



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN**

**FUNDAMENTOS DEL PROTOCOLO INTERNET
VERSION 6 (IPv6)**

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A:

ANTONIO ARAUJO SAUCEDO

ASESOR: ING. MARICELA SERRANO FRAGOSO



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradecimientos

A mis padres **Graciela Saucedo Cruz** y **Antonio Araujo González** por ayudarme a alcanzar una importante meta de mi vida. Gracias mamá por tan valiosos consejos, por tus palabras de aliento, por tu apoyo y por tu ejemplo que han sido tan importantes para mí.

A mis hermanos **Lily**, **Ary** y **León** por su cariño y comprensión, por siempre creer en mí, por todo este tiempo donde lo más importante ha sido el permanecer unidos..... Los quiero.

A mi gran amigo y compañero de la facultad **Israel Alejandro de la Cruz** quien ha sido un guía para mí a lo largo de estos años.

Índice

Introducción	1
---------------------------	---

Capítulo 1 El protocolo IPv6

1.1 Antecedentes	2
1.1.1 Concepto de red	2
1.1.2 El modelo OSI	3
1.1.2.1 Capas superiores	4
1.1.2.2 Capas inferiores	5
1.1.2.3 Adyacencia lógica	6
1.1.3 TCP/IP	8
1.1.3.1 Capa de aplicación	10
1.1.3.2 Capa de transporte	11
1.1.3.3 Capa Internet	12
1.1.3.4 Direccionamiento físico	13
1.1.3.5 Esquema de direccionamiento IPv4	13
1.1.3.6 Déficit de direcciones IPv4	15
1.1.3.7 Mecanismos para preservar el espacio de direccionamiento IPv4	16
1.2 IPv6	18
1.2.1 Características IPv6	20
1.2.2 Cabecera IPv6	22
1.2.2.1 Formato de la cabecera IPv4	22
1.2.2.2 Formato de la cabecera IPv6	25
1.2.3 Cabeceras de extensión	26

Capítulo 2 Direccionamiento IPv6

2.1 Notación de las direcciones IPv6	29
2.1.1 Notación completa	29
2.1.2 Notación simplificada	29
2.2 Las subredes en IPv6	31
2.3 Clases de direcciones IPv6	32
2.3.1 Direcciones unicast	33
2.3.1.1 Direcciones de enlace local	34
2.3.1.2 Dirección de sitio local	34
2.3.1.3 Formato EUI-64	36
2.3.1.4 Dirección de agregación global	37
2.3.1.5 Asignaciones de IANA para prefijos unicast de agregación global	38
2.3.2 Direcciones multicast	40
2.3.2.1 Direcciones multicast asignadas	42
2.3.2.2 Direcciones multicast solicited-node	42
2.3.3 Direcciones anycast	43

2.3.3.1 Dirección anycast reservada	44
2.3.4 Direcciones especiales	45
2.3.4.1 Direcciones IPv6 con direcciones IPv4 insertadas	45
2.3.4.2 Dirección Loopback.....	46
2.3.4.3 Dirección no especificada	46
2.4 Direcciones IPv6 requeridas.....	46
2.4.1 Direcciones IPv6 requeridas para nodos	46
2.4.2 Direcciones IPv6 requeridas para routers	47
2.5 IPv6 en Ethernet.....	47
2.6 Internet IPv6.....	48
2.6.1 Políticas de asignación de direcciones IPv6	49
2.6.1.1 Políticas de asignación inicial.....	49
2.6.1.2 Políticas de asignación actual	50
2.6.1.3 Reasignación del espacio de dirección	51
2.6.1.4 Asignación de prefijos de producción.....	51

Capítulo 3 Enrutamiento

3.1 Introducción.....	53
3.2 Cálculo y mantenimiento de rutas.....	54
3.3 Tipos de enrutamiento	56
3.3.1 Enrutamiento estático	57
3.3.2 Enrutamiento dinámico	57
3.3.2.1 Enrutamiento por vector de distancia	61
3.3.2.2 Enrutamiento por estado de enlace.....	63
3.4 Enrutamiento IPv6	63
3.4.1 Distancias administrativas	63
3.4.2 Protocolos IGP para IPv6	64
3.4.3 Protocolos EGP para IPv6	67

Capítulo 4 Coordinación de redes con IPv6

4.1 ICMPv6	71
4.2 Descubrimiento MTU de ruta IPv6 (PMTUD)	74
4.3 Protocolo de descubrimiento de vecinos (NDP).....	75
4.3.1 Mecanismo de reemplazo de ARP en IPv6.....	76
4.3.2 Autoconfiguración	79
4.3.2.1 Publicación de prefijo	80
4.3.2.2 Petición de publicación de router	81
4.3.2.3 Detección de duplicado de dirección (DAD)	83
4.3.2.4 Renumeración de prefijo	84
4.3.3 Redirección de router	85
4.4 El servicio DNS	86
4.4.1 Jerarquía de nombres.....	86
4.4.2 Formato del mensaje DNS	88
4.5 DHCPv6	91
4.6 Seguridad IPv6.....	93
4.6.1 Cabecera de autenticación IPSec (AH).....	93
4.6.2 Cabecera de encapsulación de seguridad de la información (ESP)	93

Capítulo 5 Mecanismos de coexistencia y transición IPv6

5.1 Introducción.....	94
5.2 Pila dual	95
5.2.1 Solicitud de dirección IPv4	98
5.2.2 Solicitud de dirección IPv6.....	98
5.2.3 Solicitud de direcciones IPv4 e IPv6	99
5.3 Túneles IPv6	99
5.3.1 túnel configurado	102
5.3.2 Túnel Broker	104
5.3.3 Túnel Server	105
5.3.4 Túnel 6to4.....	106
5.3.5 Túnel ISATAP.....	109
5.3.6 Túnel Teredo	110
5.3.7 Entornos específicos de cada mecanismo para establecer túneles.	111
5.4 Mecanismos de traducción	111
5.4.1 Gateway de nivel de aplicación.....	111
5.4.2 NAT-PT	113
Conclusiones	116
Apéndices	i
Glosario	viii
Bibliografía	

Introducción.

IPv6 surge no únicamente como una nueva tecnología para reemplazar a IPv4, IPv6 representa la evolución natural de Internet para las siguientes décadas y su principal objetivo es el de sustentar un estándar global que permita la comunicación de redes y dispositivos que no solo se limitan a computadoras, como por ejemplo PDAs, teléfonos celulares, televisión, radio, máquinas industriales entre otros, dentro de una sola red digital.

IPv6 fue presentado en 1992 y su diseño y desarrollo se ha basado en la experiencia que ha dejado el funcionamiento de IPv4 durante más de dos décadas. Esta experiencia evidenció los aciertos, pero sobre todo las deficiencias del protocolo IPv4 que aunque ha demostrado una gran flexibilidad al soportar al Internet actual, no está preparado para darle cabida a la gran cantidad de dispositivos que a nivel mundial requerirán conectarse a Internet.

La tarea de suplantar globalmente al protocolo IPv4 por IPv6 pasará por un largo proceso donde ambos protocolos deberán convivir (este proceso se denomina de coexistencia y transición) y demanda mucho trabajo de parte de todas las entidades relacionadas e interesadas en IPv6, como por ejemplo los desarrolladores, los organismos de estandarización, las empresas, gobiernos e instituciones que actualmente colaboran en conjunto para impulsar el uso de IPv6 y al mismo tiempo generan el soporte necesario que respalda a usuarios que ya se han decidido a dar el salto hacia este relativamente nuevo protocolo.

