezado. El encabezado IP tiene un nuevo formato que está diseñado para minimizar los procesos de encabezamiento. Esto se logra removiendo los campos opcionales hacia encabezados de extensión que se ubican después del encabezado

IPv6. Los encabezados de IPv4 e IPv6 no son interoperables. Un host o un router deben estar implementados con soporte para IPv4 e IPv6 para poder reconocer y procesar ambos formatos de encabezamiento. El nuevo encabezado IPv6 es dos veces el tamaño del encabezado IPv4.

Espacio de Direcciones más grande. IPv6 tiene direcciones de origen y destino de 128 bits (16 bytes). El gran espacio de direcciones IPv6 se ha diseñado para permitir múltiples niveles de alojamiento de direcciones y de subredes desde el *backbone* de Internet hasta las subredes individuales dentro de una organización. Con un número de direcciones disponibles mucho más grande, las técnicas de NAT ya no serán necesarias.

Soporte requerido para encabezado IPSec. El soporte para encabezados IPSec es uno de los requerimientos de la suite de protocolos IPv6. IPSec consiste de un encabezado de autenticación AH (*Authentication Header*) que provee integridad de datos, autenticación y protección a todo el paquete IPv6, un encabezado ESP (*Encapsulating Security Payload*) que provee integridad de datos, autenticación, confidencialidad de información y de protección para la carga útil encapsulada y de un protocolo que habilita las configuraciones de seguridad IPSec para las comunicaciones unicast IKE (*Internet Key Exchange*).

Mejor soporte para priorizar la entrega de datos. Los nuevos campos en el encabezado IPv6 definen cómo será manejado e identificado el tráfico de datos. Dicho tráfico será priorizado usando un campo de Clase de Tráfico TC (*Traffic Class*). El campo de Nivel de Flujo LF (*Level Flow*) en el encabezado IPv6 permite a los routers proveer e identificar una administración especial de los paquetes que fluyen.

Nuevo protocolo para la interconexión de nodos vecinos. El protocolo de Descubrimiento de Vecino ND (*Neighbor Discovery*) es una serie de mensajes del protocolo ICMPv6 que administra la interconexión entre nodos vecinos. El protocolo ND reemplaza y extiende al protocolo ARP, Router Discovery ICMPv4 y mensajes redireccionados ICMPv4 con mensajes ND unicast y multicast eficientes.

Extensibilidad. El protocolo IPv6 se puede extender fácilmente para nuevas características agregando encabezados de extensión después del encabezado IPv6.

A diferencia de las opciones en el encabezado IPv4, que sólo puede soportar 40 bytes de opciones, el tamaño de extensión del encabezado IPv6 está conformado sólo por el tamaño del paquete IPv6.

2.4 Comparación entre IPv4 e IPv6

En la Tabla N° 2.1, se detallan algunas diferencias claves entre IPv4 e IPv6.

TABLA N° 2.1 Diferencias entre IPv4 e IPv6

IPv4	IPv6
Direcciones de origen y destino son del tamaño de 32 bits (4 bytes).	Direcciones de origen y destino son del tamaño de 128 bits (16 bytes).
Soporte para el encabezado IPSec es opcional.	Soporte para el encabezado IPSec es requerido.
Con el encabezado IPv4 no está presente la identificación de flujo de paquetes para priorizar la entrega de datos administrado por routers.	Con el encabezado IPv6 está presente la identificación de flujo de paquetes para priorizar la entrega de datos administrado por routers usando el campo de Nivel de Flujo.
La fragmentación se realiza por el host emisor y en routers, disminuyendo el rendimiento del router.	La fragmentación se realiza sólo por el host emisor.
No tiene requisitos de tamaño paquete del nivel de enlace y deben poder reensamblar un paquete de 576 bytes.	El nivel de enlace debe soportar un paquete de 1280 bytes y debe poder reensamblar un paquete de 1500 bytes.
El encabezado incluye una verificación de suma (checksum).	El encabezado no incluye una verificación de suma.
El encabezado incluye opciones.	Todos los datos opcionales son movidos al encabezado de extensión IPv6.
ARP utiliza tramas de solicitud de broadcast ARP para resolver una dirección IPv4 a una dirección de nivel de enlace.	Las tramas de solicitud de broadcast ARP son reemplazadas con mensajes de Solicitud de Vecino multicast.
IGMP (Internet Group Management Protocol) se usa para administrar los miembros del grupo de la subred local.	IGMP es reemplazado por mensajes MLD (Multicast Listener Discovery).
ICMP Router Discovery se usa para determinar la dirección IPv4 de la mejor puerta de enlace por defecto y es opcional.	ICMP Router Discovery es reemplazado por mensajes ICMPv6 Router Solicitation and Router Advertisement; y es reuqerido.
Las direcciones de broadcast se usan para enviar tráfico a todos los nodos de una subred.	No existen direcciones de broadcast IPv6. En lugar de eso se usa un ámbito de enlace local a todos los nodos de dirección multicast.
Debe ser configurado manualmente o a través de un servidor DHCP para IPv4.	No requiere configuración manual o DHCP para IPv6.
Usa registros de recursos de la dirección de host (A) en el Sistema de Nombres de Dominio DNS para mapear nombres de host a direcciones IPv4.	Utiliza registros AAAA en el DNS para mapear nombres de host a direcciones IPv6.
Usa registros de recursos de puntero (PTR) en el dominio DNS IN-ADDR.ARPA para mapear direcciones IPv4 a nombres de host.	Usa registros de recursos de puntero (PTR) en el dominio DNS IP6.ARPA para mapear direcciones IPv6 a nombres de host.

2.5 Beneficios de IPv6

IPv4 ha probado, por medio de su larga vida, ser un mecanismo flexible y poderoso en un sistema de redes. Sin embargo, empezó a mostrar ciertas limitaciones, no sólo respecto

a la necesidad del incremento del espacio de direcciones IP, iniciado, por ejemplo, por nuevas poblaciones de usuarios en países como China e India y por las nuevas tecnologías de dispositivos siempre conectados (cables, DSL, PDA's, teléfonos móviles 3G, etc.) sino también debido al crecimiento potencial de VoIP.

IPv6 agrega mejoras para el enrutamiento y autoconfiguración de la red. Los dispositivos conectados a la red serán dispositivos Plug-and-Play (compatibles). Con IPv6, no se va a requerir configurar direcciones IP privadas en forma dinámica, puerta de enlace, máscara de subred o cualquier otro parámetro. El equipo, estando conectado a la red, automáticamente obtendrá todos los datos requeridos para la configuración.

Las principales ventajas de IPv6 pueden resumirse como:

Escalabilidad. IPv6 tiene direcciones de 128 bits frente a IPv4 que soporta hasta 32 bits. Con IPv4, el número de direcciones IP disponibles es $2^{32} \sim 10^{10}$.

IPv6 ofrece un espacio de 2^{128}. Por lo tanto, el número de direcciones únicas disponibles en cada nodo es $2^{128} \sim 10^{39}$.

Seguridad. IPv6 incluye en sus especificaciones, características de seguridad como la encriptación de carga útil y autenticación en el origen de la comunicación.

Aplicaciones en tiempo real. Para proveer un mejor soporte del tráfico en tiempo real (como VoIP), IPv6 incluye en sus especificaciones: "flujos por nivel". Por medio de este mecanismo, los routers pueden reconocer el flujo de extremo a extremo a los cuales pertenecen los paquetes transmitidos.

Esto es similar al servicio ofrecido por MPLS (*Multi-Protocol Label Switching*).

Plug-and-Play. IPv6 incluye un mecanismo Plug-and-Play que facilita la conexión de equipos a la red.

La configuración requerida es automática.

Movilidad. IPv6 incluye mecanismos de movilidad más eficientes, en particular importancia para redes móviles.

Protocolo optimizado. IPv6 engloba mejores prácticas que IPv4 y elimina características obsoletas y poco usadas de IPv4. Esto resulta en un Protocolo de Internet mucho mejor optimizado.

Direccionamiento y enrutamiento. IPv6 mejora la jerarquía de direccionamiento y enrutamiento de paquetes.

Extensibilidad. IPv6 ha sido diseñado para ser extensible y ofrece soporte para nuevas opciones y extensiones.

2.6 Terminología básica de IPv6

Para comprender mejor IPv6, se debe conocer algunos conceptos acerca de los elementos de red comunes que proveen un fundamento básico para comprender el funcionamiento del protocolo IPv6. Los elementos de una red IPv6 se muestran en la Fig.2.7.

Nodo. Cualquier dispositivo que ejecuta una implementación de IPv6. Esto incluye hosts y routers.

Router. Un nodo que puede reenviar paquetes IPv6 no necesariamente a sí mismo. Sobre una red IPv6, un router advierte también su presencia y la información de configuración de host.

Host. Un nodo que no puede reenviar paquetes IPv6 explícitamente no direccionadas a sí mismo. Un host representa el origen y destino del tráfico IPv6 y silenciosamente descarta el tráfico recibido que no está explícitamente dirigido a sí mismo.

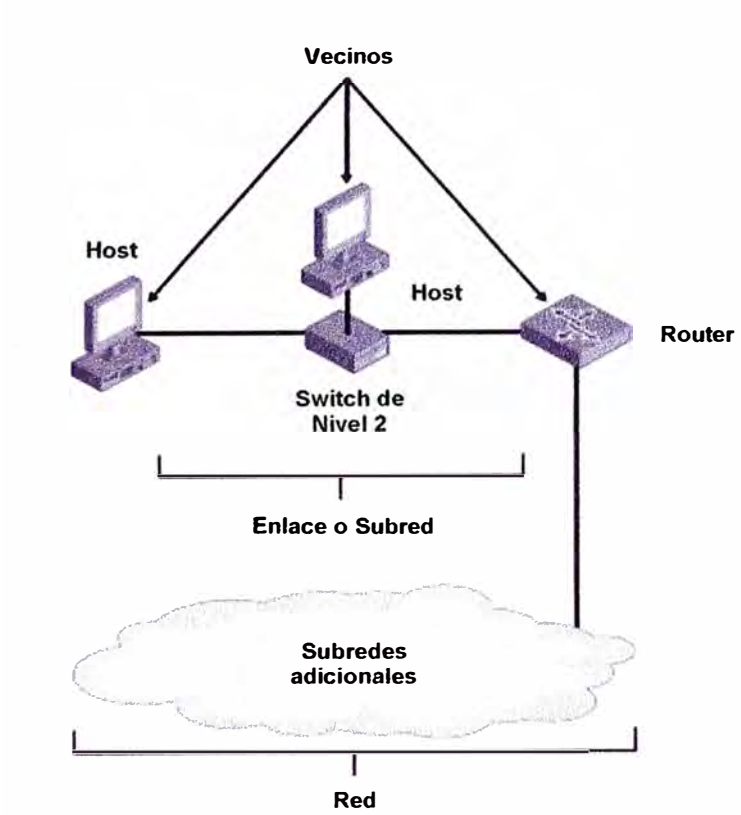

Fig.2.7 Elementos de una red IPv6

Protocolo de nivel superior. Un protocolo por encima de IPv6 que usa IPv6 como su transporte. Esto incluye a los protocolos del nivel de Internet como ICMPv6 y protocolos del nivel de Transporte como TCP y UDP (pero no a los protocolos de nivel de Aplicación como FTP y DNS, los cuales usan TCP y UDP como su transporte).

Subred. El conjunto de interfaces de red que están rodeadas de routers y que usan el mismo prefijo de dirección unicast IPv6 de 64 bits. Muchas tecnologías del nivel de Enlace están ya definidas por IPv6, incluyendo la tecnología conocida para una LAN (como Ethernet y Wireless IEEE 802.x) y tecnologías WAN (como el protocolo *PPP* y *Frame Relay*).

Red. Dos o más subredes conectadas por medio de routers.

Vecinos. Varios nodos conectados en el mismo enlace.

Los nodos vecinos en IPv6 tienen un significado especial debido al protocolo ND de IPv6, el cual tiene la facilidad de resolver direcciones vecinas de nivel de enlace así como detectar y monitorear la accesibilidad de nodos cercanos.

Interfaz. Es la representación de un anexo físico o lógico de un nodo para un enlace. Un ejemplo de una interfaz física es un adaptador de red. Un ejemplo de una interfaz lógica es una interfaz de "túnel" que se usa para enviar paquetes IPv6 a través de una red IPv4 encapsulando el paquete IPv6 dentro de un encabezado IPv4.

Dirección. Un identificador que puede ser usado como origen o destino de paquetes IPv6 que están asignados en el nivel de IPv6 para una interfaz o un conjunto de interfaces.

Paquete. El protocolo PDU (*Protocol Data Unit*) que existe en el nivel de IPv6 y que está compuesto de un encabezado IPv6 y carga útil.

Enlace MTU. La Unidad de Transmisión Máxima MTU (*Maximum Transmission Unit*) que representa el número de bytes en el paquete más grande de IPv6 que puede ser enviado en un enlace.

Camino MTU. El tamaño máximo del paquete IPv6 que puede ser enviado sin realizar la fragmentación de host entre origen y destino sobre una ruta en una red IPv6.

Sitio. Un sitio es una red basada en protocolos IP que opera anónimamente y que está conectada a Internet IPv6. Los arquitectos y administradores de red dentro del sitio determinan el plan de direccionamiento y las políticas de enrutamiento para la red de una organización.

La Fig.2.8, muestra una red de una organización basada en IPv6 y su conexión con redes IPv4. Una organización puede tener múltiples sitios. La conexión actual para Internet IPv6 puede usar cualquiera de los siguientes tipos de conexión:

Conexión Directa. La conexión a internet IPv6 utiliza un enlace de red de área ancha (como *Frame Relay* por ejemplo) y se conecta a un proveedor de servicios ISP con soporte para IPv6.

Conexión por Túnel. La conexión a internet IPv6 utiliza un túnel IPv6 sobre IPv4 y se conecta a un router de efecto túnel IPv6.

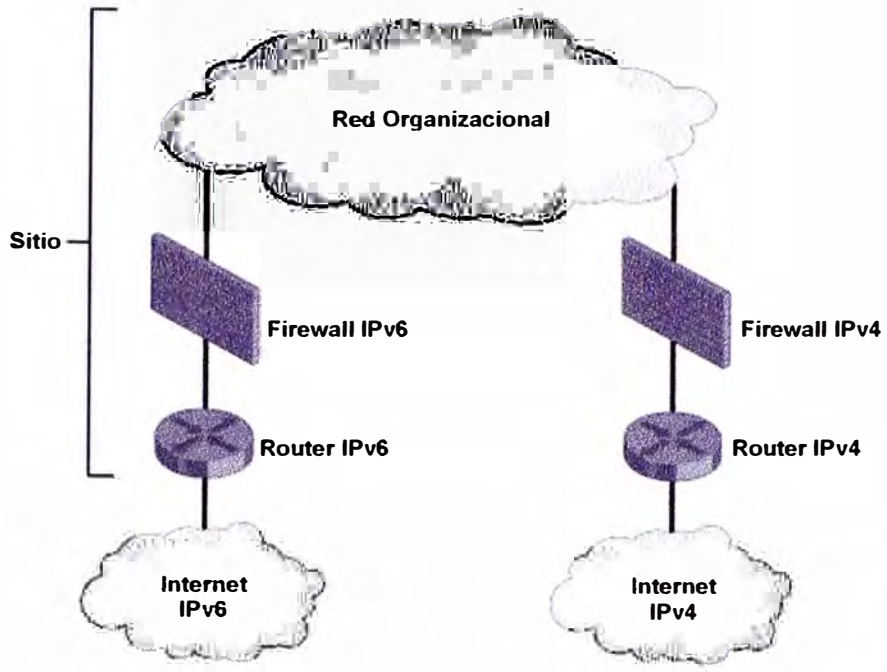

Fig.2.8 Una red Apto para IPv6 conectada a Internet IPv4 e IPv6

2.7 Clases de Direcciones IPv4

Con IPv4, las direcciones de 32 bits pueden ser representadas como:

Clase de dirección | ID de red | ID de host

La parte de red puede contener cualquier *ID de red* o un *ID de red* y de subred. Por definición, cualquier red y cualquier host o dispositivo tiene una única dirección IP.

La Fig.2.9, muestra las clases de direcciones tradicionales en IPv4.

Los tipos de direcciones IPv4 tradicionales son:

Clase A. Este tipo de dirección usa el primer bit del espacio de 32 bits (bit *0*) para identificarla como una dirección de clase A, este bit está configurado como 0 (cero). Los bits 1 al 7, representan el identificador de red (*ID de red*) y desde el bit *8* hasta el *31* identifica a la computadora personal, dispositivo terminal, host o servidor en la red (*ID de host*). Este espacio de direcciones soporta $2^7 - 2 = 126$ redes y aproximadamente 16 millones de dispositivos (2^{24}) en cada red.

Clase B. Esta clase usa los primeros 2 bits (bit *0* y bit *1*) del espacio de 32 bits para identificarla como una dirección de clase B, estos bits están configurados como *10*. Desde

el bit *2* hasta el bit *15* representa el *ID de red* y desde el bit *16* hasta el *31* son para identificar una PC, dispositivo terminal, host o servidor en la red. Este espacio de direcciones soporta 2^{14}-2=*16,382* redes y 2^{16}-2=*65,134* dispositivos en cada red.

Clase C. Usa los primeros 3 bits (bit *0*, *1* y *2*) del espacio de 32 bits para identificarla como una dirección de clase C, estos bits están configurados como *110*. Desde el bit *3* hasta el bit *23* representa el *ID de red* y desde el bit *24* hasta el *31* son para identificar a una PC, dispositivo terminal, host o servidor en la red. Este espacio de direcciones soporta cerca de 2 millones de redes (2^{21} - 2) y $2^8 - 2 = 254$ dispositivos en la red.

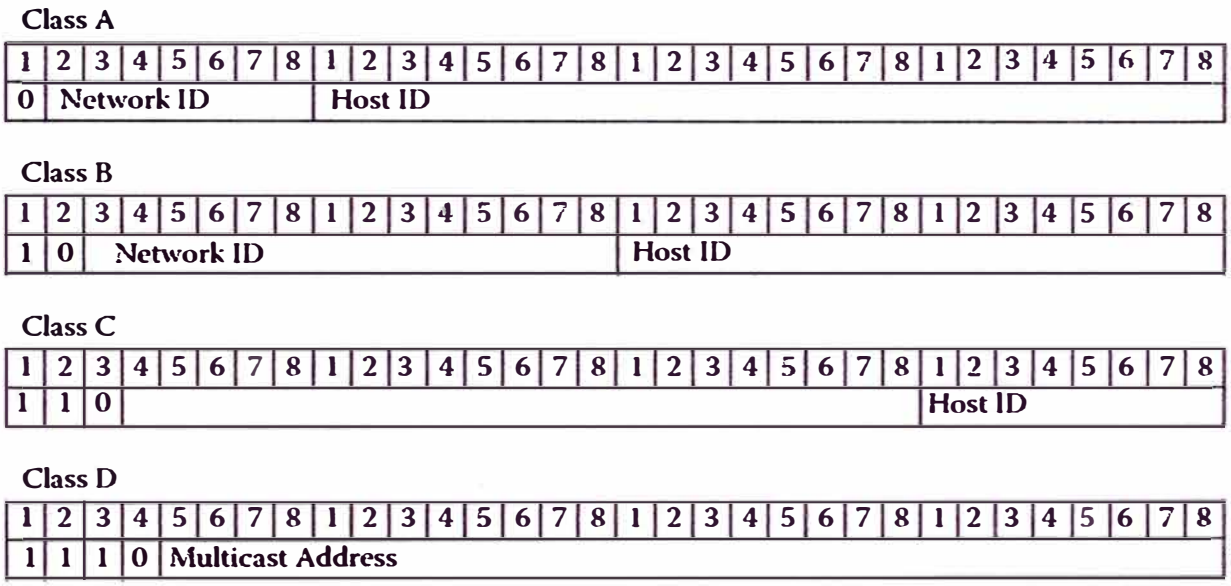

Fig.2.9 Clases de Direcciones IPv4

Clase D. Esta clase es usada para multidifusión (broadcasting) en la que todos los dispositivos en la red reciben los mismos paquetes. Esta clase de direcciones usan los primeros 4 bits (bit *0*, *1*, *2* y *3*) del espacio de 32 bits para identificarla como una dirección de clase D, estos bits están configurados como *1110*. Estas direcciones son usadas en aplicaciones IP Multicast (por ejemplo IPTV).

2.8 NAT en IPv4

Las direcciones IPv4 pueden ser asignadas en forma pública o privada (Intranet). Las direcciones de una Intranet pueden ser de los rangos *10.0.0.0/8*, *172.16.0.0/12* y *192.168.0.0/16*. En el caso de direcciones privadas de una Intranet, una función NAT se usa para mapear las direcciones internas hacia direcciones públicas externas cuando el límite de la red privada a pública es cruzado. Esto impone un número de limitaciones, particularmente porque el número de direcciones públicas registradas y disponibles para

una compañía es muy pequeño comparado con el número de dispositivos internos que requieren una dirección.

Las direcciones públicas, son direcciones globales únicamente asignadas por la IANA (*Internet Assigned Numbers Athority*). Las direcciones IP son direcciones de nodos de red en el Nivel 3, cada dispositivo en una red (Internet o una Intranet) deben tener una dirección única. En IPv4, esta dirección es una dirección binaria de 32 bits (4 bytes) usada para identificar cada dispositivo. Esto es representado por la nomenclatura *w.x.y.z* (donde cada letra *w,x,y,z* pueden tener valores desde 1 hasta 255, 0 es un caso especial).

Como un acercamiento temporal y práctico para aliviar la escasez de direcciones, las organizaciones usan los mecanismos de NAT e incluso es usado por usuarios domésticos para enfrentar este problema. Este mecanismo consiste en usar solamente un pequeño grupo de direcciones públicas IPv4 para una sola red que tiene acceso a Internet. Los innumerables dispositivos internos tienen direcciones IP asignadas desde un rango de direcciones específicas clase A, B o C que son únicas localmente pero que están duplicadas y reutilizadas dentro de otras organizaciones.

Un número de protocolos no pueden viajar a través de dispositivos NAT, por lo tanto el uso de NAT implica que muchas aplicaciones (tal como VoIP) no puedan ser usadas eficientemente con todas sus ventajas.

La necesidad del uso obligatorio de NAT desaparece con IPv6.

2.9 El espacio de direcciones en IPv6

El formato de direccionamiento IPv6 está descrito en la *RFC 2373*. Una dirección IPv6 consta de 128 bits en vez de 32 bits como en una dirección IPv4. El número de bits correlativos en el espacio de direcciones es como se muestra en la Tabla N° 2.2.

TABLA N° 2.2 Tamaño del Espacio de Direcciones

Versión de IP	Tamaño de Dirección
IPv6	128 bits, los cuales permiten usar 2^{128} ó 340,282,366,920,938,463,463,374,607,431,768,211,453 ($3.4*10^{38}$) posibles direcciones.
IPv4	32 bits, los cuales permiten usar 2^{32} ó 4,294,967,296 posibles direcciones.

El tamaño relativamente grande de las direcciones IPv6 está destinado a ser subdividido dentro de una jerarquía de dominios de enrutamiento que refleje la topología moderna de

Internet en estos días. El uso de 128 bits provee múltiples niveles de jerarquía y flexibilidad en el diseño de direccionamiento y enrutamiento jerárquico.

Las direcciones IPv6 están representadas en ocho grupos, cada uno de 16 bits, separados por el carácter ":". Cada grupo de 16 bits está representado por cuatro dígitos hexadecimales, es decir que cada dígito tiene un valor entre *0* y *F* (*0, 1, 2, 3, ... , 9, A, B, C, D, E, F*; con *A*=10, *B*=11, así hasta *F*=15).

Un ejemplo de la representación de una dirección IPv6 sería *3223:0BA0:01E0:D001:0000:0000:D0F0:0010*.

Dos de los grupos de cuatro dígitos tienen el valor 0000, los cuales pueden ser omitidos o reemplazados con el símbolo: "::" Así en el caso anterior tendríamos: *3223:0BA0:01E0:D001::D0F0:0010*.

Otro ejemplo sería *3223:0BA0::1234*. La cual representa la forma abreviada de: *3223:0BA0:0000:0000:0000:0000:0000:1234*.

Existe otro método para representar subredes o grupos de direcciones IPv6 que se basan en el número específico de bits que son designados en la subred, empezando de izquierda a derecha, usando los bits restantes para designar a algún dispositivo dentro de la red. Por ejemplo, la notación: *3223:0BA0:01A0::/48*. Esto indica que la parte de la dirección IP usada para representar a la subred tiene 48 bits. Porque cada dígito hexadecimal tiene 4 bits, esto indica que la parte usada para representar a la subred está conformada por 12 dígitos, el cual es: *3223:0BA0:01A0*. Los demás dígitos de la dirección IP se usarían para representar nodos dentro de la red. Existe un número direcciones IPv6 especiales:

Direcciones virtuales de loopback. Esta dirección está especificada en IPv4 como la dirección *127.0.0.0*. En IPv6, esta dirección se representa como *::1*.

Direcciones no asignadas (no especificadas) (::). Esta dirección no está asignada a ningún nodo debido a que se usa para indicar la ausencia de una dirección.

Direcciones de túnel IPv6 sobre IPv4 dinámicas/automáticas. Estas direcciones están definidas como direcciones IPv4 compatibles con IPv6 y permiten el envío de tráfico IPv6 sobre redes IPv4 en un modo transparente. Estas son representadas como por ejemplo: *::156.55.23.5*.

Representación automática de direcciones IPv4 sobre IPv6. Estas direcciones permiten que nodos de sólo IPv4 todavía puedan operar en redes IPv6.

Éstas están definidas como direcciones IPv4 mapeadas sobre IPv6 y están representadas como *::F:F:F:F*, por ejemplo: *::F:F:F:F.156.55.43.3*.

2.10 Direccionamiento IPv6

El esquema de direccionamiento IPv6 está definido en las especificaciones de Arquitectura de Direccionamiento IPv6 de la IETF (*Internet Engineering Task Force*) de la *RFC 4291*, abril de 2003. Estas especificaciones definen las direcciones que pueden ser usadas en una implementación IPv6 y las guías de varias configuraciones de arquitectura para diseñadores de red del espacio de direcciones IPv6.

2.10.1 Sintaxis de direcciones IPv6

Las direcciones IPv4 se representan en formato decimal; mientras que las de versión IPv6 son representadas en sistema hexadecimal, esto debido a la facilidad de uso y conversión entre este sistema y el binario.

Un ejemplo de una representación de una dirección IPv6 en binario sería:

0010000000000001000011011011100000000000000000000010111100111011

0000001010101010000000001111111111111111000101000100111000101110 10

La dirección de 128 bits se divide en bloques de 16 bits:

0010000000000001 0000110110111000 0000000000000000 0010111100111011

0000001010101010 0000000011111111 1111111000101000 1001110001011010

Cada bloque de 16 bits es convertido a hexadecimal y separado por dos puntos. El resultado es el siguiente: *2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A*

La representación de dirección IPv6 será simplificado más aún suprimiendo los ceros dentro de cada bloque de 16 bits. Sin embargo, cada bloque debe tener al menos un dígito. Suprimiendo los ceros, en el ejemplo anterior tendríamos el modo simplificado siguiente: *2001:DB8:0:2F3B:2AA:FF:FE28:9C5A.*

2.10.2 Simplificación de ceros

Algunos tipos de direcciones IPv6 contienen secuencias largas de ceros. Para simplificar la representación de una dirección IPv6, cuando se tiene una secuencia en la que varios bloques contiguos son ceros, se representa por los dos puntos *::*. Así, la dirección local *FE80:0:0:0:2AA:FF:FE9A:4CA2* puede ser simplificado a *FE80::2AA:FF:FE9A:4CA2.*

La dirección multicast *FF02:0:0:0:0:0:0:2* puede ser simplificada a *FF02::2.*

2.10.3 Prefijos en IPv6

El prefijo es la parte de la dirección donde los bits tienen valores arreglados o son los bits que definen una red o una subred. Los prefijos para subredes IPv6 y rutas

simplificadas están expresados de la misma forma que la notación CIDR (*Classless Inter-Domain Routing*) de IPv4.

