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

MECANISMOS PARA LA TRANSICIÓN AL PROTOCOLO DE INTERNET VERSIÓN 6

Daniel Fernando López Juárez
Asesorado por el Ing. Mario Enrique Sosa Castillo

Guatemala, octubre de 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

MECANISMOS PARA LA TRANSICIÓN AL PROTOCOLO DE INTERNET VERSIÓN 6

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR:

DANIEL FERNANDO LÓPEZ JUÁREZ

ASESORADO POR EL ING. MARIO ENRIQUE SOSA CASTILLO
AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. José Milton De León Bran
VOCAL V	Br. Isaac Sultán Mejía
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

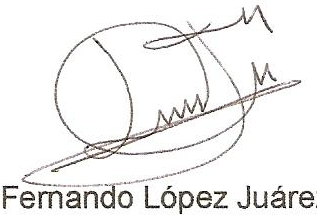
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Juan Álvaro Díaz Ardavin
EXAMINADOR	Inga. Pedro Pablo Hernández Ramírez
EXAMINADOR	Inga. Marlon Pérez Türk
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

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

MECANISMOS PARA LA TRANSICIÓN AL PROTOCOLO DE INTERNET VERSIÓN 6,

tema que me fuera asignado por la Dirección de la Escuela de Ciencias y Sistemas, con fecha enero de 2009.



Daniel Fernando López Juárez.

Guatemala, 20 de Enero de 2009

Señores
Coordinación de Revisión de Trabajo de Graduación
Carrera de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

En atención a la designación de que fuera objeto para asesorar el trabajo de tesis con título "MECANISMOS PARA LA TRANSICIÓN AL PROTOCOLO DE INTERNET VERSIÓN 6" del estudiante Daniel Fernando López Juárez con número de carné 200413322, Tengo el agrado de comunicar que procedí a efectuar dicha asesoría, encontrándose el trabajo concluido satisfactoriamente mediante la culminación de cada una de las actividades planificadas.

Sin otro particular me suscribo de ustedes,

Atentamente,

Ing. Mario Enrique Sosa Castillo

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

Guatemala, 22 de Julio de 2009

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

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante DANIEL FERNANDO LOPEZ JUAREZ, titulado: **"MECANISMOS PARA LA TRANSICION AL PROTOCOLO DE INTERNET VERSION 6"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

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

Atentamente,

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

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION TESIS

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"MECANISMOS PARA LA TRANSICIÓN AL PROTOCOLO DE INTERNET VERSIÓN 6",*** *presentado por la estudiante* ***DANIEL FERNANDO LÓPEZ JUÁREZ,*** *aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

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

Ing. Marlon Antonio Pèrez Turk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 28 de octubre 2009

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.451.09

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **MECANISMOS PARA LA TRANSICIÓN AL PROTOCOLO DE INTERNET VERSIÓN 6,** presentado por el estudiante universitario **Daniel Fernando López Juárez,** autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, octubre de 2009

/cc
c.c. archivo.

ACTO QUE DEDICO A:

Diosito y La Virgen María, por el gran amor y por guiar mi camino para alcanzar una meta más en la vida.

Mis padres: Miguel Alfredo López García y Rosa María Juárez de López, por su apoyo y motivación incondicional para continuar con los estudios de la carrera.

Mis Hermanos: Josué Alfredo López Juárez, por la motivación brindada en cada momento de debilidad para continuar esforzándome en los momentos más difíciles de la carrera. Mi hermana Adriana Isabel López Juárez, por su cariño y motivación brindada en cada momento.

Daniel Fernando López Juárez

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

6to4: Tecnología de túneles automáticos utilizada para proveer conectividad unicast entre sitios y hosts IPv6 a través de Internet IPv4. Esta es una tecnología de túneles de Router a Router, Host a Router y de Router a Host.

APIPA Automatic Private Internet Protocol Addressing - Direccionamiento Privado Automático del Protocolo de Internet. protocolo utilizado para obtener la configuración de red cuando el sistema está configurado para obtener una dirección dinámicamente, y al iniciar, éste no encuentra un servidor DHCP.

ARP Address Resolution Protocol - Protocolo de resolución de direcciones. Protocolo por medio del cual se puede obtener la dirección fisica (dirección MAC) de un dispositivo por medio de su dirección logica de red.

Bit Binary DigiT. Unidad mínima de almacenamiento de la información. Su valor puede ser 0 ó 1 ó verdadero o falso.

Broadcast Envió de información a múltiples destinos que son desconocidos para el transmisor. Normalmente utilizado por los Router para reconocimientos de Host.

Byte Generalmente usado para nombrar un grupo de ocho bits que son usados para identificar caracteres.

Cache Parte de la memoria RAM o del disco duro utilizada por el ordenador para almacenar temporalmente cierta cantidad de información susceptible de ser utilizada con cierta frecuencia, logrando así más rapidez en el tiempo de respuesta.

Conmutación Cambiar, permutar una cosa por otra.

Datagrama	Unidad de información transmitida por los protocolos de nivel de red. El datagrama contiene no sólo los datos: entre otras informaciones, se añade la dirección del emisor de los datos, así como la de su destinatario. Esta información le permite al protocolo TCP/IP encaminar (transportar a través de las redes y host que hagan falta) los datos desde el origen a su destino.
DHCP	Dynamic Host Configuration Protocol. Método que asigna automáticamente direcciones IP a clientes de una red.
direcciones Link-local	Direcciones de red destinadas para uso en un enlace de datos local.
DNS	Domain Name System - Sistema de Nombres de Dominio. Utilizado para convertir nombres alfanuméricos en sus correspondientes direcciones IP. Obviamente, los humanos tenemos más facilidad para recordar nombres que para recordar números, de modo que nosotros llamamos a un servidor por su nombre; para ello, un servidor DNS se encarga de traducirlo a su código numérico (dirección IP). Un servidor DNS convierte, por ejemplo, la dirección www.yahoo.com en 64.58.76.223, la dirección www.whitehouse.gov (la Casa Blanca) en 193.126.242.89. o www.elpais.es (diario El País) en 212.80.177.133.
Encapsulación	Proceso de ocultar todos los detalles de un objeto que no contribuyen a sus características esenciales. Método de transmisión del tráfico de la red que usa un protocolo de red encerrándose en otro protocolo de red.
Ethertype	Campo de dos octetos en el marco de paquetes Ethernet utilizado para identificar que protocolo es encapsulado en el marco de datos.
Host	Un host es una computadora que se encuentra dentro de una red, y que ofrece algún tipo de servicio o recurso al resto.
ICMPv6	Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet Versión 6. Realiza las funciones de control y administración de transacciones.

Interfaz Dispositivo electrónico entre dos soportes que permite intercambiar información entre diferentes elementos lógicos de un sistema informático y presentar al usuario los resultados de la acción.

IPsec IP SECURITY. Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

ISATAP Intra-Site Automatic Tunnel Addressing Protocol. Es un mecanismo de transición de IPv6 para transmitir paquetes de IPv6 entre un infraestructura IPv4 por medio de la encapsulación de los paquetes IPv6 dentro de encabezados IPv4.

ISP Internet Service Provider - Proveedor de Servicios Internet. Organización o empresa que establece la conexión entre los usuarios e Internet. Generalmente, los ISP ofrecen servicios de conexión, correo electrónico, hospedaje de páginas Web y el software de navegación por la Web. El ISP ofrece un número de teléfono, por lo general local, para que los usuarios se conecten a su servidor y puedan acceder a la Red mundial.

LoopBack Interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.1 y ::1 para el caso de IPv6.

Multidifusión Método de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y, por lo tanto, por múltiples usuarios.

NAT Network Address Translation - Traducción de Dirección de Red. Mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

QoS Quality of Service - Calidad de Servicio.

Teredo: Tecnología para la transición hacia IPv6 que provee asignación de direcciones y túneles automáticos de host a host para trafico IPv6 cuando nodos del tipo IPv6/IPv4 se encuentran detrás de uno o varios traductores de direcciones de red (NATs) IPv4.

UDP User Datagram Protocol. Protocolo de transmisión de datos similar a TCP, cuya principal diferencia, es que no reenvía los datos dañados, por lo que es más rápido que TCP. Este protocolo se suele usar para la transmisión de datos más rápida de lo normal.

Unidifusión Por contraposición a broadcast y multicast, unicast es la comunicación establecida entre un solo emisor y un solo receptor en una red.

RESUMEN

El presente trabajo está dividido a manera de tratar una introducción inicial hacia los conceptos de IP para luego poder cubrir lo referente a la transición del protocolo IPv4 hacia IPv6.

A lo largo del primer capítulo se abarcan conceptos básicos sobre el protocolo en su versión 4 y se da una breve descripción sobre la nueva versión IPv6, cubriendo las características principales y los problemas por los cuales se origina la necesidad de IPv6.

En el segundo capítulo se hace énfasis en los mecanismos por medio de los cuales se pueda llevar a cabo la transición, identificando los distintos tipos de dispositivos que pueden existir en una infraestructura en la que intervengan los dos protocolos y tratando a cada uno de estos mecanismos de manera general.

Los mecanismos principales para la transición son basados en túneles por medio de los cuales los paquetes IPv6 puedan viajar, por medio de la encapsulación dentro de un paquete IPv4, a lo largo de una arquitectura IPv4. Los capítulos 3, 4 y 5 tratan a mayor detalle tres tecnologías que permiten realizar este tipo de comunicación, estos son ISATAP, 6to4 y Teredo.

En la parte final del trabajo se resume a manera de pasos que deben de ser seguidos para poder llegar a una arquitectura que permita la comunicación por medio de IPv6 en un ámbito global.

OBJETIVOS

General:

Definir la necesidad del IPv6, identificando y describiendo claramente las tecnologías existentes que permitan llevar a cabo la transición hacia la nueva versión del protocolo de internet.

Específicos:

1. Comprender la necesidad del IPv6.
2. Realizar un estudio y definición del IPv6.
3. Describir las diferencias entre IPv4 e IPv6.
4. Conocer las mejoras implementadas dentro del IPv6.
5. Identificar los mecanismos que permitan realizar la transición hacia el IPv6.
6. Describir detalladamente los mecanismos que permitan realizar la transición hacia el IPv6.
7. Dar a conocer los pasos necesarios para realizar la transición al IPv6.

INTRODUCCIÓN

La versión actual del protocolo de internet IPv4, establecida desde el año 1981 y sin cambios significativos desde entonces, ha probado ser una arquitectura robusta, interoperable y fácil de implementar al superar la prueba a una escala muy grande como lo es la interconexión de redes a través de internet.

Sin embargo, este protocolo no fue pensado para un gran crecimiento y por tanto afronta su mayor problema al no poder soportar el crecimiento exponencial que ha llevado internet, previendo que la cantidad total de direcciones que puedan ser asignadas por IPv4 llegaran a agotarse entre los años 2011 y 2012.

La nueva versión del protocolo IPv6 o conocida también como IPng, por la denominación de Nueva Generación del Protocolo de Internet, ha sido propuesta desde los años 90. Esta versión del protocolo ofrece una solución al problema del agotamiento de direcciones y a los demás problemas encontrados en IPv4.

IPv6 está destinado a sustituir a IPv4 pero se necesita de un largo camino para llegar a ello. La buena noticia es que el recorrido por este camino ya se ha iniciado y nos encontramos en una etapa en la cual se intenta el trabajo mutuo entre ambos protocolos para poder llegar así a una etapa final en la que toda la arquitectura que sea únicamente IPv6.

Mediante el presente trabajo se trataran los mecanismos por medio de los cuales se pretende iniciar el camino hacia una total arquitectura IPv6, a través de tecnologías que permitan un inicial trabajo en conjunto de IPv4 e IPv6.

1. PROTOCOLO DE INTERNET

Durante el desarrollo del internet fueron experimentados distintos tipos de conexión entre los computadores, por lo cual fue necesaria la creación de un método que permitiera unificar estos distintos tipos de comunicación, el Protocolo de Internet (IP) es el protocolo utilizado para permitir la comunicación entre el nodo origen y el nodo destino a través de una red de datos conmutados.[1]

Al hablar de conmutar se hace referencia al intercambio de una cosa por otra y en el sentido de las redes significa el traslado de los paquetes a bits para que estos puedan ser enviados de un dispositivo a otro a través de un medio físico. En este tipo de comunicación la información es dividida en paquetes que contienen además de los datos a transmitir, un encabezado de datos entre los cuales se incluyen las direcciones del nodo que envía los datos y del que los debe de recibir. [1]

El protocolo IP es parte del conjunto de protocolos TCP/IP y es uno de los protocolos de internet más importantes al permitir el desarrollo y transporte de paquetes de datos aunque sin garantizar su entrega. El formato de los paquetes IP será descrito más adelante.

Este protocolo implementa dos funciones básicas, direccionamiento y fragmentación. Los routers utilizan las direcciones que se encuentran en la cabecera de

[1] Internet," Enciclopedia Microsoft® Encarta® Online 2008

los paquetes IP para transmitirlos hacia su destino. La selección del camino más apropiado para un paquete se denomina encaminamiento.

El protocolo de Internet utiliza cuatro campos clave para prestar su servicio: el tipo de servicio (TOS), el tiempo de vida (TTL), Opciones, y suma de control de Cabecera. Los cuatro campos van especificados en el encabezado del paquete a enviar.

El tipo de servicio indica la calidad del servicio deseado. Es un conjunto de parámetros que se utilizan para determinar de qué modo hay que tratar a cada uno de los paquetes. El tipo de servicio permitirá determinar parámetros de comunicación como, la tecnología de enlace que se utilizará para el siguiente salto, el camino a seguir por el paquete, su prioridad en las colas, etc.

El tiempo de vida se refiere al periodo de vida de un paquete IP, este no es fijado en tiempo específicamente sino que en cantidad de saltos máximos que el paquete podrá realizar para llegar a su destino. Este valor se define en el remitente del mensaje y se reduce en una unidad en todos los hosts por los que va atravesando. El paquete se destruirá si el tiempo de vida alcanza un valor de cero antes de que el paquete llegue a su destino. La suma de control permite una verificación de que la información contenida en el paquete ha sido transmitida correctamente. Si al recibir un nuevo paquete la suma es inválida, el paquete se descarta por quien detectó el error.

1.1 Antecedentes

El protocolo de internet en su versión 4 fue la primera versión que se implemento extensamente y con la cual se formulo la base a Internet. Este protocolo fue muy bien aceptado y se obtuvo un crecimiento del mismo muy rápidamente, con lo cual se originaron problemas que no fueron posibles resolver con la misma versión del

protocolo y por lo cual en 1992 se publica un llamado a proponer la Nueva Generación del Protocolo de Internet.[2]

Para 1995 se publica la propuesta de IPv6 definida en la especificación RFC1883 y con lo cual para el siguiente año se crea una red de pruebas denominada 6Bone. [3]

Japón, China y Corea del Sur anunciaron que para el año 2005 adoptarían completamente el protocolo en su versión 6, iniciando con los registros de código de país para Japón (.jp) y Corea (.kr) para que estos fueran visibles en los servidores raíz de DNS. [3]

El 4 de febrero del 2008 fueron añadidos a los servidores raíz de la red un pequeño número de registros que están escritos completamente en IP versión 6. [3]

1.2 Protocolo de internet versión 4

El protocolo de internet en su versión 4 (IPv4) formo la base del internet al ser el primer protocolo que se implementó exitosamente. Este protocolo fue lanzado en el año 1981 e implementa direcciones de 32 bits logrando un máximo aproximado de 4 mil millones de direcciones, las cuales debido al gran auge del internet se encuentran ya en escases. [4]

En su implementación inicial no se tomaron en cuenta varios factores que afectan en estos momentos con el crecimiento del internet, esta versión del protocolo de internet proporciona una gran cantidad de direcciones IP pero que ahora ya no son suficientes para cubrir todas las necesidades que han surgido y que puedan surgir en el futuro.

[2] "Introducción a las Tecnologías de Internet", M. Farias-Elinos
[3] "Introducción a las Tecnologías de Internet", M. Farias-Elinos
[4] (ARIN, 2007)

1.3 Protocolo de internet versión 6

La versión 6 del protocolo de internet (IPv6) surge como respuesta a todos los problemas detectados en la versión 4 y que no fueron tomados en cuenta en su momento. El principal problema que se intenta resolver es la escases de direcciones, para lo cual en IPv6 existe un total de 3.4x10^38 direcciones, utilizando direcciones de 128 bits en notación hexadecimal al contrario de las anteriores direcciones de 32 bits del IPv4.[5]

1.4 Necesidades de IPv6

Al momento de la creación y estandarización del IPv4 no se estimo que este protocolo tendría una gran aceptación y que se convirtiera en una arquitectura de carácter mundial con un gran número de usuarios que crece día a día.

Los principales problemas que se presentan con el IPv4 y que pretenden ser resueltos con el IPv6 se listan a continuación.

- Direcciones disponibles
- Seguridad
- Facilidad de administración
- Direccionamiento
- Dispositivos móviles
- Multiprotocolo

[5] (ARIN, 2007)

1.4.1 Direcciones disponibles

En la versión 4 del protocolo se cuenta con direcciones de 32 bits, lo cual brinda un máximo de cuatro mil millones de direcciones disponibles para ser asignadas. Este total de direcciones ya no es suficiente debido al crecimiento exponencial de Internet y a la estructura de asignación de las direcciones que regularmente recurre a un desperdicio de una gran cantidad de direcciones por cada red de dispositivos. [6]

1.4.2 Seguridad

El incremento en el número de usuarios y de sistemas que necesiten de internet sugiere que se definan mecanismos de seguridad para brindarles esquemas de autentificación, privacidad y protección contra ataques malintencionados.[7]

1.4.3 Facilidad de Administración

La nueva arquitectura debe de facilitar la administración de la red, esto mediante mecanismos como la autoconfiguración de los equipos que sean conectados a la red que facilite la gestión de la misma. [8]

1.4.4 Direccionamiento

Los routers poseen tablas de encaminamiento con un límite al número de rutas que un nodo puede manejar y debido a que el Internet crece mucho más rápido que la tecnología que la mantiene, los routers pronto alcanzarían su capacidad máxima y empezaran a desechar rutas, con lo que la red comenzaría a fragmentarse en subredes sin acceso entre sí.[9]

[6] (Hinden & Deering, 1998)
[7] (Pethia, Crocker, & Fraser, 1991)
[8] (Droms, 1993)
[9] (Manning, 1996)

1.4.5 Dispositivos móviles

El campo de las comunicaciones móviles está en auge, cada día se cuenta con más dispositivos que necesiten de una dirección IP para poder conectarse a la red, como lo pueden ser computadoras móviles y aparatos celulares. Debido a esto se necesita una nueva arquitectura con mayor flexibilidad y capaz de afrontar el reto que supone la movilidad de sus usuarios incluyendo la seguridad de las comunicaciones en este tipo de sistemas. [10]

1.4.6 Multiprotocolo

Es necesaria la utilización de mecanismos que permitan abstraer al usuario de la tecnología de las capas inferiores y que le permita al mismo concentrarse únicamente en los aspectos que sean relevantes para su trabajo. Con la necesidad de la convivencia de cada vez más cantidades de protocolos se necesita que la nueva tecnología sea capaz de trabajar con todos ellos y que este proceso sea transparente para los usuarios finales.

1.5 Diferencias de IPv4 e IPv6

La característica principal que diferencia al IPv6 del anterior IPv4 es la estructura de las direcciones IP al estar formadas por 128 bits, brindando así una cantidad mucho mayor de direcciones que su antecesor.

Con las direcciones de 128 bits se posibilitará incluir la dirección física de la interfaz de red de la máquina en la propia dirección IP y facilitar de forma considerable el proceso de autoconfiguración.[11]

[10] (Simpson, 1994)
[11] (Microsoft Corporation, 2003 (actualización 2008))

Otras diferencias de la nueva versión del protocolo de internet se listan a continuación:

- Se codifica directamente en el datagrama qué acción debe adoptar una máquina cuando ésta no es capaz de reconocer alguna de las opciones del mismo.
- Se incluyen cabeceras destinadas a la autentificación y la encriptación de los datagramas.
- Se permite que la fuente encamine directamente sus datagramas, como soporte a su política o necesidades de enrutamiento.
- Los datagramas ya no tienen un límite de longitud de 65536 bytes.
- El soporte de encapsulados es muy natural, dado su diseño de cabeceras encadenadas.
- En caso de ser necesaria la fragmentación esta es realizada por la fuente de los datos.
- IPv6 no incluye una suma de control en la cabecera como en IPv4.
- Las direcciones están divididas en ocho segmentos de 16 bits cada una, separados por dos puntos en vez de un simple punto.

1.6 Características de IPv6

El protocolo IPv6 tiene las características siguientes:

- Nuevo formato de encabezado
- Espacio de direcciones más grande
- Infraestructura de direcciones y enrutamiento eficaz y jerárquica
- Configuración de direcciones con y sin estado
- Seguridad integrada
- Mejora de la compatibilidad para la calidad de servicio
- Nuevo protocolo para la interacción de nodos vecinos
- Capacidad de ampliación

1.6.1 Nuevo formato de encabezado

El encabezado IPv6 tiene un nuevo formato que está diseñado para reducir al mínimo la sobrecarga del encabezado. Esto se consigue al mover los campos que no son esenciales y los campos de opciones a encabezados de extensión que se colocan a continuación del encabezado IPv6. La simplificación del encabezado IPv6 permite un procesamiento más eficaz en los enrutadores intermedios.

Los encabezados IPv4 y los encabezados IPv6 no son interoperables y el protocolo IPv6 no es compatible con el protocolo IPv4. Un host o un enrutador deben utilizar simultáneamente una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado.