A pesar de todo este esfuerzo, considero que en nuestro país no se le ha dado la justa relevancia y por lo tanto no existe la suficiente difusión para IPv6 salvo algunas excepciones. El objetivo de este trabajo es exponer de manera general las características más importantes, así como aspectos del funcionamiento del protocolo IPv6. En el primer capítulo se presentan algunos antecedentes, además de la estructura general del protocolo IPv6. El segundo capítulo plantea el aspecto de direccionamiento IPv6 y la organización de Internet IPv6.

El tercer capítulo revisa de manera breve los cambios que sufrieron los protocolos de enrutamiento para poder soportar a IPv6. En el capítulo cuatro analiza como se coordinan las redes IPv6 dejando ver algunos de sus mecanismos más interesantes y de mayor utilidad. Finalmente el capítulo cinco explica algunos de los mecanismos que permiten la coexistencia de los protocolos IPv4/IPv6.

Capítulo 1

El protocolo IPv6

1.1 Antecedentes.

Antes de describir al protocolo IPv6 es importante plantear algunos antecedentes, uno de estos es el concepto de red.

1.1.1 Concepto de red.

La palabra “red” es la que inmediatamente nos viene a la mente cuando se menciona al protocolo IP. Los diversos significados que adopta el concepto de red convergen en los siguientes puntos: primero, una red debe tener miembros, segundo, los miembros deben estar conectados entre sí de alguna manera y tercero, todos los miembros de la red deben establecer claramente la comunicación con cada uno de ellos para que tenga lugar una comunicación efectiva. Por lo tanto en una red de datos:

- Las entidades conectadas a una red son llamadas host, dispositivos o de manera general nodos.
- El enlace mediante el cual tiene lugar la comunicación se llama medio de red.
- Las reglas que gobiernan la manera en que los datos son intercambiados entre dispositivos se logran a través de un protocolo común de red.

Conjuntando estos tres conceptos se produce una definición formal de una red:

Una red de datos es un conjunto de computadoras y otros dispositivos que usan un protocolo común de red para compartir recursos entre sí a través de un medio de red. Las redes surgen como respuesta a la necesidad de compartir rápida y eficientemente recursos entre equipos. Una red puede utilizarse para compartir datos, compartir

recursos de software y hardware y también se le puede utilizar para centralizar la administración y soporte.

Dispositivos de red.

El término dispositivo se utiliza para describir cualquier entidad que está conectada a una red. Estas pueden ser computadoras, impresoras o unidades hardware especiales relativas a la misma red como servidores, conmutadores, routers, etc.

Medios de una red.

El enlace físico usado para conectar miembros de una red se denomina medio. Los medios de la red facilitan la comunicación al proporcionar el “puente” para que la comunicación tenga lugar. Los medios de una red se presentan en dos categorías: cableados, e inalámbricos. Algunos ejemplos de medios cableados son el cable de par trenzado, el cable coaxial y el cable de fibra óptica. Dentro de los ejemplos de medios inalámbricos se encuentran las ondas de radio y la radiación infrarroja.

Protocolos.

El lenguaje que utilizan los miembros de una red se llama protocolo de red. Los protocolos facilitan la comunicación y el “entendimiento” entre dispositivos al proporcionarles un lenguaje común. Este lenguaje común es un conjunto de procedimientos, reglas o especificaciones formales que definen entre otras cosas el formato, la integridad y la transmisión de los datos. Un protocolo de red que detalla de manera muy clara el proceso de comunicación entre dos dispositivos conectados a través de una red es el modelo OSI.

1.1.2 El modelo OSI.

El modelo OSI es un estándar internacional desarrollado por la Organización Internacional para la Normalización (ISO) que desde 1983 establece las bases para la comunicación entre dos computadoras. Este modelo propone dividir en siete niveles las tareas necesarias para establecer una sesión de comunicación entre dos computadoras. La organización de las siete capas se basa en la secuencia natural de los acontecimientos que se producen durante la sesión de comunicaciones.

El establecimiento de las siete capas dentro de la estructura del modelo OSI, se guió bajo los siguientes principios:

1. Una capa se creará en situaciones en donde se necesita un nivel diferente de abstracción.
2. Cada capa deberá efectuar una función bien definida.
3. La función que realizará cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.
4. Los límites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfases.
5. El número de capas deberá ser lo suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa y por otra parte también deberá ser lo suficientemente pequeño para que su arquitectura no llegue a ser difícil de manejar.

Bajo estas normas las primeras cuatro capas cumplen con la función del flujo de datos y también son llamadas capas inferiores. Las tres capas restantes cumplen con funciones de aplicación, se les denominan también capas superiores. La estructura del modelo OSI se muestra en la figura 1.1.

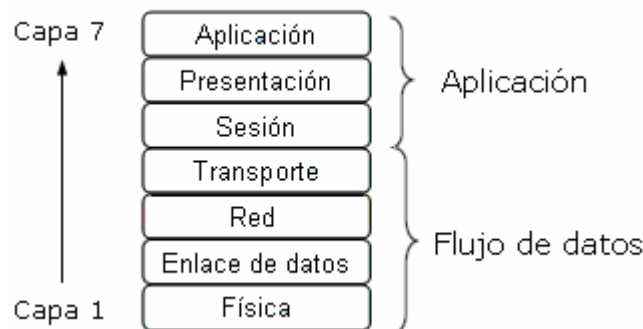


Figura 1.1 El modelo OSI

1.1.2.1 Las capas superiores.

Capa 7: Aplicación.

En esta capa es donde el usuario interactúa con la computadora, es decir en esta capa están los protocolos que definen las aplicaciones orientadas al usuario. Los

protocolos de esta capa identifican al dispositivo interlocutor de comunicaciones, determinan la disponibilidad de recursos y sincronizan la comunicación. Esta capa difiere de las demás debido a que no proporciona servicios a ninguna otra capa, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto, correo electrónico, transferencia de archivos, etc.

Capa 6: Presentación.

Es la capa responsable de administrar el modo en que se codifican los datos. Debido a que no todos los sistemas de computadoras utilizan el mismo esquema de codificación, la capa de presentación permite la traducción entre esquemas de codificación que de otro modo serían incompatibles, como por ejemplo, el Código americano normalizado para el intercambio de información (ASCII) y el código ampliado de caracteres decimales codificados en binario (EBDIC).

Capa 5: Sesión.

Esta capa establece, mantiene y administra sesiones entre las aplicaciones. Por lo general en muchos protocolos las funciones realizadas por esta capa se integran a las funciones de la capa de transporte.

1.1.2.2 Las capas inferiores.

Capa 4: Transporte.

De manera concreta la capa de transporte es responsable de la integridad de las transmisiones de un extremo a otro, identificando paquetes dañados o perdidos durante su transmisión y generando automáticamente una solicitud de retransmisión. Otra función de la capa de transporte es la re-secuenciación de paquetes que llegan en un orden inadecuado. La capa de transporte aísla a las capas superiores, de los procesos de transporte.

Capa 3: Red.

Los protocolos de esta capa son responsables de establecer la ruta que se utilizará entre los dispositivos origen y destino que se ubican en redes geográficamente separadas. Para esto utiliza una arquitectura de direccionamiento lógico.

La capa de red depende de la capa superior e inferior para la detección/corrección de errores de transmisión.

Capa 2: Enlace de Datos.

La capa de enlace de datos es responsable de proporcionar validez de un extremo a otro a los datos que se están transmitiendo. Para lograr esto la capa de enlace tiene su propia estructura de direcciones que se aplica a los dispositivos de red que residen localmente en el mismo dominio de capa de enlace de datos.