Un prefijo IPv6 se representa con la notación: *dirección/longitud de prefijo*. Por ejemplo, la dirección *2001:DB8:2A0:2F3B::/64* es un prefijo de subred y la dirección: *2001:DB8:3F::/48* es un prefijo de ruta simplificada.

Comúnmente las implementaciones de IPv4 usan una representación decimal de la longitud del prefijo conocido como *máscara de subred*. En IPv6 no se usa una máscara de subred, sólo soporta la notación de *longitud de prefijo*.

Un prefijo IPv6 es relevante sólo para rutas o rango de direcciones, no para direcciones individuales unicast. En IPv4 es común representar una dirección con su longitud de prefijo. Por ejemplo, la dirección *192.168.29.7/24* (equivalente a *192.168.29.7* con la máscara de subred *255.255.255.0*) denota una dirección IPv4 con una máscara de subred de 24 bits. La longitud del prefijo está incluida para que se pueda determinar cuáles bits identifican a la subred y cuáles al host en la red de conexión. El tamaño del prefijo se usa para separar el prefijo de subred del *ID de host*.

Sin embargo, en IPv6 no se usa una notación de prefijo de subred de longitud variable. En el nivel de subred de IPv6 para direcciones unicast definidas actualmente, el número de bits usados para identificar la subred de comunicación es siempre 64 y el número de bits usados para identificar al host en la subred es también 64.

Los prefijos en las direcciones IPv6 con una longitud de prefijo más grande que 64 bits, pueden ser usados en enlaces point-to-point entre routers.

2.10.4 Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6, las cuales son:

Unicast. Una dirección unicast identifica una sola interfaz dentro del alcance del tipo de dirección. El alcance de una dirección es la región de la red IPv6 sobre la cual la dirección IP es única. Con la topología de enrutamiento unicast apropiada, los paquetes direccionados a una dirección unicast son entregados a una sola interfaz.

Multicast. Una dirección multicast identifica varias interfaces (o a ninguna) en el mismo host o en diferentes. Con la topología de enrutamiento multicast apropiada, los paquetes direccionados a una dirección multicast son entregados a todas las interfaces identificadas por la dirección.

Anycast. Una dirección anycast identifica a múltiples interfaces. Con la topología de enrutamiento anycast apropiada, los paquetes direccionados a una dirección anycast son entregados a una sola interfaz, la interfaz más cercana que es identificada por la dirección.

La interfaz más cercana está definida como ser lo más cercano en términos de distancia de enrutamiento. Una dirección multicast se usa para comunicaciones de un punto a varios otros, con la entrega de datos a múltiples interfaces. Una dirección anycast se usa para comunicaciones de un punto a otro o de un punto a varios, con la entrega de datos a una sola interfaz.

En todos los casos, las direcciones IPv6 identifican interfaces, no nodos. Un nodo es identificado por cualquier dirección unicast asignada a cualquiera de sus interfaces.

La *RFC 4291* no define direcciones de broadcast. Todos los tipos de direcciones broadcast en IPv4 son realizadas en IPv6 usando direcciones multicast. Por ejemplo, la direcciones de subred y de broadcast limitadas de IPv4, se reemplazan con el ámbito de enlace local a todos los nodos de la dirección multicast de *FF02::1*.

2.10.4.a Direcciones IPv6 Unicast

Los siguientes tipos de direcciones se clasifican como direcciones IPv6 unicast:

Direcciones Unicast Globales. Estas direcciones son equivalentes a las direcciones públicas en IPv4. Son globalmente enrutables y alcanzables en la Internet IPv6. El ámbito de una dirección global es toda la red de Internet IPv6.

La *RFC 4291* define direcciones globales como todas las direcciones que no son las de loopback, unicast de enlace local, no especificadas o direcciones multicast. Sin embargo, la Fig.2.10, muestra la estructura de una dirección unicast global definida en la *RFC 3587* que están siendo usadas actualmente en la red Internet IPv6.

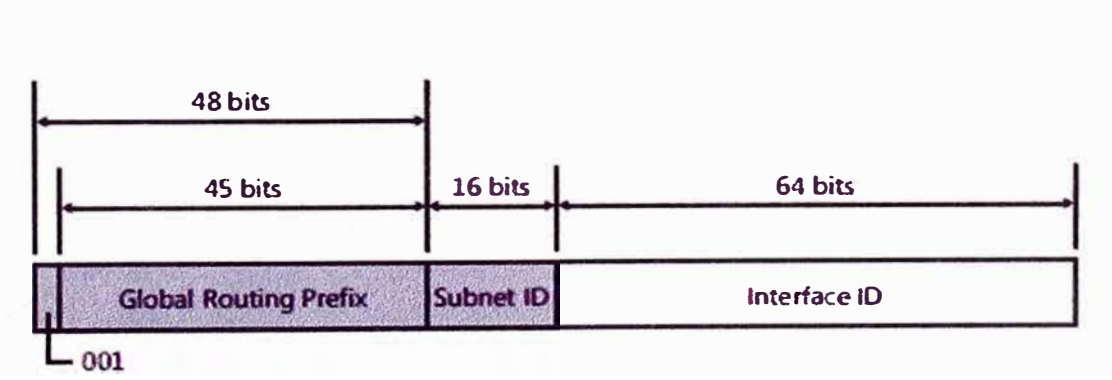

Fig.2.10 Estructura de Direcciones Unicast Globales definidas en la *RFC 3587*

Los campos de una dirección unicast global están definidos como:

Parte fija configurado a 001. Los tres bits de orden más alto están configurados a 001.

Prefijo de enrutamiento global. Indica los prefijos de enrutamiento global para un sitio específico de una organización. La combinación de los tres bits fijos y el prefijo de 45 bits son usados para el prefijo de sitio de 48 bits, el cual es asignado a un sitio individual de una organización.

ID de subred. Esto es usado en un sitio de la organización para identificar subredes dentro su sitio. El tamaño de este campo es de 16 bits. El sitio de la organización puede usar estos 16 bits para crear 65,536 subredes o niveles múltiples de jerarquía de direccionamiento y una infraestructura de enrutamiento eficiente. La estructura de enrutamiento de la red en la organización no es visible para el ISP.

ID de interfaz. Indica la interfaz o una subred específica dentro del sitio. El tamaño de este campo es de 64 bits. Este *ID* es equivalente al *ID de host* en IPv4.

Los campos dentro de una dirección global crean una estructura topológica de tres niveles, como se muestra en la Fig.2.11.

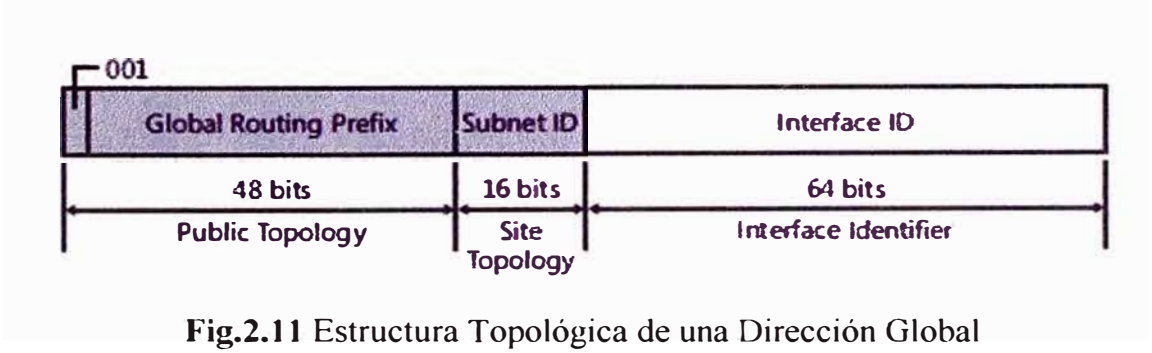

Fig.2.11 Estructura Topológica de una Dirección Global

La topología pública es la colección de todos los ISP que proveen acceso a Internet IPv6. La topología de sitio es el conjunto de subredes dentro del sitio de la organización. El identificador de interfaz especifica una interfaz única en una subred dentro del sitio de la organización.

Existen también direcciones unicast de uso local, estas direcciones no tienen un ámbito global y pueden ser reutilizadas.

Direcciones Locale de Enlace. Las direcciones de enlace local IPv6, identificadas por los 10 bits iniciales estando configuradas a *1111111010* y los siguientes 54 bits configurados a *0*, son usados por nodos al comunicarse con nodos cercanos en el mismo enlace. Por ejemplo en una red IPv6 de un solo enlace sin router, se usan las direcciones de enlace local para comunicarse entre host. La direcciones IPv6 de enlace local son similares a las

direcciones IPv4 de enlace local definidos en la *RFC 3927* que usa el prefijo *169.254.0.0/16*. El ámbito de este tipo de direcciones es el enlace local.

Una dirección de enlace local es requerida por algunos procesos del protocolo ND y siempre es configurada en forma automática, aún en la ausencia de las otras direcciones unicast. La Fig.2.12, muestra la estructura de una dirección de enlace local.

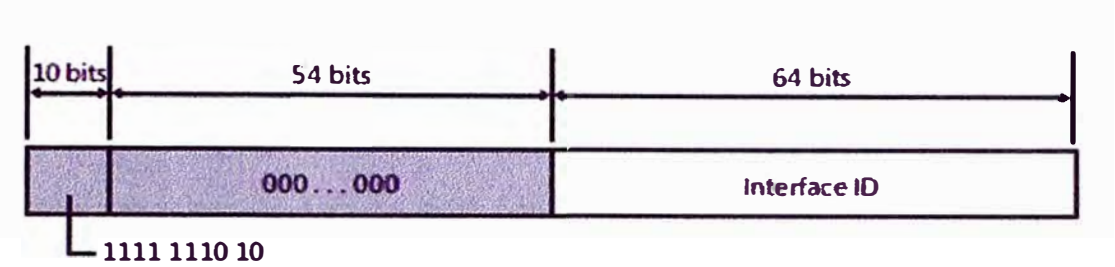

Fig.2.12 Estructura de una Dirección Local de Enlace

Las direcciones locales de enlace siempre empiezan con *FE80*. Con el identificador de interfaz de 64 bits, el prefijo para las direcciones de enlace local es siempre *FE80::/64*. Un router IPv6 nunca reenvía tráfico de enlace local más allá del enlace.

Direcciones Locales de Sitio. Estas direcciones identificadas por la configuración de los primeros 10 bits a *1111111011*, son equivalentes al espacio de direcciones IPv4 privadas (*10.0.0.0/8*, *172.16.0.0/12* y *192.168.0.0/16*). Por ejemplo, en Intranets privadas que no tienen una conexión directa enrutada a Internet IPv6, puede usar direcciones de sitios locales sin estar en conflicto con direcciones globales. Las direcciones locales de sitio no están accesibles desde otros sitios y los routers no deben reenviar tráfico de sitios locales fuera del sitio. Estas direcciones pueden ser usadas adicionalmente para direcciones globales. El ámbito de estas direcciones es el sitio.

A diferencia de las direcciones locales de enlace, las direcciones locales de sitio no son configuradas automáticamente y deben ser asignadas a través de cualquier dirección de autoconfiguración.

Los primeros 10 bits siempre están fijados para direcciones locales de sitio, empezando con *FEC0::/10*. Después de los 10 bits fijos es un campo *ID de subred* que provee 54 bits con los cuales se pueden crear subredes dentro de la organización. Se puede tener una estructura de subred o se puede dividir el orden más alto de bits del campo *ID de subred* para crear una infraestructura de enrutamiento jerárquica y simplificada. Después del campo *ID de subred* hay un campo *ID de interfaz* de 64 bits que identifica la interfaz específica en una subred.

La Fig.2.13, muestra la estructura de una dirección local de sitio.

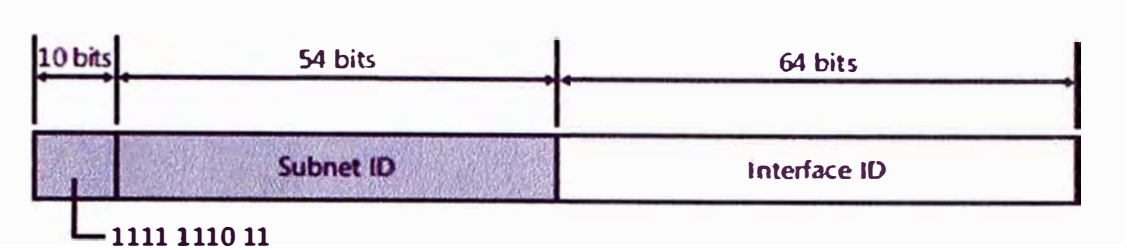

Fig.2.13 Estructura de una Dirección Local de Sitio

Las direcciones locales de sitio han sido formalmente desaprobadas en la *RFC 3879* para futuras implementaciones de IPv6. Sin embargo, las implementaciones existentes de IPv6 pueden continuar usando direcciones locales de sitio.

Para poder representar direcciones de Uso Local, se utilizan *ID's de Zona*. La sintaxis especificada en la *RFC 4007* para identificar la zona asociada con una dirección de uso local es *Dirección%ID_zona*, en la cual *Dirección* es una dirección IPv6 unicast de uso local y *ID_zona* es un valor entero que representa a la zona.

Por ejemplo, en Windows se usan los siguientes comandos con el *ID de zona*:

ping fe80::2b0:d0ff:fee9:4143%3

En este caso, 3 es el índice de interfaz de la interfaz adjuntada al enlace, conteniendo la dirección de destino.

tracert fec0::f282:2b0:d0ff:fee9:4143%2

En este caso, 2 es el *ID de sitio* de la organización de sitio, conteniendo la dirección de destino.

Direcciones locales únicas. Las direcciones locales de sitio proveen un direccionamiento privado alternativo para direcciones globales para el tráfico de Internet. Es posible que se duplique el uso de direcciones locales de sitio en una organización lo cual añade complejidad y dificultad para las aplicaciones, routers y administradores de red.

Para reemplazar las direcciones locales de sitio con un nuevo tipo de dirección privada y única a través de todos los sitios de la organización, la *RFC 4193* define direcciones unicast IPv6 locales únicas.

Los primeros 7 bits tienen el valor binario fijado a *1111110*. Todas las direcciones locales tienen el prefijo de dirección *FC 00::/7*. La bandera local *L* es configurado a *1* para indicar que el prefijo está asignado localmente. El valor *0* de *L* no está definido en la *RFC*

3879. Por consiguiente, las direcciones locales únicas dentro de una organización con el valor de *L* configurado a *1* tiene el prefijo de dirección de *FD00::/8*.
La Figura 2.14, muestra la estructura de una dirección local única.

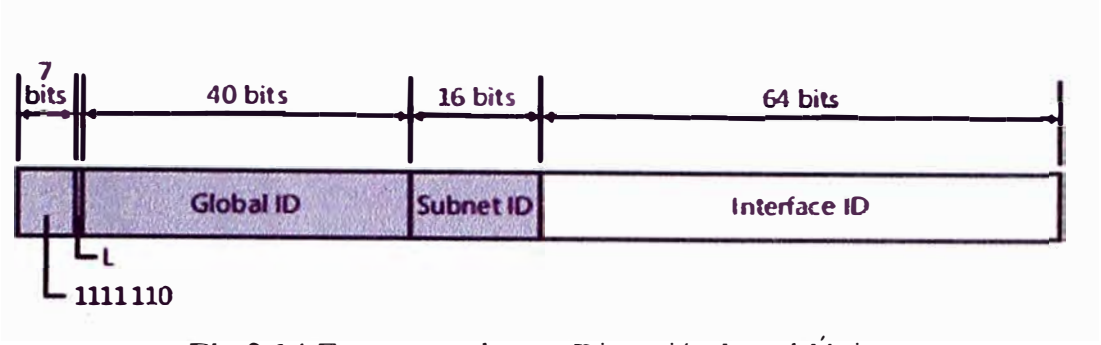

Fig.2.14 Estructura de una Dirección Local Única

El *ID Global* identifica un sitio específico en una organización y está configurado a un valor de 40 bits derivado aleatoriamente. Derivando un valor aleatorio para el *ID Global*, una organización puede tener estadísticamente prefijos únicos de 48 bits asignados a sus sitios. Adicionalmente, dos organizaciones que usan direcciones locales únicas anexadas tienen una baja probabilidad de duplicar un prefijo de dirección local única de 48 bits, minimizando el renumerado del sitio. A diferencia del Prefijo de nrutamiento Global en direcciones globales, los *ID's Globales* en prefijos de direcciones locales únicas no están diseñados para ser simplificados.

Las organizaciones no publicarán sus prefijos de direcciones locales únicas fuera de ésta o crear entradas DNS con direcciones locales únicas en servidores DNS. Dichas organizaciones pueden crear fácilmente políticas de filtrado en sus límites de Internet para prevenir que todo el tráfico direccionado sea reenviado. Las direcciones locales únicas no necesitan de un *ID de Zona* porque estas direcciones tienen un ámbito global.
La dirección global y la dirección local única comparten la misma estructura más allá de los primeros 48 bits de la dirección. En ambas direcciones, el *ID de subred* de 16 bits identifica una subred dentro de una organización. Es por esto que se puede crear una infraestructura de enrutamiento de subredes que es usado por ambas direcciones (globales y locales).

Por ejemplo, una subred específica en una organización puede ser asignada por el prefijo global *2001:DB8:4D1C:221A::/64* y el prefijo local *FD0E:2D:BA9:221A::/64*, donde la subred está identificada en ambos tipos de prefijos por el valor *221A* del *ID de subred*. Aunque el identificador de subred es el mismo para ambos prefijos, las rutas para

dichos prefijos deben ser propagadas a través de la infraestructura de enrutamiento a fin de que esas direcciones basadas en ambos prefijos sean accesibles.

Direcciones IPv6 Especiales. Las siguientes direcciones son direcciones IPv6 especiales:

Dirección No Especificada. La dirección no especificada (*0:0:0:0:0:0:0:0* ó *::*) se usa sólo para indicar la ausencia de una dirección. Ésta es equivalente a la dirección no especificada *0.0.0.0* en IPv4. Este tipo de dirección nunca es asignada a una interfaz o usada como una dirección de destino.

Dirección de Loopback. La dirección de loopback (*0:0:0:0:0:0:0:1* ó *::1*) está asignado a una interfaz de loopback, habilitando un nodo para enviar paquetes a sí mismo. Esto es equivalente a la dirección de loopback *127.0.0.1* en IPv4. Los paquetes direccionados a la dirección de loopback nunca deben ser enviados en un enlace o reenviados por un router IPv6.

Direcciones de Transición. Para ayudar en la transición de IPv4 a IPv6 y en la coexistencia de ambos tipos de hosts, se definen las siguientes direcciones:

Direcciones IPv4 compatibles. Las direcciones IPv4 compatibles, *0:0:0:0:0:0:w.x.y.z* ó *::w.x.y.z* (donde *w.x.y.z* es la representación decimal de una dirección pública IPv4), se usan para nodos IPv6/IPv4 que se comunican con infraestructuras IPv6 sobre IPv4 que usa direcciones públicas IPv4 como en Internet. Las direcciones IPv4 compatibles están desaprobadas en la *RFC 4291*.

Direcciones IPv4 mapeadas. Estas direcciones que tienen la representación *0:0:0:0:0:FFFF:w.x.y.z* ó *::FFFF:w.x.y.z*, se usan para representar direcciones IPv4 como una dirección IPv6.

Direcciones 6to4. Es una dirección del tipo: *2002:WWXX:YYZZ:Subnet ID:Interface ID*, donde *WWXX:YYZZ* es la representación hexadecimal de *w.x.y.z* (una dirección pública IPv4) y es asignada a un nodo para la tecnología de transición 6to4.

Direcciones ISATAP. Es una dirección del tipo: *Prefijo de 64 bits:0:5EFE:w.x.y.z*, donde *w.x.y.z* es una dirección privada IPv4 y es asignada a un nodo para la tecnología de transición ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*).

Direcciones Teredo. Es una dirección global que usa el prefijo *2001::/32* y es asignada a un nodo para la tecnología de transición Teredo.

Más allá de los primeros 32 bits, las direcciones Teredo se usan para codificar direcciones IPv4 a un servidor Teredo, banderas, una dirección externa de un cliente Teredo y un número de puerto UDP.

2.10.4.b Direcciones IPv6 Multicast

En IPv6, el tráfico multicast opera de la misma manera que en IPv4. Los nodos IPv6 ubicados arbitrariamente pueden escuchar el tráfico multicast en una dirección IPv6 multicast arbitraria. Los nodos IPv6 pueden escuchar múltiples direcciones multicast al mismo tiempo y pueden ingresar o dejar un grupo multicast en cualquier momento.

Las direcciones multicast IPv6 tienen los primeros 8 bits configurados a *11111111*, por lo que una dirección IPv6 multicast siempre empieza con *FF*. Estas direcciones no pueden usarse como direcciones de origen o como destinos intermedios en un encabezado de extensión de enrutamiento. Más allá de los primeros 8 bits, estas direcciones incluyen una estructura adicional para identificar banderas, su ámbito y el grupo multicast. La Fig.2.15, muestra la estructura de una dirección IPv6 multicast.

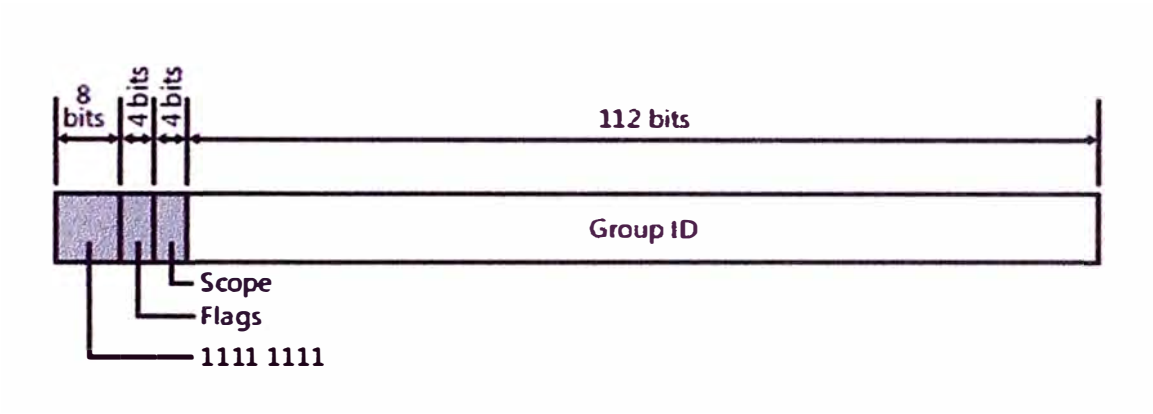

Fig.2.15 Estructura de una Dirección IPv6 Multicast

Banderas. Indica las banderas configuradas en la dirección multicast. El tamaño de este campo es de 4 bits, conformado por tres banderas y los bits de bajo orden. El primer bit de orden bajo es la bandera transitoria *T*, cuando está configurado a 0, esta bandera indica que la dirección multicast es asignada permanentemente por la IANA (*Internet Assigned Numbers Authority*). Cuando está configurado a 1, la bandera *T* indica que la dirección multicast es transitoria (no asignada permanentemente). El segundo bit de orden bajo es para la bandera de Prefijo *P*, el cual indica si la dirección multicast se basa en un prefijo de dirección multicast. La *RFC 3306* describe la bandera *P*. El tercer bit de bajo orden es para la bandera de la dirección de Punto de Encuentro *R* (*Rendezvous Point*), el cual indica si la dirección multicast tiene incrustada una dirección de punto de encuentro. La *RFC 3956* describe la bandera *R*.

Ámbito. Indica el ámbito de una dirección IPv6 para el cual el tráfico multicast está dirigido para ser entregado. El tamaño de este campo es de 4 bits. Además de usar información provista por los protocolos de enrutamiento multicast, los routers usan el ámbito multicast para determinar si el tráfico puede ser reenviado.

La Tabla N° 2.3, muestra los valores para el campo Ámbito asignado en la *RFC 4291*. Todos los demás valores están disponibles.

TABLA N° 2.3 Valores definidos para el campo Ámbito

Valor del Campo Ámbito	Ámbito
0	Reservado
1	Ámbito local de interfaz
2	Ámbito local de enlace
3	Reservado
4	Ámbito local Admin
5	Ámbito local de sitio
8	Ámbito local de organización
E	Ámbito global
F	Reservado

Por ejemplo, el tráfico de la dirección multicast de *FF02::2* tiene un ámbito local de enlace. Un router IPv6 nunca reenvía este tráfico más allá del enlace local.

ID de Grupo. Identifica el grupo multicast y es único dentro del ámbito. El tamaño de este campo es de 112 bits. Los *ID's de Grupo* asignados permanentemente son independientes del ámbito. Los *ID's de Grupo* transitorios son relevantes sólo para un ámbito específico. Las direcciones multicast conocidas desde *FF01::* hasta *FF0F::* están reservadas.

Para identificar todos los nodos de los ámbitos de enlace e interfaz local, se definen las siguientes direcciones:

FF01::1 (ámbito local de interfaz a todos los nodos de direcciones multicast).

FF02::1 (ámbito local de enlace a todos los nodos de direcciones multicast).

Para identificar todos los routers para la interfaz local, enlace local y ámbitos locales de sitio, se definen las siguientes direcciones:

FF01::2 (ámbito local de interfaz a todos los routers de direcciones multicast).

FF02::2 (ámbito local de enlace a todos los routers de direcciones multicast).

FF05::2 (ámbito local de sitio a todos los routers de direcciones multicast).

Las direcciones multicast IPv6 reemplazan todas las formas de direcciones broadcast de IPv4. La red de broadcast IPv4, subred de broadcast y direcciones de broadcast (*255.255.255.255*) son reemplazados por el ámbito local de enlace a todos los nodos de direcciones multicast (*FF02::01*) en IPv6.

2.10.4. c Direcciones IPv6 Anycast

Una dirección anycast es asignada a múltiples interfaces. Los paquetes direccionados a una dirección anycast son reenviados por la infraestructura de enrutamiento a la interfaz más cercana en la cual la dirección anycast es asignada. Para facilitar la entrega, la infraestructura de enrutamiento debe darse cuenta de las interfaces que tienen direcciones anycast asignadas a ellos y su distancia en términos de métricas de enrutamiento. Esto se logra con la propagación de rutas de host a lo largo de la infraestructura de enrutamiento de la parte de la red que no puede simplificar la dirección anycast usando un prefijo de enrutamiento.

Por ejemplo, para la dirección anycast *3FFE:2900:D005:6187:2AA:FF:FE89:6B9A*, las rutas de host para esta dirección se propagan dentro de la infraestructura de enrutamiento de la organización asignando el prefijo de 48 bits *3FFE:2900:D005::/48*. Las rutas de host para todos los nodos asignados a esta dirección anycast son necesarias en las tablas de enrutamiento de todos los routers dentro de la organización debido a que un nodo asignado a esa dirección anycast puede estar ubicado en cualquier parte de la Intranet de la organización.