El nuevo encabezado IPv6 sólo tiene el doble de tamaño que el encabezado IPv4, a pesar de que las IPv6 son cuatro veces mayores que las direcciones IPv4.[12]

[12] Características de IPv6 - (Microsoft Corporation)

1.6.2 Espacio de direcciones más grande

IPv6 utiliza direcciones de origen y destino de 128 bits (16 bytes). El amplio espacio de direcciones de IPv6 se ha diseñado para permitir múltiples niveles de división en subredes y asignación de direcciones de la red principal de Internet a las subredes individuales de una organización.

Aunque actualmente sólo un pequeño porcentaje de direcciones posibles se asignan para el uso de hosts, hay disponibles muchas direcciones para su uso en el futuro. Al tener un número mucho mayor de direcciones disponibles, ya no son necesarias las técnicas de conservación de direcciones, como la implementación de NAT. [13]

1.6.3 Infraestructura de direcciones y enrutamiento eficaz y jerárquico

Las direcciones globales de IPv6 que se utilizan en la parte IPv6 de Internet están diseñadas para crear una infraestructura eficaz, jerárquica, que se puede resumir y que tiene en cuenta la existencia de múltiples niveles de proveedores de servicios de Internet. En la red Internet IPv6, los enrutadores de red tienen tablas de enrutamiento mucho más pequeñas. [13]

1.6.4 Configuración de direcciones con y sin estado

Para simplificar la configuración de los hosts, IPv6 admite la configuración de direcciones con estado, como la configuración de direcciones con la presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones sin la presencia de un servidor DHCP).

[13] Características de IPv6 - (Microsoft Corporation)

Con la configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (direcciones locales del vínculo, direcciones Link-local) y con direcciones derivadas de prefijos anunciados por los enrutadores locales. Incluso sin la presencia de un enrutador, los hosts del mismo vínculo se pueden configurar automáticamente con direcciones locales del vínculo y comunicarse sin necesidad de configuración manual. [13]

1.6.5 Seguridad integrada

La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares para las necesidades de seguridad de red y aumenta la interoperabilidad entre diferentes implementaciones de IPv6. [14] Más información sobre IPsec para IPv6 se encuentra en la tesis "Seguridad en IP con el protocolo IPESEC para IPV6" de Erick Fernando Luján Montes.

1.6.6 Mejora de la compatibilidad para la calidad de servicio

Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico. La identificación del tráfico, mediante un campo Flow Label (etiqueta de flujo) en el encabezado, permite que los enrutadores identifiquen y proporcionen un control especial de los paquetes que pertenecen a un flujo dado. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec. [14]

1.6.7 Nuevo protocolo para la interacción de nodos vecinos

El protocolo para el Descubrimiento de vecinos en IPv6 consiste en un conjunto de mensajes ICMPv6 (Internet Control Message Protocol for IPv6) que administran la interacción de nodos vecinos (es decir, nodos que se encuentran en el mismo vínculo).

[14] Características de IPv6 - (Microsoft Corporation)

El descubrimiento de vecinos reemplaza los mensajes de Protocolo de resolución de direcciones (ARP, Address Resolution Protocol), Descubrimiento de enrutadores ICMPv4 y Redirección ICMPv4 con mensajes eficaces de multidifusión y unidifusión, y proporciona funciones adicionales. [14]

1.6.8 Capacidad de ampliación

IPv6 se puede ampliar con nuevas características al agregar encabezados de extensión a continuación del encabezado IPv6. A diferencia del encabezado IPv4, que sólo admite 40 bytes de opciones, el tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6. [14]

1.7 Direccionamiento IPv6

Las direcciones en IPv6 son significativamente más grandes que las anteriores en IPv4 al estar formadas por 128 bits separadas en 8 segmentos de 16 bits cada una. Los segmentos se encuentran representados en notación hexadecimal separados por dos puntos ":". Con direcciones de 128 bits se obtiene un total de 2^128 direcciones, equivalente a 3.4 x 10^38, un número significativamente grande que no da margen a la imaginación al agotamiento de las mismas.[15]

Las direcciones IPv6 de 128 bits identifican interfaces individuales o grupos de interfaces. Puesto que cada interfaz pertenece a un único nodo, cualquiera de las direcciones de interfaces unicast de ese nodo podría ser utilizada como un identificador del nodo. Una única interfaz puede tener múltiples direcciones IPv6 de cualquier tipo; por ejemplo una interfaz podría tener una dirección unicast, otra anycast, y otra multicast simultáneamente. Estos tipos de direcciones se tratan en la sección 1.7.2[16]

[15] (ARIN, 2007)
[16] (Microsoft Corporation, 2003 (actualización 2008))

1.7.1 Formato de direcciones:

Como se mencionó anteriormente, las direcciones están divididas en grupos de 16 bits cada una. Ejemplo:

2000:A5F2: 1319:05A3: 08D3:S8CA:173F:0221

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

2001:0DB8:85A3:0000:1319:8A2E:0370:7344
2001:0DB8:85A3::1319:8A2E:0370:7344

De esta misma manera, si más de dos grupos consecutivos son nulos, pueden ser reducidos con "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

2001:0DB8**:0000:0000:0000:0000:**1428:57AB

2001:0DB8:**0000:0000:0000::**1428:57AB -> se reduce solo un grupo de ceros.

2001:0DB8**:0:0:0:0:**1428:57AB -> todos son representados con un solo cero

2001:0DB8**:0::0:**1428:57AB -> se comprimen dos grupos de ceros

2001:0DB8::1428:57AB -> se comprimen todos los grupos de ceros.

1.7.2 Tipos de direcciones en IPv6:

Unicast. Las direcciones unicast identifican a una única interfaz, es decir, un paquete enviado a una dirección unicast será entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

El octeto de nivel superior de las direcciones de multicast tiene el valor hexadecimal FF. Cualquier otro valor de este octeto identifica a una dirección de unicast.[17]

[17] (6DISS, 2007)

Anycast. Las direcciones anycast identifican un grupo de interfaces, de forma que un paquete enviado a una dirección anycast será entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano según la distancia asignada en el protocolo de encaminamiento. [17]

Multicast. Las direcciones multicast identifican, al igual que las anycast, a un grupo de interfaces, pero un paquete enviado a una dirección multicast, es enviado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6, su misión ha sido suplantada por las direcciones multicast. [17]

1.7.3 Identificación de los tipos de direcciones

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

::

La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1

La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4

La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo obsoleto.

::ffff:0:0

La dirección IPv4 mapeada es usada como un mecanismo de transición en terminales duales.

fe80::

El prefijo de *enlace local* (*link local*) específica que la dirección sólo es válida en el enlace físico local.

fec0::

El *prefijo de emplazamiento local* (*local prefix*) específica que la dirección sólo es válida dentro de una organización local. En el RFC 3879 se declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial.

ff00::

El prefijo de multicast es usado para las direcciones multicast.

En la siguiente tabla se muestra la equivalencia entre direcciones IPv4 e IPv6:

Tabla I Equivalencia entre direcciones IPv4 e IPv6

Dirección IPv4	**Dirección IPv6**
Clases de dirección IP	No aplica
Direcciones multicast (224.0.0.0/4)	Direcciones multicast IPv6 (FF00::/8)
Dirección de broadcast	No aplica
Dirección no especificada 0.0.0.0	Dirección no especificada ::
Dirección Loopback 127.0.0.1	Dirección Loopback ::1
Direcciones IP Publicas	Direcciones Globales
Direcciones Privadas	Direcciones Site-local (FEC0::/10)
Direcciones APIPA (169.254.0.0/16)	Direcciones Link-local (FE80::/64)
Sintaxis: notación de punto decimal (.)	Notación de dos puntos hexadecimal (:)
Mascara: notación de punto o largo de prefijo	Únicamente largo de prefijo
DNS: registros A	Registro de recursos AAAA
DNS reversible: dominio IN-ADDR.ARPA	Dominio IP6.ARPA

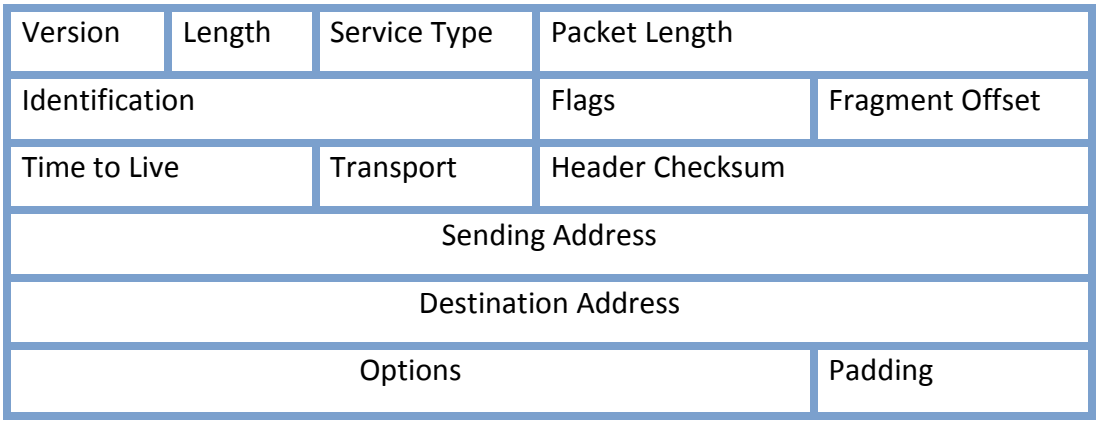
1.7.4 Estructura de encabezado IPv6

El nuevo encabezado de los paquetes en IPv6 es mucho más eficiente que el anterior encabezado de los paquetes IPv4 al contener menos campos, permitiendo así:

- Encabezados simplificados
- Reducción del costo de manipulación de los paquetes ordinarios
- Mantener baja la sobrecarga de ancho de banda producto del aumento en el tamaño del campo de direcciones.
    - Eliminación del Checksum al nivel de red
    - Se elimina la fragmentación de la red
- Flexible y extensible
- Seguridad

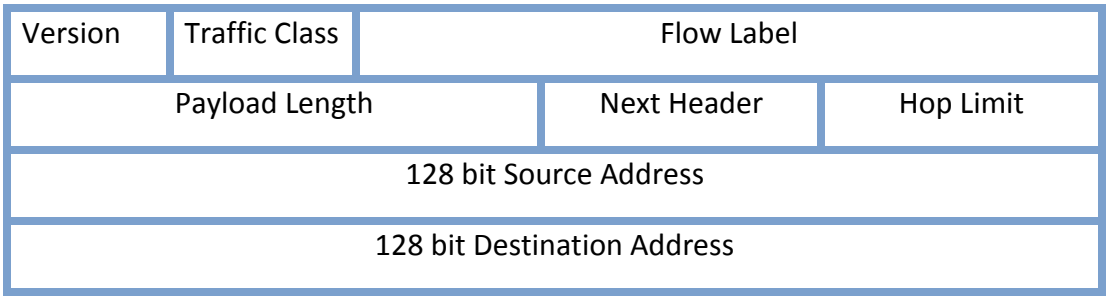
La estructura del encabezado para IPv4 es mostrado en la Figura 1 y la del encabezado de IPv6 se muestra en la Figura 2:

Figura 1: Encabezado de paquetes IPv4[18]



[18] (6DISS, 2007)

Figura 2: Encabezado de paquetes IPv6[19]



La cantidad de campos de encabezado en IPv4 de un total de 13 es reducida a tan solo 8 en el encabezado de IPv6, eliminando campos que producían redundancia de información y que no eran necesarios.

La especificación de cada uno de los campos se describe a continuación:

Versión:

4 bits y siempre vale 6. Este campo debería distinguir las versiones de IP, de forma que todas pudieran identificarse como un mismo protocolo a nivel de enlace con el mismo valor de Ethertype. Sin embargo, en la práctica muchas implementaciones de IPv4 no comprueban este campo sino que suponen que el paquete es IPv4 cuando el encabezado de nivel de enlace especifica protocolo IP. Por esto, a pesar de existir el campo versión es necesario asignar a IPv6 un valor propio en el nivel de enlace, como si se tratara de un protocolo diferente de IPv4.

Clase de tráfico:

1 Byte, utilizado para especificar parámetros de QoS de acuerdo a la especificación de la arquitectura Differentiated Services. Los valores del 0 al 7 indican poca sensibilidad al tiempo lo que permite encolar el tráfico. Los valores del 8 al 15 indican prioridad del tráfico fuera de flujo por lo que no se puede encolar este tipo de tráfico.

[19] (6DISS, 2007)

Etiqueta de flujo:

Permite identificar los paquetes que pertenecen a una sesión concreta entre dos hosts, usado típicamente para solicitar una determinada QoS.

Largo carga útil:

2 Bytes que indican el tamaño del paquete en bytes, sin considerar los 40 Bytes de encabezado. Como el valor máximo codificable es 65535, el paquete máximo será de 65575.

Siguiente encabezado:

1 Byte, sirve para indicar si el encabezado está seguido por alguno de los encabezados opcionales.

Si no existen opciones, este campo indica el protocolo de nivel de transporte al que pertenece el paquete, utilizando los mismos códigos que en IPv4.

Límite saltos:

1 Byte, equivalente al campo TTL de IPv4, donde el máximo número de saltos especificables es 255.

Dirección fuente:

16 Bytes para especificar la IPv6 del nodo fuente.

Dirección destino:

16 Bytes para especificar la IPv6 del nodo destino.

El encabezado total de un paquete en IPv6 está formado por 40 Bytes, tan solo el doble que un encabezado IPv4 considerando que es mucho más eficiente y se reducen los campos que producían redundancia innecesaria de información.

Un encabezado IPv6 puede tener cero, uno o más encabezados de extensión, cada uno identificado por el número colocado en el campo "siguiente encabezado". Los encabezados de extensión no son analizados en cada nodo de la ruta, sino sólo en el nodo o nodos finales, con la excepción del encabezado de opciones de salto a salto.[20]

La siguiente tabla muestra una comparación entre los campos del encabezado IPv4 y el encabezado IPv6:

Tabla II: Comparación entre encabezados IPv4 e IPv6

Campo del encabezado IPv4	**Cambio en encabezado IPv6**
Versión	Nuevo valor: 6
Internet Header Length	Removido
Type of Service	Trafic Class
Total Length	Payload Length
Identification	Removido
Fragmentation Flags	Removido
Fragment Offset	Removido
Time to Live	Hop Limit field
Protocol	Next Header
Header Checksum	Removido
Source Address	Similar, Nuevo largo de 128 bits
Destination Address	Similar, Nuevo largo de 128 bits
Options	Removido

[20] (6DISS, 2007)

1.8 Enrutamiento IPv6

El enrutamiento es el proceso de reenviar paquetes entre segmentos de red conectados. En las redes basadas en IPv6, el enrutamiento es la parte de IPv6 que proporciona capacidades de reenvío entre hosts que se encuentran en segmentos independientes que pertenecen a una red mayor basada en IPv6.

El enrutamiento en IPv6 promueve una gran ventaja, el mecanismo de enrutamiento flexible. Debido a la forma en que los Identificadores de red de IPv4 eran asignados, los principales enrutadores de Internet deben mantener grandes tablas de enrutamiento. Estos enrutadores deben conocer todas las rutas para poder reenviar los paquetes que se dirigen a cualquier nodo de Internet. Con su capacidad de agregar direcciones, IPv6 permite direcciones flexibles y reduce drásticamente el tamaño de las tablas de enrutamiento.[21]

1.8.1 Enrutadores IPv6

Los enrutadores IPv6 proporcionan el medio principal para unir dos o más segmentos de red IPv6 físicamente independientes. Todos los enrutadores IPv6 tienen las características siguientes:

- Son físicamente hosts múltiples. Un host de hosts múltiples físicos es un host de la red que utiliza dos o más interfaces de conexión de red para conectarse a cada segmento de red físicamente independiente.
- Permiten el reenvío de paquetes a otros hosts IPv6.

Los enrutadores IPv6 se pueden implementar mediante diversos productos de hardware y software. Comúnmente se utilizan enrutadores que son dispositivos de hardware dedicados que ejecutan software especializado.

[21]Protocolo Internet versión 6 - (Microsoft Corporation)

Independientemente del tipo de enrutadores que se utilicen, todo el enrutamiento IPv6 depende del uso de una tabla de enrutamiento para la comunicación entre los segmentos de red.[22]

1.8.2 Tablas de enrutamiento

Una tabla de enrutamiento es utilizada por un enrutador IPv6 para mantener información acerca de otras redes y hosts IPv6. Los segmentos de red se identifican mediante un prefijo de red IPv6 y una longitud de prefijo. Además, las tablas de enrutamiento proporcionan información importante a cada host local respecto a cómo deben comunicarse con redes y hosts remotos.[23]

Antes de enviar un paquete IPv6, el equipo inserta la dirección IPv6 de origen y la dirección IPv6 de destino en el encabezado IPv6, luego, el equipo examina la dirección IPv6 de destino, la compara con una tabla de enrutamiento IPv6 mantenida localmente y realiza la acción adecuada. El equipo realiza una de las tres acciones siguientes:

- Pasa el paquete a un nivel de protocolo IPv6 superior en el host local.
- Reenvía el paquete a través de una de las interfaces de red conectadas.
- Descarta el paquete.

IPv6 busca en la tabla de enrutamiento la ruta más similar a la dirección IPv6 de destino. La ruta, en orden de más a menos específica, se determina de la manera siguiente:

1. Una ruta que coincide con la dirección IPv6 de destino (una ruta de host con una longitud de prefijo de 128 bits).
2. Una ruta que corresponde al destino con la mayor longitud de prefijo.
3. La ruta predeterminada (el prefijo de red ::/0).

[22] IPv6 routing - (Microsoft Corporation)
[23] IPv6 routing - (Microsoft Corporation)

2. MECANISMOS DE TRANSICIÓN HACIA IPV6

La transición de IPv4 hacia IPv6 es una tarea difícil y que tomara un largo tiempo para que una infraestructura únicamente IPv6 llegue a suceder. Se han definido ya varios caminos que nos lleven por una adecuada transición, y estos mecanismos son los que se detallaran a lo largo de este capítulo.

2.1 Tipos de nodos

En una infraestructura en la que interactúen nodos con capacidad para IPv6, nodos con capacidad IPv4 y nodos con capacidad para ambos protocolos, es necesario realizar la siguiente clasificación:

- Nodos IPv4-only
- Nodos IPv6-only
- Nodos IPv6/IPv4
- Nodos IPv6
- Nodos IPv4

2.1.1 Nodos solo IPv4 (IPv4-only):

Nodo que implementa únicamente IPv4, solamente tiene direcciones IPv4 y no soporta IPv6. De este tipo de nodos es la mayoría de hosts y routers que se encuentran instalados a la fecha. [24]

[24] IPv6 Transition Technologies - (Microsoft Corporation, 2003 (actualización febrero 2008))

2.1.2 Nodos solo IPv6 (IPv6-only):

Nodo que implementa únicamente IPv6, solamente tiene direcciones IPv6 y no soporta IPv4. Únicamente se puede comunicar con aplicaciones y con otros nodos IPv6, no es muy común todavía pero llegara a tener mayor prevalencia en dispositivos como teléfonos celulares que soporten el protocolo.[24]

2.1.3 Nodos IPv6/IPv4

Este tipo de nodo implementa tanto IPv4 como IPv6.[24]

2.1.4 Nodo IPv4

Es un nodo que implementa IPv4, puede ser un nodo IPv4-only o IPv6/IPv4.[24]

2.1.5 Nodo IPv6

Nodo que implementa IPv6, puede ser únicamente IPv6 o IPv6/IPv4[24]

2.2 Utilizando ambos IPv6 e IPv4

Con este mecanismo, a través del cual se pretende migrar de los dispositivos que utilizan únicamente IPv4, hacia nodos tipo IPv6/IPv4 y finalmente a una infraestructura únicamente de IPv6, es necesario que los Host puedan identificar o buscar destinatarios tanto con IPv6 y con IPv4.[25]

Para poder utilizar las capas de internet, tanto para IPv6 como para IPv4 en un mismo equipo, se pueden utilizar dos tipos de arquitecturas:

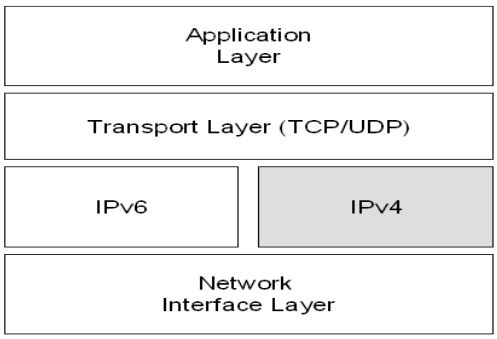
- Arquitectura capa IP Dual
- Arquitectura Pila Dual

[25]IPv6 Transition Technologies - (Microsoft Corporation, 2003 (actualización febrero 2008))

2.2.1 Arquitectura capa IP dual

Este tipo de arquitectura utiliza tanto la capa de internet IPv6 e IPv4 mediante la implementación de los protocolos de la capa de transporte TCP y UDP.

Figura 3: Arquitectura capa IP dual



De este modo, un dispositivo puede soportar ambos protocolos, y ya sea una o la otra pila puede ser deshabilitada por razones operativas. Los nodos IPv6/IPv4 pueden operar en uno de los siguientes tres modos:[26]

1. Pila IPv6 habilitada y pila IPv4 deshabilitada
2. Pila Ipv6 deshabilitada y pila Ipv4 habilitada
3. Ambas pilas habilitadas.