Este direccionamiento se denomina direccionamiento físico. Las capas física y de enlace de datos son indispensables en cualquier tipo de comunicación.

Capa 1: Física.

La capa física se responsabiliza de la transmisión de datos en forma de bits. Recibe datos de la capa 2 y transmite su contenido en serie un bit a la vez. También recibe el flujo entrante de datos, un bit a la vez y entonces los transmite a la capa de enlace de datos. Esta capa no tiene mecanismos para determinar el significado de los bits que transmite o recibe. A esta capa únicamente le competen las características físicas sean eléctricas, mecánicas así como de procedimiento de la señal (voltaje, temporización, etc) y del medio (cable coaxial, fibra óptica, cable de par trenzado, etc).

1.1.2.3 La adyacencia lógica.

Identificar y organizar por capas la secuencia de eventos que soporta una sesión de comunicaciones de red es un concepto sumamente útil. Uno de los beneficios más importantes de este método es que permite un concepto conocido como adyacencia lógica, que se refiere a la aparente capacidad de los protocolos de la misma capa que operan en las computadoras de origen y de destino para comunicarse directamente entre sí. Por ejemplo los protocolos de la capa tres de una computadora origen son adyacentes lógicamente a los protocolos de la misma capa de la computadora destino con los que se están comunicando. La adyacencia lógica también se conoce como comunicaciones “par-a-par” (peer-to-peer). Es evidente que este no es el modo real en el que se establece la comunicación. La orientación vertical de la pila de protocolos OSI es una reafirmación del flujo real de procesos y datos dentro de cada computadora.

Las diferencias entre el flujo lógico y el flujo real de la sesión de comunicaciones se ilustran en la figura 1.2 utilizando el modelo de referencia OSI.

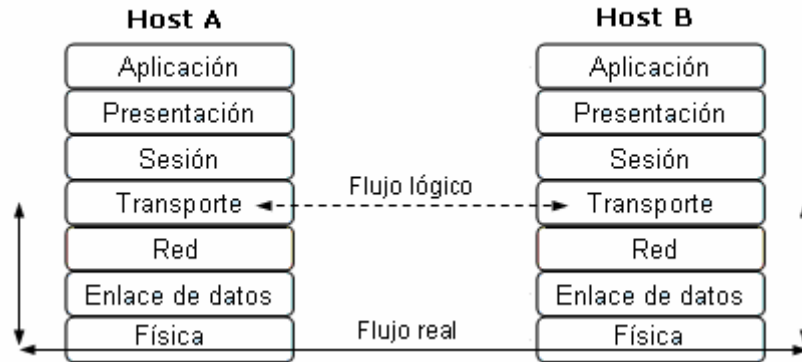


Figura 1.2 Flujo real frente a flujo lógico de comunicaciones en capas

Aunque las comunicaciones fluyen verticalmente a través de cada pila de protocolos, cada capa se percibe a sí misma como capaz de comunicarse directamente con sus capas equivalentes en las computadoras remotas. Para permitir la adyacencia lógica de las capas, cada capa de la pila de protocolos de la computadora de origen añade una cabecera a los datos recibidos desde la capa superior. Esta cabecera es reconocida y utilizada sólo por esa capa o sus equivalentes de otras computadoras. La pila de protocolos de la computadora receptora elimina las cabeceras, capa a capa, a medida que los datos son enviados a su aplicación. Este proceso que se muestra en la figura 1.3 permite ver que las únicas capas que son realmente adyacentes y pueden comunicarse directamente son las capas físicas.

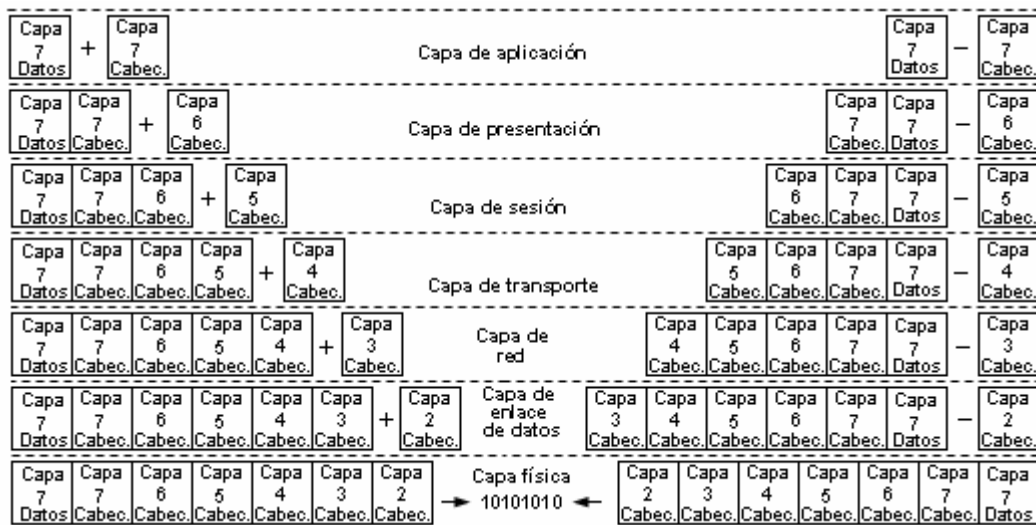


Figura 1.3 Uso de las cabeceras en capas para soportar la adyacencia lógica

Este proceso de intercambio de información entre capas iguales se basa en las Unidades de datos de protocolo (PDU). En cada nivel se utiliza un PDU específico, como se presenta en la figura 1.4. En las capas superiores solo se hace referencia a los datos. El PDU de la capa de transporte se denomina “segmento”, el de red se llama “paquete”, y el de enlace de datos se conoce como “trama”. Finalmente en la capa física solo se ven bits codificados.

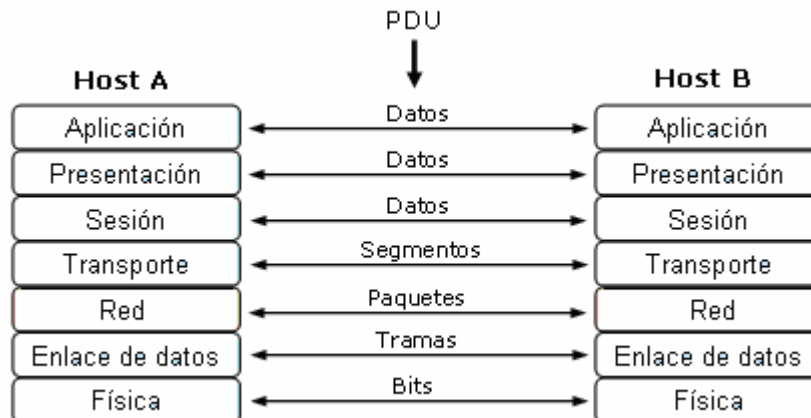


Figura 1.4 Comunicación entre capas

El modelo OSI por su diseño es excelente para explicar el proceso de comunicaciones entre dos dispositivos, por que proporciona un acercamiento teórico más específico que otros modelos. Sin embargo no ha podido posicionarse como un protocolo aceptado a gran escala. El protocolo OSI se ha visto opacado por el conjunto de protocolos TCP/IP.

1.1.3 TCP/IP

El estándar abierto de Internet desde un punto de vista histórico y técnico es el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP), este fue desarrollado por el Departamento de Defensa de Estados Unidos con la finalidad de proporcionar un sistema seguro de comunicaciones con independencia del medio físico. TCP/IP fue adoptado finalmente como estándar militar en 1983 después de 14 años de desarrollo y procesos de prueba en la red denominada ARPANET. El éxito de ARPANET fue inmediato al grado que numerosas organizaciones, desde universidades a corporativos se enlazaron a ella. Estas adhesiones hicieron que ARPANET evolucionara de su plan original dando forma a lo que conocemos actualmente por Internet.