Tal como la *RFC 4291*, las direcciones anycast se usan sólo como direcciones de destino y están asignadas solamente a routers. No es posible determinar si una dirección de destino unicast dada es además una dirección anycast.

Dirección Anycast del router de subred. Esta dirección está definida en la *RFC 4291*. Está creada desde el prefijo de subred por una interfaz dada. Cuando la dirección anycast del router de subred es construida, los bits en el prefijo de subred están compuestos de sus valores apropiados y los demás bits son configurados a 0. La Fig.2.16, muestra la estructura de una dirección anycast del router de subred.

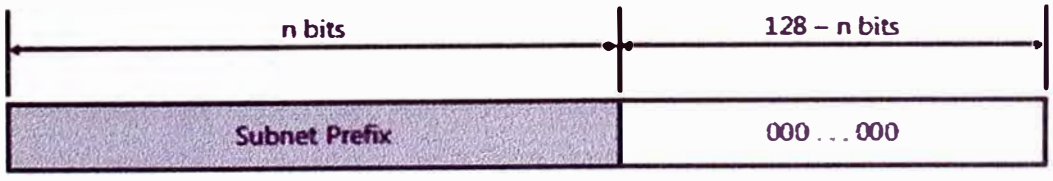

Fig.2.16 Estructura de una Dirección Anycast del router de subred

Todas las interfaces de router adjuntas a una subred son asignadas a la dirección anycast del router de subred para esa subred. Esta dirección se usa para comunicarse con el router más cercano conectado a una subred específica.

2.11 Direcciones IPv6 para Hosts

Un host IPv4 con un solo adaptador de red comúnmente tiene una sola dirección IPv4 asignada a ese adaptador. Sin embargo, en un host IPv6, usualmente tiene múltiples direcciones IPv6 asignadas para cada adaptador. Las interfaces en un host típico IPv6 están asignados por las siguientes direcciones unicast:

Una dirección local de enlace para cada interfaz.

Direcciones unicast adicionales para cada interfaz (las cuales pueden ser una o múltiples direcciones globales o direcciones local únicas).

La dirección de loopback (*::1*) para la interfaz de loopback.

Los hosts típicos de IPv6 son siempre multidirigidos porque siempre tienen por lo menos dos direcciones con las cuales pueden recibir paquetes una dirección local de enlace para tráfico de enlace local y una dirección global o dirección local única enrutable.

Adicionalmente, cada interfaz en un host IPv6 escucha el tráfico de datos en las siguientes direcciones multicast:

El ámbito local de interfaz a todos los nodos de direcciones multicast (*FF01::1*)

El ámbito local de enlace a todos los nodos de direcciones multicast (*FF02::1*)

Las direcciones de nodos solicitados para cada dirección unicast asignada.

Las direcciones multicast de grupos asociados.

2.12 Direcciones IPv6 para Routers

Las interfaces en un router IPv6 están asignadas por las siguientes direcciones unicast:

Una dirección local de enlace para cada interfaz.

Direcciones adicionales unicast para cada interfaz (las cuales pueden ser una o múltiples direcciones globales o direcciones local únicas)

La dirección de loopback (*::1*) para la interfaz de loopback.

Adicionalmente, las interfaces de un router IPv6 están asignadas por las siguientes direcciones anycast:

Una dirección anycast del router de subred para cada subred.

Direcciones anycast adicionales (lo cual es opcional).

Además, las interfaces de un router IPv6 escuchan el tráfico de datos en las siguientes direcciones multicast:

El ámbito local de interfaz a todos los nodos de direcciones multicast (*FF01::1*)

El ámbito local de interfaz a todos los routers de direcciones multicast (*FF01::2*)

El ámbito local de enlace a todos los nodos de direcciones multicast (FF02::1)

El ámbito local de enlace a todos los routers de direcciones multicast (*FF02::2*)

El ámbito local de sitio a todos los routers de direcciones multicast (*FF05::2*)

La dirección de nodo solicitada para cada dirección unicast asignada.

Las direcciones multicast de grupos asociados.

2.13 Subnetting en el espacio de direcciones IPv6

Tal como en IPv4, el espacio de direcciones IPv6 puede dividirse usando bits de orden alto que realmente no tienen valores fijos para crear prefijos de direcciones subneteadas (*subnetted*).

Estos prefijos están usados ya sea para resumir un nivel en la jerarquía de enrutamiento o direccionamiento (con una longitud de prefijo menor a 64 bits), o para definir una subred específica o segmento de red (con una longitud de prefijo de 64 bits). *Subnetting IPv4* difiere de *subnetting IPv6* en la definición de la porción del *ID de host*.

En IPv4 el *ID de host* puede ser de una longitud variable, dependiendo del esquema de subred. Para las direcciones IPv6 unicast definidas actualmente, el *ID de host* es la parte del *ID de interfaz* de la dirección IPv6 unicast y siempre tiene un tamaño fijo de 64 bits.

Para los administradores de red dentro de una organización, el espacio de direcciones de subredes en IPv6 consiste en el uso técnicas de subredes para dividir la porción del *ID de subred* de un prefijo de dirección local única o global de manera que permita la simplificación de rutas y la delegación del espacio de direcciones restantes en diferentes partes de una Intranet IPv6.

Para las direcciones locales globales o únicas, los primeros 48 bits son fijos. Para las direcciones globales, estos 48 bits están fijados y ubicados por un ISP.

Para las direcciones locales únicas, estos primeros 48 bits están fijados a *FD00::/8* y el *ID global* aleatorio de 40 bits asignado a un sitio de una organización.

El proceso de subredes de la porción *ID de subred* de una dirección local global o única requiere de dos pasos:

Paso1: Determinar el número de bits a usarse para la subred.

Paso2: Enumerar los nuevos prefijos de direcciones subneteadas.

2.14 Equivalencias entre direcciones IPv4 e IPv6

El resumen de la relación entre direcciones IPv4 e IPv6, se muestra la Tabla N° 2.4.

TABLA N° 2.4 Conceptos de Direccionamiento IPv4 y sus Equivalencias en IPv6

Dirección IPv4	Dirección IPv6
Direcciones multicast (224.0.0.0/4).	Direcciones multicast IPv6 (FF00::/8).
Direcciones de broadcast.	No aplicable en IPv6.
Dirección No especificada es 0.0.0.0	Dirección No especificada es ::
Dirección de loopback es 127.0.0.1	Dirección de loopback es ::1
Direcciones IP públicas.	Direcciones unicast globales.
Direcciones IP privadas (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).	Direcciones locales únicas (FD00::/8) ó direcciones locales de sitio (FEC0::/10).
Direcciones APIPA (169.254.0.0/16).	Direcciones locales de enlace (FE80::/64)
Representación en notación decimal.	Representación en notación hexadecimal.
Representación de prefijo: Máscara de subred en notación decimal o notación de longitud de prefijo.	Representación de prefijo: Sólo notación de longitud de prefijo.

2.15 El paquete del Protocolo IPv6

La estructura de un paquete IPv6 consiste de un encabezado IPv6, encabezados de extensión y la unidad de datos de protocolo de nivel superior. La Fig.2.17, muestra la estructura de un paquete IPv6:

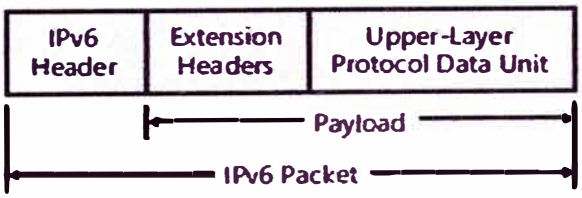

Fig.2.17 Estructura de un Paquete IPv6

Los componentes de un protocolo IPv6 son los siguientes:

Encabezado IPv6. El encabezado IPv6 siempre está presente y tiene un tamaño fijo de 40 bytes.

Encabezados de Extensión. Son de longitudes variables y pueden estar o no presentes. Si están presentes, un campo de *Encabezado Siguiente* en el Encabezado IPv6 indica el primer *Encabezado de Extensión*. Dentro de cada *Encabezado de Extensión* hay otro campo de *Encabezado Siguiente*, que indica el siguiente *Encabezado de Extensión*. El último *Encabezado de Extensión* indica el encabezado para el protocolo de nivel superior,

tal como TCP, UDP o ICMPv6 contenidos dentro del protocolo de unidad de datos de nivel superior.

El encabezado IPv6 y los encabezados de extensión, reemplazan el encabezado existente de IPv4 y sus opciones. El nuevo formato de *Encabezado de Extensión* permite que IPv6 sea extendido y pueda soportar capacidades y necesidades futuras. A diferencia del encabezado IPv4, los encabezados de extensión IPv6 no tienen tamaño máximo y pueden expandirse para acomodar toda la data de extensión necesaria para la comunicación IPv6.

Unidad de Datos de Protocolo de Nivel Superior. El protocolo de nivel superior PDU consiste de un encabezado de protocolo de nivel superior y su carga útil (un mensaje ICMPv6, un segmento TCP o un mensaje UDP).

La carga útil del paquete IPv6 es la combinación de los encabezados de extensión y el protocolo PDU. Normalmente, ésta puede ser de hasta una longitud de 65,536 bytes.

Los paquetes IPv6 con carga útil mucho mayores a 65,536 en su longitud, se les conoce como "*jumbogramas*" y también pueden ser enviados.

2.15.1 Encabezado IPv4

Antes de examinar el encabezado IPv6, se revisará brevemente la estructura del encabezado IPv4 tal como se muestra en la Fig.2.18.

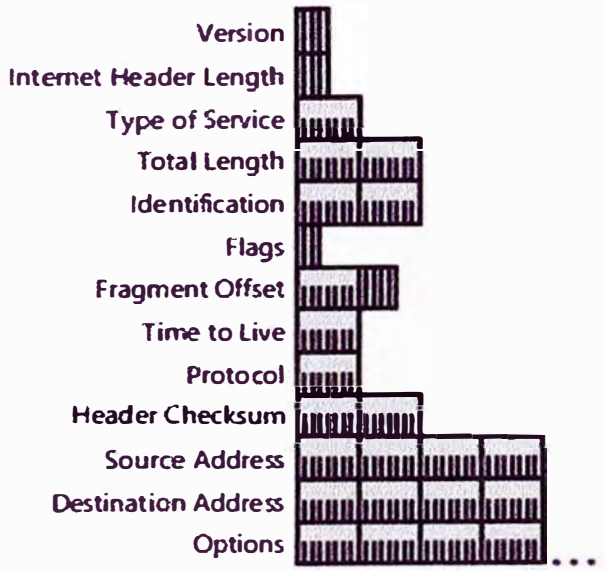

Fig.2.18 Estructura del Encabezado IPv4

Haciendo una comparación entre el encabezado IPv4 e IPv6, las equivalencias entre ambos se puede ver según la Tabla N° 2.5.

TABLA N° 2.5 Campos de Encabezado IPv4 y su Equivalente IPv6

Campo de encabezado IPv4	Campo de encabezado IPv6
Versión	El mismo campo pero con un número de versión diferente.
Tamaño de encabezado de Internet	Removido en IPv6. No incluye un tamaño de encabezado porque el encabezado IPv6 siempre está fijado a 40 bytes.
Tipo de servicio	Reemplazado por el campo de Clase de Tráfico.
Tamaño total	Reemplazado por el campo de Tamaño de Carga útil, el cual indica sólo el tamaño de la carga útil.
Identificación Banderas Fragment offset	Removido en IPv6. La información de fragmentación no está incluida en IPv6. Está contenido en un fragmento del encabezado de extensión.
Tiempo de vida	Reemplazado por el campo de Límite de Salto.
Protocolo	Reemplazado por el campo de Encabezado Siguiente.
Chequeo de encabezado	Removido en IPv6. El nivel de enlace tiene un chuqueo que realiza la detección de errores a nivel de bit para todo el paquete IPv6.
Dirección de origen	El campo es el mismo sino que con un tamaño de 128 bits.
Dirección de destino	El campo es el mismo sino que con un tamaño de 128 bits.
Opciones	Removido en IPv6. Los encabezados de extensión en IPv6 reemplazan las Opciones de Ipv4.

2.15.2 Encabezado IPv6

El encabezado IPv6 es una versión mejorada del encabezado IPv4. Éste, elimina campos que son innecesarios y raramente usados; y añade un campo que provee un mejor soporte para el tráfico en tiempo real. La Fig.2.19, muestra la estructura del encabezado IPv6 descrito en la *RFC 2460*. Cada campo se define como:

Versión. Número de versión de 4 bits del protocolo de Internet = 6.

Clase de tráfico. Campo de clase de tráfico de 8 bits.

Etiqueta de flujo. Campo de 20 bits.

Tamaño de carga útil. Entero sin signo de 16 bits, que representa el resto del paquete que sigue al encabezado de IPv6, en octetos.

Encabezado Siguiente. Selector de 8 bits. Identifica el tipo de encabezado que va inmediatamente después del encabezado de IPv6. Emplea los mismos valores que el campo de protocolo IPv4.

En la Tabla N° 2.6, se muestran los valores típicos del Encabezado Siguiente.

Límite de salto. Entero sin signo de 8 bits. Disminuye en uno cada nodo que reenvía el paquete. El paquete se desecha si el límite de salto se reduce a cero.

Dirección de origen. Dirección de 128 bits del emisor inicial del paquete.

Dirección de destino. Dirección de 128 bits del destinatario previsto del paquete. El destinatario previsto no es necesariamente el destinatario si existe un encabezado de encaminamiento opcional.

TABLA N° 2.6 Valores típicos del campo de Encabezado Siguiente

Valor (en decimal)	Encabezado
0	Encabezado de Opciones de salto a salto
6	TCP
17	UDP
41	Encabezado IPv6 Encapsulado
43	Encabezado de Enrutamiento
44	Encabezado de Fragmentación
50	Encabezado de Carga Útil de seguridad encapsulado
51	Encabezado de Autenticación
58	ICMPv6
59	Encabezado No Próximo
60	Encabezado de Opciones de Destino

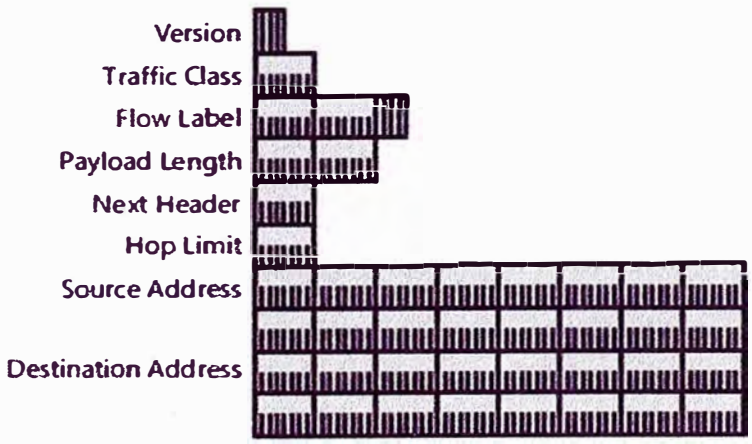

Fig.2.19 Estructura del Encabezado IPv6

2.15.3 Encabezados de Extensión IPv6

Las opciones de IPv6 se colocan en *Encabezados de Extensión* independientes que se ubican entre el encabezado de IPv6 y el encabezado de capa de transporte de un paquete.

Ningún router procesa ni examina la mayoría de los *Encabezados de Extensión* de IPv6 durante el recorrido de distribución del paquete hasta que éste llega a su destino. Esta función supone una mejora importante en el rendimiento de los routers en paquetes que contienen opciones. En IPv4, la presencia de cualquier opción hace que el router examine todas las opciones.

A diferencia de las opciones de IPv4, los encabezados de extensión de IPv6 pueden tener un tamaño arbitrario. Asimismo, la cantidad de opciones que lleva un paquete no se limita a 40 bytes. Aparte de la forma de procesar las opciones de IPv6, esta función permite que las opciones de IPv6 se apliquen a funciones que no resultan viables en IPv4.

Para mejorar el rendimiento al controlar los encabezados de opciones subsiguientes, así como el protocolo de transporte que va después, las opciones de IPv6 siempre son un múltiplo entero de 8 octetos. El múltiplo entero de 8 octetos mantiene la alineación de los encabezados subsiguientes. Están definidos los siguientes encabezados de extensión en IPv6:

Encaminamiento. Encaminamiento extendido, por ejemplo ruta holgada fijada en origen de IPv4.

Fragmentación. Fragmentación y montaje.

Autenticación. Integridad y autenticación, y seguridad.

Encapsulado de carga útil. Confidencialidad.

Opciones de salto a salto. Opciones especiales que necesitan procesamiento salto a salto.

Opciones de destino. Información opcional que el nodo de destino debe examinar.

2.15.4 Protocolos de Pila doble IPv6

En general, el término pila doble se refiere a una duplicación completa de todos los niveles de la pila de protocolos de aplicaciones en la capa de red. Un ejemplo de duplicación completa es un sistema que ejecuta los protocolos OSI y TCP/IP.

El sistema operativo *Solaris* es de pila doble, lo que significa que implementa los protocolos IPv4 e IPv6. Al instalar el sistema operativo, se elige entre habilitar los protocolos IPv6 en la capa de IP o utilizar únicamente los protocolos IPv4 predeterminados. El resto de la pila TCP/IP es idéntica. Por lo tanto, en IPv4 e IPv6 pueden ejecutarse los mismos protocolos de transporte, TCP y UDP. Además, se pueden ejecutar las mismas aplicaciones.

La Fig.2.20, muestra el funcionamiento de los protocolos IPv4 e IPv6 como pila doble en las distintas capas del conjunto de protocolos de Internet.

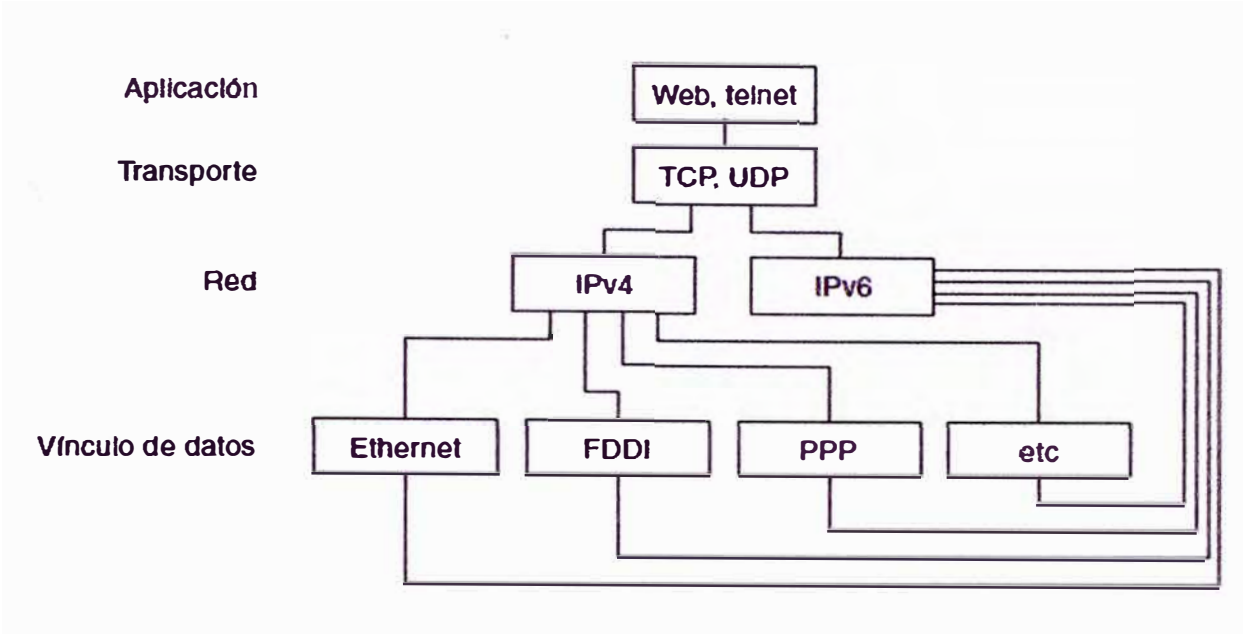

Fig.2.20 Arquitectura de Protocolos de Pila Doble

En el caso hipotético de pila doble, los subconjuntos de routers y hosts se actualizan para admitir IPv6, además de IPv4. Con este planteamiento de pila doble, los nodos actualizados siempre pueden interoperar con nodos que son sólo de IPv4 mediante IPv4.

2.16Enrutamiento IPv6

La diferencia básica entre un host cualquiera y un router es que el router está configurado para aceptar paquetes solicitados por otros destinos y para reenviar esos paquetes para lo cual el router determina si es lo mejor en el siguiente salto. El router soporta además al menos un protocolo de enrutamiento a través del cual puede adquirir la información actual sobre las rutas en toda la red. Una red IPv6 está conformada de múltiples subredes IPv6 interconectadas por routers IPv6. Para proveer de accesibilidad a cualquier ubicación arbitraria en la red IPv6, las rutas deben existir enviando a host y routers a reenviar el tráfico hacia el destino deseado. Estas rutas pueden ser rutas generales como una ruta predeterminada que simplifica todas las ubicaciones o rutas específicas como rutas de subred que simplifican todas las ubicaciones en una subred específica.

2.16.1 Enrutamiento estático

Se basa en entradas en la tabla de enrutamiento que son configuradas manualmente y que no cambian con el cambio de la topología de red. Un router con una tabla de enrutamiento configurado manualmente es conocido como un router estático. Estos routers pueden trabajar bien para redes pequeñas, pero no pueden escalar bien para redes grandes o redes que cambian dinámicamente porque requiere de una administración manual. El

tiempo de vida de una ruta estática configurada manualmente es infinito por lo que los routers estáticos no son sensibles ni se recuperan de routers o enlaces caídos.

2.16.2 Enrutamiento dinámico

El enrutamiento dinámico es la actualización automática de las entradas en las tablas de enrutamiento para los cambios en la topología de red. Un router con tablas de enrutamiento configurado dinámicamente se le conoce como un router dinámico.

Las tablas de enrutamiento de routers dinámicos son construidas y mantenidas automáticamente a través de comunicaciones en curso entre routers. La habilidad para escalar y recuperar fallas de la red hace del enrutamiento dinámico la mejor elección para redes medianas, grandes y muy grandes.

2.16.3 Tecnologías de protocolo de enrutamiento

Los protocolos de enrutamiento se basan en cualquiera de las tecnologías siguientes:

Vector de distancia. Los protocolos de enrutamiento que usan esta tecnología, propagan la información de enrutamiento en la forma de un prefijo de dirección y su "distancia" (contador de saltos).

Las ventajas de los protocolos de enrutamiento basados en el vector de distancia incluyen la facilidad y simplicidad de la configuración y la ventajas están relacionadas con el tráfico de red relativamente elevado, largo tiempo de convergencia y la no disponibilidad de escalar a red mucho más grandes.

Estado de enlace. Los routers que usan protocolos basados en esta tecnología intercambian avisos de estado de enlace a través de la red para actualizar las tablas de enrutamiento. Este tipo de enrutamiento es sincronizado y reconocido.

Las ventajas son el bajo tráfico de red, menor tiempo de convergencia y la habilidad para escalar a redes mucho más grandes.

La desventaja es que los protocolos de enrutamiento que usan esta tecnología pueden ser más complejos y difíciles de configurar.

Vector de ubicación. Los routers usan protocolos de enrutamiento basados en esta tecnología para intercambiar secuencias de números de saltos indicando el camino para una ruta. La ventaja de esta tecnología es el bajo tráfico de red, menor tiempo de convergencia y la habilidad para escalar a redes mucho más grandes conteniendo múltiples sistemas anónimos.

Un sistema anónimo es una porción de red bajo los mismos permisos administrativos. La desventaja es que los protocolos pueden ser complejos y difíciles de configurar.

2.16.4 Protocolos de enrutamiento en IPv6

Los siguientes protocolos están definidos por la IETF para IPv6:

RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*), IS-IS (*Integrated Intermediate System-to-Intermediate System*) y BGP (*Border Gateway Protocol*).

RIPng para IPv6. Es un protocolo de enrutamiento de vector de distancia para IPv6 que está definido en la *RFC 2080*. Este protocolo es la adaptación del protocolo RIPv2 definido en la *RFC 1723*, para anunciar prefijos de red IPv6. Tiene una estructura de paquete simple y usa el puerto UDP *521* para anunciar periódicamente sus rutas, responder a solicitudes de rutas y anunciar asincrónicamente cambios de ruta.

RIPng para IPv6 es un protocolo de enrutamiento simple con un mecanismo de anuncio de rutas periódico diseñado para usarlo en redes IPv6 de tamaño pequeño a medianas.

OSPF para IPv6. También conocido como OSPFv3, es un protocolo de enrutamiento de estado de enlace, definido en la *RFC 2740*. Está diseñado para ser ejecutado como un protocolo de enrutamiento para un solo sistema autónomo.

Este protocolo es una adaptación del protocolo de enrutamiento OSPFv2 de IPv4 definido en la *RFC 2328*.

IS-IS para IPv6. También conocido como IS-doble, es un protocolo de enrutamiento de estado de enlace muy similar a OSPF y está definido por la ISO en el documento 10589. IS-IS soporta IPv4 y protocolos de red orientados a No conexión, el nivel de red de la suite de protocolos OSI.

BGP-4. Es un protocolo de enrutamiento de vector de ubicación definido en la *RFC 4271*. A diferencia de RIPng y OSPF para IPv6, los cuales se usan con un sistema autónomo, este protocolo está diseñado para intercambiar información entre sistemas autónomos. La información de enrutamiento BGP-4 se usa para crear un árbol de rutas (caminos), el cual describe todas las conexiones entre sistema autónomos.

La información de este árbol se usa entonces para crear rutas libres de loop en las tablas de enrutamiento de los routers BGP-4.

Los mensajes de este protocolo son enviados usando el puerto TCP 179. BGP-4 se ha definido para ser independiente de la familia de direcciones para las cuales la información de enrutamiento es propagada.

Para IPv6, BGP-4 se ha ampliado para soportar prefijos de direcciones IPv6 tal como está descrito en la *RFC 2545* y en la *RFC 4760*.

CAPÍTULO III

REQUERIMIENTOS PARA IMPLEMENTAR REDES IPV6

Durante una primera etapa, ambos tipos de protocolos deberán coexistir con sus propias estructuras y tecnologías de funcionamiento. La forma de operación de cada protocolo difiere significativamente desde la asignación del espacio de direcciones como en la manera de encapsular los paquetes y transportar la carga útil. En este capítulo se detalla un alcance sobre las diferentes tecnologías de transición desde IPv4 hacia IPv6, se describe la nueva pila de protocolos, las configuraciones de túnel entre ambos tipos de protocolos y los procedimientos a tomar en cuenta para una planificación adecuada de una implementación IPv6.

3.1 Tecnologías de Transición IPv6

Las transiciones de protocolo no son fáciles de configurar; y la transición de IPv4 a IPv6 no es la excepción. Estas transiciones están implementadas instalando y configurando el nuevo protocolo en todos los nodos de la red y verificando que las operaciones de todos los host y routers trabajen satisfactoriamente. Aunque esto podría ser fácilmente manejado en una organización pequeña a mediana, el reto de hacer una transición rápida de protocolo en una organización grande es muy difícil. Los diseñadores de IPv6 reconocieron que la transición de IPv4 a IPv6 tomará años y que podría haber organizaciones o nodos dentro de éstas que continuarán usando IPv4 indefinidamente. Por lo tanto, aunque la migración es una meta por largo tiempo, igual consideración debe darse a la coexistencia interna de los nodos IPv4 e IPv6. En la especificación de la *RFC 1752* se definen los siguientes criterios de transición:

Host existentes IPv4 pueden ser actualizados en cualquier tiempo, independiente de la actualización de otros host o routers.