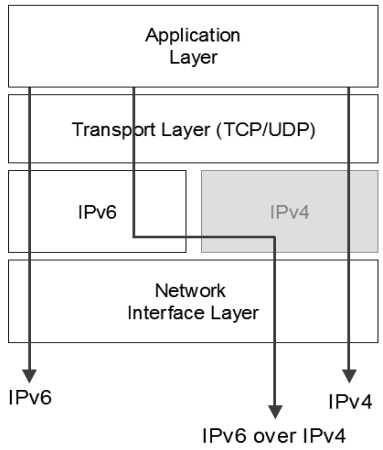
Un nodo IPv6/IPv4 con la pila IPv6 deshabilitada trabajará como un nodo IPv4-only y contrariamente, si tiene la pila IPv4 deshabilitada operará como un nodo IPv6-only.

Este tipo de de arquitectura es fácil de desplegar y extensamente soportado, pero la topología de red requiere de dos tablas de encaminamiento y de dos procesos de encaminamiento, con lo cual cada nodo en la red necesita tener actualizadas las dos pilas.

[26]IPv6 Transition Technologies - (Microsoft Corporation, 2003 (actualización febrero 2008))

Los tipos de paquetes que pueden ser creados por un nodo que implemente la pila dual son Paquetes IPv4, Paquetes Ipv6 y Paquetes IPv6 sobre IPv4+

Figura 4: Tipos de Comunicación con arquitectura de capa IP dual



2.2.2 Arquitectura de pila dual

Una arquitectura de este tipo contiene ambas capas de internet, IPv4 e IPv6, con protocolos separados e implementaciones de protocolos para la capa de transporte (TCP / UDP) por separado.[27]

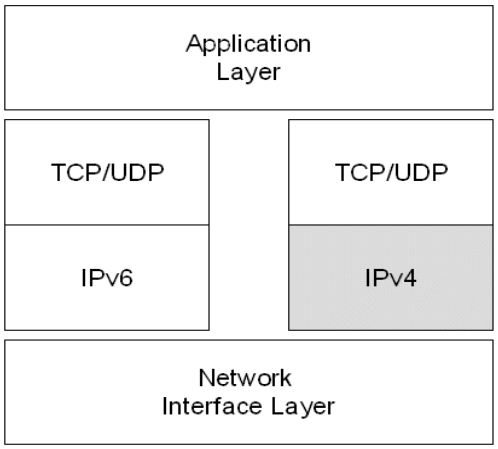
Teniendo una pila para cada protocolo IPv4 e IPv6, un equipo puede crear paquetes de cualquier tipo:

- Paquetes IPv4
- Paquetes IPv6
- Paquetes IPv6 sobre IPv4

De este modo cada nodo en la red podrá enviar y recibir paquetes tanto de IPv4 y de IPv6, con lo cual estos podrán comunicarse con cualquier nodo en la red independientemente del tipo del mismo.

[27] (Microsoft Corporation, 2003 (actualización febrero 2008))

Figura 5: Arquitectura de pila dual[27]



La arquitectura de Pila Dual puede ser implementada si una infraestructura de red solo soporta IPv6, pero algunos de los nodos de la red tienen capacidad para pila dual y hacen uso de aplicaciones IPv4.[28]

2.3 IPv6 sobre túneles IPv4

Los túneles de IPv6 sobre IPv4 son la encapsulación de paquetes IPv6 con encabezado de IPv4, de modo de que estos paquetes puedan ser enviados a través de la infraestructura de IPv4. [29]

Este método se utiliza a menudo cuando la infraestructura completa, o partes de la misma, todavía no es capaz de ofrecer la funcionalidad nativa IPv6. Por lo tanto, el tráfico IPv6 tiene que cruzar la red IPv4 existente, que es posible gracias a las técnicas de los túneles IPv6. [30]

[28] Dual Stack Transition Mechanism - (Network Dictionary)
[29] (Microsoft Corporation, 2003 (actualización febrero 2008))
[30] Additional IPv6 Infrastructure (Tunnels), (Network Dictionary)

A este método también se le llama encapsulación debido a que la información de un protocolo es encapsulada en el interior del paquete de otro protocolo, lo cual posibilita que la información pueda ser acarreada por medio del segundo protocolo, en este caso IPv4. Este mecanismo puede ser utilizado cuando dos nodos o redes que utilizan el mismo protocolo desean comunicarse a través de una red que utiliza un protocolo de red distinto. Este proceso requiere de tres etapas:

- Encapsulación
- Des encapsulación
- Administración del túnel.

Se requiere de dos extremos del túnel, que en el caso general son nodos IPv4/IPv6 de Pila Dual (normalmente routers), para manejar la encapsulación y des encapsulación. [30]

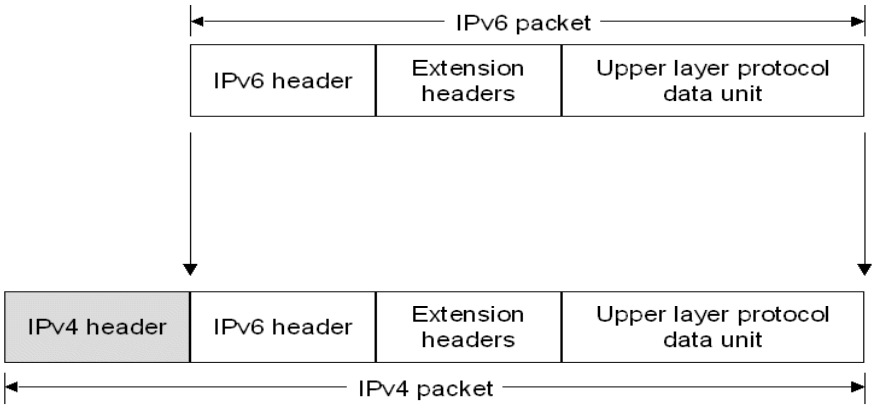
Para la encapsulación se requiere que en el encabezado del paquete se realicen las siguientes modificaciones:

- El campo Protocolo IPv4 está configurado a 41 para indicar un encapsulado de paquetes IPv6
- Los campos de direcciones de origen y de destino están configurados para las direcciones IPv4 de los extremos del túnel. Estos Extremos del túnel son configurados manualmente como parte de las interfaces de túnel. [31]

[31] (Microsoft Corporation, 2003 (actualización febrero 2008))

En la siguiente Figura se muestra como un paquete IPv6 es encapsulado dentro de un paquete IPv4.

Figura 6: Túnel IPv6 sobre IPv4 [31]



Los túneles pueden ser configurados de 4 formas distintas:

1. Router a router, que abarca un segmento del camino end-to-end entre dos hosts. Este es probablemente el método más común.
2. Host a Router, que abarca la primera parte del camino end-to-end entre dos hosts.
3. Host a Host, que abarca la totalidad del camino end-to-end entre dos hosts.
4. Router a Host, que abarca el último segmento del camino end-to-end entre dos hosts. Dependiendo de qué tipo de configuración se utiliza un túnel podría ser "configurado" (ambas partes deben ser configurados en consecuencia), "semi-configurado" (sólo un lado tiene que ser configurado, el otro lado actúa como una puerta de entrada) o " automático ", donde casi no hay nada que hacer para configurar los dos hosts.[32]

[32] Additional IPv6 Infrastructure (Tunnels), (Network Dictionary)

2.4 Infraestructura DNS

Una infraestructura DNS (sistema de nombres de dominio) es necesaria para el éxito de la convivencia entre IPv6 e IPv4 a causa de la frecuente utilización de nombres de direcciones en lugar de hacer referencia a las direcciones de red. La mejora de la infraestructura DNS consiste en rellenar los servidores DNS con registros que soporten la resolución de nombre a dirección y dirección a nombre para IPv6. Luego de que las direcciones sean obtenidas por medio de una consulta utilizando un nombre DNS, el nodo que envía debe seleccionar que direcciones utilizar para la comunicación.[33]

2.4.1 Registros de dirección

Las direcciones IPv6 se representan en el DNS mediante registros "AAAA", también llamados "*quad-A*" por la analogía de los registros "A" de IPv4.

La infraestructura DNS debe contener los siguientes registros de recursos para una exitosa resolución de nombres de dominio a direcciones: [33]

- Registros "A" para nodos IPv4
- Registros "AAAA" para nodos IPv6

2.4.2 Registros puntero

La infraestructura DNS debe contener los siguientes registros de recursos para una exitosa resolución de direcciones a nombres de dominio: [33]

- Registros PTR en el dominio IN-ADDR.ARPA para nodos IPv4
- Registros PTR en el dominio IP6.ARPA para nodos IPv6 (opcional).

[33] (Microsoft Corporation, 2003 (actualización febrero 2008))

2.4.3 Reglas para selección de direcciones

Para la resolución de nombres de dominio a direcciones de red, el nodo que consulta obtiene un conjunto de direcciones que corresponden al nombre consultado, por lo cual el nodo debe elegir que direcciones elegir como direcciones de origen y de destino para el paquete a enviar.

Esto no es un problema para un ambiente que maneja únicamente IPv4, pero para un ambiente en el que coexiste IPv4 e IPv6, el nodo debe elegir tanto el tipo como el ámbito de las direcciones de origen y destino a utilizar cuando se inicia la comunicación.[34]

El nodo debe de utilizar un conjunto de normas para la selección de direcciones, estas se encuentran definidas en el documento RFC 3484. Por default las direcciones IPv6 obtenidas en una consulta tienen mayor prioridad que las direcciones IPv4.[34]

[34] (Microsoft Corporation, 2003 (actualización febrero 2008))

3. CONFIGURACIÓN DE TÚNELES PARA IPV6

La comunicación en redes nativas IPv6 no refiere a ningún problema, pero cuando se necesita la comunicación de un nodo IPv6 a otro por medio de una infraestructura totalmente IPv4 es necesario recurrir a los túneles IPv6.

En el documento RCF 2893 se definen las siguientes configuraciones de túneles por medio de las cuales el tráfico IPv6 pueda viajar entre nodos IPv6/IPv4 a través de una infraestructura totalmente IPv4:[35]

- Router-to-Router
- Host-to-Router
- Router-to-Host
- Host-to-Host

"La clave para una transición de IPv6 satisfactoria es la compatibilidad con la base instalada existente de Hosts y Routers IPv4. El mantenimiento de la compatibilidad con IPv4 mientras se despliega IPv6 optimiza la tarea de transición de Internet a IPv6. Mientras se está desplegando la infraestructura IPv6, la infraestructura de direccionamiento de IPv4 existente puede permanecer funcional y se puede utilizar para llevar a cabo el tráfico IPv6."[36]

Las técnicas de tunelización se clasifican de acuerdo al mecanismo mediante el cual el nodo de encapsulación determina la dirección del nodo al final del túnel. En los métodos de Router-to-Router o de Host-to-Router, el paquete IPv6 se envía por el túnel a un Router. En los métodos de Host-to-Host o de Router-to-Host, el paquete IPv6 se envía por el túnel directamente hasta el destino final. [36]

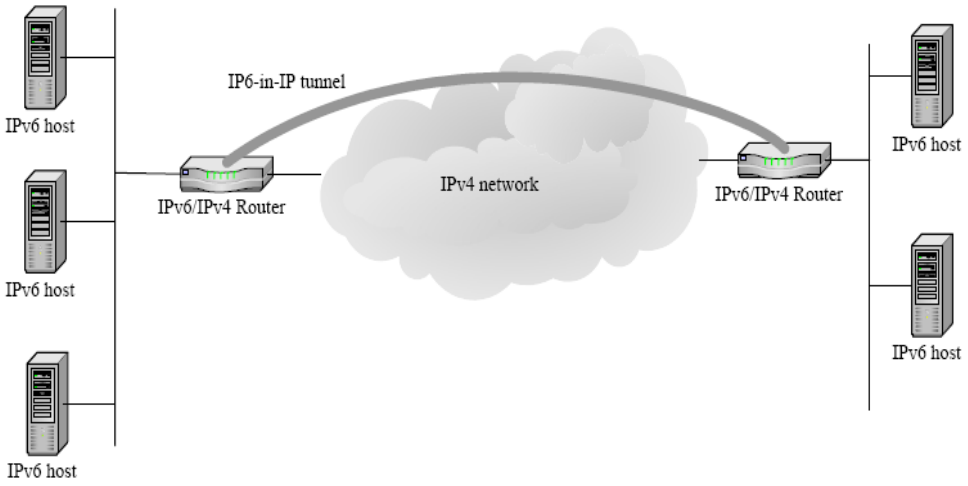
[35] (Gilligan & Nordmark, 2000)
(Microsoft Corporation, 2003 (actualización febrero 2008))
[36] (IBM)

3.1 Router- a -router

En este tipo de configuración se sitúan dos Routers IPv6 que conectan a dos infraestructuras con capacidad para IPv6 a través de una infraestructura IPv4. Los extremos del túnel abarcan un vínculo lógico en el camino entre la fuente y el destino por lo que el túnel entre los dos routers representa un único salto. [37]

En la siguiente figura se representa el Túnel de Router a Router:

Figura 7: Túnel de Router a Router[38]



Algunos ejemplos de este tipo de configuración:

- Un laboratorio de pruebas IPv6-only que utiliza un túnel para cruzar la infraestructura IPv4 de la organización para poder acceder a internet IPv6.
- Dos dominios de ruteo IPV6-only que utilizan un túnel para cruzar el internet IPv4.
- Un router 6to4 a través de la infraestructura IPv4 para buscar a otro router 6ro4.[39]

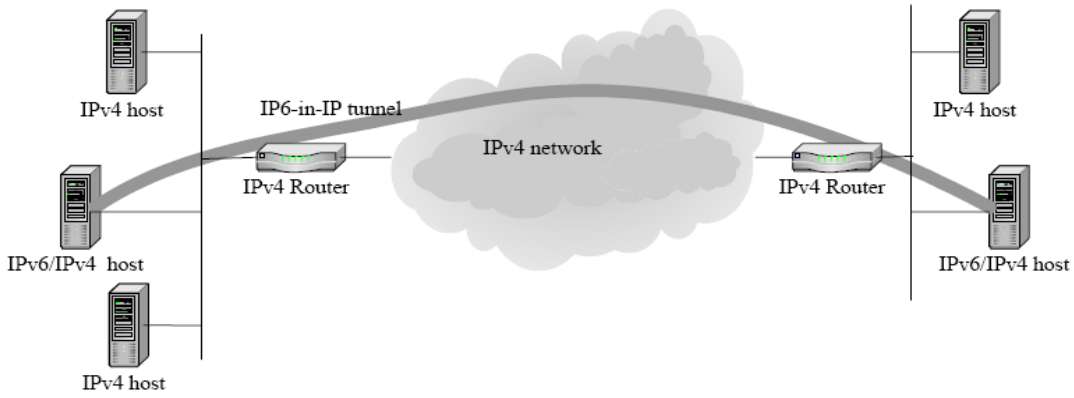
[37] (Gilligan & Nordmark, 2000)
[38] (HP, 2004)

3.2 Host – a – host

En la configuración del túnel de Host a Host, un nodo IPv6/IPv4 situado dentro de una infraestructura IPv4 crea un túnel para comunicarse con otro nodo IPv6/IPv4 situado dentro de la misma infraestructura IPv4. Los extremos del túnel abarcan el camino completo entre los nodos origen y destino y este túnel actúa como un único salto a lo largo del recorrido del paquete enviado. [40]

En cada nodo IPv6/IPv4, se crea una interfaz que represente al túnel IPv6 sobre IPv4, las rutas pueden estar presentes para indicar que el nodo de destino está en la misma subred lógica definida por la infraestructura de IPv4. En la siguiente Figura se muestra un túnel de Host a Host:

Figura 8: Túnel de Host a Host[41]



Ejemplos de este tipo de configuración:

- Nodos IPv6/IPv4 que utilizan direcciones ISATAP para atravesar la infraestructura IPv4 de la organización.
- Nodos IPv6/IPv4 que usan direcciones IPv4 compatibles para cruzar la infraestructura IpPv4 de la organización. [40]

[39] (Microsoft Corporation, 2003 (actualización febrero 2008))
[40] (Microsoft Corporation, 2003 (actualización febrero 2008))
[41] (HP, 2004)

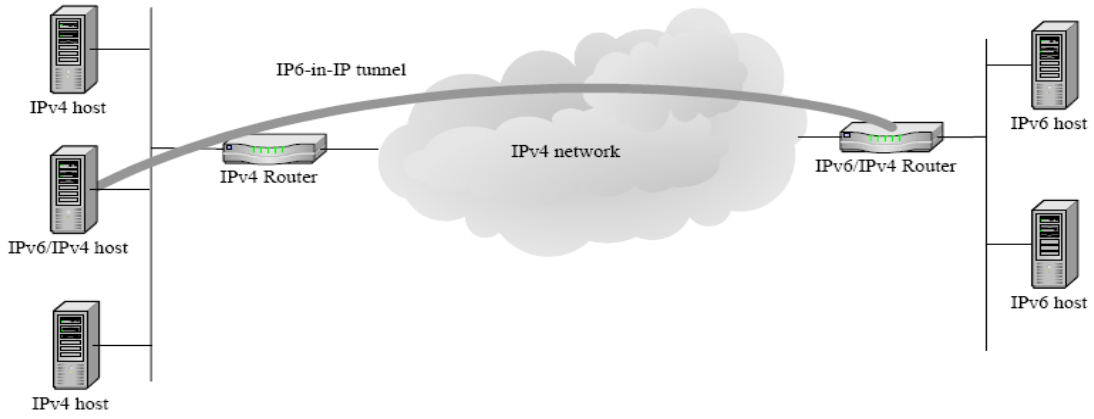
3.3 Host- a – router y router – a - host

En la configuración de Host a Router, un nodo IPv6/IPv4 que reside en una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para llegar a un router IPv6/IPv4, los extremos del túnel abarcan el primer segmento de la ruta entre el origen y el destino de los nodos. El túnel entre el host y el router actúa como un salto simple.[42]

El nodo IPv6/IPv4 se crea una interfaz de túnel que representa al túnel de IPv6 sobre IPv4 y se agrega una ruta (normalmente una ruta default) utilizando esta interfaz de túnel. El nodo envía el paquete basado en la ruta de la maquina, en la interfaz de túnel y en la dirección de destino del nodo IPv6/IPv4. Para la configuración de Router a Host, un router IPv6/IPv4 crea un túnel IPv6 sobre IPv4 para comunicarse con un nodo IPv6/IPv4 a través de una infraestructura IPv4. Los extremos del túnel abarcan el último segmento del camino entre los nodos de origen y de destino.

En la siguiente gráfica se ilustra un túnel de Host a Router para los paquetes que viajen de un host IPv4 a un host IPv4. El túnel de Router a Host se llevara en el caso de un paquete que viaje de uno de los nodos IPv6 hacia uno de los nodos IPv4.

Figura 9: Configuración de Host a Router[43]



[42] (Microsoft Corporation, 2003 (actualización febrero 2008))
[43] (HP, 2004)

3.4 Tipos de túneles

En el documento sobre los mecanismos de transición para IPv6, el RFC 2893, se describen dos tipos de túneles:

- Túneles configurados
- Túneles automáticos

3.4.1 Túneles configurados

Estos túneles requieren la configuración manual de los extremos del túnel. Las direcciones de los extremos del túnel no son derivadas de direcciones que se encuentran codificadas en la dirección "next-hop" cuando se envía o reenvía un paquete.[44] Para el control de las rutas del túnel, y para reducir la posibilidad de retransmitir ataques de denegación de servicio, configurar manualmente los túneles pueden ser una ventaja sobre la configuración automática de los túneles.[45]

Los túneles de Router a Router pueden ser configurados manualmente, la configuración de la interfaz del túnel que consiste en las direcciones IPv4 para los extremos del túnel deben ser especificadas manualmente con rutas estáticas que utilizara la interfaz del túnel.

3.4.1.1 Configuración manual de túneles en Sistemas Windows XP:

La creación de túneles estáticos en Windows XP se puede realizar mediante los siguientes pasos: [46]

1. Crear un túnel IPv6 sobre IPv4 llamado "MiTunel"

*C:\>netsh interface ipv6 add v6v4tunnel mitunel 195.251.29.15 *
195.251.29.243 enable

[44] (Microsoft Corporation, 2003 (actualización febrero 2008))
[45] (Network Dictionary, 2008)
[46] (Network Dictionary, 2008)

2. Agregar una dirección IPv6 al túnel

C:\>netsh interface ipv6 add address "mitunel" 2001:DB8:1::1

3. Agregar una ruta default a la dirección IPv6 remota del túnel para que todo el trafico IPv6 vaya a través del túnel.

C:\>netsh interface ipv6 add route ::/0 "mitunel" 2001:DB8:1::2

3.4.1.2 Configuración manual de túneles en sistemas Linux

La forma más fácil para la configuración de un túnel en un sistema Linux es por medio del comando "IP".[47]

1. Crear una interfaz para el túnel IPv6 sobre IPv4, en este caso llamada sit1:

*# ip tunnel add sit1 remote <IPv4 address of remote tunnel endpoint> *
local <local IPv4 address>

2. Activar la interfaz

 # ip link set sit1 up

3. Equipar la interfaz con una dirección IPv6

 # ip add addr <IPv6 address>/<subnet-length> dev sit1

La configuración final para la interfaz configurada podrá ser visualizada con el comando "ifconfig sit1" y deberá ser similar a la siguiente:

sit1 Link encap: IPv6-in-IPv4
inet6 addr: 2001:DB8:1::FFF0:2/112 Scope:Global
inet6 addr: FE80::80B0:B807/128 Scope:Link
UP POINTOPOINTRUNNING NOARP MTU:1480 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors: 0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0

La creación de túneles y añadir direcciones IPv6 también se puede lograr con el comando "ifconfig", pero se trata de un estilo anticuado y no debe utilizarse en las nuevas distribuciones de Linux. [47]

3.4.2 Túneles automáticos

Los túneles de este tipo no requieren de configuración manual, los extremos del túnel para un túnel automático son determinados por el uso de rutas, direcciones next-hop basadas en el destino de las direcciones IPv6, e interfaces lógicas del túnel. [48]

Este tipo de mecanismo de túnel ha sido uno de los primeros que se han formulado y desde entonces ha sido sustituido por la mayoría de mecanismos más sofisticados. Utiliza direcciones IPv4 compatibles con IPv6 en los extremos del túnel. Este método solo puede ser utilizado en comunicaciones Router a Host y Host a Host debido a que son los únicos esquemas en los que el final del túnel es a la vez el destinatario de los paquetes. “Debido a la utilización de determinadas direcciones que sólo funciona en túneles IPv6 sobre IPv4 y no viceversa.”[49]

Algunas de las tecnologías soportadas por el protocolo IPv6 para túneles automáticos son las siguientes:

- ISATAP: Es utilizado para comunicación unicast a través de una intranet IPv4 y por default se encuentra habilitada.
- 6to4: Similar al anterior, es utilizado para comunicación unicast pero a través de internet IPv4, también se encuentra habilitada por default.
- Teredo: Es utilizado para comunicación unicast a través de internet IPv4 por medio de traductores de direcciones de red (NAT). Por default este se encuentra deshabilitado.