Existen diversas razones por las que se opta implementar TCP/IP en la gran mayoría de redes en lugar del modelo OSI. Se mencionan solo algunas:

- TCP/IP y OSI difieren en la manera en que se desarrollan y prueban sus estándares. TCP/IP lleva un proceso abierto para la participación de sus usuarios en la elaboración de estándares. El desarrollo de nuevos protocolos TCP/IP o la modificación de los ya existentes también se efectúa con base en su necesidad. Además, la investigación, el desarrollo y las pruebas a nuevos protocolos o a protocolos modificados pueden efectuarse en una red de producción; el procedimiento abierto está en los documentos Petición de comentarios (RFC), y la distribución de TCP/IP es gratuito. En cambio, los protocolos OSI tienen derechos de autor y hay que pagar para adquirirlos.
- En comparación con el modelo OSI, TCP/IP resulta un protocolo más simple y confiable, además de que no está patentado, razón que ha contribuido mucho en su éxito. Los desarrolladores de TCP/IP han sostenido un enfoque de mejoramiento continuo para sus protocolos, por lo que satisface las necesidades de usuarios con diferentes perfiles.
- TCP/IP está estrechamente relacionado a Internet.

En resumen, mientras el modelo OSI establecía teóricamente el proceso de comunicaciones de manera muy precisa, en la práctica el conjunto de protocolos TCP/IP ya soportaba la red que conformaría a Internet. Sin embargo el análisis del modelo OSI no resulta trivial ya que gran parte de sus especificaciones son aplicables al conjunto de protocolos TCP/IP.

TCP/IP al igual que el modelo OSI, también se basa en la organización jerárquica por capas, pero no se apega de una forma muy estricta a capas funcionales, este estándar se enfoca a distribuir la interconectividad de manera más práctica, lo que le proporciona a los desarrolladores de protocolos una mayor flexibilidad para su implementación. La flexibilidad de TCP/IP se muestra en la tabla 1.1.

Descripción de las capas del modelo de referencia OSI	Número de capa del modelo OSI	Descripción de la capa equivalente TCP/IP
Aplicación	7	Aplicación
Presentación	6	
Sesión	5	
Transporte	4	Transporte
Red	3	Internet
Enlace de datos	2	Acceso a la red
Física	1	

Tabla 1.1 Flexibilidad del modelo TCP/IP respecto al modelo OSI

La pila TCP/IP contiene cuatro capas funcionales: Acceso a la red, Internet, Transporte y Aplicación. La pila TCP/IP se corresponde en buena parte con el modelo OSI en las capas inferiores, además soporta todos los protocolos estándar de enlace de datos y físicos. TCP/IP transfiere la información en una secuencia de paquetes. Se puede transmitir un mensaje como una serie de paquetes que se vuelven a ensamblar en la ubicación destino para recuperar el mensaje.

1.1.3.1 Capa de aplicación.

La capa de aplicación de TCP/IP conjunta la funcionalidad que se encuentra en las capas de sesión, presentación y aplicación del modelo OSI. Los diseñadores de TCP/IP pensaron que los protocolos de nivel superior deberían incluir las características de la capas de sesión y presentación. Entonces crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. Algunos de los protocolos que residen en este nivel son:

- Protocolo de transferencia de archivos (FTP). Es un protocolo que permite transferir archivos entre dos hosts. FTP es por sí mismo una aplicación.
- Protocolo trivial de transferencia de archivos (TFTP). Este protocolo en realidad es una versión reducida de FTP por lo que permite mover archivos sin ningún tipo de autenticación (sin nombre de usuario ni contraseña).

- Protocolo simple de transferencia de correo (SMTP). Protocolo que se encarga de la entrega de mensajes de correo entre dos hosts.
- Protocolo simple de gestión de red (SNMP). Es un protocolo que recopila información de red con la finalidad de supervisar su rendimiento.
- Telnet. Es un protocolo de emulación de terminal que permite conectar una computadora local con una computadora remota. La computadora local se convierte en una terminal virtual que tiene acceso a las aplicaciones y demás recursos que incorpora la computadora remota.

1.1.3.2 Capa de transporte.

La capa de transporte maneja los aspectos de calidad de servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. La capa de transporte consta de dos protocolos Protocolo de control de transmisión (TCP) y el Protocolo de datagrama de usuario (UDP).

- TCP realiza los procesos que permiten crear comunicaciones de red confiables, sin problema de flujo y con bajos niveles de error, es decir es un protocolo confiable. El protocolo TCP está orientado a la conexión. En un ambiente orientado a la conexión, se establece una conexión entre ambos dispositivos antes de que inicie la transferencia de información, con el fin de verificar que la transferencia esté autorizada y que los dispositivos estén preparados. Después de que se haya producido la sincronización, se establece una conexión y se inicia la transferencia de datos. TCP divide los mensajes en segmentos y los reensambla en el dispositivo destino. También se encarga de reenviar cualquier paquete que no haya sido recibido. Durante la transferencia, los dos dispositivos siguen comunicándose para verificar que estén recibiendo los datos fielmente.
- UDP es un protocolo de transporte no orientado a la conexión, es decir no proporciona verificación de software para la entrega de segmentos, por lo tanto proporciona una conexión entre los protocolos de la capa de Aplicación que no requieren aceptación ni sincronización por parte de TCP. Esta característica hace que la entrega de información vía UDP sea más rápida. Con UDP se intercambia confiabilidad por velocidad.

1.1.3.3 Capa Internet.

El propósito específico de la capa Internet es enviar paquetes desde cualquier red y que estos lleguen a su destino independientemente de la ruta y de las redes que tuvieron que recorrer. El protocolo que gobierna esta capa es el protocolo Internet (IP). IP es el único protocolo de red en el modelo TCP/IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada, situando a IP como el protocolo universal que permite que dos dispositivos en cualquier parte del mundo puedan comunicarse en cualquier momento.

IP recibe los datos de la capa de transporte y fragmenta esta información en paquetes. Posteriormente etiqueta cada paquete con la dirección IP del host origen y destino, la dirección IP se denomina de igual forma dirección lógica. IP también se encarga de volver a ensamblar los paquetes en el host destino en segmentos que puedan utilizar los protocolos de la capa superior. IP es un protocolo sin conexión que no se preocupa por el contenido de los paquetes. Su único propósito es dirigir y mover los paquetes hacia su destino. La capa Internet soporta otras funciones de administración de rutas. Debe proporcionar los mecanismos para resolver las direcciones de Capa 2 (direcciones físicas) en direcciones de capa 3 (direcciones lógicas) y viceversa. Los protocolos restantes que residen en esta capa proporcionan el soporte para el sistema de direccionamiento IP y el formato de paquetes.

- Protocolo de resolución de direcciones (ARP). Cuando IP prepara un paquete, conoce de antemano la dirección IP de los hosts origen y destino porque recibe esta información de los protocolos de la capa superior. Pero IP también necesita conocer las direcciones físicas de hardware para el host destino ya que tiene que proporcionar esta información al protocolo de la capa de enlace utilizado en la red. ARP proporciona el mecanismo para resolver las direcciones IP en direcciones de hardware. Para ello, ARP envía difusiones con la dirección IP del host destino y solicita a este host que responda con su dirección física.
- Protocolo Internet de control de mensajes (ICMP). ICMP es un protocolo de suministro y gestión de servicios de mensajería que utilizan los routers para mandar mensajes a los hosts que están enviando datos que deben enrutarse.