Nuevos host, usando sólo IPv6, pueden ser agregados en cualquier tiempo, sin depender de otros host o de la infraestructura de enrutamiento.

Host existentes IPv4, con IPv6 instalado, pueden continuar usando sus direcciones IPv4 y no necesitan direcciones adicionales.

Se requiere una pequeña preparación para cualquier actualización de nodos existentes IPv4 a IPv6 o implementar nuevos nodos IPv6.

La falta de dependencias entre hosts IPv4 e IPv6, la infraestructura de enrutamiento IPv4 y la de IPv6 requieren mecanismos que permitan la coexistencia libre de irregularidades. En la *RFC 2893* se definen los siguientes tipos de nodos:

Nodo de Sólo IPv4. Implementa sólo IPv4 y es asignado solamente a direcciones IPv4. Este nodo no soporta IPv6. Muchos hosts, como computadoras cliente, servidores, dispositivos de red como impresoras y routers instalados actualmente son nodos de sólo IPv4.

Nodo de Sólo IPv6. Implementa sólo IPv6 y es asignado solamente a direcciones IPv6. Este nodo puede comunicarse sólo con nodos IPv6 y aplicaciones habilitadas en IPv6. Aunque este nodo no es común hoy en día, se pondrá más prevalente en dispositivos más pequeños como teléfonos celulares y dispositivos de cómputo de bolsillo que incluirán sólo pilas de protocolo IPv6.

Nodo IPv6/IPv4. Implementa ambos, IPv4 e IPv6, y es asignado a ambos tipos de direcciones IPv4 e IPv6. Computadoras con *Windows Server 2008*, *Windows 7*, *Solaris* o *Linux* son nodos IPv6/IPv4 predeterminados.

Nodo IPv4. Implementa IPv4 y puede enviar y recibir paquetes IPv4. Un nodo IPv4 puede ser un nodo sólo de IPv4 o un nodo IPv6/IPv4.

Nodo IPv6. Implementa IPv6 y puede enviar y recibir paquetes IPv6. Un nodo IPv6 puede ser un nodo sólo de IPv6 o un nodo IPv6/IPv4.

Para que ocurra la coexistencia, el número más grande de nodos IPv4 o IPv6 pueden comunicarse usando una infraestructura de IPv4, una infraestructura de IPv6 o una infraestructura que sea la combinación de IPv4 e IPv6.

La verdadera migración se logra cuando todos los nodos IPv4 son convertidos a nodos de sólo IPv6. Sin embargo, para en futuro previsible, la migración práctica se logrará cuando otros nodos de sólo IPv4 tantos como sea posible sean convertidos en nodos IPv6/IPv4.

Los nodos de sólo IPv4 no pueden comunicarse con nodos de sólo IPv6, pero es posible usar un proxy IPv4-to-IPv6 o puertas de enlace de traducción.

Para ayudar en la transición de IPv4 a IPv6, se definen: Direcciones compatibles IPv4, Direcciones mapeadas IPv4, Direcciones ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*), Direcciones 6to4 y Direcciones Teredo.

3.2 Mecanismos de transición

Para coexistir con una infraestructura IPv4 y proveer una eventual migración a una infraestructura de sólo IPv6, los estándares de transición IPv6 definen los siguientes mecanismos:

3.2.1 Usando IPv4 e IPv6

Durante el tiempo en que la infraestructura de enrutamiento efectúe una transición desde sólo IPv4 a IPv4 e IPv6, y finalmente a sólo IPv6, los nodos deben poder alcanzar destinos usando IPv4 o IPv6. Por ejemplo, durante la transición, algunos servicios del servidor serán accesibles sobre IPv6, pero algunos otros que todavía no han sido actualizados para usar ambos protocolos, serán accesibles sólo sobre IPv4.

Para usar ambos niveles de Internet en el mismo nodo, los nodos IPv6/IPv4 pueden tener las siguientes arquitecturas:

3.2.1.a Arquitectura de Nivel Doble IP

Esta arquitectura contiene ambos niveles de Internet IPv4 e IPv6 con una sola implementación de los protocolos de nivel de Transporte tales como TCP y UDP.

Windows Server 2008 y *Windows 7* incluyen el tipo de arquitectura mostrado en la Fig.3.1. Un solo driver de Windows, *tcpip.sys*, contiene la implementación de ambos protocolos.

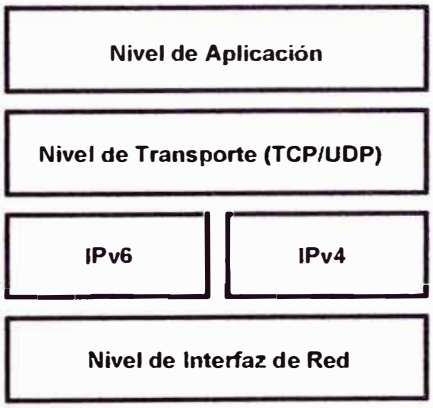

Fig.3.1 Arquitectura de Nivel Doble IP

Un nodo ejecutando cualquiera de estos sistemas operativos puede crear los siguientes tipos de paquetes:

Paquetes IPv4.

Paquetes IPv6.

Paquetes IPv6 sobre IPv4.

Estos son paquetes IPv6 que son encapsulados con un encabezado IPv4.

En la Fig.3.2, se muestran los tipos de paquetes con una arquitectura de nivel doble IP.

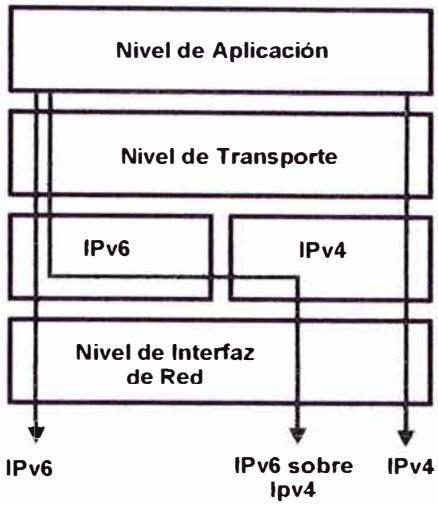

Fig.3.2 Tipos de Paquetes en una Arquitectura de nivel doble IP

3.2.1.b Arquitectura de Pila Doble

Esta arquitectura también contiene ambos niveles de Internet IPv4 e IPv6 pero con diferentes pilas de protocolo que contienen implementaciones separadas de protocolos de nivel de Transporte tales como TCP y UDP. La Fig.3.3, muestra la arquitectura de pila doble.

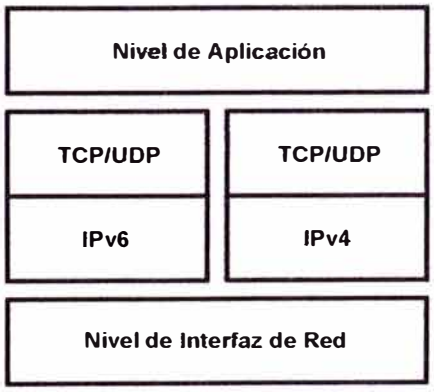

Fig.3.3 Arquitectura de Pila Doble

Windows Server 2003 y *Windows XP* tienen una arquitectura de pila doble. El driver de IPv4, *Tcpip.sys*, contiene IPv4, TCP y UDP (entre otros protocolos). El driver de IPv6. *Tcpip6.sys*, contiene IPv6 y una implementación separada de TCP y UDP. Con ambas pilas de protocolo instaladas IPv4 e IPv6, un host con *Windows Server 2003* y *Windows XP*

puede crear los mismos tipos de paquetes que en la arquitectura de nivel IP. Esto se muestra en la Fig.3.4.

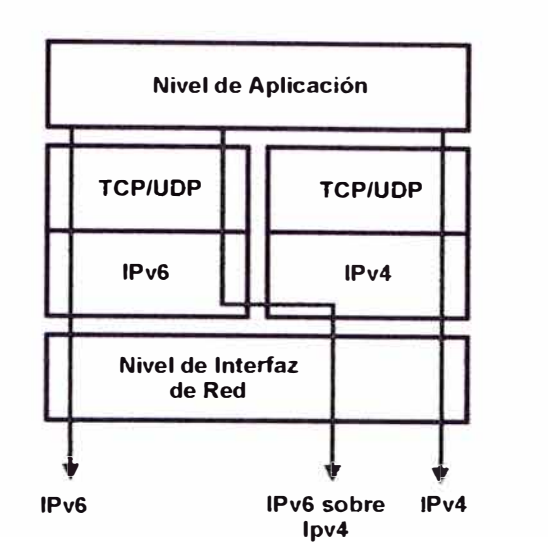

Fig.3.4 Tipos de Paquetes en una Arquitectura de Pila Doble

3.2.2 Túnel IPv6 sobre IPv4

El efecto de túnel IPv6 sobre IPv4 es la encapsulación de paquetes IPv6 con un encabezado IPv4 de tal modo que esos paquetes pueden ser enviados sobre una infraestructura de sólo IPv4. Dentro del encabezado IPv4:

El campo de protocolo IPv4 es configurado a *41* para indicar un paquete IPv6 encapsulado.

Los campos de *Origen* y *Destino* son configurados a direcciones IPv4 de los extremos del túnel IPv6 sobre IPv4. El extremo del túnel local es una dirección IPv4 asignada al emisor.

El extremo del túnel remoto es una dirección IPv4 asignada al destino o a un router intermedio. Los extremos del túnel son configurados manualmente como parte de la interfaz de túnel o son derivados automáticamente basados en la dirección de siguiente salto para la dirección IPv6 de destino y la interfaz de túnel.

El tráfico del efecto de túnel IPv6 presenta los siguientes alcances:

Los routers y firewalls que usan filtrado de paquetes deben ser configurados permitiendo el tráfico de protocolo IPv4 para ser recibido y reenviado.

La mayoría de NAT's sólo traducen tráfico TCP o UDP o deben tener un editor NAT instalado para manipular la traducción de otros protocolos IPv4.

La Fig.3.5 muestra el efecto de túnel IPv6 sobre IPv4.

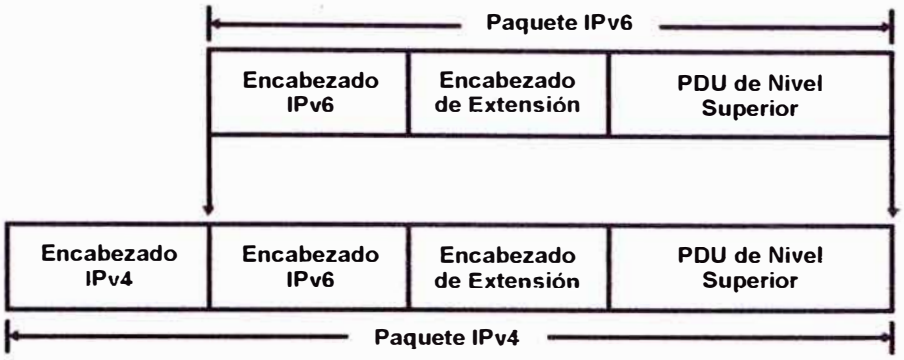

Fig.3.5 Efecto de Túnel IPv6 sobre IPv4

3.2.3 Infraestructura DNS

Se necesita de una infraestructura DNS para la coexistencia, debido al uso prevaleciente de nombres en vez de direcciones para referirse a los recursos de red. Para IPv6, la resolución de nombres a direcciones IPv6 es solicitado altamente debido a la longitud y forma poco familiar de una dirección IPv6 para la mayoría de usuarios. Actualizar la infraestructura DNS para IPv6 consiste en poblar los servidores DNS con registros *AAAA* para resolver nombres a direcciones IPv6 y con registros *PTR* para resolver direcciones IPv6 a nombres.

Registros de dirección. La infraestructura DNS debe contener los siguientes registros de recursos para la resolución satisfactoria de FQDN (*Fully Qualified Domain Names*) a direcciones:

Un registro para nodos de sólo IPv4 y nodos IPv6/IPv4.

Registros *AAAA* para nodos de sólo IPv6 y nodos IPv6/IPv4.

Registros de punteros. La infraestructura DNS debe contener los siguientes registros de recursos para la resolución satisfactoria de direcciones a *FQDN's*: Registros *PTR* en el dominio *IN-ADDR.ARPA* para nodos de sólo IPv4 y nodos IPv6/IPv4 y Registros *PTR* en el dominio *IP6.ARPA* para nodos de sólo IPv6 y nodos IPv6/IPv4.

Las reglas para la selección de direcciones están definidas en la *RFC 3484*.

3.3 Configuraciones de túnel

La *RFC 2893* define las siguientes configuraciones de túnel para el tráfico de túnel IPv6 entre nodos IPv6/IPv4 sobre una infraestructura de sólo IPv4:

3.3.1 Router-to-Router

En esta configuración, dos routers IPv6/IPv4 conectan dos infraestructuras IPv6 habilitadas sobre una infraestructura de sólo IPv4. Los puntos finales del túnel se extienden

a lo largo de un solo salto en la ruta entre origen y destino. Las rutas dentro de cada infraestructura habilitada IPv6 apuntan al router IPv6/IPv4 en su entorno. Para cada router IPv6/IPv4, existe una interfaz de túnel representando al túnel IPv6 sobre IPv4. La Fig.3.6, muestra la configuración de túnel de *router-to-router*.

Algunos ejemplos de este tipo de configuración incluyen:

Un laboratorio de prueba de sólo IPv6 que hace túnel a través de una infraestructura de sólo IPv4 de una organización para llegar hasta Internet IPv6.

Dos sitios de soporte IPv6 de una organización que hacen túnel a través del Internet IPv4.

Un router 6to4 que hace túnel a través de Internet IPv4 para llegar a otro router 6to4 o un router repetidor 6to4.

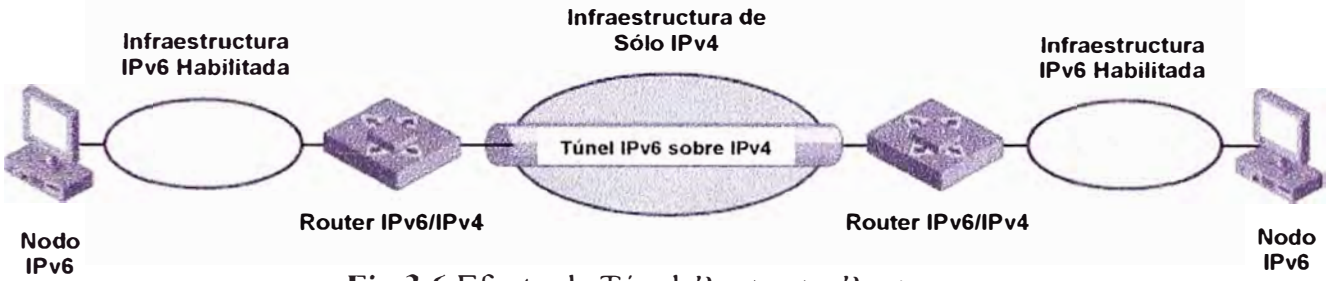

Fig.3.6 Efecto de Túnel *Router-to-Router*

3.3.2 Host-to-Router y Router-to-Host

En la configuración de túnel *host-to-router*, un host IPv6/IPv4 que reside dentro de una infraestructura de sólo IPv4 utiliza un túnel IPv6 sobre IPv4 para llegar a un router IPv6/IPv4. Los extremos del túnel se expanden en la ruta entre los nodos IPv6 de origen y destino. Sobre el nodo IPv6/IPv4, hay una interfaz de túnel representando el túnel IPv6 sobre IPv4 y una o más rutas que usa la interfaz de túnel. El nodo IPv6/IPv4 hace túnel a través del paquete IPv6 basado en la ruta compatible, la interfaz de túnel y la dirección IPv6 de siguiente salto del router IPv6/IPv4.

En la configuración de túnel *router-to-host*, un router IPv6/IPv4 crea un túnel IPv6 sobre IPv4 a través de una infraestructura IPv4 para alcanzar un nodo IPv6/IPv4. Los extremos del túnel se expanden a lo largo del último salto en el camino entre los nodos de origen y destino. Sobre el router IPv6/IPv4, hay una interfaz de túnel representando el túnel IPv6 sobre IPv4 y rutas que usa la interfaz de túnel. El router IPv6/IPv4 hace túnel a través del paquete IPv6 basado en la ruta de subred compatible, la interfaz de túnel y la dirección IPv6 de destino del nodo IPv6/IPv4.

La Fig.3.7 muestra la configuración de túnel *host-to-router* (para el tráfico que va desde *Nodo A* hasta el *Nodo B* sobre la infraestructura de sólo IPv4) y la configuración de túnel *router-to-host* (para el tráfico que va desde el *Nodo B* hasta el *Nodo A*).

Los ejemplos de las características de túnel *host-to-router* y de *router-to-host* incluyen:

Un host IPv6/IPv4 que hace túnel por medio de una infraestructura de sólo IPv4 de una organización para llegar a Internet IPv6 (túnel *host-to-router*).

Un host ISATAP que hace túnel a través de la parte de sólo IPv4 de la Intranet a un router ISATAP para alcanzar una parte con soporte IPv6 de la Intranet (túnel *host-to-router*).

Un router ISATAP que hace túnel a través de la parte de sólo IPv4 de la Intranet para alcanzar un host de destino ISATAP (túnel *router-to-host*).

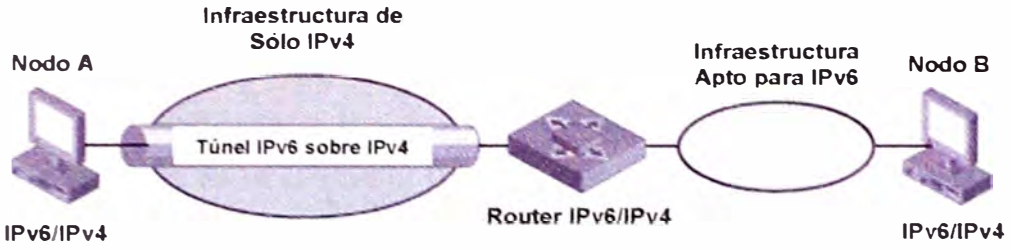

Fig.3.7 Efecto de Túnel *Host-to-Router* y *Router-to-Host*

3.3.3 Host-to-Host

En esta configuración, un nodo IPv6/IPv4 que reside dentro de una infraestructura de sólo IPv4 utiliza un túnel IPv6 sobre IPv4 para alcanzar a otro nodo IPv6/IPv4 que reside dentro de la misma infraestructura de sólo IPv4. Los extremos del túnel se expanden a lo largo del camino entero consistente en un solo salto entre los nodos de origen y destino.

Cada nodo IPv6/IPv4 tiene una interfaz que representa el túnel IPv6 sobre IPv4. Una ruta está presente para indicar que el nodo de destino está en la misma subred lógica definida por la infraestructura de sólo IPv4. Basado en la interfaz del emisor, la ruta de subred sobre el enlace y la dirección de destino, el host emisor hace un túnel a través del tráfico IPv6 hasta el destino.

Algunos ejemplos de esta característica incluyen lo siguiente:

Host ISATAP que hacen túnel mutuamente por medio del tráfico y a través de la infraestructura de sólo IPv4.

Host/routers 6to4 que hacen túnel mutuamente por medio del tráfico y a través de Internet IPv4. La Fig.3.8, muestra la característica de túnel *host-to-host*.

Fig.3.8 Efecto de Túnel *Host-to-Host*

3.4 Tipos de túneles

En la *RFC 2893* se definen los siguientes tipos de túneles:

3.4.1 Túneles Configurados

Son aquellos que requieren de una configuración manual en los extremos local y remoto. En un túnel configurado, la dirección IPv4 en el extremo del túnel remoto no está embebida o codificada en la dirección IPv6 de siguiente salto para la dirección IPv6 de destino.

Los túneles configurados manualmente se usan comúnmente para túneles *router-to-router*. La configuración de la interfaz de túnel, consistente en la direcciones IPv4 de los extremos del túnel local y remoto, debe ser especificada manualmente junto con las rutas que utiliza la interfaz de túnel.

Por ejemplo, se puede usar un túnel configurado manualmente en dos redes de laboratorio de pruebas que soportan IPv6 por medio de una Intranet de sólo IPv4 sin usar una tecnología de transición tal como ISATAP.

3.4.2 Túneles Automáticos

Un túnel automático es un túnel que no requiere de una configuración manual.

Los extremos de este tipo de túneles se determinan por medio de rutas, interfaces de túnel y direcciones de siguiente salto para direcciones IPv6 de destino.

Las plataformas *Windows Server 2008* y *Windows 7* soportan las siguientes tecnologías de túneles automáticos:

ISATAP. Usado para comunicaciones unicast entre host IPv6/IPv4 a través de una Intranet de sólo IPv4.

6to4. Usado para comunicaciones unicast entre host IPv6/IPv4 y sitios con soporte IPv6 a través de Internet IPv4 cuando los routers 6to4 o host/routers 6to4 tienen direcciones IPv4 públicas.

Teredo. Usado para comunicaciones unicast entre host IPv6/IPv4 a través de Internet IPv4.

Como se muestra en la Fig.3.9, acerca de dos subredes de un laboratorio de pruebas IPv6 ubicado en diferentes partes de una Intranet.

El *Router1* está conectado a la subred IPv6 de *2001:db8:0:1::/64* y tiene la dirección IPv4 de *131.107.47.121*.

El *Router2* está conectado a la subred de *2001:db8:0:2::/64* y tiene la dirección IPv4 de *157.54.9.211*.

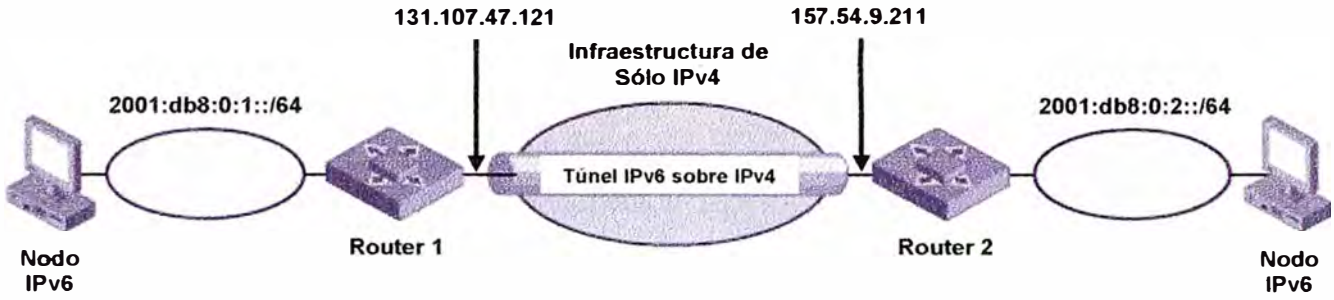

Fig.3.9 Ejemplo de Túnel Configurado Manualmente

3.5 ISATAP

El Protocolo ISATAP es una asignación de dirección y una tecnología de túnel automático *host-to-host*, *host-to-router* y *router-to-host* definida en la *RFC 4214* que provee conectividad unicast IPv6 entre hosts IPv6/IPv4 a través de una Intranet IPv4. Los hosts ISATAP no requieren de configuración manual y pueden crear direcciones ISATAP utilizando mecanismos estándar de autoconfiguración de direcciones IPv6.

Las direcciones ISATAP tienen uno de los siguientes formatos:

64-bitUnicastPrefix:0:5EFE:w.x.y.z

64-bitUnicastPrefix:200:5EFE:w.x.y.z

Donde:

64-bitUnicastPrefix es cualquier prefijo de dirección unicast de 64 bits, incluyendo prefijos de enlace local, global y local único.

::0:5EFE:w.x.y.z y *::200:5EFE:w.x.y.z* son los identificadores de interfaz administrados localmente. Para *::0:5EFE:w.x.y.z*, *w.x.y.z* es una dirección IPv4 unicast privada. Para *::200:5EFE:w.x.y.z*, es una dirección IPv4 unicast pública. La parte del *ID de interfaz* de

una dirección ISATAP contiene una dirección IPv4 embebida que determina la dirección IPv4 de destino en el encabezado del protocolo IPv4 encapsulado en el tráfico ISATAP.

3.5.1 Efecto de túnel ISATAP

El tráfico IPv6 basado en ISATAP se hace por túneles o se encapsula por medio de un encabezado IPv4 y también se le conoce como tráfico IPv6 sobre IPv4. Este efecto de túnel se hace automáticamente por medio de una interfaz de túnel ISATAP en el host emisor o por el reenvío de un router. La interfaz de túnel ISATAP trata toda la parte de sólo IPv4 de la Intranet como un solo nivel de enlace, en muchos casos de la misma forma como Ethernet.

En el caso de ISATAP la encapsulación del nivel de enlace es IPv4.

Un ejemplo de túnel ISATAP se muestra en la Fig.3.10, donde el *Host A* tiene una sola interfaz LAN y está configurada con la dirección IPv4 de *10.40.1.29*. El *Host B* tiene una sola interfaz LAN y está configurada con la dirección IPv4 de *192.168.41.30*. IPv6 sobre el *Host A* tiene la dirección ISATAP de *FE80::5EFE:10.40.1.29* asignada a su interfaz de túnel ISATAP y el *Host B* tiene la dirección ISATAP de *FE80::5EFE:192.168.41.30* asignada a su interfaz de túnel ISATAP.

Fig.3.10 Ejemplo de Configuración ISATAP

Cuando el *Host A* envía tráfico IPv6 al *Host B* destinado para la dirección ISATAP de enlace local del *Host B*, las direcciones de origen y destino para los encabezados IPv4 e IPv6 son como los que se muestran en la Tabla N° 3.1.

TABLA N° 3.1 Ejemplo de Direcciones ISATAP de Enlace Local

Campo	Valor
Dirección de Origen IPv6	FE80::5EFE:10.40.1.29
Dirección de Destino IPv6	FE80::5EFE:192.168.41.30
Dirección de Origen IPv4	10.40.1.29
Dirección de Destino IPv4	192.168.41.30

Para probar la conectividad entre hosts ISATAP, se puede usar la herramienta *ping*. Por ejemplo, se podría usar el comando siguiente desde el *Host A*:

ping fe80::5efe:192.168.41.30%10

Debido a que el destino del comando *ping* es una dirección local de enlace, se debe usar *%ZoneID* como parte de la dirección de destino para especificar el índice de interfaz desde el cual el tráfico debe ser enviado. En este caso, *%10* especifica el índice de interfaz *10*, el cual es el índice de interfaz asignado a la interfaz de túnel ISATAP en el *Host A*.

3.5.2 Componentes ISATAP

Una implementación de ISATAP consiste en hosts ISATAP, routers ISATAP y una o más subredes lógicas ISATAP. La Fig.3.11, muestra lo componentes de una Intranet Apto para IPv6 y una sola subred ISATAP.