[47] (Network Dictionary, 2008)
[48] (Microsoft Corporation, 2003 (actualización febrero 2008))
[49] (Networking Dictionary)

4. ISATAP

Por sus siglas en inglés ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) es un mecanismo de transición de IPv6 para transmitir paquetes de IPv6 entre un infraestructura IPv4 por medio de la encapsulación de los paquetes IPv6 dentro de encabezados IPv4. Gracias a este acercamiento se permite a las organizaciones iniciar una migración hacia IPv6 sin necesidad de tener que gastar grandes cantidades de dinero o tiempo para actualizar y configurar su arquitectura de ruteo con soporte de IPv6 nativo. [50]

Más específicamente ISATAP es una asignación de direcciones y una tecnología de Túneles Automáticos Host a Host, Host a Router y Router a Host que es utilizada para proveer conectividad unicast IPv6 entre hosts IPv6/IPv4 a través de una intranet IPv4. Los nodos ISATAP no requieren de ninguna configuración manual y pueden crear direcciones ISATAP utilizando mecanismos de autoconfiguración de direcciones estándares. Este mecanismo esta descrito en el RFC 4214 pero posteriormente fue suplantado por el RFC 5214. [51]

Las direcciones ISATAP hacen uso de alguno de los siguientes identificadores de interfaz:

::0:5EFE:w.x.y.z, *en el cual w.x.y.z es una dirección privada IPv4.*
::200:5EFE:w.x.y.z, *en el cual w.x.y.z es una dirección publica IPv4.*

Un identificador de interfaz ISATAP puede ser combinado con cualquier prefijo de 64 bits que sea válido para direcciones unicast IPv6.

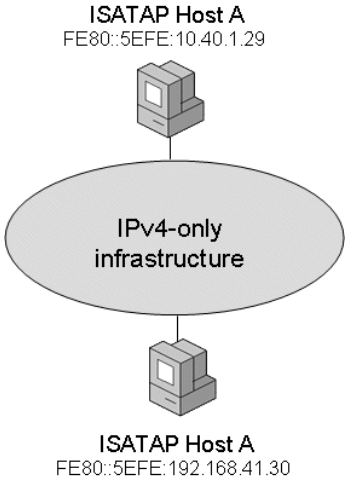
[50] (Microsoft Corporation , 2006)
[51] (Microsoft Corporation, 2003 (actualización febrero 2008))

La parte del identificador que contiene la dirección IPv4 es usada para determinar la dirección de destino IPv4 para el encabezado IPv4 cuando el trafico IPv4 direccionado por ISATAP es enviado a través de una red IPv4. [51]

Para los equipos de Windows, el protocolo de IPv6 automáticamente configura ISATAP con direcciones del tipo link-local FE80::5EFE:*w.x.y.z o* FE80::200:5EFE:*w.x.y.z* en las interfaces de túnel ISATAP para cada dirección IPv4 que es asignada al nodo. Con estas direcciones ISATAP link-local le es posible a dos host comunicarse por medio de una red IPv4-only.

Ejemplo: dos nodos, Host A y Host B con la asignación de las direcciones IPv4 10.40.1.29 y 192.168.41.30 respectivamente, recibirán una dirección ISATAP al momento de activar el protocolo IPv6. El Host A será configurado automáticamente con la dirección ISATAP FE80::5EFE:10.40.1.29 y el Host B con la dirección FE80::5EFE:192.168.41.30.

Figura 10: Ejemplo de una configuración ISATAP[52]



De esta forma cuando el Host A envía tráfico IPv6 hacia el Host B utilizando la dirección Link-local ISATAP del host B, las direcciones de origen y destino para los encabezados tanto IPv4 e IPv6 quedarían de la siguiente manera:

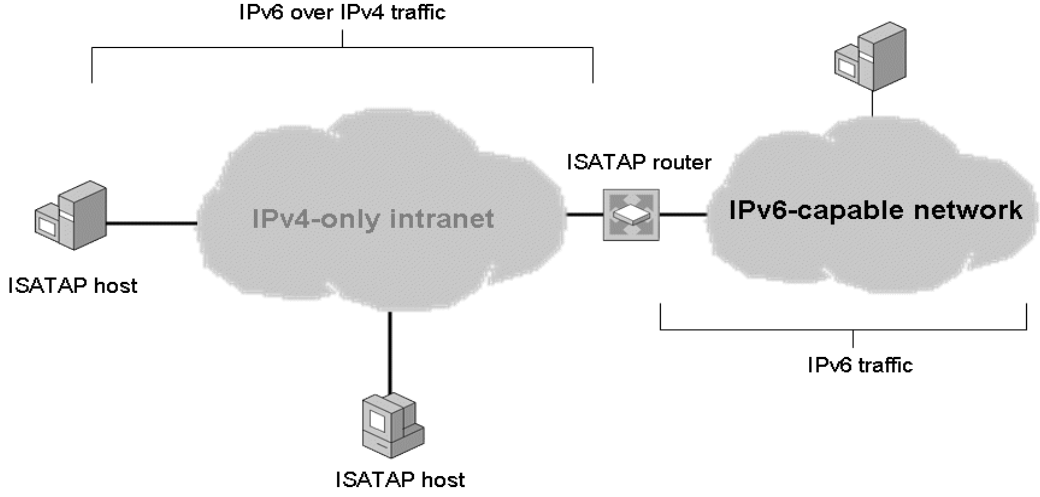
[52] (Microsoft Corporation, 2003 (actualización febrero 2008))

Campo	Valor
IPv6 - dirección de origen	FE80::5EFE:10.40.1.29
IPv6 - dirección de destino	FE80::5EFE:192.168.41.30
IPv4 - dirección de origen	10.40.1.29
IPv4 - dirección de destino	192.168.41.30

4.1 Componentes ISATAP

En la siguiente Figura se muestran cuales son los elementos de una intranet que haga uso de ISATAP:

Figura 11: Componentes de ISATAP[53]



4.1.1 Hosts ISATAP:

Los hosts ISATAP poseen una interfaz de túnel y realizan su propio túnel hacia otros nodos o routers ISATAP. Las direcciones ISATAP link-local permiten hosts en la misma subred lógica para que se comuniquen entre ellos pero no con otros nodos IPv6 en otras subredes IPv6.[53]

[53] (Microsoft Corporation, 2003 (actualización febrero 2008))

4.1.2 Router ISATAP

Los routers ISATAP son utilizados para permitir la comunicación más allá de la subred ISATAP haciendo uso de direcciones globales basadas en ISATAP. Para llevar a cabo esto los Hosts deben tunelizar sus paquetes hacia un router ISATAP.

Un router ISATAP es un router IPv6 que realiza lo siguiente:

- Anuncia los prefijos de la dirección para poder identificar la subred ISATAP en la cual los nodos se encuentran situados. Los hosts utilizan los prefijos de dirección para configurar direcciones ISATAP locales o globales.
- Transmiten paquetes entre hosts ISATAP dentro de la subred ISATAP y hosts IPv6 en otras subredes.
- Actúan como un Defaul Router para los hosts ISATAP.

Cuando un host ISATAP recibe un anuncio de un router ISATAP, este agrega una ruta default (::/0) configurando en la dirección next-hop de su interfaz de túnel ISATAP con la dirección ISATAP link-local del router. Cuando un host envía un paquete hacia destinos fuera de la subred ISATAP, el paquete es tunelizado a la dirección IPv4 del router ISATAP correspondiente a la interface de router ISATAP en la red IPv4-only, luego el router ISATAP transmite el paquete IPv6. [54]

4.2 Obtener un prefijo ISATAP

La dirección IPv4 del router ISATAP es obtenida por medio de uno de los siguientes métodos:

- La resolución exitosa del nombre “ISATAP” hacia una dirección IPv4
- Por medio del comando *netsh interface isatap set router*

[54] (Microsoft Corporation, 2003 (actualización febrero 2008))

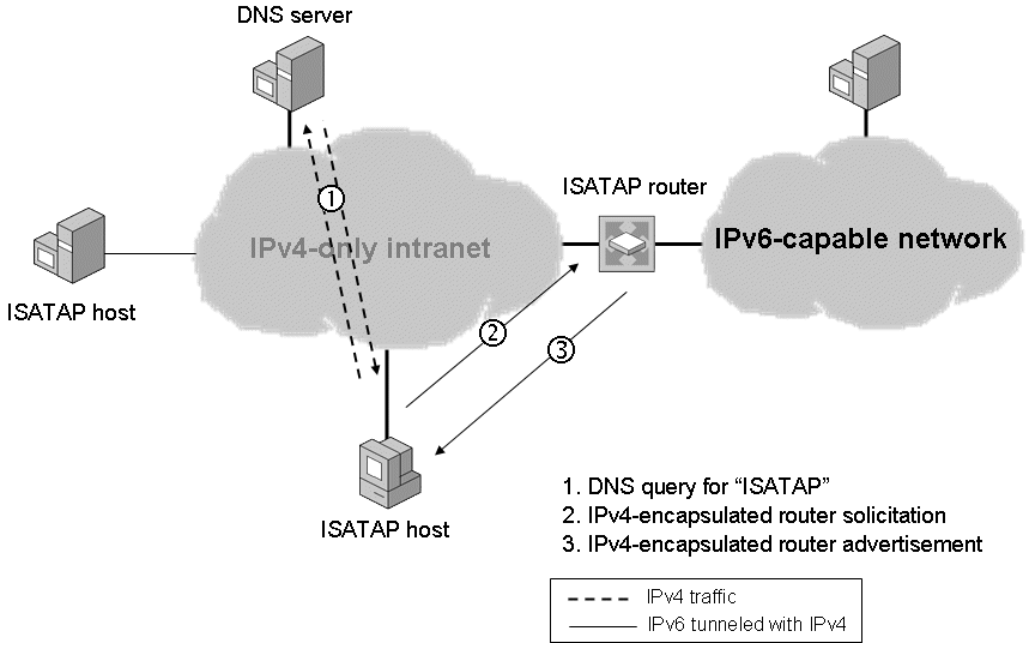
Los equipos con sistema Windows server 2003 o Windows XP hacen uso del comando *netsh interface isatap set router*

4.2.1 Resolución del nombre "ISATAP"

Al iniciar el servicio de IPv6 para un equipo de Windows, este intenta resolver el nombre "ISATAP" a una dirección IPv4 utilizando técnicas normales de resolución de nombres TCP/IP. Si la resolución del nombre es exitosa, el host envía un mensaje IPv4 encapsulado de solicitud de Router hacia el Router ISATAP, luego el router envía un mensaje IPv4 encapsulado de aviso de router unicast, este mensaje contiene el prefijo a utilizar para la configuración de direcciones basadas en ISATAP, opcionalmente también se hace conocer como el default router.[55]

El proceso para lo obtención del prefijo ISATAP es mostrado en la siguiente Figura:

Figura 12: Proceso de obtención de un prefijo ISATAP [55]



[55] (Microsoft Corporation, 2003 (actualización febrero 2008))

En la gráfica que puede visualizar la secuencia de los paquetes que son enviados a través de la red IPv4, en primer paso se consulta al servidor local de DNS sobre el nombre “ISATAP”, este responde con la dirección del router ISATAP con lo cual el host envía ahora paquetes IPv6 encapsulados con encabezado IPv4 hacia el router ISATAP.

Algunas formas comunes para la resolución de nombres por TCP/IP son las siguientes: [56]

1. Revisar el nombre de host local
2. Chequear el cache de cliente DNS, esto incluye revisar en el archivo Hosts en el directorio *SystemRoot*\system32\drivers\etc\
3. Formar el nombre de dominio y enviar una consulta DNS
4. Utilizar Link-Local Multicast Name Resolution (LLMNR) para intentar resolver el nombre “ISATAP” en la subred local.
5. Convertir el nombre ISATAP en un nombre NetBIOS "ISATAP <00> y revisar el cache de nombres NetBIOS.

4.2.2 Comando “*netsh interface isatap set router*”

La resolución automática del nombre ISATAP es la opción por default y recomendada para la configuración de la dirección IPv4 del router ISATAP, sin embargo esta acción se puede realizar manualmente mediante el comando:

netsh interface isatap set router AddressOrName

El campo *AddressOrName* se refiere al nombre del router o a la dirección IPv4 de la interfaz de intranet del router ISATAP. Por ejemplo si la dirección IPv4 del router es *192.168.39.1*, el comando se formará de la siguiente manera:

netsh interface isatap set router 192.168.39.1

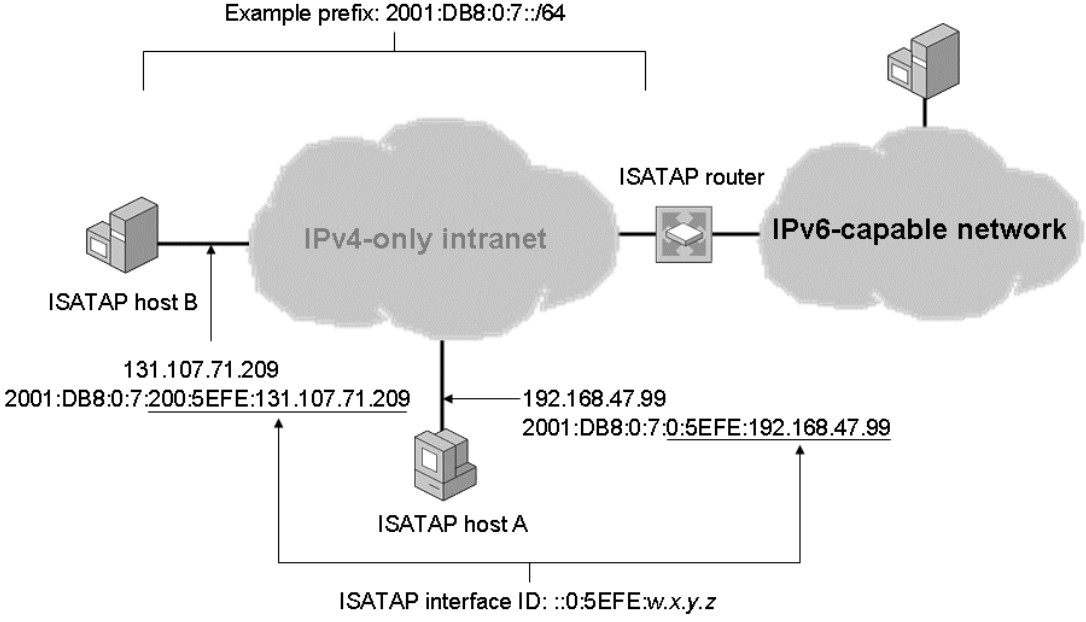
[56] (Microsoft Corporation, 2003 (actualización febrero 2008))

Luego de que ha sido configurado el host envía un mensaje IPv4 encapsulado de solicitud de Router hacia el Router ISATAP, el router envía un mensaje IPv4 encapsulado de aviso de router unicast, este mensaje contiene el prefijo a utilizar para la configuración de direcciones basadas en ISATAP, opcionalmente también se hace conocer como el default router.[56]

4.3 Ejemplo de direccionamiento ISATAP

Un ejemplo sobre la configuración de las direcciones ISATAP dentro de una subred IPv4 se muestra en la siguiente Figura:

Figura 13: ejemplo de direccionamiento ISATAP[57]



[57] (Microsoft Corporation, 2003 (actualización febrero 2008))

En la ilustración se puede visualizar al aviso realizado por el router ISATAP, haciendo conocer el prefijo global de subred 2001:DB8:0:7::/64 para la subred lógica ISATAP.

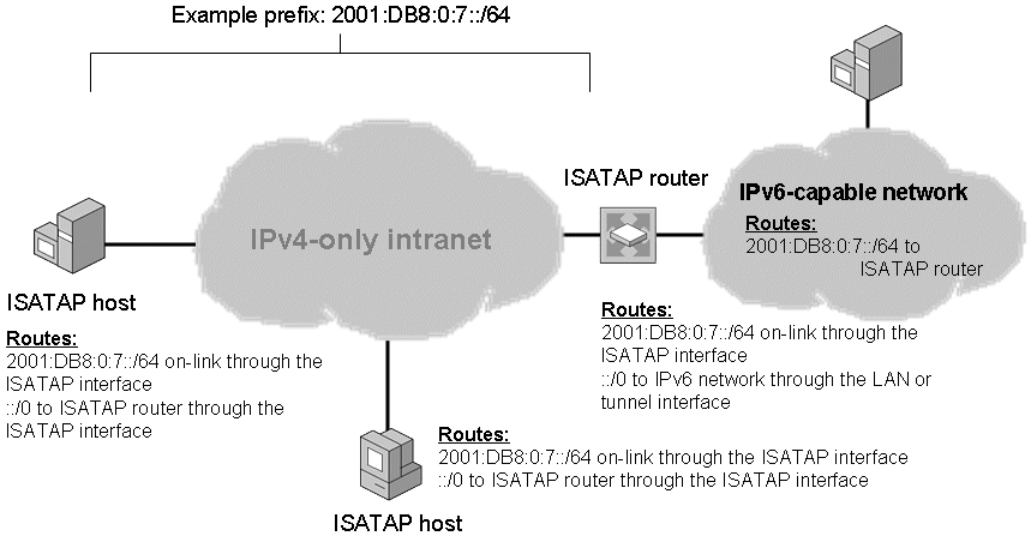
El host A configurado con una dirección IPv4 192.168.47.99 utilizara el prefijo anunciado por el router ISATAP para configurar automáticamente la dirección global ISATAP a 2001:DB8:0:7:0:5EFE:192.168.47.99. [57]

De igual manera el host B con una dirección IPv4 131.107.71.209 utilizara el prefijo para configurar automáticamente la dirección ISATAP a 2001:DB8:0:7:200:5EFE:131.107.71.209.[57]

4.4 Ruteo ISATAP

En la siguiente Figura se muestran las rutas relevantes para cada nodo dentro de la subred que les permita comunicación ISATAP.

Figura 14: Ejemplo de ruteo ISATAP[58]



[58] (Microsoft Corporation, 2003 (actualización febrero 2008))

Los hosts ISATAP utilizan las siguientes rutas:

- Una ruta on-link para el prefijo de subred lógica ISATAP que utiliza la interfaz ISATAP. Esta ruta permite al host realizar túneles host a host para buscar a otros hosts ISATAP dentro de la misma subred lógica.

- Una ruta default que utiliza la interfaz ISATAP y tiene la dirección next-hop del router ISATAP. Esta ruta permite a los hosts realizar tuneles host a router para buscar a otros hosts IPv6 en otra subred IPv6.

Un router ISATAP utiliza las siguientes rutas:

- Una ruta on-link para el prefijo de subred ISATAP que utiliza la interfaz ISATAP. Esta ruta permite al router realizar túneles router a host para buscar otros hosts ISATAP en la subred ISATAP.

- Una ruta default que contiene la dirección next-hop del siguiente router en la red IPv6. Esta ruta permite al router ISATAP reenviar trafico IPv6 a destinos que no están situados en la subred ISATAP.

Los routers de la red IPv6 utilizan una ruta para el prefijo de subred ISATAP que apunta de regreso al router ISATAP. Esta ruta permite a los routers de la red IPv6 reenviar el tráfico destinado a los hosts ISATAP. [59]

[59] (Microsoft Corporation, 2003 (actualización febrero 2008))

4.5 Configuración de un router ISATAP

La configuración de un router en un equipo con sistema Windows Server 2008 o Windows Vista, asumiendo que el router ya se encuentra configurado para el reenvió de paquetes IPv6 en sus interfaces LAN y que ya cuenta con una ruta default configurada para ser publicada, los comandos necesarios para la configuración como router ISATAP son los siguientes:

netsh interface isatap set router AddressOrName
netsh interface ipv6 set interface InterfaceNameOrIndex forwarding=enabled advertise=enabled
netsh interface ipv6 add route Address/PrefixLength InterfaceNameOrIndex publish=yes

El primer comando especifica la dirección IPv4 de la interfaz IPv4 de los routers ISATAP dentro de la intranet o el nombre del router que resuelve a la dirección IPv4 de las interfaces IPv4 de intranet de los routers.El Segundo comando habilita el reenvió e informa sobre el nombre o el índice de la interfaz de túnel ISATAP.

El tercer comando habilita la publicación del prefijo específico de subred sobre la interfaz de túnel. Este comando puede ser utilizado una o múltiples veces para informar tantos prefijos sea necesario.

Todos los prefijos configurados utilizando este comando son incluidos en el mensaje de información del router que es enviado a los hosts ISATAP.