Los routers mediante estos mensajes, pueden informar a los hosts origen si es factible alcanzar un destino determinado o cuando la memoria intermedia del router está saturada de datos. ICMP se utiliza básicamente como protocolo de soporte para el direccionamiento IP lo mismo que ARP.

1.1.3.4 El direccionamiento físico

El direccionamiento físico es conocido como plano, es decir todos los nodos en una red segmentada tienen la misma prioridad para acceder al medio. Sus características principales son:

- Una dirección física es un identificador único a nivel de hardware que viene integrado en cada interfase de red (NIC).
- Las direcciones físicas en la mayoría de los casos son inalterables.
- Los estándares de red más comunes hacen uso de direcciones físicas de 48 bits, las cuales se denominan direcciones MAC, estos 48 bits de longitud se expresan como 12 dígitos hexadecimales.
- Las direcciones físicas solo sirven para intercomunicar equipos interconectados en una red local, ya que su nomenclatura sólo hace referencia a interfaces de red.

24 bits se utilizan para describir al fabricante de la tarjeta, este número se denomina código de fabricante, los 24 bits restantes se usan para describir la singularidad de la tarjeta o número de serie. Así por ejemplo una dirección MAC se expresa del siguiente modo:

00.00.0c.03.df.60

Donde el código del fabricante es 00.00.0c y el número de serie es 03.df.60.

1.1.3.5 Esquema de direccionamiento de IPv4.

Se ha hablado de que el protocolo IP que reside en la capa tres del modelo OSI utiliza una arquitectura de direccionamiento lógico para comunicar dispositivos geográficamente muy distantes. Esta es la arquitectura de direcciones con la que opera Internet. La versión original de IP es la versión 4 (IPv4) y utiliza un esquema de

direccionamiento binario de 32 bits. Cada dirección se dividió en cuatro campos de 8 bits (un octeto) separados por puntos. Para facilitar su uso, las direcciones binarias se convirtieron al formato decimal. Cada uno de los octetos de la dirección IP se representa por un número decimal que va desde 0 hasta 255.

La dirección IPv4 decimal con puntos se dividió en clases para adaptarse a redes con diferentes necesidades de población. Estas clases se diferenciaban entre sí por el número de bits destinados a identificar a la red frente a los destinados a identificar al host. Cada clase de dirección IP está identificada por las primeras cinco letras del alfabeto: A, B, C, D y E. Cada dirección contiene dos partes, una dirección de red y una dirección de host. Solo las tres primeras clases representan diferentes proporciones entre el número de redes y hosts soportables.

Dirección de clase A.

Diseñada para dar cabida a redes extremadamente grandes, maximiza el número posible de host, pero limita el número posible de redes. El primer bit de una dirección de clase A es siempre un cero, Los 7 bits restantes del octeto identifican el número de red. Los 24 bits restantes (tres octetos) de una dirección de Clase A representan las posibles direcciones de host. El intervalo de direcciones de clase A va de 1.0.0.0 a 126.0.0.0. Esto indica que solo puede haber 126 posibles redes IP de clase A, sin embargo cada una de estas soporta 16,774,214 direcciones de host únicas. Técnicamente la dirección 127.0.0.0 también es una dirección de red de clase A, pero está reservada para pruebas loopback y no es asignable.

Dirección de clase B.

Diseñadas para dar respuesta a las necesidades de redes de tamaño moderado a grande. Los primeros 2 bits de una dirección de clase B son 10. Los siguientes 14 bits identifican el número de red, y los últimos 16 bits identifican las posibles direcciones de host. El intervalo de las direcciones de clase B posibles va de 128.1.0.0 a 191.254.0.0. Matemáticamente solo puede haber 16,382 redes de clase B y cada una de estas puede soportar 65,534 direcciones únicas.

Dirección de Clase C.

El espacio de direcciones de clase C es el más comúnmente utilizado, fue creado para dar lugar a muchas redes pequeñas. Los primeros 3 bits de una dirección de clase C son 110. Los siguientes 21 bits identifican el número de red. El último octeto se usa para el direccionamiento del host. El intervalo de posibles direcciones de red de clase C va de 192.0.1.0 a 192.255.255.254.0. Puede haber 2,097,150 redes de clase C y cada una puede soportar 254 direcciones de host únicas

Direcciones de clase D.

Los primeros cuatro bits de una dirección de clase D son 1110. Estas direcciones se utilizan para un proceso denominado multicast, pero han tenido un uso limitado, Una dirección multicast es una dirección de red única que dirige paquetes con esa dirección de destino a grupos predefinidos de direcciones IP. Las direcciones de red de clase D van de 224.0.0.0 a 239.255.255.254.

Dirección de clase E.

Se ha definido una dirección de clase E, pero está se ha reservado para propósitos de investigación. Este intervalo va por deducción, de 240.0.0.0 a 255.255.255.0. No se ha distribuido ninguna dirección de clase E para su uso en Internet.

1.1.3.6 Déficit de direcciones IPv4.

La división en clases del espacio de direccionamiento de IPv4 originalmente no estaba planeada, el crecimiento que tuvo Internet desde un principio hizo que se hiciera esta modificación, lo mismo ocurre con el sistema telefónico; ante el incremento en la demanda del servicio es necesario un cambio en el sistema de marcado, donde generalmente se añade un número a marcar. Tanto en el sistema telefónico como en el espacio de direcciones IPv4 estas divisiones crean grandes vacíos, eliminando un número considerable de direcciones potenciales. Otro factor que ha mermado de manera importante el número de direcciones IPv4 han sido las políticas de asignación iniciales en donde a cualquier organización, le era concedido un bloque de direcciones con tan solo pedirlo, esto sin verificar si la necesidad de direcciones de la organización en cuestión era real. Muchas de estas organizaciones nunca le dieron un uso adecuado a las direcciones que se les asignaron y muchas de ellas desaparecieron,

bloqueando así grandes porciones de direcciones IPv4. Esto ocurrió sobre todo con bloques de direcciones de clase A y B que son las que dan cabida a un mayor número de dispositivos.

1.1.3.7 Mecanismos para preservar el espacio de direcciones IPv4

Para contrarrestar este déficit de direcciones se han desarrollado numerosas extensiones del protocolo IP con la finalidad de mejorar la eficacia con la que puede usarse el espacio de direcciones de 32 bits. De manera breve se mencionan las más importantes.

Máscaras de subred.

La división en subredes permite al número de red de cualquier dirección IP clasificada (A, B o C) subdividirse en números de red más pequeños. Una dirección IP dividida en subredes contiene tres partes:

1. Dirección de red.
2. Dirección de subred.
3. Dirección de host.

Las direcciones de subred y de host se extraen de la porción de dirección de host de la dirección IP original. Por lo tanto su capacidad para dividirse en subredes depende directamente del tipo de dirección IP que se divide en subredes. Las subredes se identifican usando una dirección pseudo-IP conocida como la máscara de subred. La máscara de subred es un número binario de 32 bits que pueden expresarse en formato decimal con puntos y su función es indicarle a los sistemas finales (routers) de la red cuántos bits de la dirección IP se utilizan para la identificación de la red y de la subred. Estos bits se llaman prefijo de red extendido. Los bits de la máscara que identifican el número de la subred están establecidos a uno, y los bits del host a cero.

Máscara de subred de longitud variable (VLSM).