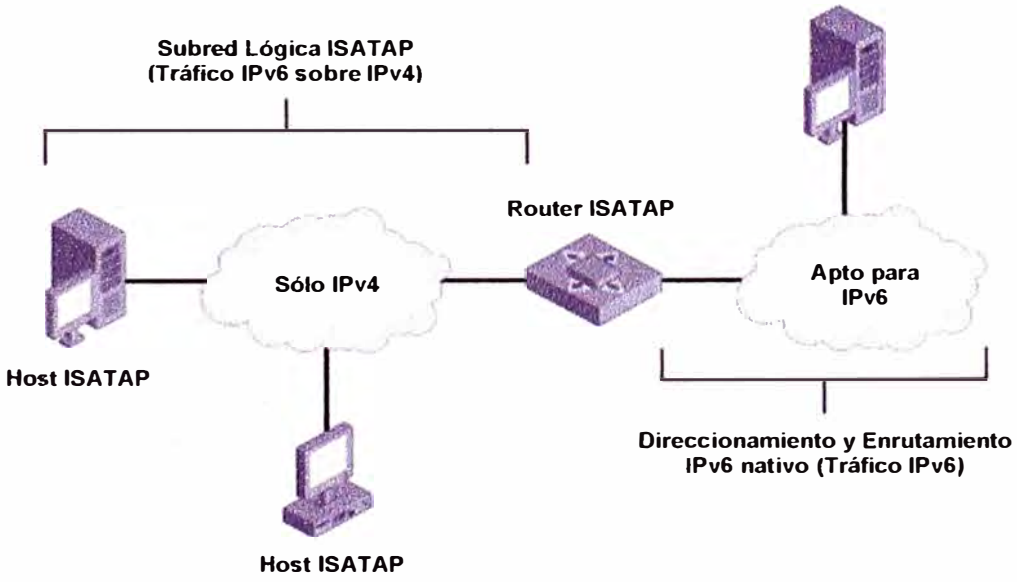

Fig.3.11 Componentes de ISATAP

La parte de *Sólo IPv4* de la Intranet es la subred ISATAP. La parte de *Apto para IPv6* de la Intranet tiene direccionamiento y routers nativos IPv6. Los hosts en la parte *Apto para IPv6* de la Intranet están configurados con direcciones locales únicas y globales en sus interfaces LAN y no necesitan usar encapsulación IPv4 para comunicarlos mutuamente usando IPv6.

Los hosts ISATAP tienen una interfaz de túnel ISATAP y realizan sus propios túneles a otros hosts ISATAP en la misma subred ISATAP (túnel *host-to-host*) o para un router ISATAP (túnel *host-to-router*). Los hosts ISATAP pueden usar direcciones ISATAP locales de enlace, locales únicas o globales para comunicarlos mutuamente. Para comunicarse con otros hosts ISATAP en la subred ISATAP usando direcciones ISATAP locales de enlace, locales únicas o globales, los hosts ISATAP hacen un túnel directamente a través de sus paquetes para cada uno de los otros hosts. Para comunicarse con hosts IPv6 en la parte Apto para IPv6 de la Intranet usando sus direcciones nativas locales únicas o globales, los hosts ISATAP hacen un túnel a través de sus paquetes para un router ISATAP.

Un router ISATAP es un router IPv6 con una interfaz de túnel que hace lo siguiente:

Reenvía paquetes entre hosts ISATAP sobre subredes ISATAP y hosts IPv6 sobre subredes Apto para IPv6.

Anuncia prefijos de dirección para hosts ISATAP en la subred ISATAP. Los hosts ISATAP usan los prefijos de dirección anunciados para configurar direcciones locales únicas ISATAP o globales.

Actúa como un router por defecto para hosts ISATAP.

3.5.3 Direccionamiento ISATAP

La Fig.3.12, muestra un ejemplo de direccionamiento ISATAP.

En esta configuración, el router ISATAP anuncia el prefijo de subred global *2001:DB8:0:7:: 64* a los hosts ISATAP en la subred ISATAP. El *Host A* ISATAP, configurado con la dirección IPv4 *192.168.47.99*, usa el prefijo de subred anunciado por el router ISATAP para configurar automáticamente la dirección ISATAP global de *2001:DB8::7:0:5EFE:192.168.47.99*.

El *Host A* trata de registrar la dirección IPv6 de registro *AAAA* para la dirección *2001:DB8::7:0:5EFE:192.168.47.99* en DNS.

Similarmente, el *Host B* ISATAP usa el prefijo de subred para configurar automáticamente la dirección global ISATAP de *2001:DB8::7:200:5EFE:131.107.71.209*.

El *Host B* trata de registrar la dirección IPv6 de registro *AAAA* para la dirección *2001:DB8::7:200:5EFE:131.107.71.209* en DNS.

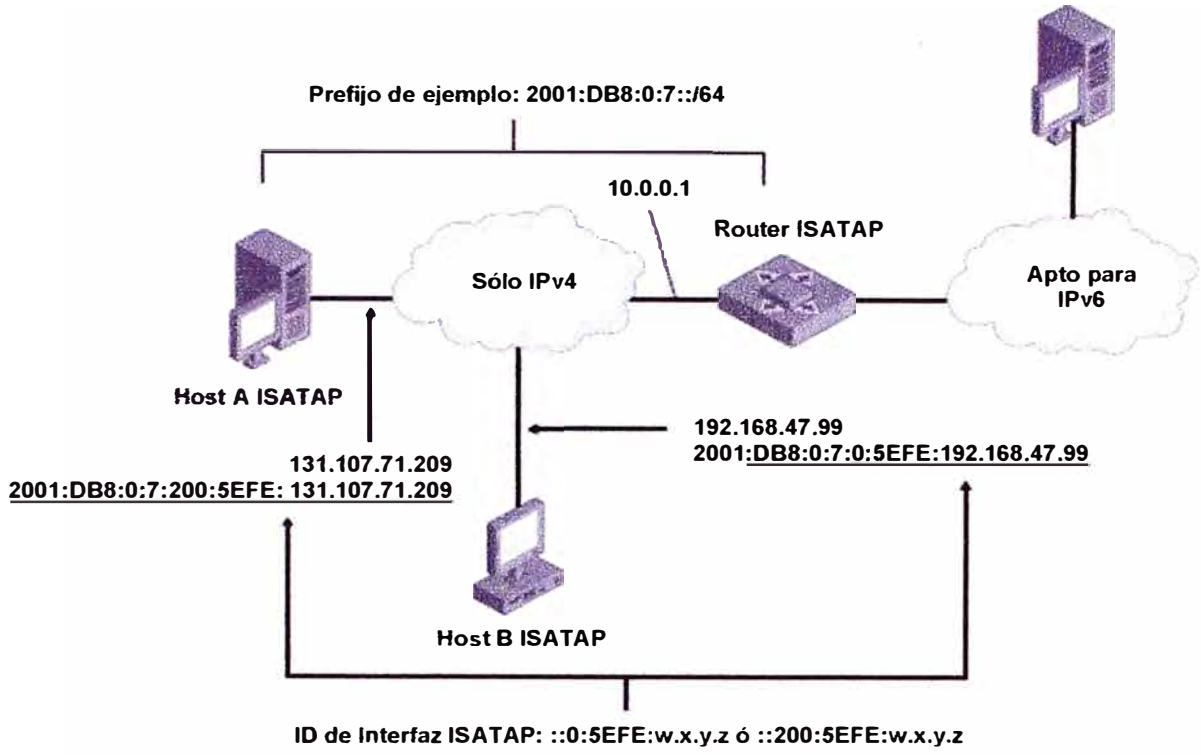

Fig.3.12 Ejemplo de Direccionamiento ISATAP

3.5.4 Enrutamiento ISATAP

La Fig.3.13, muestra las rutas relevantes de la comunicación ISATAP para el ejemplo de configuración mostrado en la Fig.3.12.

Los hosts ISATAP usan las siguientes rutas:

Una ruta en enlace para el prefijo de subred que usa la interfaz de túnel ISATAP. Esta ruta permite que los hosts ISATAP realicen efectos de túnel *host-to-host* para llegar a otros hosts ISATAP en la misma subred ISATAP. En el ejemplo de configuración, esta es la ruta *2001:DB8:0:7::/64*.

Una ruta por defecto con la dirección de siguiente salto de la dirección ISATAP de enlace local del router ISATAP (*FE80::5EFE:10.0.0.1*) que utiliza la interfaz de túnel ISATAP. Esta ruta permite que los hosts ISATAP realicen efectos de túnel *host-to-router* para llegar a los hosts IPv6 en la parte *Apto para IPv6* de la Intranet.

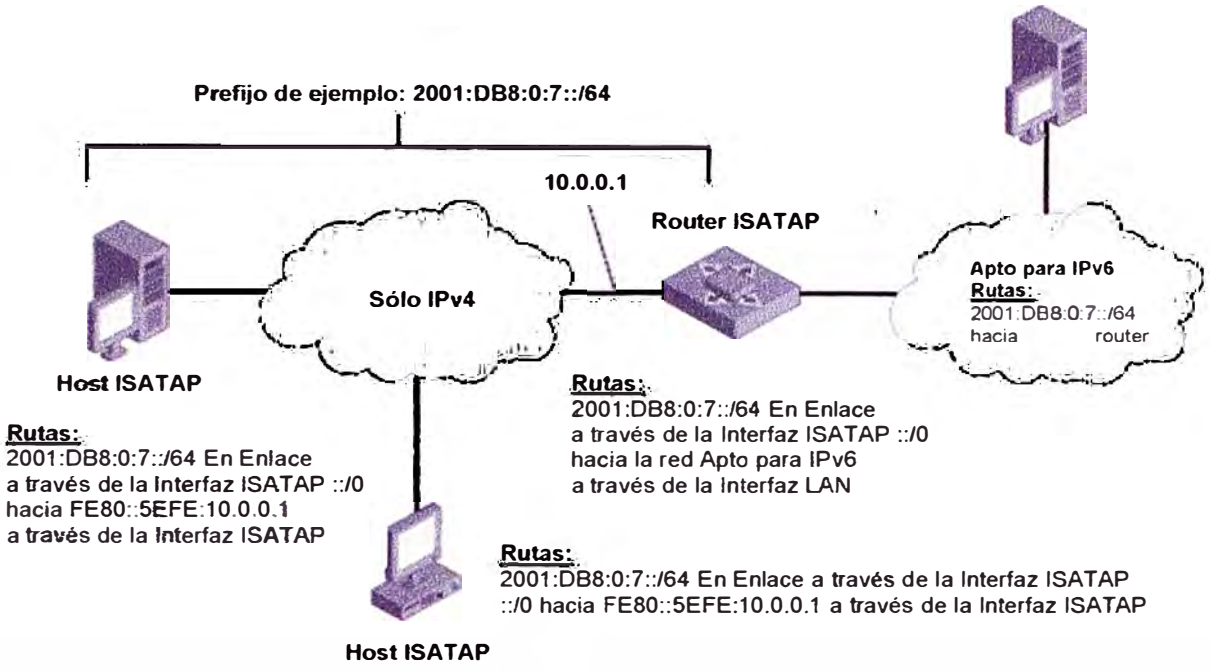

Fig.3.13 Ejemplo de Enrutamiento ISATAP

Un router ISATAP usa las siguientes rutas:

Una ruta en enlace para el prefijo de subred ISATAP que usa la interfaz de túnel ISATAP que está asociada con la interfaz de LAN conectada a la subred ISATAP. Esta ruta permite que el router ISATAP realice el efecto túnel *router-to-host* para llegar a otros hosts ISATAP en la subred ISATAP. En el ejemplo de configuración, esta es la ruta *2001:DB8:0:7::/64*.

Una ruta por defecto que usa una interfaz LAN que está conectada a la parte *Apto para IPv6* de la Intranet y tiene la dirección de siguiente salto de un router vecino. Esta ruta permite al router ISATAP reenviar el tráfico IPv6 a los destinos en la parte de *Apto para IPv6* de la Intranet.

Los routers de la red *Apto para IPv6* utilizan una ruta para el prefijo de subred ISATAP que apunta de regreso al router ISATAP. Esta ruta permite que los routers de la red *Apto para IPv6* reenvíen el tráfico destinado a los hosts ISATAP en la subred ISATAP del router ISATAP. En el ejemplo de configuración, esta es la ruta *2001:DB8:0:7::/64*.

3.6 6to4

6to4 es una asignación de dirección y una tecnología de túnel automático *router-to-router*, *host-to-router* y *router-to-host* definida en la *RFC 3056* que provee conectividad unicast IPv6 entre sitios y hosts IPv6 a través de Internet IPv4.

La tecnología 6to4 trata toda la red IPv4 como un solo enlace.

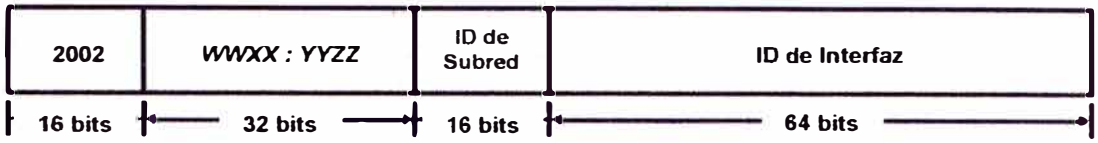

Fig.3.14 Estructura de una Dirección 6to4

La dirección 6to4 consiste en lo siguiente:

2002::/16. Es el espacio direcciones reservado para 6to4.

WWXX:YYZZ. Es la representación hexadecimal de una dirección pública IPv4 (*w.x.y.z*) asignado a un sitio o host en Internet IPv4.

ID de Subred. Se usa dentro del sitio de una organización para enumerar subredes individuales.

ID de Interfaz. Identifica un nodo sobre una subred dentro de una organización.

6to4 permite hacer lo siguiente:

Crear y usar prefijos de direcciones IPv6 globales de 48 bits (*2002:WWXX:YYZZ::/48*) basados en direcciones públicas IPv4 asignadas para la organización.

Conectar partes de *Apto para IPv6* de una Intranet juntos haciendo un túnel de tráfico IPv6 sobre Internet IPv4.

Conectar recursos de sólo IPv6 sobre Internet IPv6.

6to4 permite que se puedan asignar direcciones globales IPv6 dentro de una organización y poder llegar a ubicaciones de Internet IPv6 sin requerir de una conexión directa hacia Internet IPv6 o hacia un prefijo de dirección global IPv6 de un ISP.

3.6.1 Efecto de túnel 6to4

El tráfico 6to4 enviado a través de Internet IPv4 se hace por túneles o se encapsula por medio de un encabezado IPv4 y también se le conoce como tráfico IPv6 sobre IPv4. Este efecto de túnel se hace automáticamente por medio de una interfaz de túnel 6to4 en el host emisor o por el reenvío de un router.

La interfaz de túnel 6to4 trata toda la parte de sólo IPv4 de la Intranet como un solo nivel de enlace, en muchos casos de la misma forma como Ethernet. En el caso de 6to4 la encapsulación del nivel de enlace es IPv4.

La Fig.3.15 muestra un ejemplo de túnel 6to4, donde el *Host A* ejecutando *Windows 7* tiene una sola interfaz LAN y está configurada con la dirección IPv4 pública de *131.107.0.1*. El *Host B* que también ejecuta *Windows 7* tiene una sola interfaz LAN y está configurada con la dirección IPv4 de *157.54.0.1*. IPv6 sobre el *Host A* configura

automáticamente la dirección 6to4 de *2002:836B:1::836B:1* asignada a su interfaz de túnel 6to4 y sobre el *Host B* configura automáticamente la dirección 6to4 de *2002:9D36:1::9D36:1* asignada a su interfaz de túnel 6to4. Ambos hosts *A* y *B*, están conectados directamente a Internet IPv4.

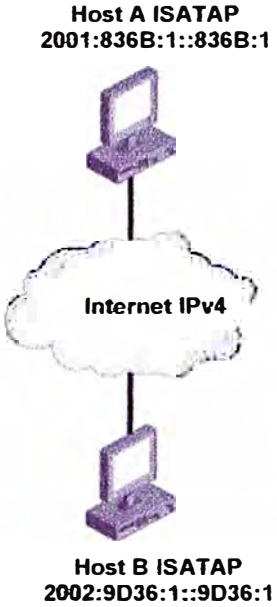

Fig.3.15 Ejemplo de una Configuración 6to4

Cuando el *Host A* envía tráfico IPv6 al *Host B* destinado a la dirección 6to4 del *Host B*, las direcciones de origen y destino para cada uno de los encabezados IPv4 y de IPv6 son como se muestran en la Tabla N° 3.2.

Para probar la conectividad entre hosts 6to4, se puede usar la herramienta *ping*. Por ejemplo, desde el *Host A*, se puede usar el siguiente comando:

ping 2002:9d36:1::9d36:1

Debido a que las direcciones 6to4 son siempre globales, no es necesario usar *%ZoneID* como parte de la dirección de destino.

TABLA N° 3.2 Ejemplo de Direcciones 6to4

Campo	Valor
Dirección de Origen IPv6	2002:836B:1::836B:1
Dirección de Destino IPv6	2002:9D36:1::9D36:1
Dirección de Origen IPv4	131.107.0.1
Dirección de Destino IPv4	157.54.0.1

La interfaz de túnel 6to4 usa su propia dirección 6to4 como una dirección de origen IPv6. Esta interfaz determina la dirección de destino IPv4 del encabezado IPv4 encapsulado desde el segundo y tercer bloques de la dirección de destino IPv6 (los primeros 32 bits después de *2002::/16*), los cuales corresponden a la dirección IPv4 embebida del *Host B*. Para la dirección de origen IPv4 en el encabezado IPv4 encapsulado, IPv4 sobre el *Host A* determina la mejor dirección de origen IPv4 para poder llegar a la dirección de destino IPv4 *157.54.0.1*.

En este caso, el *Host A* tiene solamente una dirección IPv4 asignada, además IPv4 sobre el *Host A* utiliza la dirección de origen de *131.107.0.1*.

3.6.2 Componentes 6to4

Una implementación 6to4 consiste de hosts 6to4, routers 6to4, host/routers 6to4 y repetidores 6to4.

Los componentes 6to4, son los siguientes:

Host 6to4. Un host nativo IPv6 que está configurado al menos con una dirección 6to4 (una dirección global con el prefijo *2002::/16*). Los hosts 6to4 no requieren de un soporte adicional o alguna configuración manual y pueden crear direcciones 6to4 usando mecanismos estándar de autoconfiguración de direcciones. Los hosts 6to4 no tienen una interfaz de túnel 6to4 y tampoco realizan el efecto de túnel 6to4.

Router 6to4. Un router IPv6/IPv4 que usa una interfaz de túnel 6to4 para reenviar tráfico direccionado 6to4 entre hosts 6to4 dentro de un sitio y otros routers 6to4, host/routers 6to4 o repetidores 6to4 a través de Internet IPv4. Los routers 6to4 podrían requerir de una configuración manual.

Host/router 6to4. Un host IPv6/IPv4 que usa una interfaz de túnel 6to4 para intercambiar tráfico direccionado 6to4 con otros host/routers 6to4, routers 6to4 o repetidores 6to4 a través de Internet IPv4.

A diferencia de un router 6to4, un host/router 6to4 no reenvía tráfico a otros hosts 6to4.

Repetidor 6to4. Un router IPv4/IPv4 que reenvían tráfico direccionado 6to4 entre routers 6to4 y host/routers 6to4 en Internet IPv4 y hosts de Internet IPv6. Microsoft ha desarrollado un repetidor 6to4 sobre Internet IPv4, el cual es accesible resolviendo el nombre DNS *6to4.ipv6.microsoft.com* a una dirección IPv4. La *RFC 3068* define además un prefijo anycast IPv4 para repetidores 6to4.

Los host/routers 6to4 y la Intranet, ambos conectados al router 6to4 son sitios 6to4, los cuales son redes o hosts conectados a Internet IPv4 que tienen su propio prefijo único

2002:WWXX:YYZZ::/48. Para el host/router 6to4 el sitio completo 6to4 consiste de una sola computadora. Para el router 6to4, la Intranet entera es un sitio 6to4, el cual puede consistir de hasta 65,536 subredes IPv6 (usando todas la combinaciones posibles del *ID de Subred* de 16 bits). Un sitio 6to4 puede ser creado desde cualquier dirección publica IPv6.

Dentro de un sitio 6to4 conectado a Internet IPv4 con un router 6to4, los routers IPv6 anuncian prefijos *2002:WWXX:YYZZ:SubnetID::/64* a fin de que los hosts 6to4 puedan crear una dirección 6to4 autoconfigurada. La Fig.3.16, muestra los componentes 6to4 y su ubicación en Internet IPv4 e IPv6.

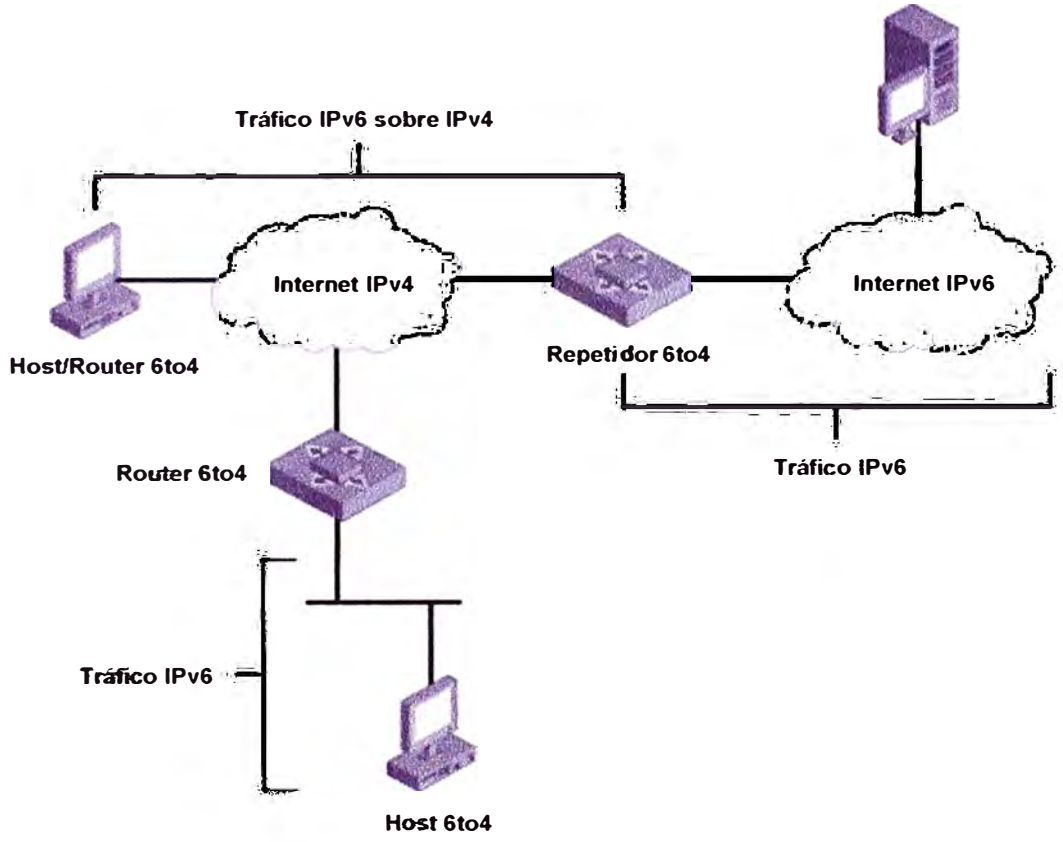

Fig.3.16 Componentes 6to4 en Internet IPv4 e Internet IPv6

3.6.3 Direccionamiento 6to4

En la Fig.3.17, se muestra el ejemplo de una configuración 6to4.

El router 6to4 está conectado directamente a Internet y ha sido asignada la dirección IPv4 pública de *157.60.0.1*. Desde la dirección IPv4 pública, la Intranet conectada al router 6to4 puede usar el prefijo de 48 bits *2002:9D3C:1::/48*. (*9D3C:1* es la notación hexadecimal de *157.60.0.1*). El router 6to4 anuncia el prefijo *2002:9D3C:1:1::/64* en la interfaz LAN conectada a la Intranet de una sola subred. La parte *ID de Subred* del prefijo

de 64 bits se puede especificar en forma manual o es determinado automáticamente por el router 6to4. Los hosts IPv6 en la subred de la Intranet configuran una dirección IPv6 basada en el prefijo *2002:9D3C:1:1::/64* usando una dirección de autoconfiguración IPv6 estándar. En el ejemplo, el *Host A* 6to4 se configura automáticamente con la dirección IPv6 *2002:9D3C:1:1::1*.

El *Host/router B* 6to4 está conectado directamente a Internet y le ha sido asignado la dirección pública IPv4 de *131.107.0.1*. El protocolo IPv6 para *Windows Server 2008* y *Windows 7* deriva automáticamente una dirección de la forma *2002:WWXX:YYZZ::WWXX:YYZZ*.

Por lo tanto, el *Host/router B* 6to4 se asigna a sí mismo la dirección IPv6 *2002:836B:1::836B:1*. (*836B:1* es la notación hexadecimal para *131.107.0.1*). Para determinar la dirección IPv4 del repetidor 6to4 en Internet IPv4, un host/router 6to4 o un router 6to4 que está ejecutando *Windows Server 2008* o *Windows 7* por defecto intenta resolver automáticamente el nombre DNS *6to4.ipv6.microsoft.com* a una dirección IPv4.

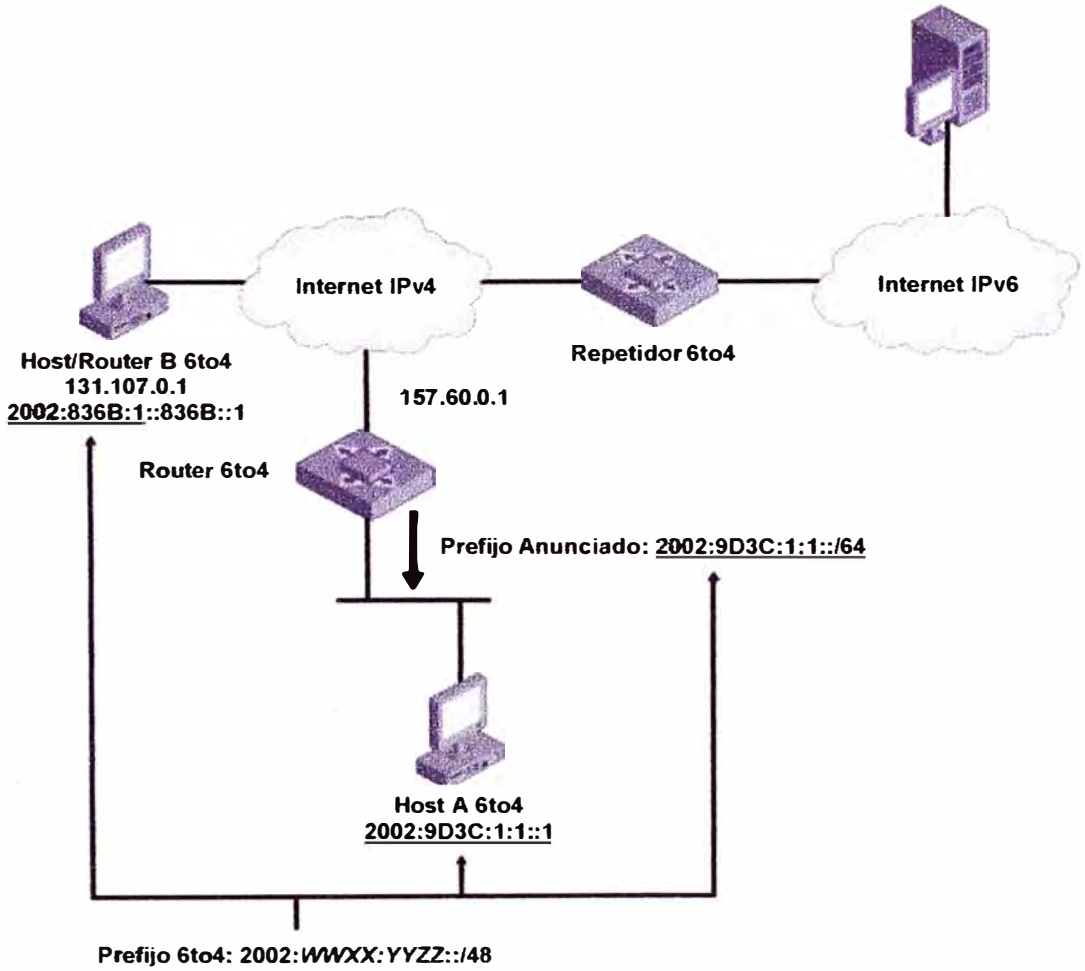

Fig.3.17 Ejemplo de una Configuración 6to4

3.6.4 Enrutamiento 6to4

La Fig.3.18 muestra las rutas relevantes de comunicación para el ejemplo de configuración de la Fig.317.