4.6 Configuración de ISATAP en LINUX

Para la instalación de ISATAP en un sistema Linux son necesarios los siguientes elementos: [60]

- Kernel 2.4.x con ISATAP [clients y router]
- Paquete iproute [clients y router]
- radvd con soporte ISATAP [solo router]

4.6.1 Router ISATAP en Linux

El router es el responsable por el ruteo IPv6 desde y hacia los clientes ISATAP, por lo que debe de tener conectividad IPv6 y al menos una subred /64 que va a ser dedicada a la interfaz ISATAP. [60]

La funcionalidad ISATAP es habilitada mediante la creación de un túnel en modo *isatap* por medio del comando *ip tunne.* Se debe elegir una dirección IPv4 para la dirección del router ISATAP y esta dirección no tiene que ser utilizada en ningún otro túnel IP. Como ejemplo la dirección elegida para la configuración de la interfaz ISATAP del router es w.x.y.z. [60]

 # ip tunnel add is0 mode isatap local w.x.y.z ttl 64

La interfaz del túnel puede tener cualquier nombre válido por el kernel, pero se sugiere la utilización del nombre "isX" donde x es un correlativo. [60]

Luego de que la interfaz es creada es necesario que esta sea habilitada y que se le agregue una dirección IPv6 compatible con ISATAP: [60]

 # ip link set is0 up
 # ip addr add PREFIX::5EFE:w.x.y.z/64 dev is0

[60] (litech.org, 2002)

A modo de ejemplo para un router que utilice la dirección 192.0.2.1 como dirección de router ISATAP, con un prefijo 3ffe:ffff:1234:5678::/64 asignado a los clientes, los comandos serian los siguientes: [60]

```
# ip tunnel add is0 mode isatap local 192.0.2.1 ttl 64
# ip link set is0 up
# ip addr ADD 3FFE:FFFF:1234:5678::5EFE:192.0.2.1/64 dev is0
```

Una vez que el ISATAP se ha creado y configurado, *radvd* debe estar configurado para anunciar el prefijo adecuado para los clientes ISATAP. La configuración de una interfaz radvd ISATAP es idéntica a la configuración de una interfaz Ethernet, excepto que la directiva UnicastOnly debe aparecen en la definición de la interfaz. La definición de la configuración para la interfaz anterior quedara de la siguiente manera: [61]

```
interface is0
{
   AdvSendAdvert on;
   UnicastOnly on;
   AdvHomeAgentFlag off;

   prefix 3FFE:FFFF:1234:5678::/64
   {
      AdvOnLink on;
         AdvAutonomous on;
         AdvRouterAddr off;
   };
};
```

4.6.2 Clientes ISATAP en Linux

Para los clientes únicamente es necesario crear y habilitar la interfaz ISATAP. Además se debe de especificar la dirección del router ISATAP cuando se crean los túneles a modo de que los clientes conozcan a donde enviar las solicitudes de router. [61]

```
# ip tunnel add is0 mode isatap local 192.0.40.25 v4any 192.0.2.1 ttl 64
# ip link set is0 up
```

[61] (litech.org, 2002)

Los clientes solicitaran la dirección e información de ruta del router ISATAP y se configuraran automáticamente para el acceso a la red IPv6.

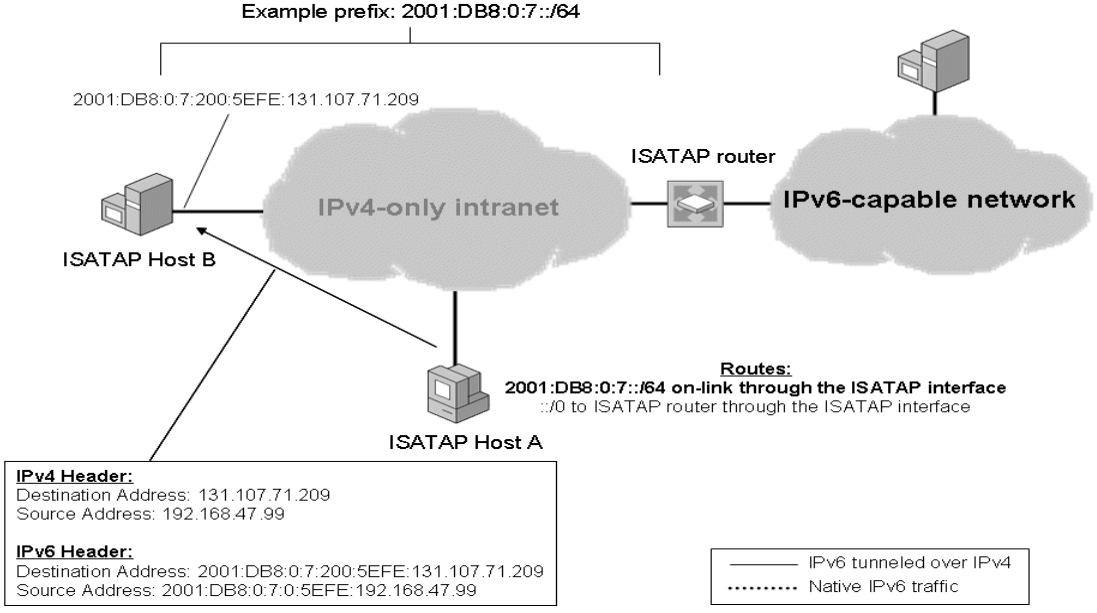
4.7 Ejemplos de comunicación ISATAP

En esta parte se ilustraran los detalles del funcionamiento de la comunicación ISATAP cuando un host envía un paquete hacia otro host dentro de la misma subred ISATAP y cuando un host ISATAP envía un paquete hacia un host IPv6 fuera de la subred lógica.

4.7.1 De host ISATAP a host ISATAP

La siguiente figura muestra como se realiza la comunicación entre dos nodos ISATAP que se encuentran dentro de la misma subred.

Figura 15: comunicación ISATAP de host a host[62]



[62] (Microsoft Corporation, 2003 (actualización febrero 2008))

El host A desea enviar un paquete hacia el host B, por lo que resuelve la dirección IPv6 del host B por medio de una consulta al DNS. Cuando se envía el paquete, el protocolo IPv6 en el host A determina que la ruta IPv6 más corta hacia el destino es la on-link 2001:DB8:0:7::/64.

Debido a que esta es una ruta on-link, la dirección next-hop IPv6 se configura con la dirección de destino 2001:DB8:0:7:200:5EFE:131.107.71.209. El paquete IPv6 y la dirección next-hop son manejadas por la interfaz ISATAP para ser procesadas. [63]

La interfaz ISATAP configura la dirección destino IPv4 dentro del encabezado IPv4 con los últimos 32 bits de la dirección next-hop, para lo cual en este caso es la dirección ISATAP del host B 131.107.71.209. El IPv4 sobre el host ISATAP A determina que la mejor dirección de origen para usar es la dirección asignada al host A 192.168.47.99, luego se envía el paquete.

En el host B se procesa el encabezado IPv4 y debido a que el campo “protocolo” tiene un valor de 41, deja el paquete IPv6 al protocolo IPv6 para su procesamiento.

4.7.2 De Host ISATAP a Host IPv6

Cuando se envía un paquete de un host ISATAP hacia un host en la red IPv6, el viaje del paquete tendrá dos partes:

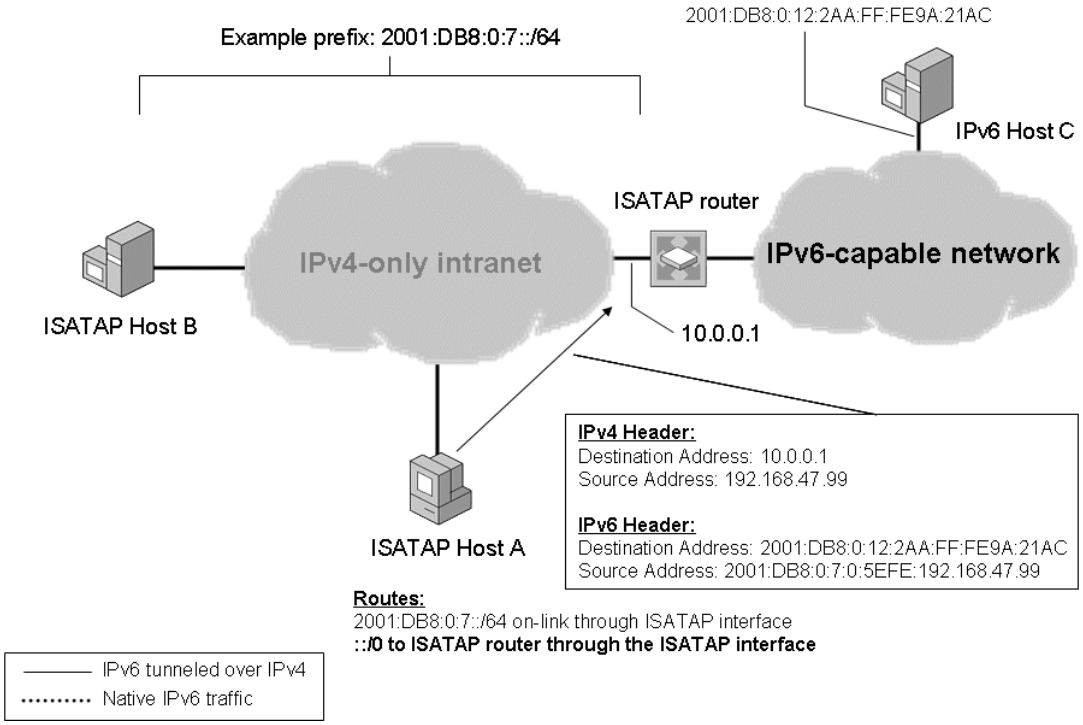
- del host ISATAP hacia el router ISATAP
- del router ISATAP hacia el host IPv6

En la gráfica, cuando el host A envía tráfico hacia un host que no se encuentra en la subred ISATAP, IPv6 en el host A realizara un proceso para determinar cuál es la ruta más cercana que concuerde con el destino, en este caso será la ruta default (::/0).

[63] (Microsoft Corporation, 2003 (actualización febrero 2008))

Esta ruta tiene una dirección IPv6 como next-hop correspondiente a la interfaz ISATAP del router. El paquete IPv6 y la dirección next-hop son manejados por la interfaz ISATAP para su procesamiento.

Figura 16: Comunicación de Host ISATAP a Host IPv6[64]



La interfaz ISATAP configura la dirección de destino IPv6 dentro del encabezado IPv4 con los últimos 32 bits de la dirección next-hop, en este caso la dirección es 10.0.0.1 correspondiente a la dirección ISATAP del router. IPv4 en el nodo A determina entonces que la mejor dirección de destino a usar es la dirección ISATAP del host A 192.168.47.99 y procede a enviar el paquete. Este es la primera parte del viaje que el paquete debe realizar para llegar a su destino.

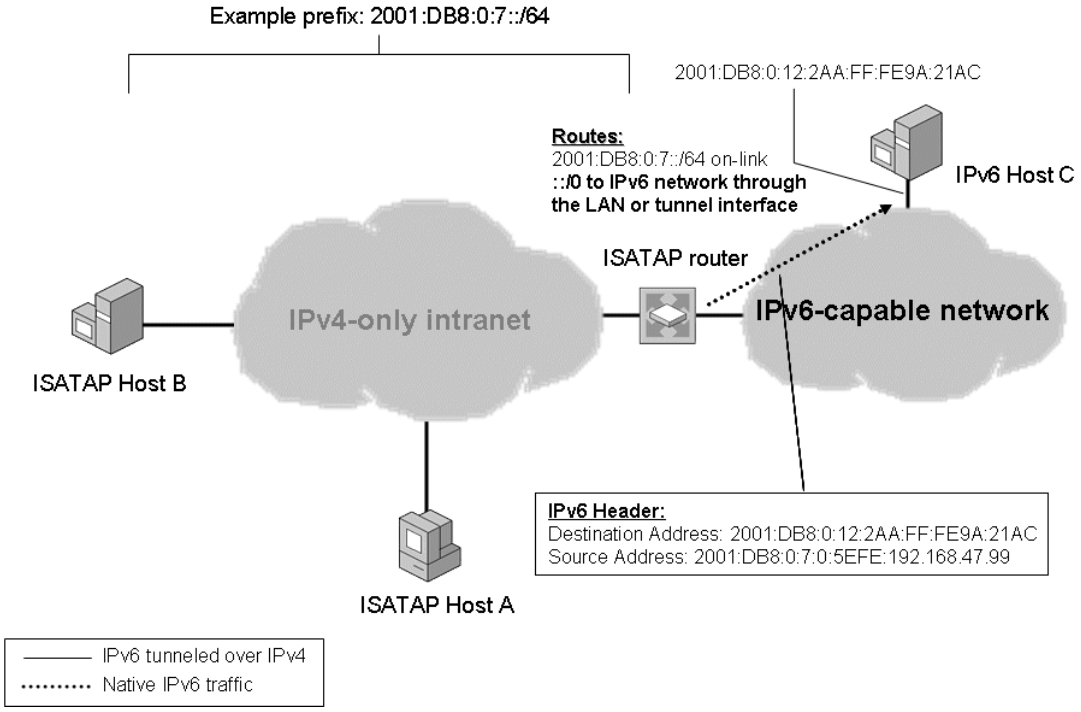
Al llegar al router, IPv4 procesa el encabezado IPv4 del paquete y debido a que el campo “Protocolo” está configurado con un valor 41, deja el paquete IPv6 para que sea procesado por el IPv6.

[64] (Microsoft Corporation, 2003 (actualización febrero 2008))

El protocolo IPv6 en el router realiza un proceso para determinar la mejor ruta hacia el destinatario y determina que esta es la ruta default. La ruta default tiene una dirección IPv6 del siguiente router IPv6 dentro de la red IPv6. El paquete IPv6 y la dirección son manejadas por la LAN o interfaz de túnel apropiada para su procesamiento. Para una interfaz LAN, al paquete se le despoja del encabezado IPv4 y el router IPv6 se encarga de reenviar el paquete IPv6 original.

Es entonces cuando el paquete IPv6 original es reenviado a través de la red IPv6 hacia su destino. La siguiente Figura muestra el viaje del paquete desde el router ISATAP hacia el host destino.

Figura 17: comunicación de Host ISATAP a Host IPv6 (parte 2)



5. TÚNELES 6to4

6to4 es otra tecnología de túneles automáticos utilizada para proveer conectividad unicast entre sitios y hosts IPv6 a través de Internet IPv4. Esta es una tecnología de túneles de Router a Router, Host a Router y de Router a Host. [65]

Este mecanismo utiliza el prefijo de dirección global 2002:*WWXX*:*YYZZ*::/48, donde WWXX:YYZZ es una representación hexadecimal de una dirección publica IPv4 asignada a un sitio o a un host.

La estructura de una dirección 6to4 es representada en la siguiente Figura.

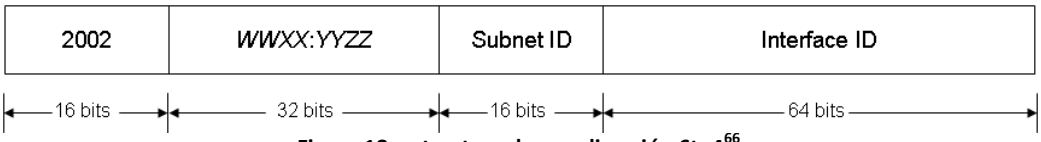


Figura 18: estructura de una dirección 6to4[66]

Los primeros 16 bits corresponden al prefijo de la dirección global (2002) y los siguientes 32 bits corresponden a una dirección IPv4 representada en formato hexadecimal. [65]

Una dirección 6to4 es una dirección IPv4 construida en base al prefijo 6to4 y una dirección IPv4 publica.

6to4 permite la asignación de direcciones globales IPv6 y buscar sitios dentro del internet IPv6 sin necesidad de obtener una conexión a internet IPv6 o un prefijo de dirección global IPv6 de un proveedor de servicios de internet ISP. [66]

[65] (Carpenter & Moore, 2001)
[66] (Microsoft Corporation, 2003 (actualización febrero 2008))

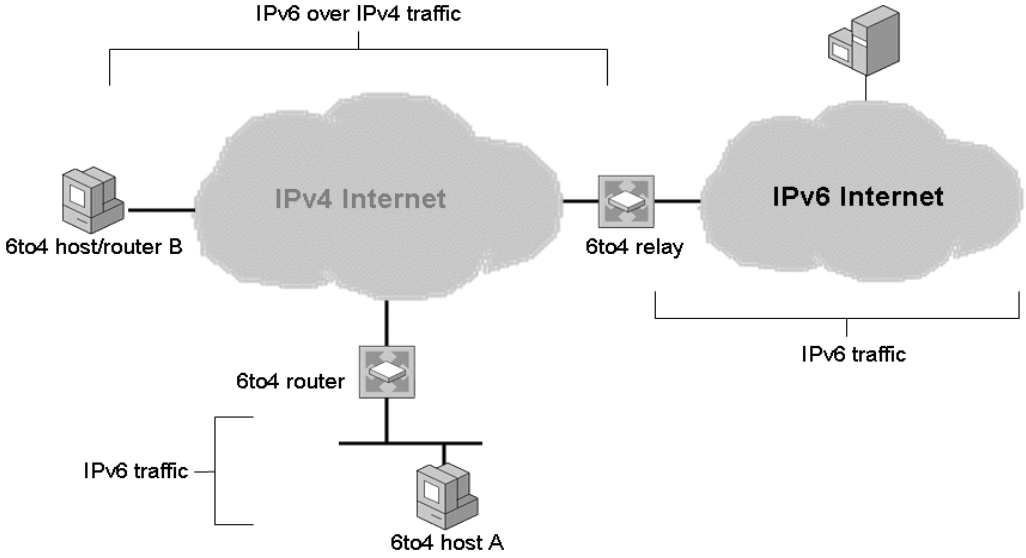
5.1 Componentes 6to4

En una arquitectura 6to4 interactúan los siguientes elementos:

- Host 6to4
- Router 6to4
- Host/Router 6to4
- Relay 6to4

Estos componentes son mostrados en la siguiente Figura:

Figura 19: Componentes 6to4[67]



5.1.1 Host 6to4

Es cualquier host que es configurado con una dirección 6to4, es decir una dirección IPv6 con el prefijo 2002::/16. Los hosts 6to4 no requieren de ninguna configuración manual y crean direcciones 6to4 utilizando mecanismos estándar de autoconfiguración de direcciones. Estos hosts no realizar tuneling IPv6 sobre IPv4. [68]

[67] (Microsoft Corporation, 2003 (actualización febrero 2008))
[68] (Carpenter & Moore, 2001)

Un host 6to4 debe tener al menos una dirección 6to4, en caso contrario este sería un nodo normal IPv6.

5.1.2 Router 6to4

Es un router IPv6/IPv4 que utiliza una interfaz de túnel 6to4 para reenviar trafico direccionado 6to4 entre los hosts 6to4 dentro de un sitio y otros routers 6to4, host/router 6to4, o relays 6to4 en la internet IPv4. Normalmente es un router entre un sitio IPv6 e internet IPv4. Estos routers requieren de adicionales configuraciones manuales. [69]

5.1.3 Host/Router 6to4

Es un host IPv6/IPv4 que utiliza una interfaz de túnel 6to4 para intercambiar trafico direccionado 6to4 con otros host/routers 6to4, routers 6to4 o relays 6to4 dentro de internet IPv4. Estos nodos no transmiten tráfico hacia hosts 6to4. [70]

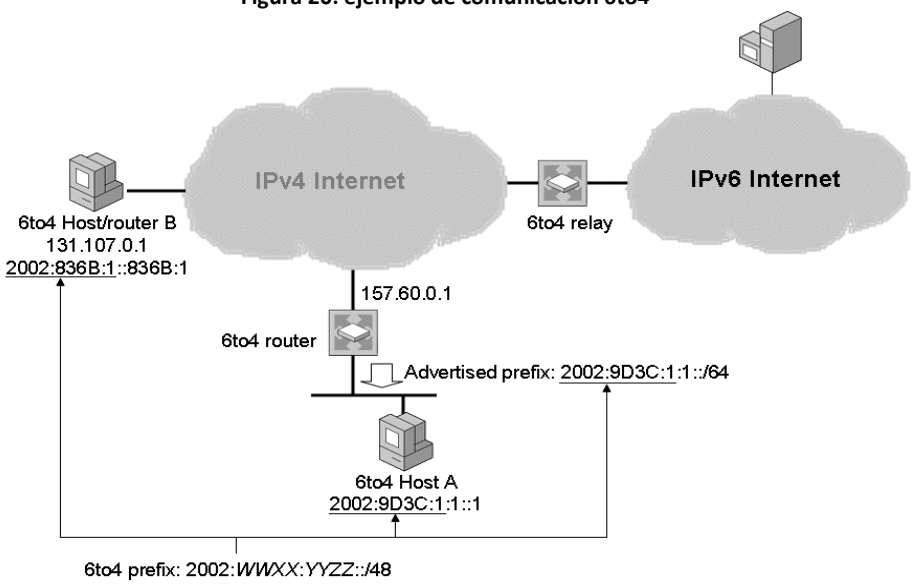
5.1.4 Relay 6to4

Son Routers IPv6/IPv4 que transmiten trafico 6to4 entre routers 6to4 y host/routers 6to4 en internet IPv4 y hosts en internet IPv6. Están configurados para transmitir tráfico entre direcciones 6to4 y direcciones IPv6 nativas.

[69] (Carpenter & Moore, 2001)
[70] (Microsoft Corporation, 2003 (actualización febrero 2008))

5.2 Ejemplo de direccionamiento

Figura 20: ejemplo de comunicación 6to4[70]



El router 6to4 está directamente conectado con internet y tiene configurada una dirección IPv4 pública: 157.60.0.1. Este router crea el prefijo de 48 bits 2002:9D3C:1::/48, en este prefijo el valor 9D3C:1 corresponde a la dirección publica del router en representación hexadecimal. El router publica el prefijo 2002:9D3C:1:1::/64 por la interfaz LAN conectada con la intranet privada. El último segmento del prefijo de 64 bits, en este caso el último 1, denominado *subnetId* puede ser configurado manualmente o determinado automáticamente por el router 6to4. [71]

Los hosts en la subred de la intranet privada configuran una dirección IPv6 basada en el prefijo 2002:9D3C:1:1::/64 utilizando configuración estándar de direcciones. En este caso la dirección para el host A se configura con el valor 2002:9D3C:1:1::1.