La división de subredes tenía la limitación de que solo se podía tener una sola máscara de subred para toda una red, después de seleccionar una máscara de subred no podían soportarse redes de tamaño diferente. En una configuración real, la necesidad de las subredes no es uniforme. VLSM permite un uso más eficaz del

espacio de direcciones IP de una organización, permitiendo al administrador de red personalizar el tamaño de una máscara de subred para los requisitos específicos de cada subred.

Enrutamiento Interdominio sin clase (CIDR).

Este mecanismo elimina las ineficaces clases de direcciones a favor de una arquitectura de direccionamiento más flexible. CIDR tiene tres características clave que amortiguan el agotamiento del espacio de direcciones IPv4.

1. Eliminación del direccionamiento con clases. Este mecanismo permite un uso más efectivo de las direcciones restantes.
2. Adición de rutas mejoradas. Mecanismo donde una sola entrada de la tabla de enrutamiento puede representar los espacios de direcciones de múltiples redes.
3. *Supernetting*. La función de supernetting no es más que usar bloques contiguos de espacios de clase C para simular un solo espacio de direcciones mayor.

Traducción de direcciones de red (NAT).

Es un mecanismo que ha aportado una solución parcial al déficit del espacio de direccionamiento IPv4, desempeñando un papel importante al permitir que grandes organizaciones utilicen pocas direcciones globales IPv4 para sus enormes redes. NAT típicamente transporta paquetes desde una red utilizando direcciones privadas hacia Internet. La Agencia de Asignación de Números de Internet (IANA) que es la organización dedicada a la coordinación central de Internet, identificó y reservó tres intervalos de dirección que pueden utilizarse para la interconexión de redes de manera interna. Estos intervalos incluyen direcciones de clase A, B y C de IPv4:

- 10.0.0.0-10.255.255.255
- 172.16.0.0-172.31.255.255
- 192.168.0.0-192.168.255.255

Estas son las direcciones privadas. Originalmente estas direcciones no podían usarse para acceder directamente a Internet. Las organizaciones que usan estas direcciones y tienen la necesidad de acceder a Internet utilizan un dispositivo NAT como intermediario entre su red interna e Internet. Desde 1990, la combinación de CIDR, NAT y el direccionamiento privado, ha aportado beneficios a la Internet al disminuir el agotamiento de las direcciones IPv4.

Estos mecanismos fueron implementados con la finalidad de extender el tiempo de vida de IPv4. IPv4 tiene más de 20 años y ha soportado cambios muy importantes como los avances tecnológicos y un cambio sustancial en la población de sus usuarios a razón de una comercialización de Internet. Esto ha creado la necesidad de crear más direcciones y del soporte de la capa Internet para nuevos tipos de servicio.

1.2 IPv6

IPv6 fue desarrollado principalmente por una razón: El déficit del espacio de direcciones IPv4. Este déficit fue evidenciado por una serie de factores, entre los que se encuentran:

- El acelerado crecimiento que Internet ha mostrado a partir de los años noventa naturalmente significa una mayor demanda de direcciones IPv4.
- Las porciones del esquema de direccionamiento IPv4 reservadas para casos especiales como las direcciones de clase D y E además de las direcciones privadas disminuyen significativamente el total de las direcciones IPv4 disponibles.
- La gran cantidad de direcciones IPv4 que innecesariamente fueron desperdiciadas durante los inicios de Internet debido a políticas de asignación inapropiadas.
- Los mecanismos para mejorar el uso del espacio de direccionamiento IPv4 y extender su tiempo de vida como CIDR, NAT y VLSM sin duda que han servido, pero no pueden durar para siempre.

Los miembros del grupo de Ingeniería de Internet (IETF) comenzaron el desarrollo de IPv6 cuando un estudio preliminar en 1990 concluyó que el espacio de direccionamiento de IPv4 podría agotarse muy pronto si Internet continuaba con las tendencias de crecimiento hasta ese momento mostradas. Los resultados de este

estudio pronosticaron que el “colapso” del esquema de direccionamiento IPv4 ocurriría entre los años 2005 y 2011.

Entonces el IETF acordó diseñar, desarrollar, y probar un nuevo protocolo con funciones mejoradas en lugar de implementar un “parche” que solo añadiera direcciones más largas. Este trabajo mostraría las limitaciones del esquema de direccionamiento IPv4 y desarrollaría un protocolo que asegurara un crecimiento confiable de Internet durante las próximas décadas.

El proceso de desarrollo de IPv6 ha sido coordinado y estructurado desde entonces gracias a la contribución de múltiples organizaciones enfocadas en resolver los problemas del protocolo IPv4.

En 1993 se publicó una lista de propuestas (RFC 1550). Tres de ellas se analizaron en detalle:

- *Common Architecture for the Internet* (CATNIP) propuesta para converger los protocolos CNLP, IP e IPX con el uso de las direcciones Network Service Access Point (NSAP). (Definido en el RFC 1707).
- El *Simple Internet Protocol Plus* (SIPP) propuesto para incrementar el tamaño de direcciones a 64 bits y mejorar la cabecera IP (Definida en el RFC 1752).
- TCP/UDP sobre CLNP (TUBA) sugerido para reemplazar al IP (capa 3) con el protocolo Connectionless Network Protocol (CNLP), donde TCP/UDP y otros protocolos superiores podían correr arriba de CLNP (Definida en el RFC 1347).

La propuesta aceptada fue SIPP, con un espacio de direccionamiento de 128 bits. El autor principal de SIPP fue Steve Deering. Un grupo de trabajo en el IETF llamado IP next generation (IPng) comenzó a trabajar en 1993, entonces las primeras especificaciones se publicaron a finales de 1995 (RFC1883). En 1996, la red de pruebas de IPv6 llamado backbone IPv6 (6bone) fue implementado sobre Internet. Los prefijos IPv6 dentro del espacio IPv6 3ffe::/16 se asignaron a los participantes del 6bone. En 1997, se realizó el primer intento de estructurar el espacio IPv6 como un formato de direcciones IPv6 basado en proveedor. Un año después, el primer intercambio IPv6 llamado 6TAP, fue realizado en el STARTAP en Chicago.

En 1999, los registros regionales de Internet (RIRs) comenzaron a asignar prefijos de producción IPv6 utilizando el espacio IPv6 2001::/16. Durante el mismo año se funda el Forum IPv6, un consorcio mundial conformado por empresas tecnológicas involucradas con Internet, organizaciones de educación e investigación con la finalidad de promover IPv6 en el mercado así como colaboraciones entre los mismos fabricantes. En el 2000, muchos fabricantes comenzaron a construir sus principales productos habilitados para IPv6. El grupo de trabajo IPng fue renombrado como IPv6 en el 2001. Con el paso de IPv4 a IPv6 viene la pregunta obligada ¿Qué pasó con IPv5? IPv5 es un protocolo reservado como recurso experimental diseñado para ofrecer calidad de servicio (QoS), definido como el Internet Stream Protocol (ST). Este puede proveer transporte en tiempo real de archivos multimedia como por ejemplo voz, video, tráfico de datos en tiempo real, a través de Internet. El IPv5 también es llamado ST2, y está documentado en el RFC 1819, y RFC1190.

1.2.1 Características de IPv6.

A continuación se presentan las mejoras más importantes de IPv6 respecto a IPv4, así como nuevas características.