El *Host A* 6to4 utiliza las siguientes rutas:

Una ruta en enlace para el prefijo de subred de la Intranet que usa la interfaz LAN. En el ejemplo de configuración mostrado en la Fig.3.17, esta es la ruta *2002:9D3C:1:1::/64*.

Una ruta por defecto que usa la interfaz LAN y tiene la dirección de siguiente salto de la dirección local de enlace del router 6to4. Esta ruta permite que el *Host A* 6to4 pueda llegar a otros hosts 6to4, host/routers 6to4 o ubicaciones en Internet IPv6.

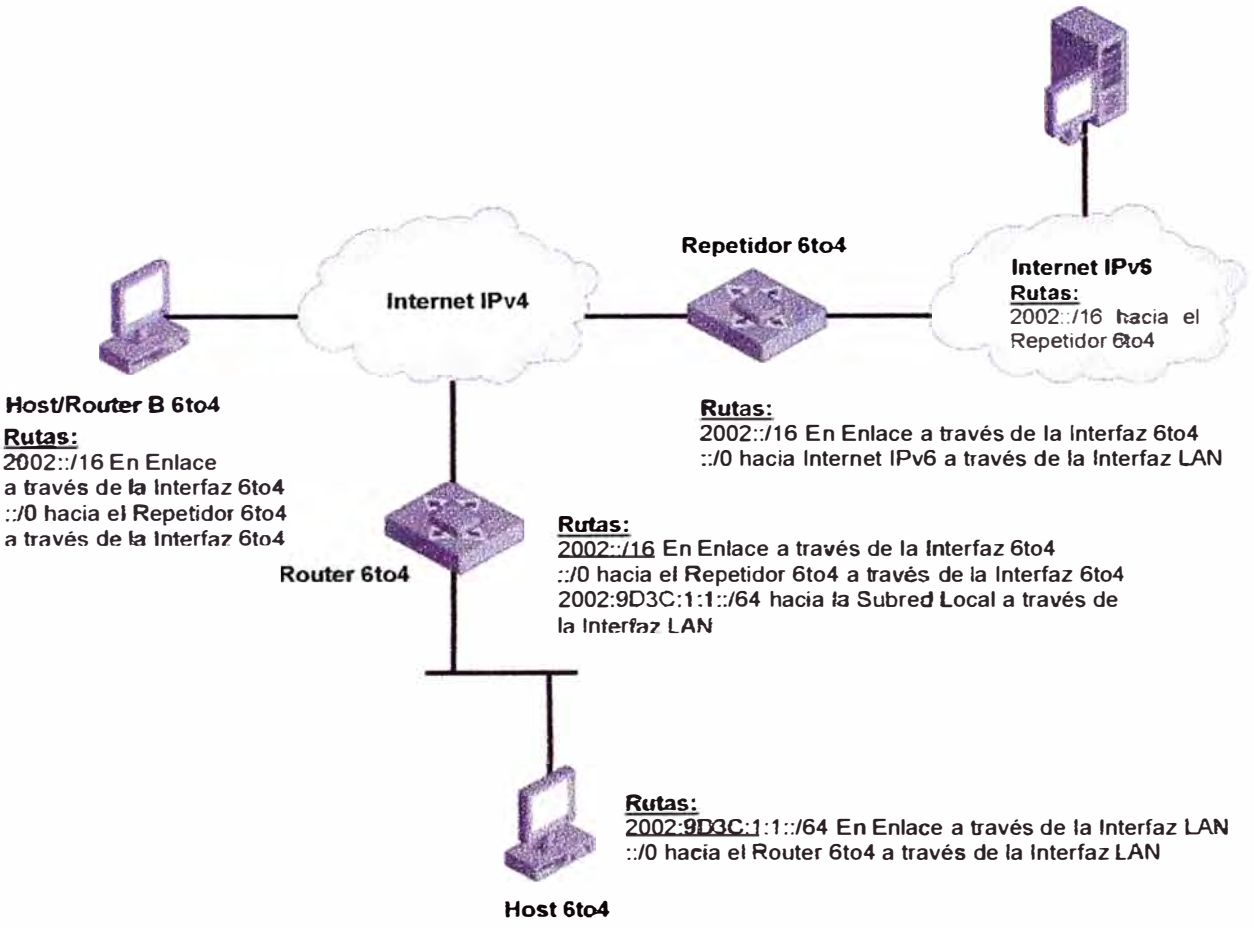

Fig.3.18 Ejemplo de Enrutamiento 6to4

El router 6to4 utiliza las siguientes rutas:

Una ruta en enlace para el prefijo de subred de la Intranet que usa la interfaz LAN. Esta ruta permite que el router 6to4 reenvíe tráfico hacia y desde hosts 6to4 en la subred de la Intranet. En el ejemplo de configuración, esta es la ruta *2002:9D3C:1:1::/64*.

Una ruta en enlace para el prefijo de dirección 6to4 (*2002::/16*) que utiliza la interfaz de túnel 6to4. Esta ruta permite que el router 6to4 realice el efecto de túnel *router-to-router* para llegar a otros routers 6to4 y al repetidor 6to4; y el efecto de túnel *router-to-host* para llegar a host/routers 6to4.

Una ruta por defecto que usa la interfaz de túnel 6to4 y tiene la dirección de siguiente salto de la dirección 6to4 del repetidor 6to4. Esta ruta permite que el router 6to4 reenvíe tráfico IPv6 a destinos IPv6 ubicados en Internet IPv6.

El repetidor 6to4 usa las siguientes rutas:

Una ruta en enlace para el prefijo de dirección 6to4 (*2002::/16*) que usa la interfaz de túnel 6to4. Esta ruta permite que el repetidor 6to4 realice un efecto de túnel *router-to-router* para llegar a routers 6to4 y el efecto de túnel *router-to-host* para llegar a host/routers 6to4.

Una ruta por defecto que usa una interfaz LAN y tiene la dirección de siguiente salto de un router vecino en Internet IPv6 (no mostrado en las figuras). Esta ruta permite que el repetidor 6to4 reenvíe tráfico IPv6 a destinos ubicados en Internet IPv6.

Para la comunicación 6to4, los routers del Internet IPv6 usan una ruta para el prefijo de dirección (*2002::/16*) que apunta de regreso al repetidor 6to4. Esta ruta permite que los routers de Internet IPv6 reenvíen tráfico destinado para hosts 6to4 o host/routers 6to4 hacia el repetidor 6to4.

3.7 Teredo

Teredo es una asignación de dirección y una tecnología de túnel automático definido en la *RFC 4380* que provee conectividad unicast IPv6 a través de Internet IPv4.

Las direcciones Teredo están relacionados con la falta de funcionalidad de 6to4 en dispositivos periféricos modernos hoy en día en Internet y configuraciones NAT multicapas haciendo túneles de paquetes IPv6 entre hosts. En contraste 6to4 hace túnel de paquetes IPv6 entre los dispositivos periféricos. Hacer túnel por medio de hosts presenta otro tema para NAT's: los paquetes IPv6 que son encapsulados con IPv4 tienen el campo Encabezado del Protocolo IPv4 configurado a *41*. Muchas NAT's sólo traducen tráfico TCP o UDP y deben ser configurados manualmente para traducir otros protocolos o tener editores NAT instalados que puedan manejar la traducción. Debido a que el protocolo de traducción *41* no es una característica común de NAT's, el tráfico IPv6 encapsulado en IPv4 no fluirá a través de NAT's típicos. Por lo tanto, para permitir que el tráfico IPv6 fluya a través de una o múltiples NAT's, Teredo encapsula el paquete IPv6 como un

mensaje UDP IPv4, conteniendo un encabezado UDP y un encabezado IPv4. Los mensajes UDP pueden ser traducidos por la mayoría de NAT's y pueden atravesar múltiples niveles de NAT's.

En resumen, Teredo es una tecnología de transición IPv6 que permite hacer túneles automáticos IPv6 entre hosts que están ubicados en Internet IPv4, aún cuando esos hosts están detrás de uno o más NAT's IPv4. El tráfico IPv6 de clientes Teredo puede fluir a través de NAT's porque es enviado como un mensaje UDP IPv4. Si NAT soporta traducción de puerto UDP entonces soporta la tecnología Teredo.

3.7.1 Beneficios del uso de Teredo

Teredo es una tecnología en contra de NAT para el tráfico IPv6. El tráfico IPv6 que hace túnel usando Teredo puede atravesar una o múltiples NAT's y permite que un cliente Teredo acceda a otros clientes Teredo en Internet IPv4 y acceda a hosts en Internet IPv6 (por medio de un repetidor Teredo). La capacidad para conectar otros clientes Teredo que están conectados a Internet IPv4 habilita la comunicación entre aplicaciones que de otra manera tendrían problemas comunicándose sobre NAT. Con Teredo, las aplicaciones habilitadas para IPv6 pueden comunicarse satisfactoriamente con mayor frecuencia sobre Internet IPv4 que en aplicaciones de sólo IPv4.

Algunos tipos de servidores de sólo IPv4 o aplicaciones específicas tienen problemas de comunicación cuando se ejecutan en una computadora que está detrás de un NAT. Esos tipos de aplicaciones requieren de una configuración manual de NAT o deberán proveer su propia solución para un NAT atravesado.

Si la aplicación es *Apto para IPv6*, puede usar Teredo, la solución de un NAT atravesado para *Windows*. No hay necesidad de configurar un NAT o modificar la aplicación para realizar su propio NAT atravesado. Por lo tanto, en vez de perder tiempo en desarrollo y en modificar aplicaciones para una solución de un NAT atravesado personalizado, los vendedores de aplicaciones deberán actualizar sus aplicaciones para ser *Apto para IPv6*.

Teredo soporta las siguientes versiones de Windows:

Windows 7.

Windows Server 2008.

Windows XP SP2.

Windows Server 2003 SP1.

Todas las implementaciones Teredo en Windows están definidas en la *RFC 4380.*

3.7.2 Componentes de Teredo

La infraestructura Teredo consiste de los siguientes componentes:

3.7.2.a Cliente Teredo

Un cliente Teredo es un nodo IPv6/IPv4 que soporta una interfaz de túnel Teredo a través del cual los paquetes han hecho túnel a otros clientes Teredo o nodos de Internet IPv6 (vía un repetidor Teredo o un repetidor de host específico Teredo). Un cliente Teredo se comunica con servidor Teredo para obtener un prefijo de dirección desde el cual una dirección IPv6 basada en Teredo es configurada o para ayudar a iniciar la comunicación con otros clientes Teredo o hosts en Internet IPv6.

3.7.2.b Servidor Teredo

Un servidor Teredo es un nodo IPv6/IPv4 que está conectado tanto a Internet IPv4 como a Internet IPv6 y soporta una interfaz de túnel sobre el cual se reciben los paquetes. La función general de un servidor Teredo es asistir en la configuración de dirección de clientes Teredo o entre clientes Teredo y hosts de sólo IPv6. El servidor Teredo escucha el puerto UDP *3544* para el tráfico Teredo.

3.7.2.c Repetidor Teredo

Un repetidor Teredo es un router IPv6/IPv4 que puede reenviar paquetes entre clientes Teredo en Internet IPv4 (usando una interfaz de túnel Teredo) y hosts de sólo IPv6 en Internet IPv6. En algunos casos, este repetidor interactúa con un servidor Teredo para ayudar a facilitar la comunicación inicial entre clientes Teredo y hosts de sólo IPv6. El repetidor Teredo escucha en el puerto UDP *3544* para el tráfico Teredo.

3.7.2.d Repetidores de Host específico Teredo

La comunicación entre clientes Teredo y hosts IPv6 que están configurados con una dirección global deben ir a través de un repetidor Teredo. Esto es requerido por hosts de sólo IPv6 conectados a Internet IPv6. Sin embargo, cuando el host IPv6 es *Apto para IPv6* y *Apto para IP* y está conectado a ambos Internet IPv4 e IPv6, la comunicación debe ocurrir entre el cliente Teredo y el host IPv6 en Internet IPv4, en vez de tener que atravesar el Internet IPv6 e ir a través de un repetidor Teredo.

Un repetidor de host específico Teredo es un nodo IPv6/IPv4 que tiene interfaz y conectividad para Internet IPv4 e IPv6 y puede comunicarse directamente con clientes Teredo en Internet IPv4, sin la necesidad de un repetidor intermedio Teredo. La conectividad a Internet IPv4 puede ser por medio de una dirección pública IPv4 o a través de una dirección privada IPv4 y un NAT vecino. La conectividad a Internet IPv6 puede ser

por medio de una conexión directa a Internet IPv6 o a través de una tecnología de transición IPv6 tal como 6to4, donde los paquetes IPv6 hacen túnel por medio de Internet IPv4. El repetidor de host específico Teredo escucha en el puerto UDP *3544* para el tráfico Teredo. La Fig.3.19, muestra los componentes de la infraestructura Teredo.

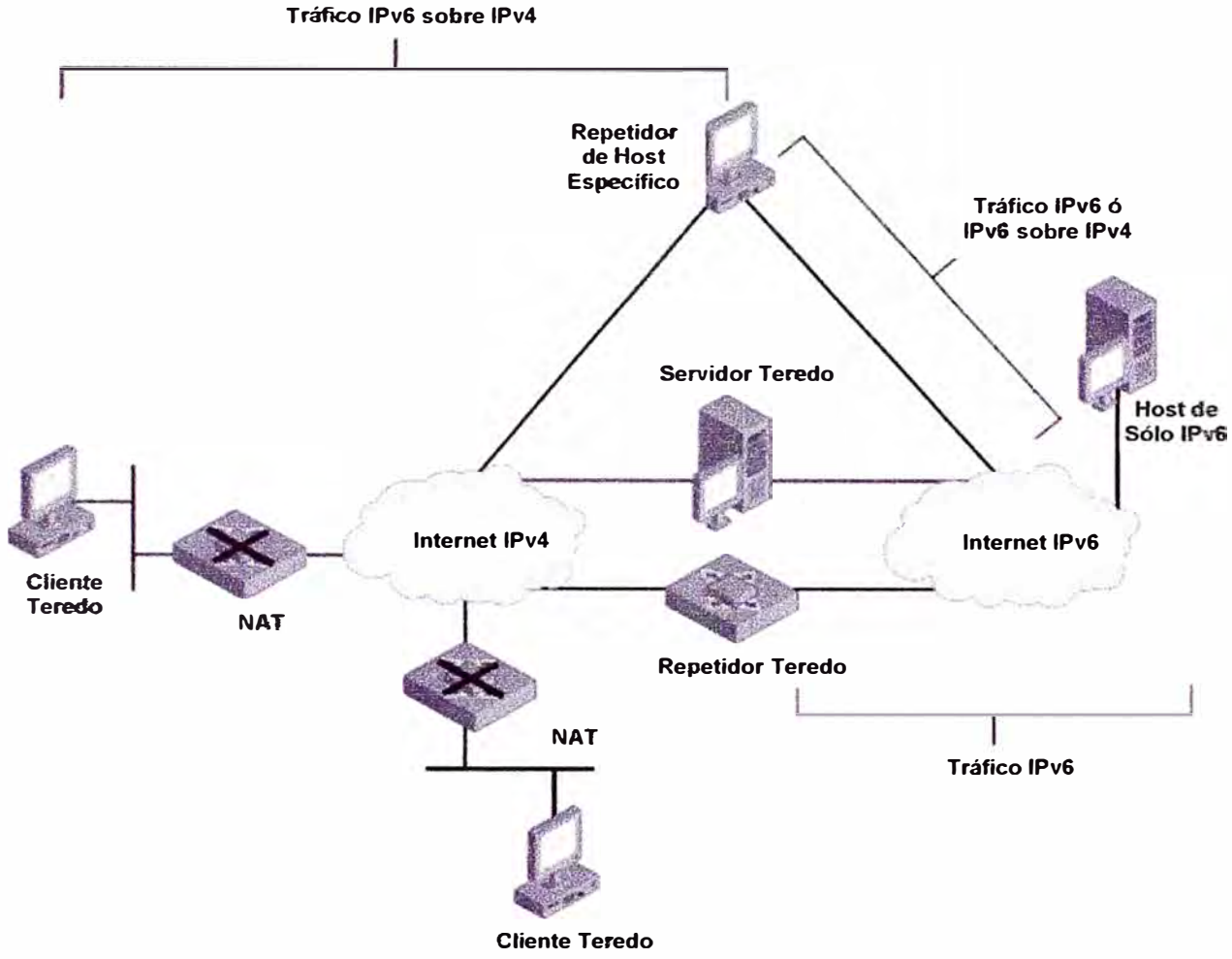

Fig.3.19 Componentes de la Infraestructura Teredo

3.7.3 Direccionamiento Teredo

Las direcciones Teredo tienen el formato mostrado en la Fig.3.20.

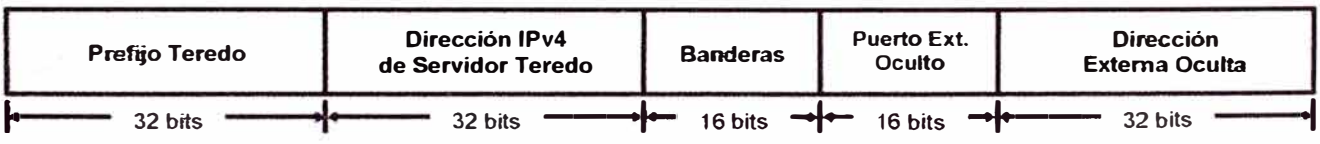

Fig.3.20 Formato de una Dirección Teredo

Una dirección Teredo consiste en lo siguiente:

Prefijo Teredo. Conforma los primeros 32 bits y es el mismo para todas las direcciones Teredo. Este prefijo Teredo que está definido en la *RFC 4380* es *2001::/32* y es el prefijo usado en *Windows Server 2008* y *Windows 7*. *Windows Server 2003* y *Windows XP* inicialmente usarán el prefijo Teredo *3FFE:831F::/32*.

Dirección IPv4 de Servidor Teredo. Los siguientes 32 bits contienen la dirección pública IPv4 del servidor Teredo que ayuda a configurar esta dirección Teredo.

Banderas. Los siguientes 16 bits están reservados para las banderas Teredo. La *RFC 4380* define el bit de orden alto como la bandera de cono. Esta bandera es configurada cuando un cliente Teredo está tras un NAT de cono. La determinación para saber si un NAT conectado a Internet es un NAT de cono ocurre durante la configuración inicial de un cliente Teredo.

Puerto Externo Oculto. Los siguientes 16 bits almacenan una versión oculta del puerto externo UDP correspondiente a todo el tráfico Teredo para sus clientes Teredo. Cuando el cliente Teredo envía su paquete inicial al servidor Teredo, el puerto de origen UDP del paquete es mapeado por NAT a un puerto externo UDP diferente. El cliente Teredo mantiene este puerto mapeado a fin de que se quede en la tabla de traducción NAT. Por lo tanto, todo el tráfico Teredo para el host usa el mismo puerto externo UDP mapeado. El puerto externo UDP es determinado por el servidor Teredo desde el puerto de origen UDP del paquete entrante enviado inicialmente por el cliente Teredo y recibido por el mismo cliente.

El puerto externo es ocultado efectuando la operación *XOR* del puerto externo con *0xFFFF*. Por ejemplo, la versión oculta del puerto *5000* en formato hexadecimal es *EC77* (*5000 =0x1388, 0x1388 XOR 0xFFFF = 0xEC77*). Algunas NAT's tratan de traducir el número de puerto externo al número de puerto interno cuando el número de puerto externo está dentro de la carga útil. Ocultando el número de puerto externo, se impide que estos tipos de NAT traduzcan el puerto externo dentro de la dirección Teredo.

Dirección Externa Oculta. Los últimos 32 bits almacenan una versión oculta de la dirección externa IPv4 correspondiente a todo el tráfico Teredo para este cliente Teredo. Algo así como el puerto externo, cuando el cliente Teredo envía su paquete inicial a un servidor Teredo, la dirección de origen IPv4 es mapeado por NAT a una dirección externa (pública) diferente. El cliente Teredo mantiene esta dirección mapeada a fin de que sea almacenada en la tabla de traducción NAT. Por lo tanto, el tráfico Teredo para el host usa la misma dirección externa pública IPv4 mapeada. La dirección externa IPv4 es

determinada por el servidor Teredo desde la dirección de origen IPv4 del paquete entrante enviado inicialmente por el cliente Teredo y recibido por el mismo cliente.

La dirección externa es ocultada por la operación *XOR* de la dirección externa con *0xFFFFFFFF*. Por ejemplo, la versión oculta de la dirección pública IPv4 *131.107.0.1* en formato hexadecimal es *7C94:FFFE* (*131.107.0.1* = *0x836B0001*, *0x836B0001 XOR 0xFFFFFFFF* = *0x7C94FFFE*). Algunas NAT's tratan de traducir la dirección externa a números de direcciones internas cuando la dirección externa está dentro de la carga útil. Ocultando la dirección externa, se impide que estos tipos de NAT traduzcan direcciones externas dentro de la dirección Teredo.

La Fig.3.21 muestra un ejemplo de una configuración Teredo con dos clientes Teredo. Un cliente Teredo está ubicado tras un NAT de cono (*Cliente A* Teredo) y otro tras un NAT restringido (*Cliente B* Teredo).

El *Cliente A* Teredo para estructurar su dirección Teredo utiliza lo siguiente:

Su servidor Teredo tiene la dirección pública IPv4 de *206.73.118.1*

Está detrás de un NAT de cono.

La dirección y puerto externo para el tráfico Teredo son *157.60.0.1*, puerto UDP *4096*.

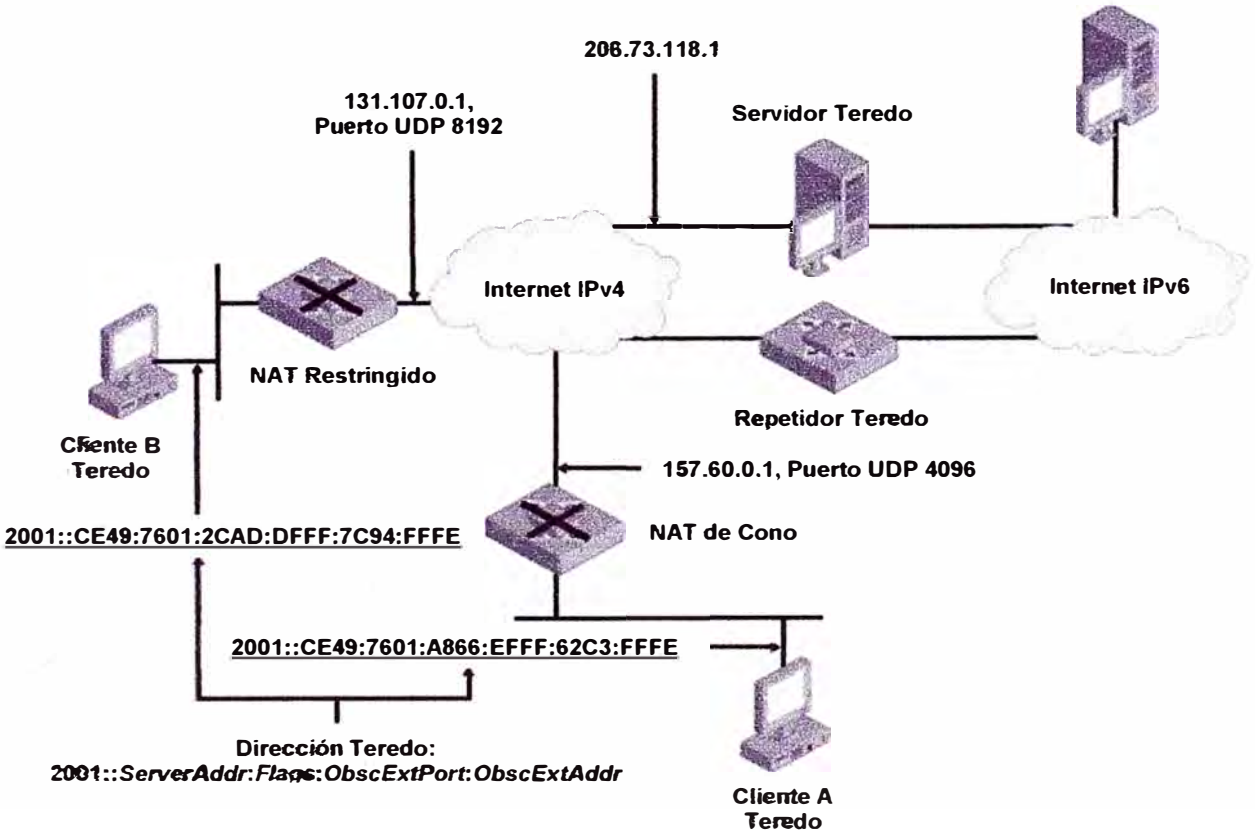

Fig.3.21 Ejemplo de Direccionamiento Teredo

Por lo tanto, usando el formato *2001::ServerAddr:Flags:ObscExtPort:ObscExtAddr* de dirección Teredo, el *Cliente A* Teredo deriva la siguiente dirección IPv6 *2001::CE49:7601:A866:EFFF:62C3:FFFE*. Esto se basa en lo siguiente:

2001::/32 es el prefijo Teredo.

CE49:7601 es la versión hexadecimal de *206.73.118.1*.

A866 es el campo de bandera en el que la bandera de cono está configurado a 1 (indicando que el *Cliente A* Teredo está ubicado tras un NAT de cono), las banderas *R*, *U* y *G* están configurados a 0; y los demás 12 bits están configurados por una secuencia aleatoria (*1010011100110*) para ayudar a impedir escaneos de dirección externa.

EFFF es la versión oculta del puerto UDP *4096*.

62C3:FFFE es la versión oculta de la dirección pública IPv4 *157.60.0.1*.

El *Cliente B* Teredo para estructurar su dirección Teredo utiliza lo siguiente:

Su servidor Teredo tiene la dirección pública IPv4 de *206.73.118.1*

Está detrás de un NAT restringido.

La dirección y el puerto externos para el tráfico Teredo son 131.107.0.1, puerto UDP *8192*.

Por lo tanto, el *Cliente B* Teredo deriva la siguiente dirección IPv6 *2001::CE49:7601:2CAD:DFFF:7C94:FFFE*.

Esto se basa en lo siguiente:

2001::/32 es el prefijo Teredo.

CE49:7601 es la versión hexadecimal de *206.73.118.1*.

2CAD es el campo de bandera en el que la bandera de cono está configurado a 0 (indicando que el *Cliente B* Teredo está ubicado tras un NAT restringido), las banderas *R*, *U* y *G* están configurados a 0; y los demás 12 bits están configurados por una secuencia aleatoria (*1011101010110*) para ayudar a impedir escaneos de dirección externa.

DFFF es la versión oculta del puerto UDP *8192*.

7C94:FFFE es la versión oculta de la dirección pública IPv4 *131.107.0.1*

La direcciones Teredo son asignadas sólo a clientes Teredo. Los servidores Teredo, repetidores Teredo y repetidores de host específicos Teredo no tienen una dirección Teredo asignada.