El host/router B está conectado directamente a internet y se configura con la dirección pública IPv4 131.107.0.1. El protocolo IPv6 en equipos Windows Server 2008

[71] (Microsoft Corporation, 2003 (actualización febrero 2008))

y Windows Vista configura automáticamente una dirección de la forma 2002:*WWXX*:*YYZZ*::*WWXX*:*YYZ,* de este modo el nodo B se asigna automáticamente la dirección IPv6 2002:836B:1::836B:1.

5.3 Selección de direcciones

Si en un host existen únicamente direcciones 6to4 y en otro host cuenta tanto con una direcciones 6to4 y una direcciones IPv6, entonces para ambos hosts serán utilizadas las direcciones 6to4. [72]

Si ambos hosts cuentan con una direccione 6to4 y una direccione IPv6, entonces las direcciones 6to4 deben ser utilizadas para ambos, o bien, se pueden utilizar las direcciones nativas IPv6 para ambos hosts. [72]

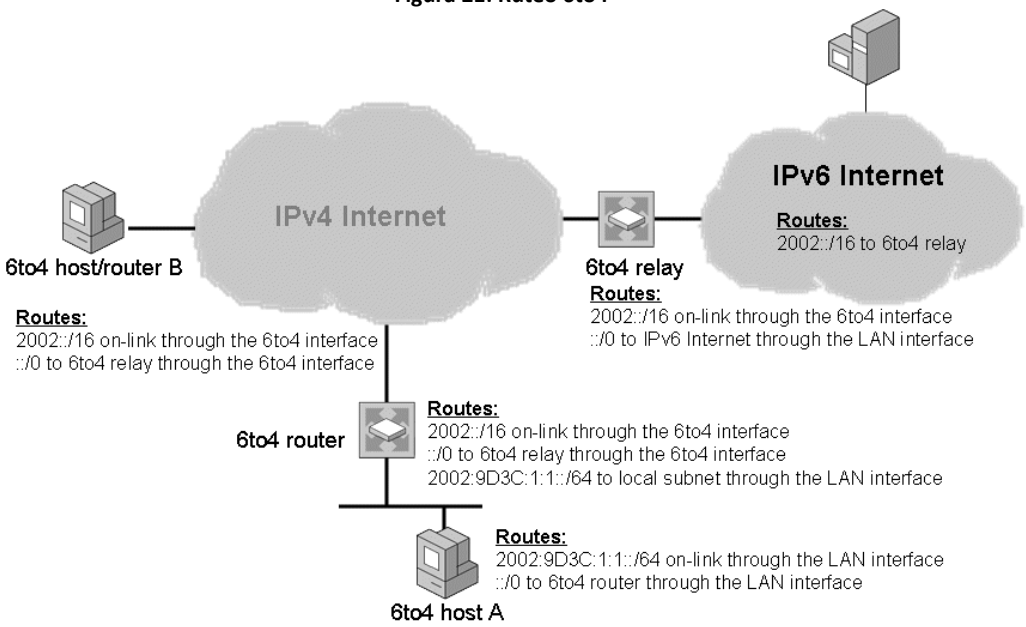
5.4 Ruteo en 6to4

Cada nodo involucrado dentro de la arquitectura 6to4 cuenta con rutas 6to4 que le permitan transmitir tráfico hacia los demás nodos en la arquitectura.

Un ejemplo de las rutas necesarias para cada nodo en particular es descrito mediante la configuración en la siguiente imagen:

[72] (Carpenter & Moore, 2001)

Figura 21: Ruteo 6to4[73]



5.4.1 Rutas de un host 6to4

Utiliza una ruta on-link para el prefijo de la subred de la intranet en su interfaz LAN. En la Figura, esta ruta es la ruta 2002:9D3C:1:1::/64.

El host 6to4 también cuenta con una ruta default a través de la interfaz LAN hacia el router 6to4. Por medio de esta ruta el host 6to4 puede comunicarse con otros host 6to4 y con otros nodos en internet IPv6. Un host 6to4 contara con mas rutas, pero estas son las rutas básicas que el host 6to4 necesita para comunicarse dentro de la infraestructura de la Figura 21.

5.4.2 Rutas de un Router 6to4

El router necesita de una ruta on-link en su interfaz LAN que contenga el prefijo de subred, esta ruta le permite al router 6to4 transmitir los paquetes con los hosts 6to4 que se encuentren dentro de la subred de intranet. Para el ejemplo esta ruta cuenta con el valor 2002:9D3C:1:1::/64.

[73] (Microsoft Corporation, 2003 (actualización febrero 2008))

Una ruta on-link con el prefijo de la dirección 6to4 2002::/16 es utilizada por la interfaz de túnel 6to4. Esta ruta permite que el router realice túneles router a router con cualquier otro router o relay 6to4, o túneles router a host para poder localizar host/routers 6to4 por medio de internet IPv4.

Una ruta default es utilizada por la interfaz de túnel 6to4 apuntando hacia la dirección del relay 6to4. Con esta ruta el router 6to4 puede transmitir paquetes IPv4 hacia nodos que se encuentren dentro de internet IPv6.

5.4.3 Rutas de un Relay 6to4

Necesita de una ruta on-link con el prefijo de la dirección 6to4 2002::/16 que utilice la interfaz de túnel 6to4, esta ruta permitirá al relay 6to4 realizar túneles router a router para localizar a otros router 6to4, o túneles router a host para localizar a host/routers 6to4.

El relay 6to4 utilizara una ruta default que utilice su interfaz LAN que apunte hacia el siguiente router situado en la internet IPv6, con esta ruta el relay 6to4 podrá transmitir trafico IPv6 hacia destinos IPv6 que se encuentren en la internet IPv6.

5.4.4 Routers de Internet IPv6

Los routers que se encuentren en internet IPv6 necesitaran de una ruta con el prefijo de la subred 2002::/16 que apunte hacia el relay 6to4, esto permitirá a los routers transmitir el tráfico hacia los nodos en la arquitectura 6to4.

5.5 Configuración 6to4 en Linux

Para la configuración de túneles 6to4 en un sistema Linux, es necesario que el kernel cuente con soporte para túneles 6to4. Los pasos necesarios para la configuración son los siguientes:

Como primer punto se debe calcular el prefijo de red 6to4 en base a una dirección publica IPv4 y el prefijo 6to4. En este caso si la dirección publica fuera 1.2.3.4, cada segmento de 8 bits debe ser convertido a notación hexadecimal y serán agrupados en segmentos de 16 bits. De esta manera el prefijo 6to4 generado será 2002:0102:0304::

La primera dirección 6to4 generada será: 2002:0102:0304::1.

Existen dos métodos para la configuración de túneles 6to4, por medio del comando "IP" o con los comandos "ifconfig" y "route".

5.5.1 Configuración con el comando IP

1. Crear una interfaz de túnel:

 # /sbin/ip tunnel add tun6to4 mode sit ttl <ttldefault> remote any local <localipv4address>

2. Levantar la interfaz:

 # /sbin/ip link set dev tun6to4 up

3. Agregar direcciones 6to4 a la interfaz:

 # /sbin/ip -6 addr add <local6to4address>/16 dev tun6to4

4. Agregar una ruta default a la red IPv6 global utilizando la dirección anicast IPv4 de todos los routers 6to4

 # /sbin/ip -6 route add 2000::/3 via ::192.88.99.1 dev tun6to4 metric 1

5. Algunas versiones de IP no soportan las direcciones IPv6 compatibles con IPv4 por lo cual puede ser necesaria la utilización de la dirección IPv6 relacionada:

 # /sbin/ip -6 route add 2000::/3 via 2002:c058:6301::1 dev tun6to4 metric 1

5.5.2 Configuración con el comando *ifconfig*

1. Creación de un túnel genérico, en este caso llamado sit0

 # /sbin/ifconfig sit0 up

2. Agregar dirección local 6to4 a la interfaz

 # /sbin/ifconfig sit0 add <local6to4address>/16

3. Agregar una ruta default hacia la red global IPv6

 # /sbin/route -A inet6 add 2000::/3 gw ::192.88.99.1 dev sit0

5.5.3 Eliminar un túnel 6to4

Para remover un túnel, también se puede realizar mediante los dos comandos IP o ifconfig. Por medio del comando IP:

 # /sbin/ip -6 route flush dev tun6to4
 # /sbin/ip link set dev tun6to4 down
 # /sbin/ip tunnel del tun6to4

Y por medio del comando ifconfig:

/sbin/route -A inet6 del 2000::/3 gw ::192.88.99.1 dev sit0
/sbin/ifconfig sit0 del <local6to4address>/16
/sbin/ifconfig sit0 down

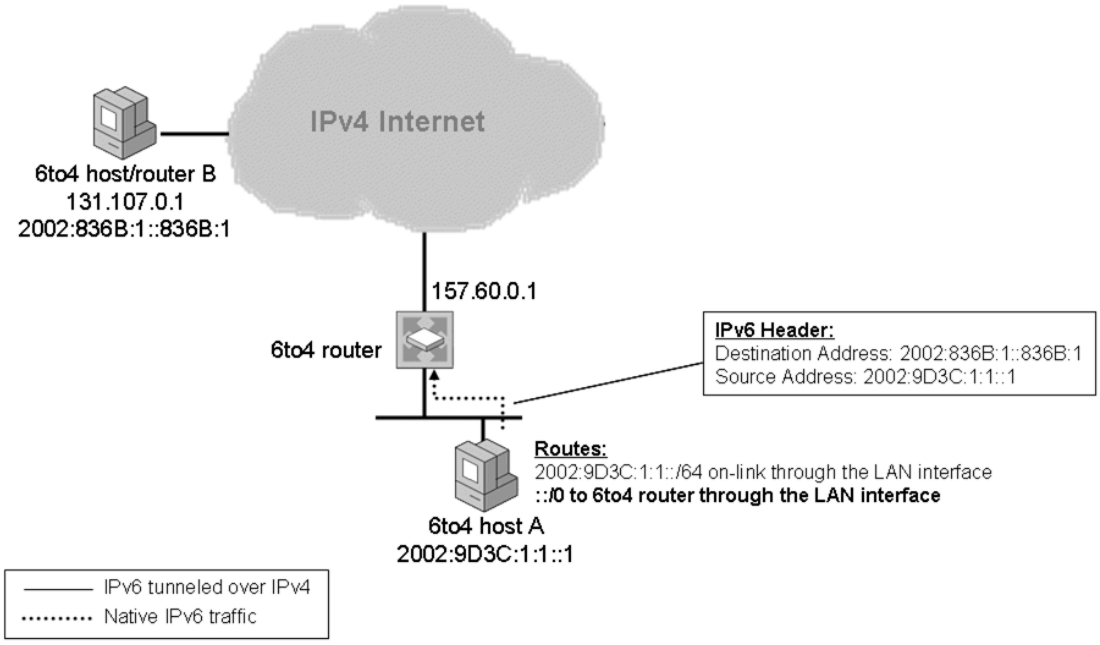
5.6 Ejemplos de comunicación 6to4

En esta parte se explicara el recorrido que toma un paquete para viajar desde un host 6to4 hasta un host/router 6to4, y el camino que debe recorrer para poder llegar desde el host 6to4 hasta un host IPv6 que se encuentre dentro de la red que cuenta únicamente con capacidad de IPv6.

5.6.1 De Host 6to4 a host/routes 6to4

Para la ilustración del viaje que realiza un paquete desde un host 6to4 hasta un host/router 6to4, se hará uso de la siguiente Figura.

Figura 22: Comunicación de host a host/router 6to4[74]



En la Figura se muestra al host A, que es un host 6to4, este nodo desea enviar un paquete hacia el nodo B, el cual es un host/router 6to4. El viaje que realiza el paquete tendrá dos partes:

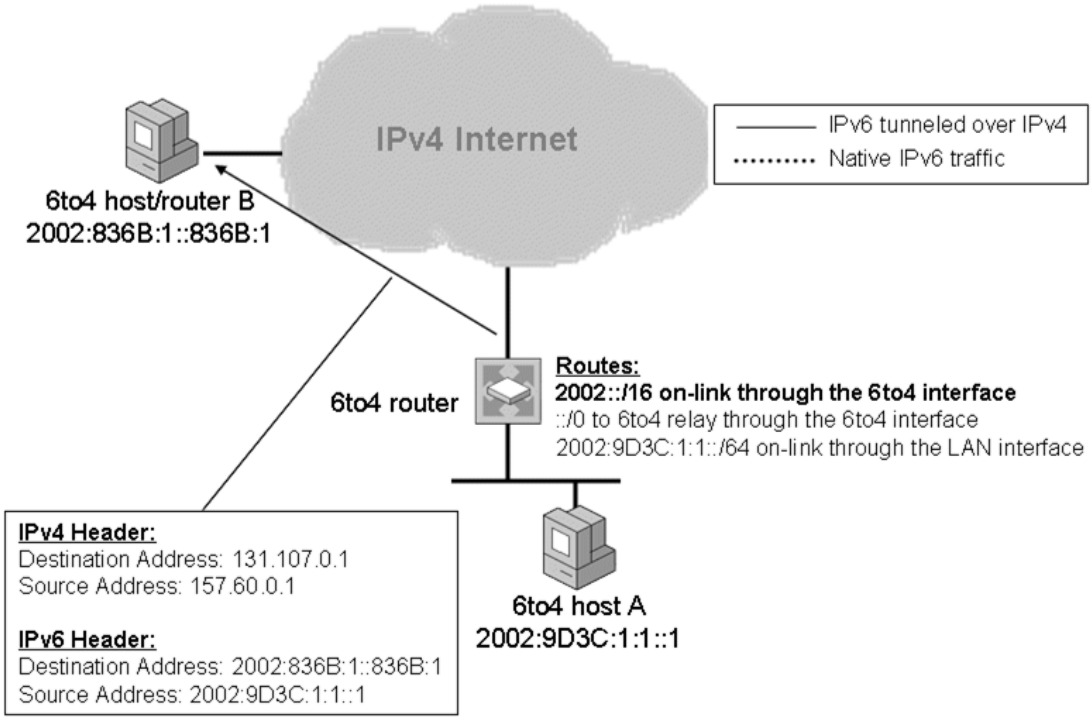
[74] (Microsoft Corporation, 2003 (actualización febrero 2008))

- Del host A hacia el router 6to4
- Del router 6to4 hacia el nodo B

En la primera parte del camino el protocolo IPv6 en el host A realiza un proceso para determinar la mejor ruta hacia el host B, de este modo encuentra que la mejor ruta es su ruta default que apunta hacia el router 6to4. El host A realiza una resolución de nombres normal y envía el paquete IPv6 hacia el router 6to4. La primer parte del viaje del paquete IPv6 es mostrada en la Figura 22.

La segunda parte del camino del paquete hacia el host/router 6to4 es mostrada por la figura 23:

Figura 23: Comunicación del router al host/router 6to4[75]



[75] (Microsoft Corporation, 2003 (actualización febrero 2008))

En esta parte del camino, el protocolo IPv6 situado en el router 6to4 realiza una búsqueda de la mejor ruta, determinando que la ruta que mejor se ajusta al destino del paquete es la 2002::/16, esta ruta esta direccionada hacia la dirección 2002:836B:1::836B:1 la cual corresponde con la dirección IPv6 de destino del paquete a enviar.

El paquete IPv6 y la dirección determinada como la mejor ruta son pasadas a la interfaz 6to4 para ser procesados.

En la interfaz 6to4 del router se configura a la dirección de destino IPv4 dentro de un encabezado IPv4 con los 32 bits correspondientes al segundo y tercer block de la dirección del siguiente salto IPv6, la cual corresponde a la dirección IPv4 del host/router 6to4 131.107.0.1. Dentro del router 6to4 el protocolo IPv4 determina que la mejor dirección de origen para el paquete es la dirección IPv4 asignada al router 157.60.0.1 y procede a enviar el paquete. El paquete IPv6 es enviado entonces como un paquete IPv6 encapsulado dentro de un paquete IPv4.

Al recibir el paquete en el host/router 6to4, el protocolo IPv4 se encarga del procesamiento y al descubrir que el campo “protocolo” se encuentra configurado con un valor 41 deja el paquete al protocolo IPv6 para que se encargue de su procesamiento.

5.6.2 De un Host 6to4 hacia un host IPv6

El trayecto que sigue un paquete desde un host 6to4 hasta un host IPv6 es dividido en 3 partes para su explicación:

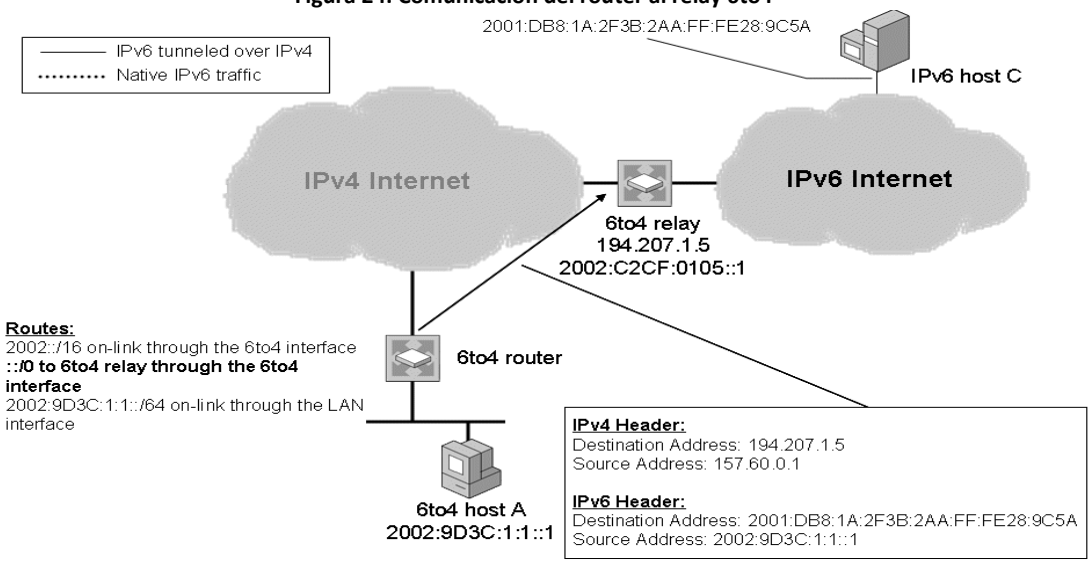
- Del host 6to4 al router 6to4
- Del router 6to4 al relay 6to4
- Del relay 6to4 al host IPv6

La primera parte del viaje, del host al router 6to4, es similar a la del ejemplo anterior, en la que el host 6to4 se encarga de resolver la dirección del nodo IPv6 mediante DNS y posteriormente envía el paquete IPv6 hacia el router 6to4.

En la segunda parte, el protocolo IPv6 dentro del router 6to4 se encarga de determinar la mejor ruta hacia el destino del paquete. La mejor ruta es a través de la interfaz 6to4 que apunta hacia la dirección IPv6 del relay 6to4 con la dirección 2002:C2CF:0105::1. Luego de esto tanto la dirección como el paquete IPv6 son pasados a la interfaz 6to4 para que esta se encargue procesarlos.

La interfaz 6to4 del router se encarga de configurar una dirección IPv4 en un encabezado IPv4 del paquete a enviar. Esta dirección IPv4 corresponde a los 32 bits del segundo y tercer segmento de la dirección 6to4 del relay, esta dirección (194.207.1.5) corresponde a la dirección IPv6 del relay. Posteriormente el protocolo IPv4 en el router determina a la dirección 157.60.0.1 (dirección IPv4 del router) como la mejor dirección de origen para el paquete a enviar. En la Figura 24 se muestra el paquete al ser enviado del router hacia el relay 6to4.

Figura 24: Comunicación del router al relay 6to4[76]

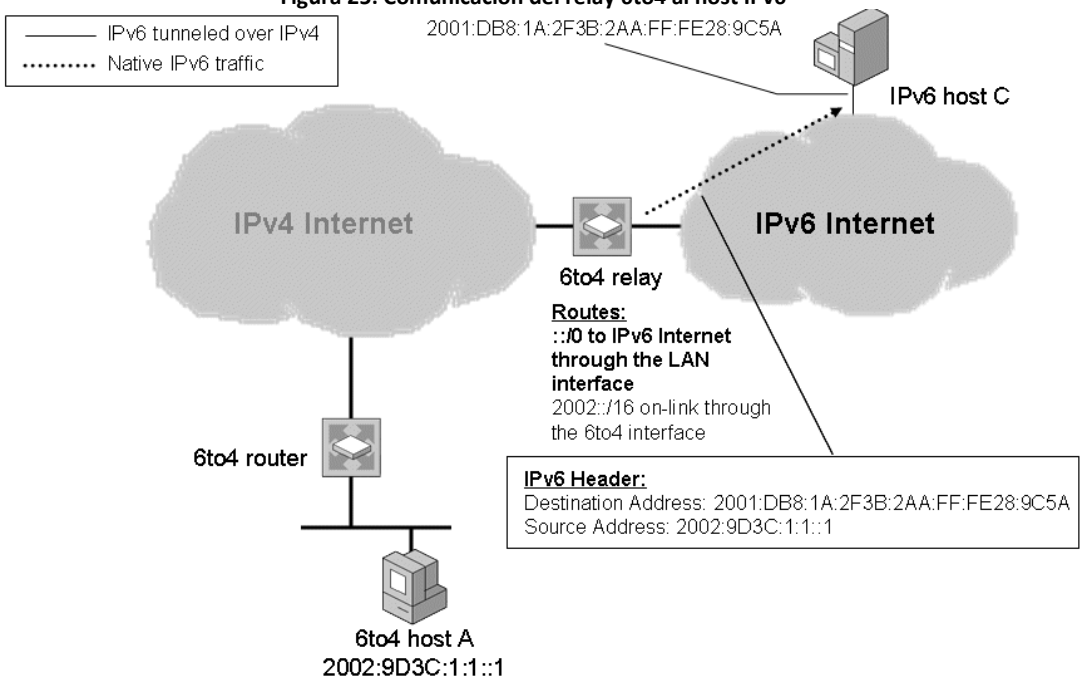


[76] (Microsoft Corporation, 2003 (actualización febrero 2008))

El último trayecto que debe realizar el paquete corresponde al viaje del relay 6to4 hacia el host IPv6. El paquete es procesado en el relay por el protocolo IPv4 y determina que es un paquete IPv6 por el valor 41 en campo “protocolo”, entonces deja el paquete al protocolo IPv6 para procesarlo, este protocolo debe determinar la mejor ruta hacia el destino del paquete por lo que realiza un proceso determinando que la mejor ruta es su ruta default ::/0 la cual debe apuntar al siguiente router IPv6 situado en la internet IPv6.