- El esquema de direcciones de 128 bits, proporciona un número de direcciones IP prácticamente ilimitado.
- Múltiples niveles de jerarquía ayudan a agregar rutas, esto promueve un enrutamiento escalable y eficiente de Internet.
- La transición entre proveedores IPv6 es transparente para los usuarios finales con el mecanismo de reenumeración.
- La cabecera IPv6 es más eficiente que la cabecera IPv4.
- IPv6 fue diseñado para proporcionar mecanismos de seguridad y movilidad mucho más eficientes que los incluidos en el protocolo IPv4.
- Diversos mecanismos de transición fueron diseñados con IPv6, para permitir una gradual transición de las redes IPv4 hacia redes IPv6.
- IPv6 incluye en su estándar el mecanismo “plug and play”*, lo cual facilita a los usuarios la conexión de sus equipos a la red. La configuración del dispositivo que se conecta a Internet IPv6 se realiza de manera automática.

- IPv6 aplica en su diseño las buenas prácticas de IPv4 y elimina las características no utilizadas u obsoletas de IPv4, esto promueve una optimización del protocolo de Internet.

Durante las especificaciones de diseño de IPv6 estuvo a debate el uso de direcciones fijas a 64 bits contra el direccionamiento de longitud variable de más de 160 bits. Finalmente utilizando direcciones de longitud fija de 128 bits para IPv6 se encontró que era la elección más adecuada. Con IPv4, el número de nodos direccionables en teoría es de 4,294,967,296 (2^{32}), lo que representa cerca de dos direcciones por cada tres personas (basado en una población mundial de 6 billones de personas en el 2005). Por otra parte, la longitud de 128 bits en IPv6 representa $3.4 \cdot 10^{38}$ direcciones, lo que permite aproximadamente $5.7 \cdot 10^{28}$ direcciones IPv6 para cada persona en el mundo. No obstante como sucede en cualquier esquema de direccionamiento, no todas las direcciones pueden ser usadas, pero un número más que suficiente está disponible para cualquier tipo de uso. Incrementar el número de bits por dirección también significa incrementar el tamaño de la cabecera IP. Debido a que cada cabecera IP contiene la dirección de origen y la dirección destino, el tamaño del campo de direcciones para IPv4 es de 64 bits y para IPv6 es de 256 bits. La figura 1.5 muestra la comparación el modelo de referencia OSI respecto al de IPv6, IPv6 representa únicamente un cambio en la capa de red. Esto fue una importante consideración durante el desarrollo de IPv6. Las otras capas de los dos modelos de referencia OSI permanecen igual, lo cual significa que protocolos como TCP y UDP usados con IPv4 continúan corriendo en el protocolo IPv6.

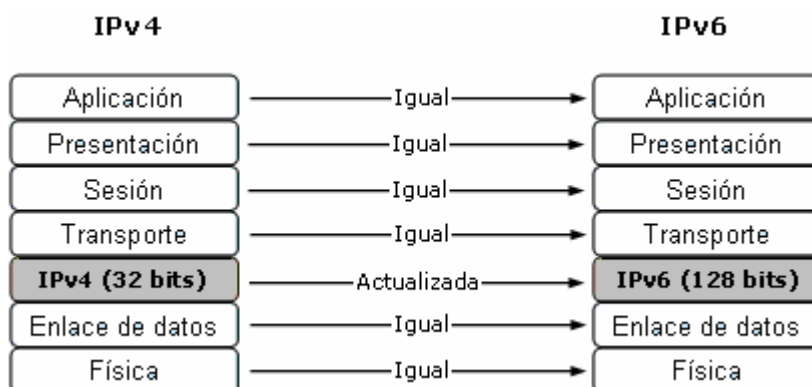


Figura 1.5 IPv4 e IPv6 con respecto al modelo de referencia OSI

Protocolo de Datagrama Usuario (UDP) en IPv6.

Para su implementación en IPv6, UDP sufrió una ligera pero importante modificación. El campo Suma de verificación (checksum) dentro del paquete UDP ahora es obligatorio en IPv6 y no opcional como en IPv4. Por lo tanto este campo debe ser procesado por el nodo origen IPv6 antes de que un paquete UDP sea enviado.

Protocolo de Control de Transporte (TCP) en IPv6.

Debido a la complejidad y gran flexibilidad demostrada por TCP, ningún cambio fue propuesto para su implementación en IPv6. Durante el desarrollo de IPv6 se decidió continuar corriendo TCP y UDP en IPv6 sin modificaciones estructurales sustanciales.

1.2.2 La cabecera IPv6.

Debido a que el protocolo IPv6 es una actualización del protocolo IPv4, se describe la cabecera IPv4 como un referente, mostrando los campos que continúan o que sufren alguna modificación en IPv6, y aquellos que por diversas causas ya no resultan útiles.

1.2.2.1 Formato de la cabecera IPv4.

Un paquete IP tiene dos componentes fundamentales:

- Cabecera IP. La cabecera IP contiene los campos de datos que usan los routers para enviar el paquete hacia su destino. Estos campos identifican el protocolo de transporte, el emisor, el receptor, además de otros parámetros.
- Carga útil. Representa la información (datos) que será entregado por el nodo origen.

La cabecera básica IPv4 contiene 12 campos, cada uno de ellos cumple con una función específica. La figura 1.6 muestra el formato de cabecera IPv4.

Versión	HLEN	Tipo de servicio	Longitud total	
Identificación			Ind.	Compensación de fragmentos
Tiempo de vida	Protocolo		Suma de verificación	
Dirección IP origen				
Dirección IP destino				
Opciones				Relleno

Figura 1.6 Formato de la cabecera IPv4

- **Versión** (4 bits). Muestra la versión de la cabecera IP. En IPv4 este campo contiene el valor 4.
- **Longitud de la cabecera** (4 bits). Este campo contiene la longitud la cabecera medida en bytes.
- **Tipo de servicio** (8 bits). Especifica el trato que recibe el paquete durante su transmisión a través de los routers de la ruta de entrega.
- **Longitud Total** (16 bits). El tamaño del paquete IP en bytes, incluyendo la cabecera y la carga. Este campo de 16 bits implica que el tamaño máximo de un paquete IPv4 es 65,535 bytes.
- **Identificación** (16 bits), **Indicadores** (3 bits), y **Compensación de fragmentos** (13 bits). Campos relacionados con la fragmentación de paquetes que realizan los routers cuando el MTU a lo largo de la ruta es más pequeño que el MTU del emisor. El MTU es el máximo tamaño en bytes de un paquete IP que será transmitido en un medio de comunicación específico, como Ethernet, FastEthernet, etc. Para Ethernet, el MTU es 1500 bytes.
- **Tiempo de vida** (8 bits). Este campo se disminuye en 1 cada vez que el paquete pasa a través de un router intermediario. Cuando este campo contiene el valor 0, el paquete es eliminado, y un mensaje de error ICMPv4 es enviado al nodo origen.
- **Protocolo** (8 bits). Especifica el protocolo de la capa superior usado en la carga del paquete, como por ejemplo TCP, UDP, ICMP, o cualquier otro protocolo especificado por la IANA.
- **Suma de verificación de la cabecera** (16 bits). Representa la suma de verificación de la cabecera IP y se utiliza para la verificación de errores. Este campo es verificado por cada router intermediario a lo largo de la ruta.
- **Dirección origen IPv4** (32 bits). La dirección IPv4 del host origen.
- **Dirección destino IPv4** (32 bits). La dirección IPv4 del host destino.

Los siguientes campos son opcionales:

- **Opciones** (variable). Permite que IP soporte opciones como las referentes a la seguridad.
- **Relleno** (variable). El relleno es usado para asegurar que el encabezado IP sea múltiplo de 32 bits.