3.7.4 El Paquete de datos Teredo

Formato del Paquete de datos Teredo. La Fig.3.22, muestra el formato de datos del paquete Teredo definido en la *RFC 4380*.

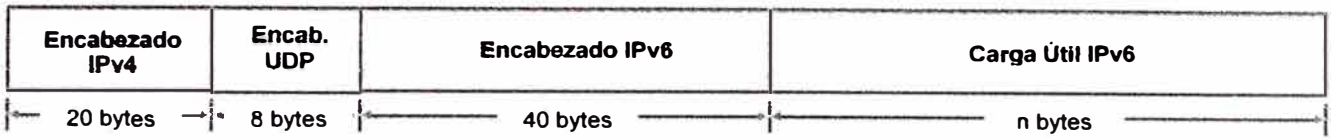

Fig.3.22 Formato del Paquete de Datos Teredo

Un paquete Teredo consta de:

Un Encabezado IPv4 conteniendo las direcciones IPv4 de origen y destino correspondientes a los extremos del túnel automático y puede ser traducido por un NAT.

Un Encabezado UDP que contiene los puertos UDP de origen y destino para el tráfico Teredo y puede ser traducido por un NAT.

Un Encabezado IPv6 que contiene las direcciones IPv6 de origen y destino, de las cuales al menos una es una dirección Teredo.

La Carga Útil IPv6 que contiene varios encabezados IPv6 de extensión o ninguno y al PDU (*Protocol Data Unit*) de nivel superior del paquete IPv6 encapsulado.

Paquetes de burbujas Teredo. Un paquete de burbuja es enviado para crear o mantener un mapeo NAT y consiste de un encabezado IPv6 sin carga útil IPv6. La Fig.3.23, muestra el paquete de burbuja Teredo.

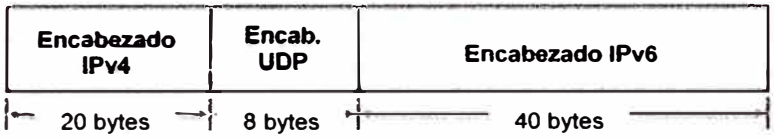

Fig.3.23 Paquete de Burbuja Teredo

En el encabezado IPv6, el campo de *Siguiente Encabezado* es configurado a *59*, indicando que no hay carga útil presente.

Indicadores Teredo. Teredo usa dos indicadores diferentes definidos en la *RFC 4380*, el indicador de *Autenticación* y el indicador de *Origen*, cuyos encabezados son usados para contener autenticación o información de dirección o puerto.

Indicador de Autenticación. Este indicador es usado para proteger el intercambio de mensajes de routers entre un cliente Teredo y un servidor Teredo. Ambos (servidor y cliente) están configurados con un código secreto, el cual se usa para estructurar la autenticación de datos en el Indicador de Autenticación. Este indicador está ubicado entre el encabezado UDP y el paquete IPv6.

Indicador de Origen. Este indicador se usa para indicar una dirección pública IPv4 y un número de puerto UDP de en cliente Teredo, repetidor Teredo o un repetidor de host específico Teredo. Un ejemplo es cuando un servidor Teredo envía un mensaje de anuncio del router en respuesta al mensaje de solicitud del router del cliente Teredo. En este caso, el indicador de Origen contiene la dirección externa IPv4 (pública) y número de puerto correspondiente al tráfico Teredo de un cliente Teredo.

3.7.5 Enrutamiento Teredo

La Fig.3.24, muestra las rutas que existen para habilitar la accesibilidad entre hosts Teredo, servidores Teredo, repetidores Teredo, repetidores de host específico Teredo y host de sólo IPv6.

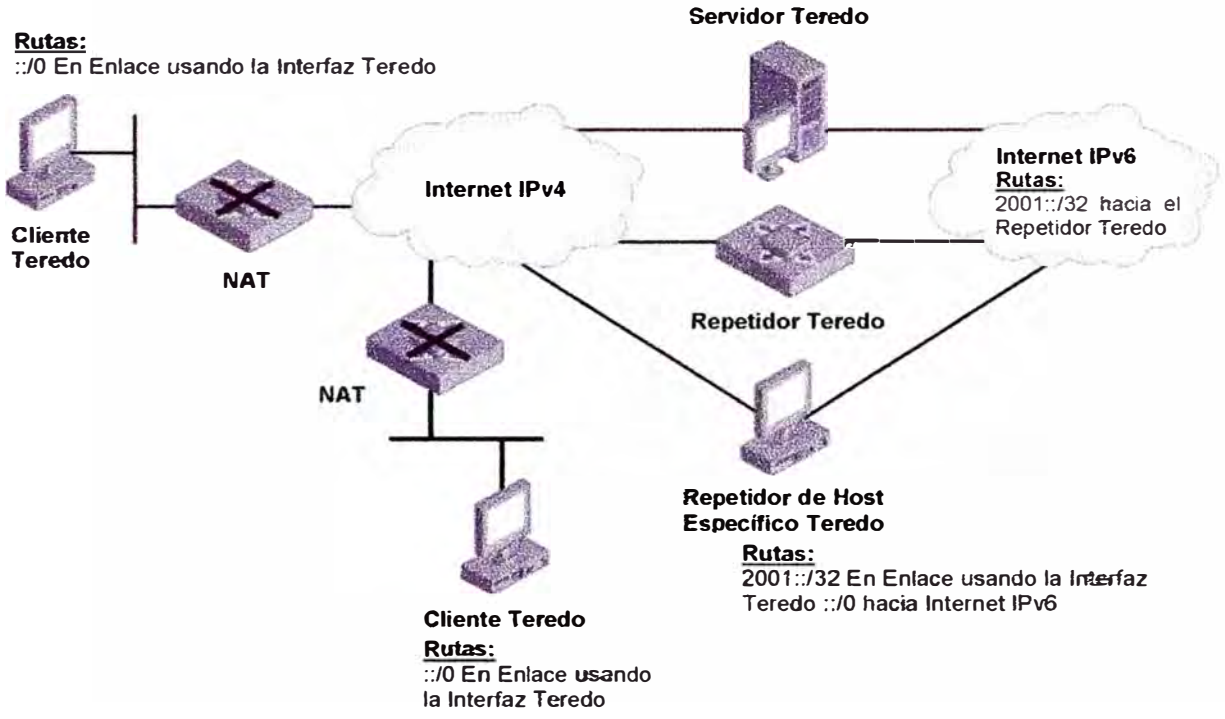

Fig.3.24 Rutas Teredo

En Internet IPv6, las rutas *2001::/32* de la infraestructura de enrutamiento se usan para reenviar paquetes usando el prefijo Teredo al repetidor Teredo más cercano.

Los servidores Teredo, repetidores Teredo y repetidores de host específico Teredo tienen una ruta *2001:: 32*, la cual considera todas las direcciones que usan el prefijo como en enlace usando la interfaz de túnel Teredo. Esta interfaz, es una interfaz lógica que realiza la encapsulación automática de IPv4 y UDP para los paquetes reenviados.

Los servidores Teredo, repetidores Teredo y repetidores de host específico Teredo tienen además, una ruta por defecto (*::/0*) que apunta a Internet IPv6. Por lo general, esta ruta por defecto contiene una dirección IPv6 de siguiente salto de un router vecino en Internet IPv6 usando una interfaz física que está conectada a Internet IPv6.

3.8 Planeamiento de la Implementación IPv6

Es importante describir que para implementar una red IPv6 no es necesario que se haga una conversión de una red de sólo IPv4 a sólo IPv6, sino que se planifique del mejor modo posible las ventajas que se tienen con la nueva estructura de red IPv6 ya que por muchos años más y tal vez siempre, existan redes IPv6 que coexistan con IPv4.

Cuando se implementa IPv6, se deberá considerar lo siguiente como parte del planeamiento:

Plataforma que soporte IPv6. En el caso de Microsoft, se ha implementado el soporte de protocolo IPv6 en las siguientes plataformas: *Windows 7*, *Windows Server 2008*, *Windows Vista*, *Windows Server 2003*, *Windows XP SP1* o superior.

También existen otras plataformas con soporte al protocolo IPv6 como son: *Unix Solaris 10*, *Linux Debian*, *RedHat*, *Mandriva*, *Fedora Core*, *Ubuntu* y otras dostribuciones.

Aplicaciones que soporten IPv6. Aunque casi todas las aplicaciones en las últimas versiones de *Windows* soportan IPv6, esto dependerá de la forma en que los desarrolladores y programadores estructuren cada vez más nuevas aplicaciones que puedan ejecutarse en plataformas con soporte para IPv6.

Direccionamiento unicast IPv6. Se deberá determinar cómo enumerar las subredes individuales de una organización. El direccionamiento de subredes para IPv6 es mucho más sencillo que IPv4, debido a la longitud del prefijo de 64 bits para redes LAN y la abundancia relativa del espacio de direcciones para las organizaciones.

Conectividad IPv6 basada en túneles. Se puede usar cualquiera de los siguientes métodos: ISATAP, 6to4, Teredo o Túneles Configurados manualmente.

Conectividad nativa IPv6. La conectividad nativa IPv6 consiste de las siguientes capacidades: Enrutamiento Unicast (el cual es requerido) y Enrutamiento Multicast (el cual es opcional).

Resolución de nombre con DNS. Se debe asegurar que la infraestructura DNS soporte lo siguiente:

Registros *AAAA* para direcciones IPv6.

Actualizaciones dinámicas DNS a fin de que los hosts IPv6 puedan registrar automáticamente registros *AAAA*.

Registros *PTR* en el dominio reverso de *IP6.ARPA*.

Actualizaciones dinámicas DNS a fin de que los hosts IPv6 puedan registrar automáticamente registros *PTR*.

Servicio DHCPv6. Al usar DHCPv6 se debe considerar lo siguiente:

Usar DHCPv6 en subredes *Apto para IPv6* sólo cuando el camino de enrutamiento entre el agente repetidor DHCPv6 en la subred y el servidor DHCPv6 soporten el reenvío de tráfico IPv6.

Se deberá determinar si los hosts IPv6 en la parte de *Apto para IPv6* de la Intranet usarán direcciones estáticas o no.

Se deberá poder configurar los routers IPv6 con los valores de bandera apropiados.

Se deberá configurar un agente repetidor DHCPv6 para cada subred IPv6 y configurar dicho agente con direcciones IPv6 de los servidores DHCPv6.

Se deberá determinar la ubicación y configuración de los servidores DHCPv6.

Seguridad basada en Host y Tráfico IPv6. La seguridad deberá basarse en:

Proteger paquetes IPv6.

Protección de hosts de posibles ataques o escaneos.

Control del tipo de tráfico que se intercambia en Internet, usando firewalls basados en routers o en hosts.

Entrega priorizada de tráfico IPv6. La prioridad en la administración del tráfico enviado debe basarse en las siguientes condiciones:

Aplicación que es enviada.

Direcciones IPv6 de origen o destino.

Protocolos (TCP, UDP o ambos).

Puertos de origen o destino (TCP o UDP).

Políticas adecuadas en la calidad del servicio (QoS).

3.9 Implementación de IPv6

La implementación de la conectividad IPv6 en una Intranet IPv4 puede constar de los siguientes pasos:

Configuración de una red IPv6 de prueba. Para crear una red de prueba IPv6, se debe considerar lo siguiente: Crear conectividad funcionando IPv4, configurar la conectividad IPv6 una vez hecho el túnel basado en ISATAP, configurar la conectividad basada en IPv6

nativa, usar resolución de nombres para direcciones IPv6, configurar una Infraestructura de Sólo IPv6.

Iniciar la migración de aplicaciones. Para migrar las aplicaciones usadas en una Intranet para el soporte de IPv6, se debe hacer lo siguiente: Inventariar las aplicaciones y proyectar el trabajo y planificar la migración de la aplicación.

Configurar DNS para que soporte registros AAAA y actualizaciones dinámicas. Lo cual consiste en configurar, actualizar o mejorar los servidores DNS para que soporten registros *AAAA* en IPv6 y actualizaciones dinámicas para esos registros en los dominios apropiados. Opcionalmente, se puede aplicar lo mismo para que soporten registros *PTR*.

Implementar una Infraestructura de Túnel IPv6 con ISATAP. Para permitir que los hosts IPv6/IPv4 se comuniquen sin una infraestructura de enrutamiento nativo IPv6, implementar una infraestructura ISATAP consiste de prefijos de subred lógicos ISATAP, la enumeración apropiada de routers ISATAP (al menos una para cada subred lógica ISATAP) y registros *A* DNS para el nombre "ISATAP" en los dominios apropiados a fin de que los hosts ISATAP puedan determinar la ubicación de routers ISATAP.

Mejorar Hosts de Sólo IPv4 a Sólo IPv6. Para esto se debe hacer lo siguiente: Instalar la versión 6 del protocolo TCP/IP usando los comandos adecuados dependiendo de la plataforma a utilizar y actualizar los sistemas antiguos con versiones actuales. (Ya que las actuales vienen con soporte para IPv6 en forma predeterminada).

Empezar con la Implementación de una Infraestructura nativa IPv6. Determinar cuándo iniciar con la implementación IPv6 depende del departamento IT de una organización y ver que esté listo para poder manipular operaciones y administrar una red dual con soporte tanto para IPv4 como para IPv6 y que se requiera usar el tráfico nativo IPv6 para las aplicaciones.

Además, se deberá tomar en cuenta lo siguiente: Habilitar el reenvío de multicast IPv6, configurar y habilitar el protocolo IPv6 de enrutamiento multicast escogido, configurar servidores DHCPv6 y la configuración de routers IPv6 con los valores apropiados de bandera.

Conectar partes de la Intranet sobre Internet IPv4 e IPv6. Para conectar diferentes partes de una Intranet por medio de Internet IPv4, se puede configurar lo siguiente: 6to4 con protección IPSec del tráfico que hizo túnel 6to4, conexiones VPN (*Virtual Private Network*) de sitio a sitio. Para conectar diferentes partes de una Intranet por medio de Internet IPv6, se puede usar incluso conexiones VPN de sitio a sitio.

CAPÍTULO IV

INTEGRACIÓN DE REDES IPV6 EN EL PERÚ

Las redes actuales se interconectan cada vez más con una mayor cantidad de nodos que se expanden alrededor del mundo por medio de una troncal principal que es la base de desarrollo tecnológico basado en Internet en cada país y viene desarrollándose año tras años con el esfuerzo de estudiantes, técnicos y profesionales involucrados en el tema de tecnologías de información y gracias a las nuevas aplicaciones con soporte a nuevos y sofisticados dispositivos que mejoran la calidad de vida y simplifican acciones tanto en la labor diaria como en el trabajo de cada persona en el mundo. En la red global de Internet IPv6 existen muchas otras subredes que se conectan entre sí para intercambiar varios tipos de información. Las principales redes nacieron con el objetivo de realizar proyectos de investigación y se propagaron con buenos resultados hasta la actualidad.

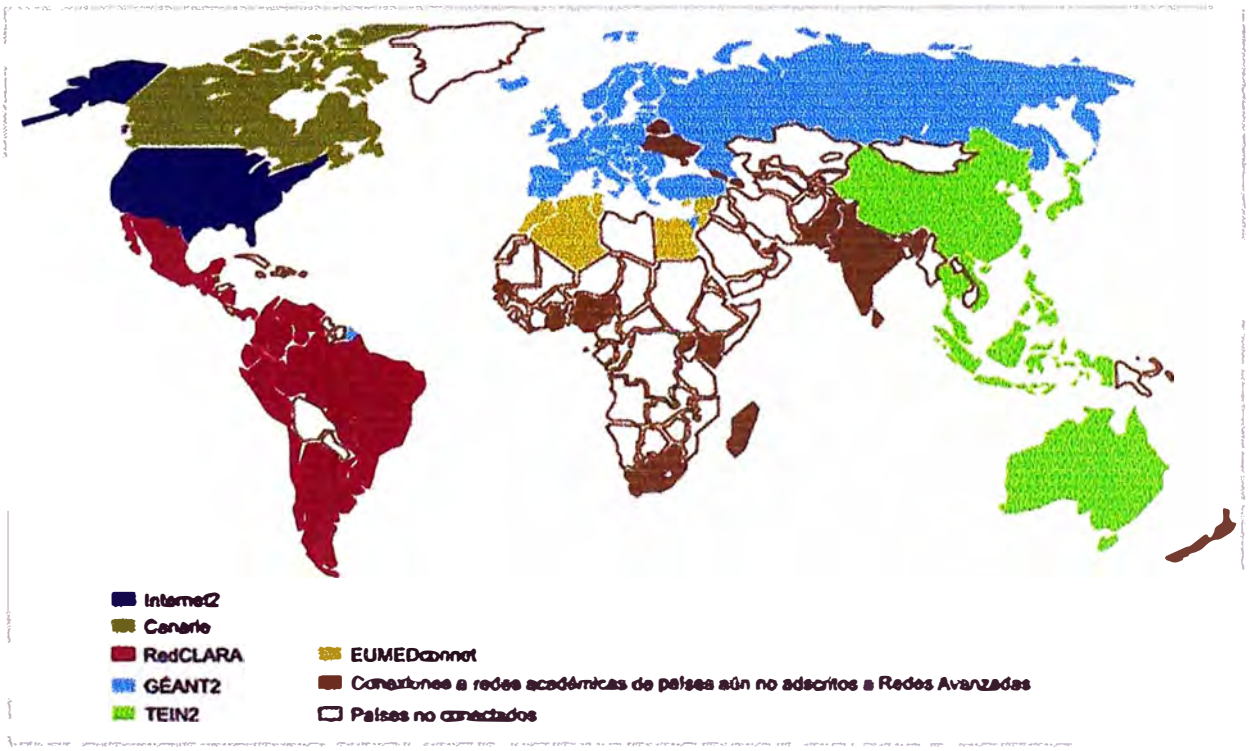

Fig.4.1 Redes Avanzadas en el mundo

4.1 IPv6 en el Mundo actual

La agrupación de redes para el desarrollo e implementación de IPv6 se sustentan en el grupo de Redes Avanzadas, las cuales se ubican geográficamente en diversos puntos del planeta formando redes de índole nacional en cada país. Es por ello que nacen las Redes Nacionales de Investigación y Educación (NREN), las cuales integran consorcios que no son más redes mucho más grandes unidas en una gran troncal (backbone). Estas redes mayores, a su vez establecen asociaciones que les permiten interconectarse, permitiendo la interconexión global de las Redes Avanzadas: es el fin de las barreras para el desarrollo de la investigación, la ciencia, la educación y la innovación.

Dentro del grupo de redes avanzadas en el mundo, podemos mencionar los siguientes: Canadá, CANARIE: Canada's Advanced Research and Innovation Network, EE.UU., Internet2, América Latina, Consorcio CLARA, red: RedCLARA, Asia-Pacífico, APAN, TEIN2: Trans-Eurasia Information Network, Sudáfrica, TENET , TERENA: Trans-European Research and Education Networking Association, GÉANT2, EUMEDCONNECT.

4.2 Red Avanzada CLARA

La red global conecta a todos los puntos en el planeta, es así que en Latinoamérica se cuenta con varios nodos de conexión hacia las principales redes implementadas ya con IPv6 y que comparten nodos junto a IPv4 usando las diferentes tecnologías de transición.

Como principal proyecto de implementación de redes IPv6 en Latinoamérica, se cuenta con la Cooperación Latinoamericana de Redes Avanzadas (CLARA), la cual tiene como nodos principales de acceso a los países de Chile y Brasil en Sudamérica, México y Panamá en Centroamérica; y a través de ellos, la interconectividad con España y Estados Unidos.

4.2.1 Descripción Técnica de CLARA

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

La troncal (*backbone*) de RedCLARA está compuesta por nueve nodos enrutadores principales, conectados en una topología punto-a-punto. Cada nodo principal representa a un PoP (Punto de Presencia) para RedCLARA, ocho de ellos están ubicados en un país de América Latina -São Paulo (SAO - Brasil), Buenos Aires (BUE - Argentina), Santiago (SCL - Chile), Lima (LIM - Perú), Guayaquil (GYE - Ecuador), Bogotá (BOG - Colombia), Panamá (PTY - Panamá) y Tijuana (TIJ - México)- y el noveno, en Miami

(MIA - Estados Unidos). La Fig.4.2, muestra la topología de red CLARA hasta marzo de 2010.

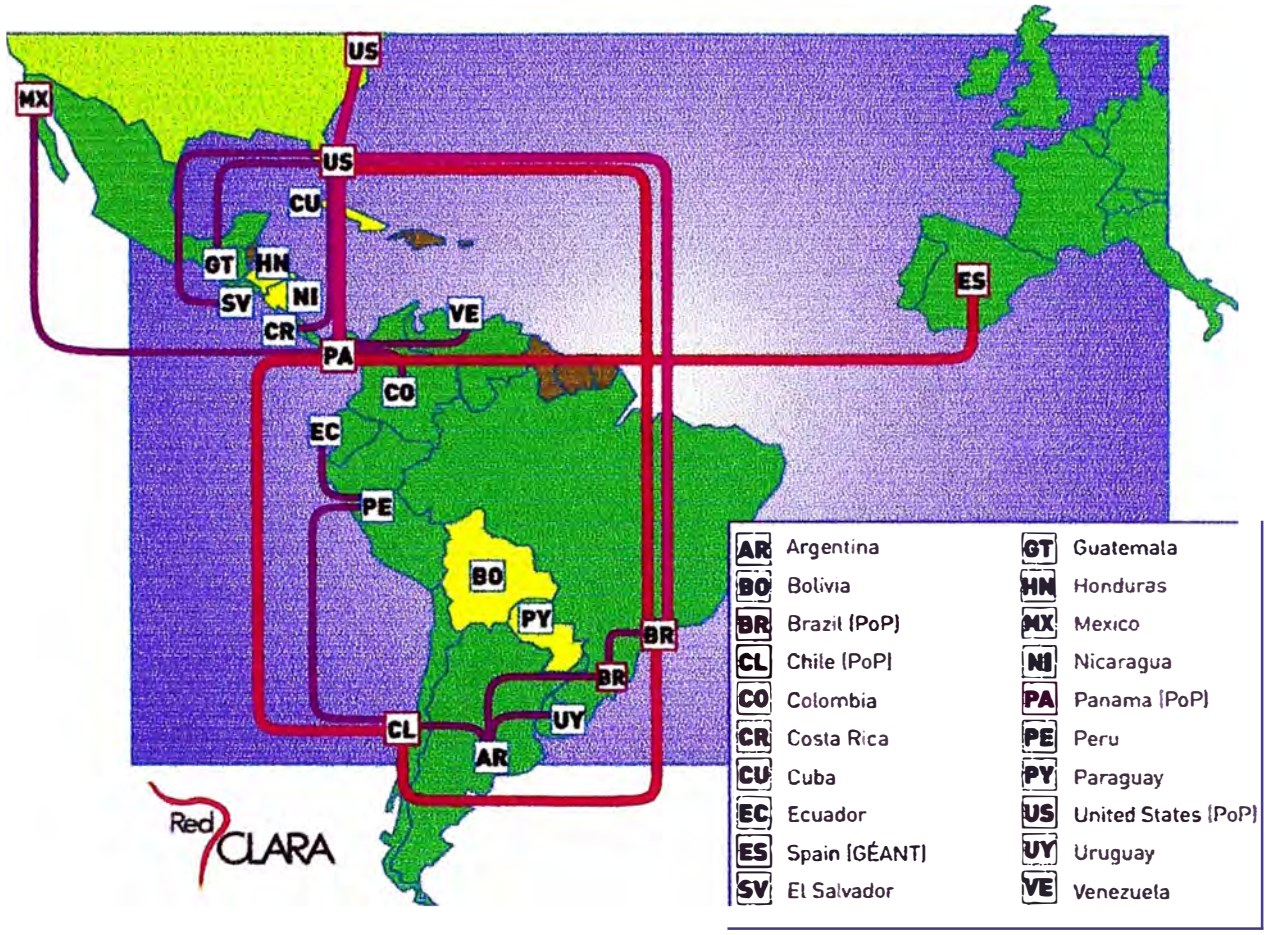

Fig.4.2 Topología de red CLARA actual

La Fig.4.3, muestra la troncal de la red CLARA y las actuales redes avanzadas interconectadas en Latinoamérica hasta junio de 2008. Todas las conexiones de las redes nacionales latinoamericanas NREN a red CLARA son a través de uno de estos nueve nodos. La troncal de red CLARA está interconectada con la red paneuropea GÉANT2 a través del enlace del PoP de CLARA en SAO con el punto de acceso de GÉANT2 en Madrid (España - ES), posibilitado por el Proyecto ALICE (finalizado en marzo de 2008), y, con Estados Unidos, mediante los enlaces establecidos en los PoP de CLARA en SAO y TIJ, el primero con el PoP de *AtlanticWave* y el segundo con el PoP de *PacificWave*, estos dos últimos accesos son posibilitados por WHREN-LILA.

Cuando una NREN latinoamericana hace conexión con RedCLARA, lo hace a través de uno de los nueve nodos de la troncal de RedCLARA; esta conexión le brinda a estas

NREN y a sus miembros (clientes), acceso a RedCLARA, otorgándoles un Punto de Intercambio.

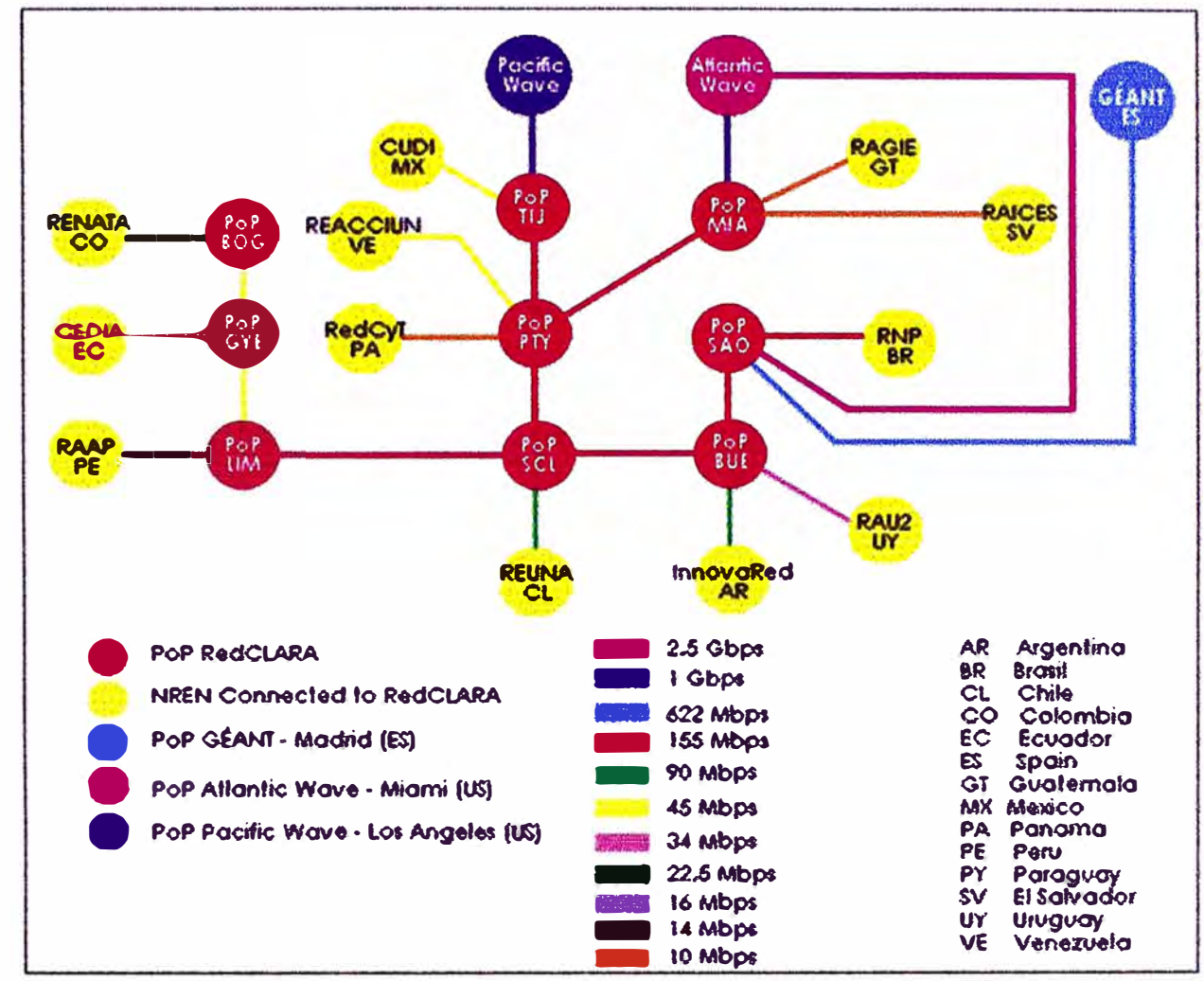

Fig.4.3 Troncal de RedCLARA y actuales NREN latinoamericanas

Servicios de Red CLARA. Esta red tiene varios grupos de trabajo que brindan servicios en tecnologías basados en: Multicast IPv6, Disponibilidad de Ancho de Banda (QoS), Mediciones, Servicios específicos para proyectos: Mallas Computacionales (Grids), Videoconferencia, Voz sobre IP, Seguridad, Enrutamiento avanzado, Capacitación, entre otros.