El paquete es procesado en la interfaz apropiada del relay eliminando el encabezado IPv4 y se envía el paquete IPv6 original. La siguiente figura muestra el camino del paquete hasta su nodo destino.

Figura 25: Comunicación del relay 6to4 al host IPv6[77]



[77] (Microsoft Corporation, 2003 (actualización febrero 2008))

6. TEREDO

Teredo es una tecnología para la transición hacia IPv6 que provee asignación de direcciones y túneles automáticos de host a host para tráfico IPv6 cuando nodos del tipo IPv6/IPv4 se encuentran detrás de uno o varios traductores de direcciones de red (NATs) IPv4. Para atravesar los NATs IPv4, se envían paquetes IPv6 como mensajes IPv4 basados en el protocolo de datagramas de usuario (UDP). A través de este capítulo se presenta una visión general de TEREDO, incluyendo el direccionamiento y detalles de la explicación de cómo se entabla la comunicación entre clientes TEREDO y otros nodos.[78]

Similar a Teredo, 6to4 es permite conectividad a través de la red IPv4. Sin embargo, 6to4 funciona correctamente cuando cuanta con un router 6to4 al borde del sitio. El router 6to4 utiliza una dirección IPv4 pública para construir el prefijo 6to4 y funciona como un transmisor en la red.

6to4 se basa en la configuración de una dirección pública 6to4 y la implementación de router 6to4 en el borde de cada dispositivo, pero muchas oficinas hacen uso de NAT para poder conectarse a internet, y en muchos casos el dispositivo encargado de la funcionalidad NAT no es capaz de actuar como un router 6to4.

Teredo resuelve este problema de la falta de funcionalidad 6to4 de los dispositivos de borde de internet y de la configuración de múltiples capas NAT por túneles para paquetes IPv6 entre los hosts dentro de los sitios. Otro problema para los NATs es que los paquetes IPv6 encapsulados en IPv4 tienen el valor 41 en el campo protocolo y debido a que muchos NATs solo trasladan paquetes TCP o UDP, TEREDO se encarga de encapsular los paquetes IPv6 dentro de mensaje UDP IPv4.

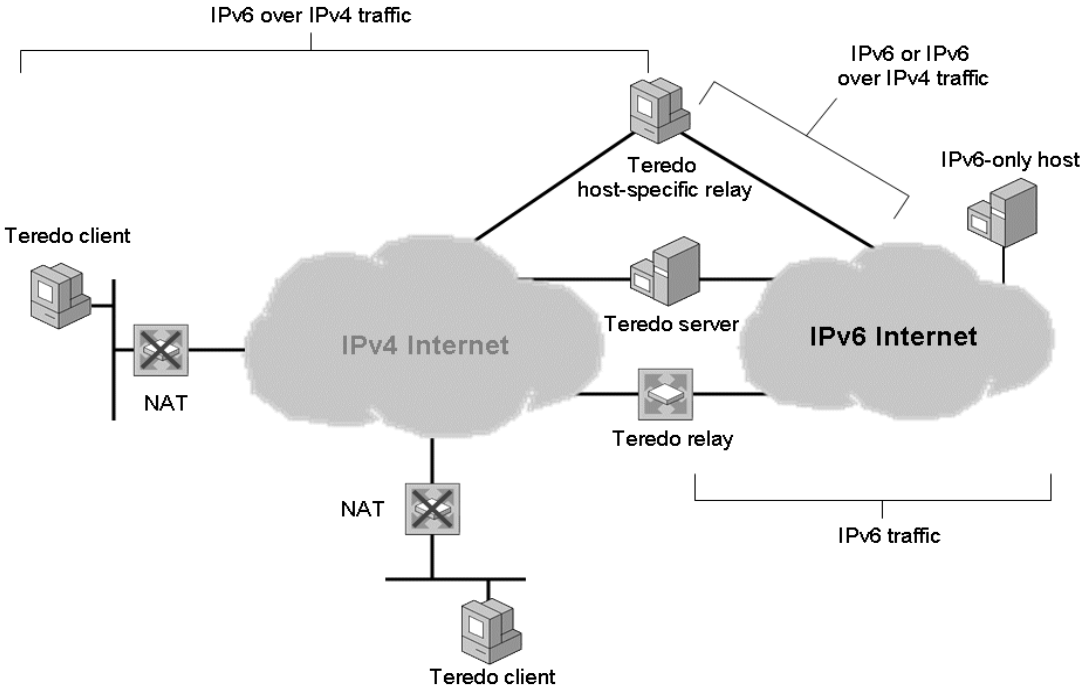
[78] (Microsoft TechNet, 2003)

6.1 Componentes de Teredo

La infraestructura TEREDO consiste en los siguientes componentes:

- Clientes Teredo
- Servidores Teredo
- Relays Teredo
- Relay Hosts-specific Teredo

Figura 26: componentes Teredo[79]



6.1.1 Clientes Teredo

Un cliente Teredo es un nodo que soporta una interfaz de túnel Teredo a través de la cual los paquetes son tunelizados hacia otros clientes Teredo o hacia nodos en internet IPv6 por medio de relays Teredo. [80]

[79] (Microsoft Corporation, 2003 (actualización febrero 2008))
[80] (Microsoft TechNet, 2003)

Un cliente Teredo se comunica con un servidor Teredo para obtener un prefijo de dirección del cual una dirección IPv6 basada en Teredo es configurada o para ayudara a iniciar la comunicación con otros clientes o hosts en internet IPv6.

6.1.2 Servidores Teredo

Es un nodo IPv6/IPv4 que está conectado a internet IPv4 y a internet IPv6, soporta una interfaz de túnel Teredo a través de la cual los paquetes son recibidos. Su principal función es asistir en la configuración de direcciones de los clientes Teredo y facilitar la comunicación inicial entre los clientes. El servidor Teredo escucha por tráfico Teredo en el puerto UDP 3544. [81]

6.1.3 Relay Teredo

Un Relay Teredo es un router IPv6/IPv4 que utiliza una interfaz Teredo para poder transmitir paquetes entre clientes Teredo sobre internet IPv4 y hosts IPv6-only en internet IPv6. En algunos casos el relay Teredo interactúa con un servidor Teredo para ayudar a facilitar la comunicación inicial entre clientes Teredo y hosts IPv6-only. El relay Teredo también escucha por tráfico en el puerto UDP 3544. [81]

6.1.4 Relay Host-specific Teredo

La comunicación entre un cliente Teredo y un host IPv6 que está configurado con una dirección global debe realizarse a través de un relay Teredo. Esto es necesario únicamente para los hosts IPv6-only que se encuentran conectados a internet IPv6, sin embargo si un host IPv6 tiene capacidad para IPv4 y se encuentra conectado tanto a internet IPv4 y a internet IPv6, la comunicación se deberá realizar entre el cliente Teredo y el Host IPv6 a través de internet IPv4 en vez de tener que atravesar la Internet IPv6 e ir a través de un relay Teredo.

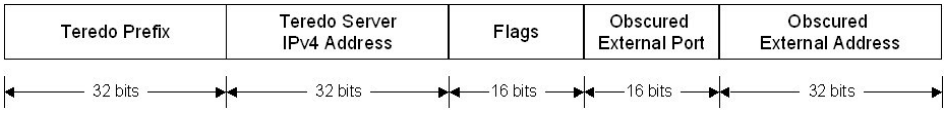
[81] (Microsoft TechNet, 2003)

Un relay Host-specific Teredo es entonces un nodo IPv6/IPv4 que está conectado tanto a internet IPv4 y a internet IPv6 y se puede comunicar directamente con clientes Teredo sobre internet IPv4 sin necesidad de utilizar un relay Teredo como intermediario. La conexión con internet IPv4 puede ser realizada por medio de una dirección pública IPv4 o a través de una dirección privada IPv4 y un vecino NAT, la conexión con internet IPv6 puede ser directa o por medio de un mecanismo de transición como 6to4. [81]

6.2 Formato de direcciones Teredo

El formato de las direcciones Teredo es mostrado a través de la siguiente Figura:

Figura 27: Formato de direcciones Teredo[82]



Las direcciones teredo consisten de las siguientes partes:

- Prefijo Teredo
- Dirección IPv4 del servidor Teredo
- Banderas
- Puerto externo oculto
- Dirección externa oculta

[82] (Microsoft Corporation, 2003 (actualización febrero 2008))

6.2.1 Prefijo Teredo

Corresponde a los primeros 32 bits de la dirección Teredo y es el mismo prefijo para todas las direcciones Teredo. Este prefijo está definido en el RFC 4380 y corresponde al valor 2001::/32.

6.2.2 Dirección IPv4 del servidor Teredo

Los siguientes 32 bits contienen la dirección pública IPv4 del servidor Teredo que ayudo al cliente a configurar su dirección Teredo.

6.2.3 Banderas

Los 16 bits siguientes corresponden a los bits de bandera, estos son representados de la siguiente manera CRAAAAUG AAAAAAAA. El bit C corresponde al "Cone Flag" y el bit R es reservado para uso futuro.

El bit U corresponde a Universal/Local flag (configurado en 0), el bit G es por Individual/Group flag (configurado en 0) y los bits A son números generados aleatoriamente para impedir que un usuario malicioso determine el resto de la dirección Teredo por medio de la captura de los paquetes de intercambio para la configuración inicial entre el cliente y el servidor Teredo.[83]

6.2.4 Puerto externo oculto

16 bits siguientes en la dirección Teredo corresponden a una versión oculta del puerto externo UDP correspondiente a todo el tráfico Teredo para este cliente Teredo. Cuando un cliente Teredo envía su paquete inicial hacia un servidor Teredo, el puerto de origen UDP es mapeado por NAT a uno diferente, en este caso llamado puerto externo UDP. El puerto externo UDP es determinado por el servidor Teredo por el puerto origen UDP del paquete inicial enviado por el cliente Teredo y es enviado de vuelta al cliente Teredo. [83]

[83] (Microsoft TechNet, 2003)

El puerto externo es ocultado por medio de una operación XOR entre el valor del puerto externo y el valor 0xFFFF. Obscurecer u ocultar el puerto externo impide la traducción de los NATs del puerto externo dentro de la carga de los paquetes que son transmitidos por medio de ellos.

6.2.5 Dirección externa oculta

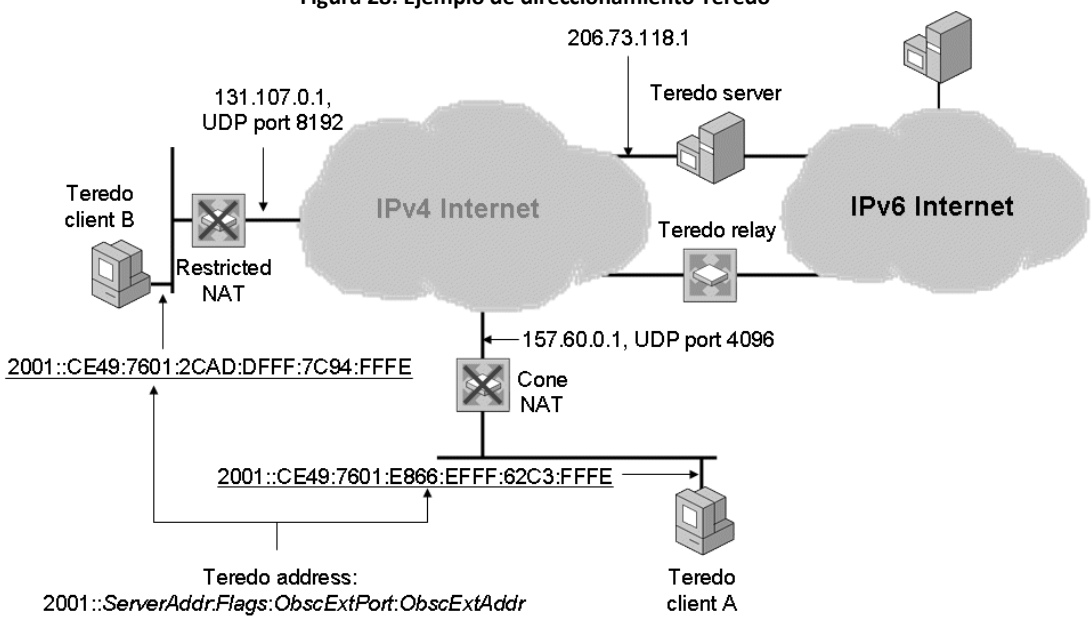
Esta corresponde a los últimos 32 bits de la dirección Teredo, y está conformada por una versión oculta de la dirección IPv4 del cliente Teredo. De igual manera que el puerto externo UDP, cuando el cliente teredo envía el paquete inicial hacia el servidor Teredo, la dirección origen del paquete es mapeada por NAT a una dirección distinta, la dirección externa (dirección pública). Todo el tráfico del host utiliza la misma externa, mapeada y pública dirección IPv4.

La dirección externa IPv4 es determinada por el servidor Teredo por la dirección de origen IPv4 del paquete inicial enviado por el cliente Teredo y es enviada de vuelta al cliente. [83]

La dirección externa es oculta por medio de una operación XOR entre la dirección externa y el valor 0xFFFFFFFF. Obscurecer u ocultar la dirección externa impide la traducción de los NATs de la dirección dentro de la carga de los paquetes que son transmitidos por medio de ellos.

En la siguiente Figura se muestra un ejemplo del direccionamiento Teredo:

Figura 28: Ejemplo de direccionamiento Teredo[84]



Para el cliente Teredo A se utiliza lo siguiente para formar su dirección Teredo:

- La dirección IPv4 de su servidor Teredo 206.73.118.1
- Se encuentra detrás de un cono NAT (bit C de las banderas)
- La dirección y puerto externos para el trafico Teredo es 157.60.0.1, puerto UDP 4096.

Utilizando el formato de las direcciones Teredo, la dirección correspondiente al nodo A es 2001::CE49:7601:E866:EFFF:62C3:FFFE. Esta dirección es formada en base a los siguientes puntos:

- Prefijo Teredo 2001::/32
- CE49:7601 es la versión hexadecimal de la dirección 206.73.118.1
- E866 corresponde a las banderas en las que el bit C tiene 1, los bits U y G son 0 y los demás bits son generados aleatoriamente.
- EFFF es la versión oculta del puerto UDP 4096
- 62C3:FFFE es la versión oculta de la dirección 157.60.0.1

[84] (Microsoft Corporation, 2003 (actualización febrero 2008))

De manera similar se forma la dirección Teredo para el cliente Teredo B. para formar su dirección se toma en cuenta que:

- La dirección IPv4 de su servidor Teredo 206.73.118.1
- Se encuentra detrás de un cono NAT (bit C de las banderas)
- La dirección y puerto externos para el trafico Teredo es 131.107.0.1, puerto UDP 8192

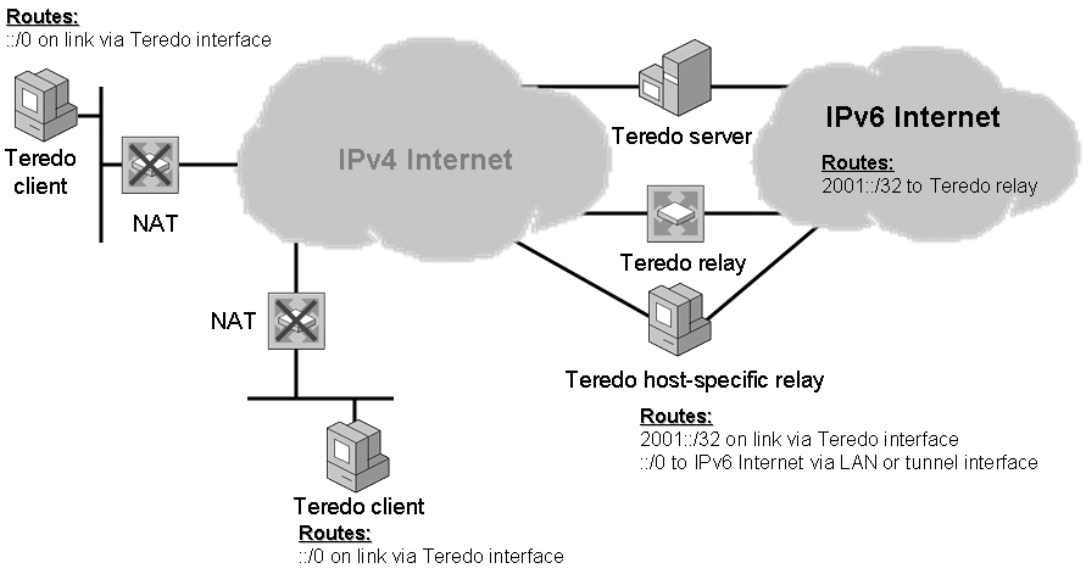
Utilizando el formato de las direcciones Teredo, la dirección correspondiente al nodo B es 2001::CE49:7601:2CAD:DFFF:7C94:FFFE. Esta dirección es generada basada en los siguientes puntos:

- Prefijo Teredo 2001::/32
- CE49:7601 es la versión hexadecimal de la dirección 206.73.118.1
- DFFF corresponde a las banderas en las que el bit C tiene 1, los bits U y G son 0 y los demás bits son generados aleatoriamente.
- EFFF es la versión oculta del puerto UDP 8192
- 7C94:FFFE es la versión oculta de la dirección 131.107.0.1

6.3 Ruteo teredo

Por medio de la siguiente figura se muestran las rutas de los nodos Teredo que permiten el envió de paquetes entre los dispositivos Teredo:

Figura 29: Ruteo Teredo[85]



En el lado de internet IPv6, deben existir rutas 2001::/32 que son utilizadas para transmitir paquetes hacia el relay Teredo más cercano.

Los hosts Teredo utilizan una ruta default que considera a todas las direcciones Ipv6 como on-link y utilizan una interfaz de túnel Teredo. Cuando se utiliza esta ruta, la dirección next-hop es configurada con la dirección de destino del paquete Ipv6 y la interfaz next-hop es configurada con la interfaz de túnel Teredo, esta interfaz se encarga entonces de decidir cómo se enviara el paquete. [86]

Los servidores, relays y relays host-specific Teredo utilizan las rutas:

- Una ruta on-link para el prefijo Teredo utilizado por la interfaz.

[85] (Microsoft Corporation, 2003 (actualización febrero 2008))
[86] (Microsoft TechNet, 2003)

- Una ruta default que esta direccionada a internet Ipv6 por medio de una interfaz LAN o de túnel.

Cuando una interfaz de túnel Teredo transmite un paquete, esta distingue entre los siguientes tres casos:

1. El destino es otro cliente Teredo en el mismo link Ipv4
2. El destino es otro cliente Teredo en otro sitio
3. El destino es un nodo en internet Ipv6

6.4 Funcionamiento de teredo

La configuración inicial para los clientes Teredo es realizada mediante una serie de mensajes de solicitud de router a un conjunto de servidores Teredo. Las respuestas son utilizadas para derivar una dirección Teredo y determinar cuando el cliente se encuentre situado a la par de un NAT.

Basado en los mensajes de aviso recibidos de los routers, el cliente teredo forma su dirección en base a lo siguiente:

- Los primeros 64 bits son configurados con el valor de la opción de prefijo incluido en el paquete recibido del router. El prefijo de 64 bits publicado por el servidor consiste en el prefijo Teredo de 32 bits y los 32 bits de la dirección Ipv4 del servidor Teredo.
- Los siguientes 16 bits son los campos de banderas
- Los siguientes 16 bits corresponden al oculto número del puerto externo UDP que es incluido en un encabezado especial de Teredo incluido en el mensaje publicado por el servidor.
- Los últimos 32 bits son para la oculta dirección externa Ipv4 incluida en el encabezado especial Teredo.

6.5 Camino hacia IPv6

En esta parte se intentara resumir a manera general los pasos que se deben seguir para poder realizar una correcta migración desde IPv4, pasando por una etapa de trabajo conjunto, hasta una arquitectura en la que trabaje únicamente IPv6.

El camino que se debe recorrer implica la concientización con los directivos principales en cada organización, sobre la real necesidad de migración a IPv6, siendo este quizá la parte más complicada del camino debido a que no es un problema que sea visible a los usuarios y actualmente para ellos pueda esta no ser una necesidad de gasto incluida dentro de sus planes, pero al no ser tomado en cuenta podrán afrontarse con gastos mucho más grandes en un futuro no muy lejano.