Ingeniería de Tráfico. Uso de Ingeniería de Tráfico MPLS en la troncal.

Las aplicaciones sensitivas al retardo podrían "indicar" a la red su requerimiento por una vía diferente.

Los túneles definidos manualmente deberían prevalecer por sobre la decisión normal de proceso de enrutamiento IGP.

4.2.2 Países Interconectados

A la fecha se encuentran conectadas a RedCLARA las redes nacionales de investigación y educación (NREN) de: Argentina, Brasil, Chile, Colombia, Ecuador, El Salvador, Guatemala, México, Panamá, Perú, Uruguay, Venezuela. En las metas futuras de conexión a RedCLARA se encuentran: Bolivia, Costa Rica, Cuba, Honduras, Nicaragua y Paraguay.

Algunos de los participantes de la red CLARA son: RETINA, UBA, UTN, Argentina; RNP, Brasil; UniCauca, UniPamplona, Colombia; Grupo de trabajo IPv6,Cuba; REUNA, UACH, Chile; ITAM, UNAM, UDG, ULSA, México; RAU, Uruguay; RAAP, Perú.

4.2.3 Conexiones al resto del mundo

Gracias a Red CLARA y a su conexión a la red paneuropea GÉANT2, América Latina se conecta con Europa a 622 Mbps a través de la conexión entre São Paulo (Brasil) y Madrid (España). A través de los enlaces que posee GÉANT2 con TEIN2 (*Trans-Eurasia Information Network*) y EUMEDCONNECT, RedCLARA accede también a la zona Asia-Pacífico y a la cuenca Mediterránea, respectivamente.

Gracias al proyecto WHREN-LILA, RedCLARA se conecta también con Estados Unidos, lo que se lleva a cabo mediante los enlaces del nodo de Tijuana (México) con San Diego (Costa Pacífico de EE.UU.) y del de São Paulo con Miami. Cabe destacar que el enlace establecido con San Diego, permite a RedCLARA acceder a las conexiones hacia el Asia-Pacífico, donde, además, CLARA posee calidad de miembro asociado de APAN, la Red Avanzada del Asia-Pacífico.

4.2.4 Iniciativas de conexión

WHREN-LILA (*Western Hemisphere Research and Education Network Linking Latin America*).

Este proyecto fue fundado en 2005 con el financiamiento de la Fundación Nacional (NSF) de Ciencias de los Estados Unidos (Award #OCI-0441095) y el Proyecto Fapesp nº 04/14414-2 de la Red Académica de São Paulo (ANSP).

WHREN-LILA establece un enlace de Fibra Oscura entre Tijuana (MX) y San Diego (US) que permite conectar el Nodo RedCLARA entre Tijuana con CENIC (*Corporation for Education Network Initiatives of California*), y además un enlace de 1,2 Gbps vía LAN Nautilus entre São Paulo y el Nodo de Miami del Proyecto.

Existen dos conexiones de WHREN/LILA:

PW (PacificWave). Es un proyecto conjunto entre CENIC y PNWGP (*Pacific Northwest Gigapop*), el cual es operado con la colaboración de la Universidad del Sur de California y la Universidad de Washington. A la fecha cuenta con una treintena de miembros y CLARA forma parte de la lista.

CLARA se une a PW mediante uno de sus tres nodos que están ubicados en Los Ángeles, California, a una velocidad de 1GbE (Gigabit Ethernet).

AW (AtlanticWave). Es una red de investigación internacional distribuida, un punto de intercambio y conexión que se extiende por la costa atlántica de Norte y Sudamérica. Su objetivo principal es la de facilitar las colaboraciones en investigación y educación entre las instituciones estadounidenses y latinoamericanas.

AW fue lanzada oficialmente en noviembre de 2006 por la Asociación de Investigación Universitaria del Sudeste (SURA) junto a un grupo de organizaciones sin fines de lucro que colaboran con la iniciativa, con el objetivo de mejorar la colaboración en la investigación internacional. Para la comunidad CLARA, la conexión a AW, sumada a las ya establecidas conexiones con PacificWave y, claro, con GÉANT2 en Europa, amplía enormemente la capacidad de la red y lo que las redes nacionales conectadas a RedCLARA pueden obtener de estas conexiones es un nuevo horizonte para sus proyectos colaborativos y el desarrollo de sus aplicaciones.

4.3 La red IPv6 actual en el Perú

En el Perú, tenemos la red Red Académica Peruana (RAAP) la cual está conectada a las demás redes que integran las NREN's.

4.3.1 Características de RAAP

RAAP es una red de comunicaciones implementada en IPv6, tiene arquitectura abierta con soporte multiprotocolo y permite usar servicios de banda ancha. Uno de sus objetivos es mantener una independencia de conexión con la red Internet IPv4 actual la cual está orientada al ámbito comercial.

La presentación oficial de la RAAP se dio el 29 de septiembre de 2005 en el campus universitario de la PUCP.

La arquitectura de red integrará las universidades e institutos de investigación del país en una sola red, además de poder interconectar otro tipo de instituciones tales como del sector salud, centros educativos, bibliotecas y todo aquello que implique desarrollo y mejore así la calidad educativa en nuestro país.

Esta red usa actualmente nuevos protocolos y arquitecturas de red IPV6 garantizando así una adecuada calidad de servicio en las nuevas aplicaciones de +D y permitiendo la creación de redes privadas virtuales (VPN) para utilizarlas en de grupos de investigación y desarrollo.

RAAP es el Nodo Nacional que nos brinda acceso a toda la comunidad académica y de investigación nacional independientemente de los proveedores actuales de Internet.
Actualmente, la arquitectura de red está conformada por una red IP VPN a nivel nacional, con un Nodo Principal.

El Nodo Principal, tiene comunicación hacia redes internacionales de investigación basada en IPv6. El Nodo Principal, también enrutará el tráfico de datos provenientes de Ecuador y Colombia; según el proyecto CLARA, hacia las redes basadas en IPv6.

Los routers implementados, tienen la capacidad de enrutar tráficos de paquetes tanto de IPv4 como de IPv6, así como voz y video sobre ambos protocolos IP.

4.3.2 Aplicaciones soportadas

Todas las aplicaciones que corren y correrán sobre la RAAP son aplicaciones orientadas a la colaboración entre personas y a accesos interactivos a información y herramientas, imposibles hoy de realizar; al menos eficientemente, con la Internet actual.

Todas son aplicaciones que requieren de algo más: de redes avanzadas soportadas por tecnologías de última generación; ya disponibles (la RAAP es un ejemplo), que permiten entre otros aspectos contar con mayores anchos de banda, multicasting, calidad superior de transmisión y recepción, etc.

Los campos de aplicación afectados abarcan prácticamente todas las disciplinas que podemos tener en la educación superior: ciencias, artes y humanidades.

La necesidad de estas redes avanzadas de alto rendimiento, ha propiciado el desarrollo de tecnologías, entre las que destaca el IPv6 (usado por la RAAP).

Entre los campos susceptibles de ser afectados con las múltiples aplicaciones factibles de llevar a cabo con el auxilio de las redes avanzadas de comunicación, podemos citar los siguientes:

Manejo a distancia de instrumentos de gran capacidad , por ejemplo, el uso desde el hemisferio sur, de telescopios o microscopios de enorme potencia instalados en el hemisferio norte, o viceversa.

Conferencias a distancia con oyentes activos situados en diversas latitudes, compartiendo gráficos, videos; con comunicación en tiempo real y calidad de TV.

Edificios inteligentes: encender las luces y poner algo de música en el equipo de casa, o encender la licuadora a la 6:30 p.m. para ahuyentar a cualquier amigo de lo ajeno. Esto no es una noticia, salvo por el hecho de hacerlo desde una notebook, desde cualquier parte del mundo, mientras movemos las cámaras de seguridad instaladas en la casa, para ver en tiempo real, que todo vaya bien.

Mecanismos de colaboración para investigadores, docentes y estudiantes en línea y distribuido en diversas partes del mundo, con posibilidad de acceder concurrentemente a gráficos, videos, forums, etc.

Acceso a bibliotecas multimedia disponibles en cualquier parte del mundo.

Visualización de datos en 3 dimensiones : aplicaciones de telemedicina basadas en holografías de alta calidad. Estado del tiempo en línea.

Simulaciones con grandes cantidades de datos descentralizados y utilizando software compartido.

Video bajo demanda .

Teleaudiciones. Clases de música a distancia.

Seguridad, movilidad (en el sentido de la autoconfiguración), etc.

Telemedicina y Salud: Cardiología, radiología, telepatología, Diagnóstico a distancia. Aplicaciones en tiempo real en cualquier lugar del mundo con acceso transparente personalizado y seguro a: bases de datos, instrumentos de alto costo y sistemas computacionales avanzados.

Astronomía : Radioastronomía (VLBI), grids de observatorios.

Geografía : Sistemas de información geográfica. Intercambio seguro y rápido de grandes volúmenes de información.

Tecnología de Redes de Telecomunicaciones : Multicast, Voz sobre IP, Ipv6.

Ciencias de la tierra : Oceanografía, meteorología.

Instrumentación remota : Robótica, nanotecnología, microscopía, excavaciones remotas computarizadas.

Visualización : realidad virtual, anatomía digital.

Teleinmersión , Super cómputo compartido, Bibliotecas Digitales.

4.3.3 Integrantes

Conformada inicialmente por las siguientes instituciones:

Universidad Nacional Mayor de San Marcos (UNMSM)

Universidad Nacional de Ingeniería (UNI)

Universidad Peruana Cayetano Heredia (UPCH)

Universidad Nacional Agraria La Molina (UNALM)

Pontificia Universidad Católica del Perú (PUCP)

Instituto Peruano de Energía Nuclear (IPEN)

Instituto Nacional de Investigación y Capacitación en Comunicaciones (INICTEL)

4.4 Fabricantes de equipos IPv6

Entre los principales fabricantes de equipos, se puede mencionar:

Cisco Systems. Implementa los principales mecanismos de transición IPv6 como parte de su solución, tales como efecto de túnel y pila doble. Cisco ha estado activo en la definición e implementación de la arquitectura IPv6 dentro de la IETF (*Internet Engineering Task Force*), además es miembro fundador del Forum IPv6.

Juniper Networks. Es un proveedor de routers para proveedores de servicios de internet. Incluye características fundamentales IPv6 como soporte de tipos de direcciones IPv6, sistemas de autoconfiguración, protocolo ND (Neighbor Discovery), ICMPv6 y un número de mecanismos de transición incluyendo túneles configurados y pila doble.

Alcatel-Lucent. Es otro proveedor de routers e incluye características en sus equipos tales como arquitectura de direccionamiento IPv6, autoconfiguración de direcciones, ND, ICMPv6, OSPF y BGP-4 (extensiones de enrutamiento para IPv6) y mecanismos de transición 6to4.

4.5 Proveedores de servicios IPv6

Dentro de los proveedores de servicios de internet con soporte IPv6 y de mayor envergadura en el mundo, podemos mencionar a los siguientes:

Norteamérica

Moonv6. Proyecto grande de red basado en IPv6 y está tomando lugar en varios sitios en EE.UU. y juega un papel importante en asegurar la interoperatividad y los objetivos de migración han sido identificados y demostrados.

AT&T. es un participante del proyecto Moonv6. AT&T ofrece un acceso mucho más ancho de Internet IPv6 usando tecnologías de túneles o superposición de redes para el soporte de IPv6 nativo. Además ha establecido interconexiones de red con otros proveedores del backbone IP como Global Crossing, permitiendo así, el intercambio de tráfico IPv6 a través de muchas otras redes. Dentro del rango de servicios ofrecidos por AT&T podemos mencionar: Conectividad IPv6 implementado sobre múltiples servicios como PPP, Frame

Relay y ATM; y servicios de acceso remoto o satelital creando túneles para soportar tráfico IPv6 sobre IPv4.

Global Crossing. Tiene instalado IPv6 en forma nativa en todos sus routers de acceso a servicios de Internet. IPv6 está habilitado en los servicios de transporte basados en IPv6 que provee el backbone IP de Global Crossing bajo el nombre del producto de Acceso de Internet Dedicado y VPN IP. Este acceso de internet dedicado es un servicio de acceso a internet escalable provisionado directamente en el backbone de red basado en fibra óptica de Global Crossing. Este es un servicio habilitado desde 64Kbps hasta SONET/SDH OC-48/STM-16 y 10B-E, Fast Ethernet, Gigabit Ethernet (GigE).

Los servicios de acceso de pila doble se proveen para asistir a los usuarios en la etapa de transición hacia IPv6. Otras características relacionadas incluyen IPv4/IPv6 nativo sobre MPLS, direcciones IPv6 y DNS IPv6.

Europa

European Internet Exchange Association. Hay cientos de proveedores de servicios de internet en Europa y están relacionados en Puntos de Intercambio de Internet IXP (*Internet Exchange Points*)

BT-UK6x. Es un operador de intercambio de servicios de internet IPv6 y está ubicado en Londres. Dentro de los servicios que ofrece, incluyen: conexiones IPv6 nativas, conexiones IPv6 basado en túneles, alojamiento de direcciones, internetworking IPv4/IPv6. No sería económico, escalable o administrable que todos esos proveedores se conecten individualmente. Por esta razón existe una infraestructura de red física BT-UK6x a la que se pueden conectar todos los ISP.

Asia-Pacífico

Servicios Relacionados con IPv6 de la *NTT Communications*. Ofrece servicios de Gateway IPv6 con un ancho de banda máximo de 155Mbps, es cual también es ofrecido en Japón, Estados Unidos, Europa, Corea, Taiwan, Hong Kong, Australia, Malaysia and otros países. También ofrece servicios basados en túneles IPv6 ofrecido con una variedad de tecnología como Línea Dedicada, ISDN, ADSL y fibra óptica, servicio dual IPv4/IPv6, servicio multicast, servicios de conectividad de pila doble IPv6/IPv4 y acceso a Ethernet dual IPv6. La Fig.4.4, muestra la estructura del servicio dual IPv4/IPv6 de NNT Communications.

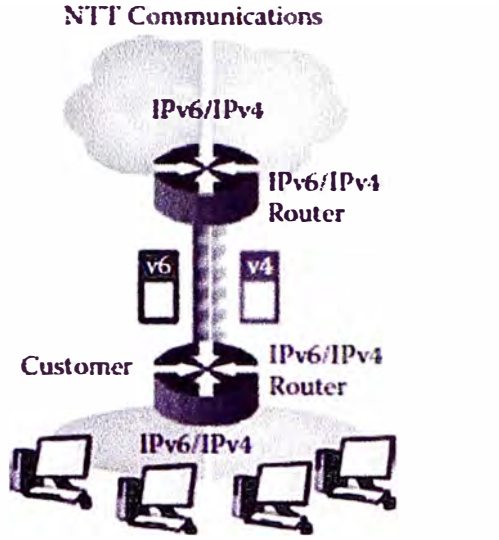

Fig.4.4 Servicio dual IPv4/IPv6 de NNT Communications

Laboratorio KDDI/KDDI. Servicio basado en IPv6 nativo a través de línea dedicada y ATM. También ofrece servicio IPv6 basado en túneles y de tecnología 6to4.

Japan Telecom. Ofrece servicios IPv6 basados en túneles, servicio Ipv6 nativo y servicios de pila doble.

4.6 Costos de Implementación

Para llevar a cabo una migración adecuada en un ambiente de servicios y soporte IT, habrá que tomar en cuenta los costos al menos en las siguientes áreas administrativas:

Formación del personal no técnico (usuarios) para la implementación de la nueva red en sus dispositivos.

Formación de personal técnico para la administración de IPv6 en las redes de la organización.

Actualización del software necesario incluyendo el Sistema Operativo.

Configuración de los dispositivos a nivel de Sistema Operativo para utilizar direcciones IPv6.

Configuración de software de los dispositivos que tengan que manejar varias VLAN.

Configuración de los diferentes Sistemas Operativos para administrar las preferencias entre IPv4 e IPv6 en caso de que el host de destino tenga ambas direcciones.

Configuración de las aplicaciones de red para que soporten ambos tipos de direccionamiento.

Administración de conmutadores Ethernet.

Administración de rutas IPv4 e IPv6 y anunciamiento de prefijos IPv6 (administración de routers).

Administración de reglas de filtrado IPv4 e IPv6.

Administración y soporte de firewalls Ipv4 e IPv6.

Actualización de los scripts de backup y mantenimiento del sistema.

Modificación y pruebas de los sistemas de gestión y configuración automáticas de computadoras.

Como es de notar, a nivel de sistema operativo no habrá costos adicionales, ya que lo soportan, sólo serán temas de actualización.

Los costos adicionales van a ser significativos de acuerdo a la arquitectura de red a implementar, en qué áreas y bajo qué condiciones; sin interrumpir el trabajo actual de las redes ya instaladas.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

La migración al protocolo IPv6, deja las siguientes conclusiones luego del análisis realizado.

El proceso de migración durará unos años más así que aún se seguirá usando redes IPv4 con la diferencia que deberán soportar desde ya, el nuevo protocolo porque la tendencia de la tecnología actual hace necesario el uso de IPv6 por la cantidad de dispositivos nuevos que se están creando y el crecimiento de la red mundial para que estos nuevos dispositivos puedan interconectarse en la red actual.

Para un usuario común este cambio es transparente, el problema surge cuando se requiera de nuevas instalaciones con nuevos equipos para lo cual deberá existir un soporte y conocimientos adecuados acerca del hardware y arquitectura de red, mecanismos de transición a utilizar y toda una ingeniería para la implementación del protocolo IPv6.

La tendencia a que en el Perú se masifique esta tecnología está un poco lejana todavía debido a diferentes factores tales como la situación económica del país, la arquitectura de red actual, la poca cantidad de proveedores de servicios de internet y los costos elevados de los equipos y dispositivos aptos para la migración.

RECOMENDACIONES

Se recomienda lo siguiente para adecuarnos a este nuevo protocolo de red y hacer uso de las características que ofrece como poder usar direcciones IP de 128 bits haciendo casi imposible la saturación de direcciones en Internet.

Estar preparados para el cambio y conocer más sobre las nuevas tecnologías ya que IPv6 integrará todos los dispositivos existentes y aquellos que están aún en proceso de fabricación.

ANEXO
GLOSARIO

Autoconfiguración. Proceso mediante el cual un host configura automáticamente su dirección IPv6 a partir del prefijo del sitio y la direcciónMAC local.

AH. Authentication Header.

APIPA. Automatic Private Internet Protocol Addressing.

ARP. Address Resolution Protocol.

BGP. Border Gateway Protocol.

Carga útil. Los datos que se transportan en un paquete. La carga útil no incluye la información de encabezado que se necesita para que el paquete llegue a su destino.

CIDR. Dirección de encaminamiento entre dominios sin clase. Formato de dirección IPv4 que no se basa en clases de red (clase A, B y C). Las direcciones CIDR tienen un tamaño de 32 bits. Utilizan la notación decimal con puntos IPv4 estándar, más un prefijo de red. Dicho prefijo define el número de red y la máscara de red.

Datagrama IP. Paquete de información que se transfiere por IP.Un datagrama IP contiene un encabezado y datos. En el encabezado figuran las direcciones del origen y el destino del datagrama. Otros campos del encabezado permiten identificar y volver a combinar los datos con los datagramas adjuntos en el destino.

Descubrimiento de vecinos. Mecanismo de IP que permite a los host encontrar otros host que residen en un vínculo conectado.

DHCP. Dynamic Host Configuration Protocol.

Dirección privada. Dirección IP que no se puede encaminar por Internet. Las redes internas utilizan las direcciones privadas en los host que no necesitan conexión con Internet.

Dispositivo VLAN. Interfaces de red que proporcionan reenvío de tráfico en el nivel de Ethernet (vínculo de datos) del protocolo de pila IP.

Encabezado IP. Veinte bytes de datos que identifican un paquete de Internet de forma exclusiva. El encabezado contiene direcciones de origen y destino del paquete. Una opción del encabezado permite agregar más bytes.

Encapsulado. Proceso de colocación de un encabezado y carga útil en el primer paquete, que posteriormente se coloca en la carga útil del segundo paquete.

ESP. Encabezado de extensión que proporciona integridad y confidencialidad a los datagramas. ESP es uno de los cinco componentes de la arquitectura para seguridad IP (IPsec).

FDDI. Fiber Distributed Data Interface.

Filtro de paquetes. Función de servidor de seguridad que se puede configurar para permitir o denegar el paso de determinados paquetes a través de un servidor de seguridad.

Hop (salto). Medida que se usa para identificar la cantidad de encaminadores que hay entre dos hosts o sistemas. Si un origen y un destino están separados por tres encaminadores, los sistemas están a una distancia de cuatro saltos.

Host. Sistema que no reenvía paquetes. Al instalar el sistema operativo Solaris, de forma predeterminada un sistema se convierte en host. Es decir, el sistema no puede reenviar paquetes. En general, un host tiene una interfaz fisica, aunque también puede constar de varias interfaces.

IANA. Internet Assigned Numbers Authority.

ICMP. Siglas inglesas de Internet Control Message Protocol (protocolo de mensajes de control de Internet). Se utiliza para administrar e intercambiar mensajes de control.

IEEE. Institute of Electricals and Electronic Engineers.

IETF. Internet Engineering Task Force.

IKE. Siglas inglesas de Internet Key Exchange (intercambio de claves en Internet). IKE automatiza el suministro de material de claves autenticadas para la SA (Security Association) de IPsec.

ISATAP. Intra-Site Automatic Tunnel Addressing Protocol.

IP encapsulado. Mecanismo para colocar en túneles paquetes IP dentro de paquetes IP.

IPSec. Seguridad IP. Arquitectura de seguridad que proporciona protección a los datagramas IP.

IPv4. Internet Protocol version 4. IPv4 en ocasiones se denomina IP. Esta versión admite un espacio de direcciones de 32 bits.

IPv6. Internet Protocol version 6. IPv6 admite espacio de direcciones de 128 bits.

ISO. International Organization for Standardization.

IS-IS. Intermediate System to Intermediate System.

LLC. Logical Link Control.

MAC. Media Access Control.

MPLS. Multiprotocol Label Switching.
MTU. Siglas en inglés deMaximum Transmission Unit, unidad de transmisión máxima. El tamaño, en octetos, que puede transmitirse por un vínculo. Por ejemplo, una red Ethernet tiene unaMTUde 1500 octetos.

NAT. Del inglésNetwork Address Translation. Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red. Se utiliza para limitar la cantidad de direcciones IP globales que se necesitan.

ND. Neighbor Discovery.

Nodo. En IPv6, cualquier sistema compatible con IPv6, ya sea host o router.

OSI. Open Systems Interconnection.

OSPF. Open Shortest Path First.

Paquete. Grupo de información que se transmite como una unidad a través de líneas de comunicaciones. Contiene un encabezado IP y una carga útil.

PDU. Protocolo Data Units.

Pila IP. TCP/IP se suele denominar "pila". Este término designa las capas (TCP, IP y en ocasiones otras) a través de las cuales se transfieren todos los datos en los extremos de cliente y servidor de un intercambio de datos.

Pila doble. Pila de protocolo TCP/IP con IPv4 e IPv6 en la capa de red; el resto de la pila permanece idéntico. Si al instalar el sistema operativo Solaris se habilita IPv6, el sistema recibe la versión de pila doble de TCP/IP.

Red externa. Cualquier otra red que no sea la red principal del nodo móvil.

Red principal. Red cuyo prefijo coincide con el prefijo de red de una dirección permanente de nodo móvil.

RIP. Routing Information Protocol.

TCP/IP. (Transmission Control Protocol/Internet Protocol) es el protocolo o lenguaje de comunicaciones básico de Internet. También se usa como protocolo de comunicaciones en redes privadas (tanto Intranets como Extranets).

Teredo. Es una tecnología que sirve para establecer automáticamente túneles IPv6, encapsula IPv6 dentro del actual IPv4.

Túnel. La ruta a la que sigue un datagrama cuando se encapsula.

VPN. Una sola red lógica y segura que emplea túneles en una red pública como Internet.

BIBLIOGRAFÍA

Handbook of IPv4 to IPv6 Transition

John J. Amoss & Daniel Minolli

Auerbach Publications - 2008

IPv6: Theory, Protocol and Practice

Pete Loshin

Morgan Kaufmann Publishers - 2004

Understanding IPv6

Joseph Davies

Microsoft Press - 2008

Deploying IPv6 Networks

Ciprian Popoviciu, Eric Levy-Abegnoli & Patrick Grossetete

Cisco Press - 2006

TCP/IP Professional Reference Guide

Gilbert Helt

Auerbach Publications - 2001

TCP/IP Analysis and Troubleshooting Toolkit

Kevin Burns

Wiley Publishing, Inc - 2003

Running IPv6

Iljitsch van Beijnum

Apress - 2006

TCP/IP Foundations

Andrew G. Blank

Sybex - 2004

Transición a IPv6 en un departamento universitario

Omar Walid Llorente

DIT - Universidad Politécnica de Madrid - 2004

IETF

http://www.ietf.org

The IPv6 Forum

http://www.ipv6forum.com

IPv6 México

http://www.ipv6.unam.mx

RAAP

http://www.raap.org.pe

INICTEL

http://www.inictel-uni.edu.pe

CLARA

http://www.redclara.net

Ex-Proyecto 6bone

http://www.6bone.net

IPv6 Task Forces

http://www.ipv6tf.org

Información de IPv6

http://www.ipv6.org

Grupos de usuarios en Linux

http://www.v6.linux.or.jp

Linux online

http://www.linux.org/docs/ldp/howto/Linux%2BIPv6-HOWTO/information-onlineinformation.html

Investigación IPv6 de Microsoft

http://ipv6.research.microsoft.com

Google sobre IPv6

http://ipv6.google.com

CISCO

http://www.cisco.com

IANA

http://www.iana.org

Proyecto ISABEL

http://isabel.dit.upm.es

LACNIC

http://lacnic.net/sp

RFC

http://www.rfc-editor.org