La transición deberá de ser un proceso invisible para los usuarios finales, mediante un trabajo de mayor carácter Técnico, los usuarios no deberán afrontarse con problemáticas ocasionadas por la migración hacia IPv6.

De esta manera los pasos necesarios para la migración hacia IPv6 podrán ser resumidos de la siguiente manera:

1. Concientización
2. Actualización de aplicaciones
3. Actualización de la arquitectura DNS
4. Actualización de los hosts a nodos IPv6/IPv4
5. Implementar una metodología de túneles
6. Actualizar la infraestructura de ruteo.

Concientización

Esta es la etapa más importante, debido a que se requiere educar sobre estos conceptos y hacer comprender la necesidad de participar en el camino hacia IPv6 y no quedarse sin tomar acción ante estos problemas pudiendo recaer mas tarde en problemas mayores que impliquen gastos más elevados para las empresas.

La etapa de concientización ya se está viviendo y está siendo generada a nivel global por parte de las organizaciones principales encargadas de la administración y distribución de direcciones de internet, como puede ser LACNIC para América Latina y el Caribe. Como sucedió en los inicios de internet con IPv4, IPv6 tiene un rápido despliegue a lo largo de la comunidad Académico científica, desarrollándose primero en redes de universidades y centros de investigación.

Pero IPv6 necesita que sea considerado a un nivel mayor, a nivel global en el cual es muy importante la participación de los gobiernos por medio de regulaciones que impulsen el despliegue y luego la aceptación del nuevo protocolo.

Junto con la tarea de facilitar la adopción y difundir el conocimiento de la versión 6 del protocolo de Internet es necesario que se realicen actividades que busquen:

- Difundir el conocimiento del estado de desarrollo de la versión 6 del protocolo IP en la prensa especializada en tecnología.
- Dar a conocer los resultados de pruebas concretas de funcionalidades técnicas a través de medios especializados.
- Hacer tomar conciencia a los responsables de las áreas de Tecnologías del Sector Público y Privado, para que consideren el soporte a IPv6 en la definición futura de sus arquitecturas de sistemas.

Actualización de aplicaciones

Independizar a las aplicaciones y servicios a modo de que les sea indiferente trabajar con el protocolo de internet versión 4 o versión 6 sin ningún inconveniente.

Mediante el portal de IPv6 bajo el dominio de LACNIC, se encuentran registradas y clasificadas todo tipo de aplicaciones o servicios que permiten el trabajo con IPv6. El listado puede ser encontrado en el siguiente link: http://portalipv6.lacnic.net/es/ipv6/aplicaciones-0[87]

Actualizar la infraestructura DNS

Se necesita que se actualice la infraestructura DNS para que soporte registros del tipo AAAA para poder resolver direcciones de IPv6 y opcionalmente que soporte registros PTR en el dominio reversible IP6.ARPA para la realización de la opción inversa.

Se debe asegurar de que los servidores de DNS soporten la actualización dinámica para los registros AAAA de modo que los hosts IPv6 puedan registrar automáticamente sus nombres y direcciones IPv6.

Actualización de los hosts a nodos IPv6/IPv4

Todo tipo de dispositivo que era utilizado en la anterior infraestructura IPv4 debe de ser actualizado para que permita la comunicación tanto con IPv4 y con IPv6. Esto podrá ser realizado mediante la implementación de mecanismos como una capa IP dual o una arquitectura de pila doble. El DNS también debe permitir que al realizar una consulta esta pueda contener direcciones de ambos tipos de protocolo.

[87] (LACNIC)

Podrá ser realizado mediante actualización de los sistemas operativos que utilicen los dispositivos o simplemente mediante la activación del servicio ya que la mayoría de sistemas ya cuentan con soporte para IPv6 y en algunos casos esta opción únicamente se encuentra desactivada.

Implementar una metodología de túneles

Como las tecnologías descritas en este trabajo, se puede hacer uso de ISATAP para permitir la comunicación entre una intranet corporativa por medio de túneles IPv6 sobre IPv4 o la utilización de 6to4 para comunicar paquetes IPv6 a través de internet IPv4.

Finalmente, el uso de Teredo permitirá a una organización que cuente con NAT configurado entablar comunicación entre cualquier tipo de nodo a lo largo de internet IPv4 o Internet IPv6.

Actualizar la infraestructura de ruteo

Finalmente todo equipo de ruteo debe de ser actualizado y configurado para que permita tráfico IPv6 nativo. Estos routers deberán de ser capaces de publicar mensajes con los prefijos de red IPv6 para que cualquier nodo cercano a ellos pueda configurar automáticamente sus interfaces con las direcciones IPv6 adecuadas.

CONCLUSIONES

1. La principal necesidad de creación y migración hacia el protocolo de internet IPv6 se encuentra fundamentada en la gran aceptación de su antecesor IPv4, ya que no se estimó que este tendría una buena acepción ni que se convirtiera en una arquitectura de carácter mundial, como lo es el formar parte en las bases de internet, en la que el número de usuarios crece día a día.

2. IPv6 es la nueva versión del protocolo de internet que resuelve los problemas encontrados en su versión anterior IPv4, siendo el principal problema la escasez de direcciones posibles que puedan ser asignadas a los usuarios debido al crecimiento exponencial de Internet, para lo cual IPv6 provee un máximo de 2^{128} direcciones, una cantidad que no da margen a la imaginación sobre su escasez.

3. Los mecanismos identificados para la transición hacia IPv6, trabajo conjunto de IPv4 e IPv6 mediante capa IP dual o pila dual, configuración de la infraestructura DNS y la comunicación por medio de túneles configurados o automáticos, permiten a las organizaciones iniciar la migración hacia una arquitectura IPv6 nativa.

4. El protocolo ISATAP permite que se entable comunicación IPv6 entre nodos con capacidad para IPv6 e IPv4 a lo largo de una intranet IPv4, mediante la realización de túneles configurados automáticamente.

5. La tecnología 6to4 hace posible la comunicación IPv6 entre nodos con capacidad para IPv6 e IPv4 a lo largo de internet IPv4, mediante la realización automática de túneles de Router a Router, Host a Router y de Router a Host.

6. Teredo permite la asignación de direcciones y creación de túneles automáticos para transmitir tráfico IPv6 cuando nodos IPv6/IPv4 se encuentran detrás de uno o varios traductores de direcciones de red (NATs) IPv4, mediante la encapsulación de paquetes IPv6 como mensajes IPv4 basados en UDP.

7. El nuevo protocolo de Internet IPv6 ha sido diseñado bajo la necesidad de soportar un largo período de transición y coexistencia junto con su versión anterior IPv4, ya que no es posible realizar una transición de un momento a otro. La transición implica la actualización de dispositivos, aplicaciones y servicios para que permitan la coexistencia entre los protocolos y siendo IP la infraestructura básica de internet, esta debe estar disponible para permitir la innovación en los servicios.

8. La estimación del momento en que se cuente con una infraestructura total IPv6 es una tarea difícil y estará guiada por las iniciativas de transición tomadas a nivel mundial, tanto por organizaciones gubernamentales, grandes corporaciones, grupos académicos o por cualquier tipo de empresas que apoyen la transición. Sin embargo la fecha en que las direcciones IPv4 se agoten ya ha sido calculada y se estima entre los años 2011 y 2012.

9. La transición debe de ser un proceso gradual y transparente para los usuarios que poco a poco irán percibiendo mejoras en las aplicaciones existentes y en nuevas aplicaciones que no podrían ser posibles o ni siquiera fueron pensadas con IPv4, como lo pueden ser las mejoras en los dispositivos y sistemas operativos más recientes que ya cuentan soporte para IPv6 y que en la mayoría de los casos esta ni siquiera es visible para los usuarios finales como por ejemplo el Sistema Operativo Windows Vista que por default tiene habilitados los servicios de ISATAP y 6to4.

RECOMENDACIONES

1. La Elaboración de un estudio sobre el impacto que causará la migración hacia el protocolo IPv6 a nivel regional en el país de Guatemala pueda permitir identificar la importancia que representa y los problemas que se deberán afrontar al momento de no formar parte del grupo que ya ha iniciado el proceso de migración.

2. Realizar un análisis sobre el nivel de información con que cuenta la sociedad guatemalteca y las políticas que se están llevando a cabo para concientizar sobre la necesidad de migración hacia IPv6.

3. Promover actividades y talleres para dar conocer las necesidades de IPv6 y a la vez implementar prácticas con las que empresas y organizaciones a nivel local puedan iniciar el proceso de migración hacia IPv6.

4. Elaborar un estudio sobre los problemas sociales o culturales por los cuales el proceso de migración hacia IPv6 no se está llevando a cabo en pequeñas y medianas empresas como en regiones con bajo nivel económico.

REFERENCIAS BIBLIOGRÁFICAS

1. 6DISS. (2007). *http://www.6diss.org/.* Recuperado el octubre de 2008, de http://www.6diss.org/e-learning/.

2. ARIN. (5 de abril de 2007). *IPv4 e IPv6.* Recuperado el 25 de noviembre de 2008, de http://www.arin.net/about_us/media/fact_sheets/Spanish/IPv4_IPv6_spanish.pdf

3. Carpenter, B., & Moore, k. (febrero de 2001). RFC3056: Connection of IPv6 Domains via IPv4 Clouds.

4. Droms, R. (octubre de 1993). RFC1541: "Dynamic Host Configuration Protocol".

5. Gilligan, R., & Nordmark, E. (agosto de 2000). RFC2893: Transition Mechanisms for IPv6 Hosts and Routers.

6. Hinden, R. M., & Deering, S. E. (diciembre de 1998). RFC2460: "Internet Protocol, Version 6 (IPv6) Specification".

7. HP. (15 de julio de 2004). HP-UX IPv6 Transition Mechanisms. *HP-UX IPv6 Transition Mechanisms* .

8. IBM. (s.f.). *Tunelización de IPv6.* Recuperado el septiembre de 2008, de Tunelización de IPv6: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.commadmn/doc/commadmndita/tcpip_ipv6_tunnel.htm

9. LACNIC. (7 de enero de 2009). *IPv6.* Recuperado el 14 de enero de 2009, de Estadísticas IPv6: http://portalipv6.lacnic.net/es/ipv6/estad-sticas/ipv6

10. LACNIC. (s.f.). *Portal IPv6 LACNIC.* Recuperado el 12 de octubre de 2008, de Aplicaciones IPv6: http://portalipv6.lacnic.net/es/ipv6/aplicaciones-0

11. litech.org. (1 de junio de 2002). *Linux ISATAP Setup.* Recuperado el octubre de 2008, de Linux ISATAP Setup: http://www.litech.org/isatap/

12. Manning, B. (enero de 1996). RFC1879: "Class A Subnet Experiment Results and Recommendations".

13. Microsoft Corporation . (mayo de 2006). Intra-site Automatic Tunnel Addressing Protocol Deployment Guide. *Intra-site Automatic Tunnel Addressing Protocol Deployment Guide* .

14. Microsoft Corporation. (s.f.). *Características de IPv6.* Recuperado el octubre de 2008, de http://technet.microsoft.com/es-es/library/cc780593.aspx

15. Microsoft Corporation. (agosto de 2003 (actualización 2008)). Introduction to IP Version 6.

16. Microsoft Corporation. (s.f.). *IPv6 Routing.* Recuperado el octubre de 2008, de http://technet.microsoft.com/en-us/library/cc758763.aspx

17. Microsoft Corporation. (2003 (actualización febrero 2008)). IPv6 Transition Technologies. *IPv6 Transition Technologies* .

18. Microsoft Corporation. (s.f.). *Protocolo Internet versión 6.* Recuperado el octubre de 2008, de Protocolo Internet versión 6 - Enrutamiento IPv6: http://msdn.microsoft.com/es-es/library/ms172317(VS.80).aspx

19. Microsoft TechNet. (1 de enero de 2003). *Teredo Overview.* Recuperado el septiembre de 2008, de Teredo Overview: http://www.microsoft.com/technet/network/ipv6/teredo.mspx

20. Network Dictionary. (s.f.). *Networking Technologies*. Recuperado el septiembre de 2008, de Dual Stack Transition Mechanism.

21. Network Dictionary. (s.f.). *Networking Technologies*. Recuperado el septiembre de 2008, de Additional IPv6 Infrastructure (Tunnels): http://www.networkdictionary.com/Networking/Additional-IPv6-Infrastructure.php

22. Network Dictionary. (octubre de 2008). *Networking Technologies.* Obtenido de http://www.networkdictionary.com/Networking/Tunnelling-Methods-Configured-Tunnels.php

23. Networking Dictionary. (s.f.). *Networking Technologies.* Recuperado el septiembre de 2008, de Automatic Tunnels: http://www.networkdictionary.com/Networking/Automatic-Tunnels.php

24. Pethia, R. D., Crocker, S. D., & Fraser, B. Y. (noviembre de 1991). RFC1281: "Guidelines for the Secure Operation of the Internet".

25. Simpson, W. A. (agosto de 1994). RFC1688: "IPng Mobility Considerations".

ANEXOS

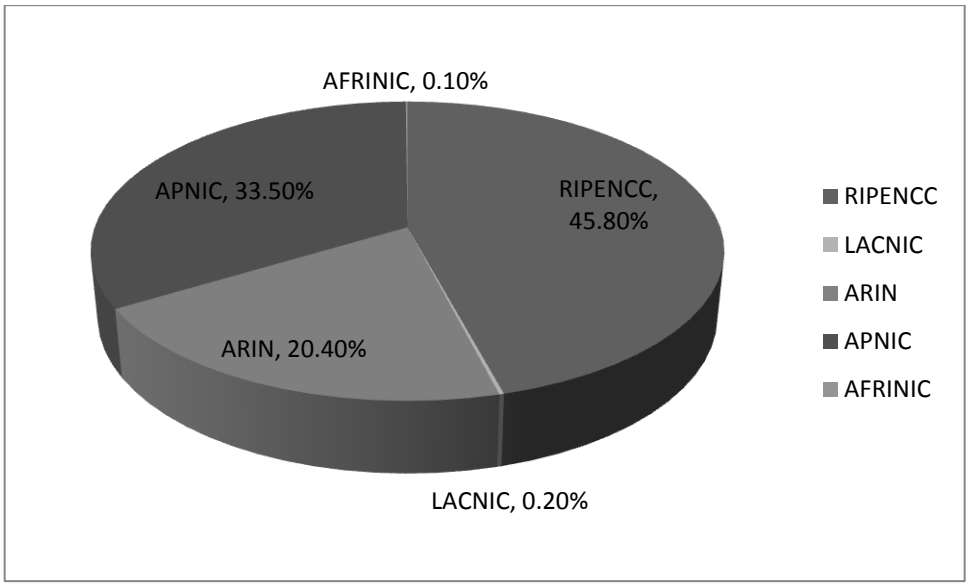
ESTADÍSTICAS

Según datos publicados por el Registro de Direcciones de Internet para Latinoamérica y el Caribe LACNIC, se presentan las siguientes tablas estadísticas mostrando información sobre las direcciones IPv6 asignadas a nivel mundial y regional.

Como referencia se utiliza la notación de direcciones /32 lo cual equivale a una de cada 4294967296 (2^{32}) direcciones.

Estadísticas Globales

Figura 30: Estadísticas Globales

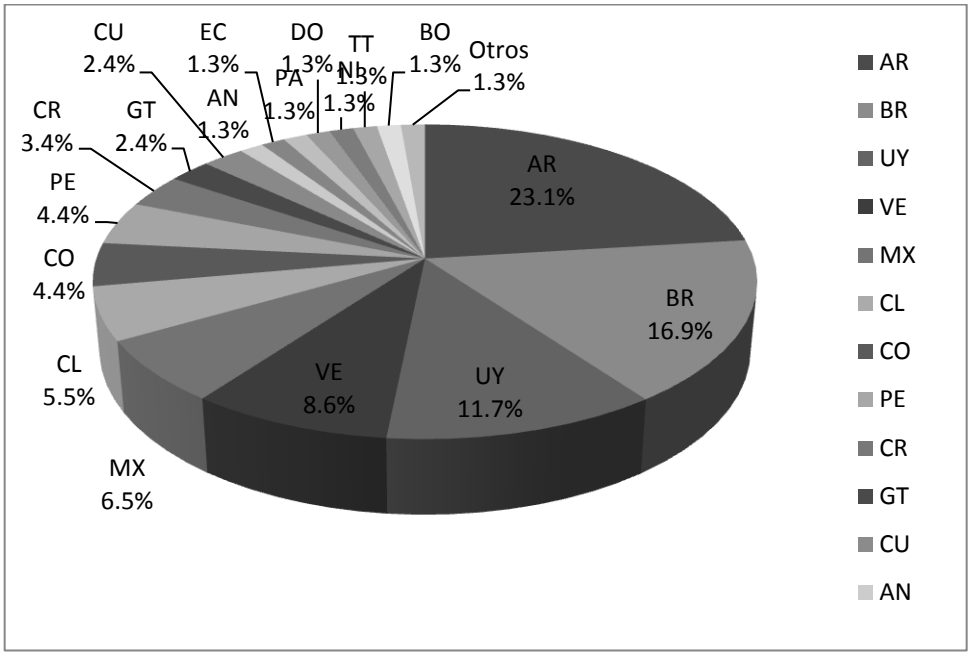


Con fecha al 14 de enero de 2009 de un total de 72478 /32 direcciones, se cuenta con un pequeño 0.2 por ciento de direcciones asignadas para América Latina y el Caribe. [88]

[88] (LACNIC, 2009)

Estadísticas Regionales

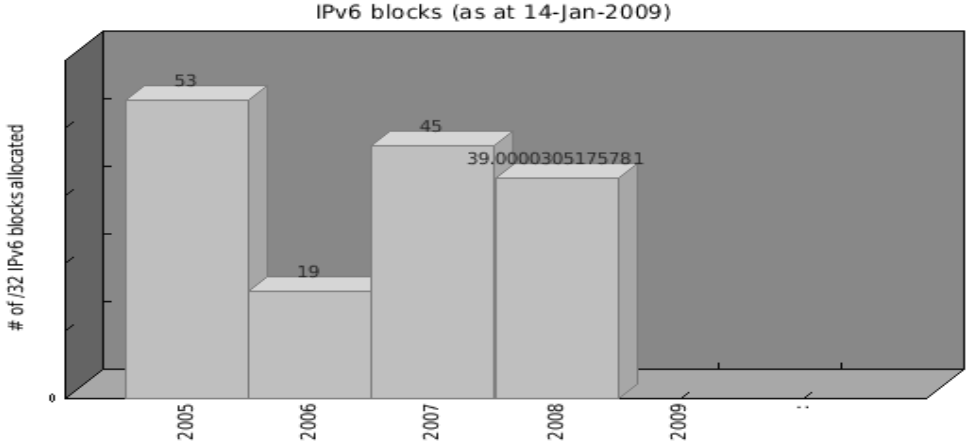
Figura 31: Distribución Regional de Direcciones IPv6



Datos obtenidos al 14 de enero de 2009 para la distribución de direcciones IPv6 de un total de 169.000030517578 /32 direcciones. Los datos indican un 2.4% de las direcciones asignadas para el sector de Guatemala bajo el dominio gt. [89]

La siguiente gráfica muestra el total de direcciones asignadas por año:

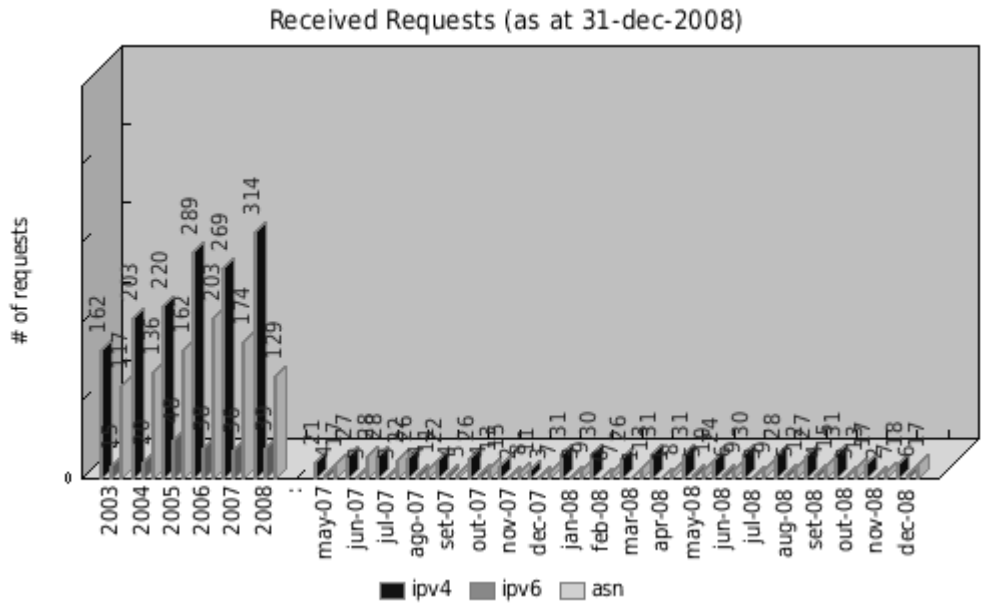
Figura 32: Direcciones IPv6 asignadas por año



[89] (LACNIC, 2009)

Solicitudes realizadas a LACNIC

Figura 33: Solicitud de direcciones a LACNIC[90]



Esta gráfica muestra la cantidad de solicitudes para recursos de Internet, direcciones IPv4 e IPv6 recibidas por LACNIC a cada meses y años anteriores.

Direcciones IPv4 disponibles

Figura 34: Stock central de direcciones IPv4[91]

Con fecha al 14 de enero de 2009 se muestra un 13.28% de direcciones no asignadas del Stock central de direcciones IPv4. Esto equivale a tan solo 32 /8 bloques de direcciones disponibles.

[90] (LACNIC, 2009)
[91] (LACNIC, 2009)