Los campos en gris de la figura 1.6 fueron eliminados en la cabecera IPv6, a continuación las razones:

- Longitud de cabecera. La longitud de la cabecera IPv4 puede variar sus 20 bytes de longitud al añadirse el campo Opciones. Sin embargo debido a que la longitud del encabezado básico IPv6 está fijado a 40 bytes, este campo pierde toda utilidad.
- Identificación, banderas y Compensación de fragmentos. Este campo fue eliminado porque el proceso de fragmentación en IPv6 ya no lo realizan los routers intermediarios, sino los nodos que originan el paquete. Esta modificación también libera a los routers intermediarios del costoso procesamiento requerido para la fragmentación.
- Suma de verificación de la cabecera. En IPv6 tanto las tecnologías de la capa 2 como los protocolos de las capas superiores realizan su propia suma de verificación y control de errores (la suma de verificación en UDP dejó de ser opcional y ahora es obligatoria). Esto implica que una suma de verificación en la capa 3 es redundante, por lo que este campo resulta innecesario.
- Opciones y Relleno. El campo de opciones es radicalmente modificado en IPv6. Las opciones son ahora manejadas por cabeceras de extensión. El campo de Relleno es también eliminado. Con esto se simplifica la cabecera IP, además de que se libera procesamiento por parte de los routers en su tarea de entrega comparado con IPv4.

Los otros campos en la cabecera IPv4 – Versión, Tipo de servicio, longitud total, Tiempo de vida, Número de Protocolo, Dirección IPv4 origen y destino- fueron modificados ligeramente.

1.2.2.2 Formato de la cabecera IPv6.

La cabecera IPv6 contiene 8 campos, los cuales ocupan un total de 40 bytes. La figura 1.7 ilustra el formato de la cabecera IPv6.

- **Versión** (4 bits). La versión IP, este campo contiene el valor 6 identificando a IPv6.
- **Clase de tráfico** (8 bits). Campo con funciones similares al campo Tipo de Servicio en IPv4. Este campo etiqueta un paquete IPv6 con un “Differentiated Services Code Point” (DSCP), que especifica la forma en que el paquete debe ser manejado.
- **Etiqueta de Flujo** (20 bits). Este campo “etiqueta” el flujo de los paquetes IPv6, es decir identifica los paquetes que requieren un mismo trato para facilitar el soporte en tiempo real. Un nodo emisor puede etiquetar secuencias de paquetes con un conjunto de opciones. Los routers guardan el registro de los flujos y pueden procesar paquetes que pertenecen al mismo flujo de manera más eficiente porque no tienen que volver a procesar cada cabecera de los paquetes.
- **Longitud de carga útil** (16 bits). Este campo representa la longitud de datos. Los datos son la parte restante del paquete después de la cabecera IPv6.
- **Siguiente Cabecera** (8 bits). Precisa el tipo de información siguiente a la cabecera básica IPv6. El tipo de información puede ser de un protocolo e la capa superior como TCP o UDP, o puede ser una de las nuevas cabeceras de extensión opcionales.
- **Límite de saltos** (8 bits). Este campo define el número máximo de saltos (routers intermedios) que un paquete IP debe pasar, cada salto decrementa el valor en 1.
- **Dirección de origen** (128 bits). Este campo identifica la dirección IPv6 del nodo origen.
- **Dirección destino** (128 bits). Este campo identifica la dirección IPv6 del destinatario del paquete.

Versión	Clase de tráfico	Etiqueta de flujo	
Longitud de carga útil		Siguiente cabecera	Límite de saltos
Dirección origen			
Dirección destino			

Figura 1.7 Cabecera básica IPv6

1.2.3 Las Cabeceras de extensión.

Además del encabezado básico IPv6, una cadena con múltiples cabeceras de extensión podría presentarse inmediatamente después de los 40 bytes. Las cabeceras de extensión proporcionan una manera distinta de manipular las opciones. Las cabeceras de extensión ofrecen información extra hacia el destino o sistemas intermedios a lo largo de la ruta cuando así se requiera y promueven mejoras importantes en el procesamiento. Un paquete IPv6 puede incluir ninguna, una o múltiples cabeceras de extensión. En la figura 1.8 se muestra un paquete IPv6 que utiliza múltiples cabeceras de extensión, formando listas de cabeceras encadenadas identificadas por el campo *Cabecera siguiente* en la cabecera anterior.

Para aplicaciones típicas de IPv6, la última cabecera de la cadena es el protocolo de la capa superior que transporta la carga útil del paquete. Por ejemplo el protocolo de la capa superior puede ser un paquete TCP, UDP o ICMPv6.

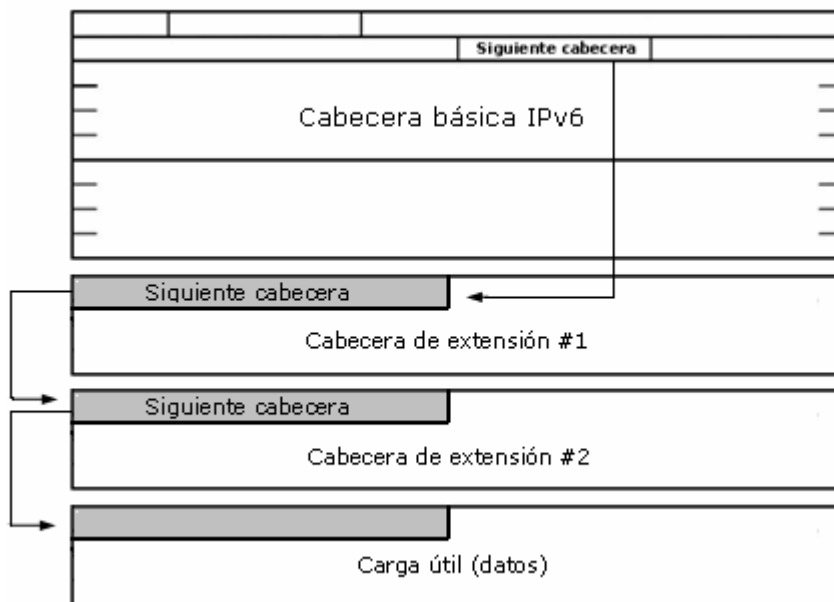


Figura 1.8 Múltiples cabeceras de extensión forman cadenas

En IPv6 se definen múltiples cabeceras de extensión, cada una se identifica por un valor particular contenido en el campo *Siguiete cabecera* en la cabecera que le antecede. A continuación se mencionan algunas cabeceras de extensión IPv6 definidas:

- **Cabecera de Opciones “Hop-by-Hop” (Protocolo 0)**. Este campo es leído y procesado por cada nodo y router a lo largo de la ruta de entrega. Una aplicación de la cabecera hop-by-hop es el envío de Jumbogramas. IPv6 puede enviar paquetes mayores a 65,535 octetos, especialmente en redes adecuadas para soportar MTUs muy grandes, estos son los Jumbogramas. IPv4 no puede enviar paquetes mayores a 65,535 octetos debido a que el campo *Longitud Total* está limitado a 16 bits. Básicamente la cabecera IPv6 tiene la misma limitante, porque el campo *Longitud de carga útil* también tiene 16 bits. Sin embargo, al utilizar un campo de 32 bits dentro de la cabecera de opciones Hop-by-Hop, el tamaño de un Jumbograma puede tener una longitud máxima de 4,284,967,295 octetos. Todavía se requiere experimentar más para conocer los alcances de este tipo de cabecera.
- **Cabecera de Opciones de Destino (protocolo 60)**. Esta cabecera transporta información opcional que es especialmente enviada a la dirección destino del paquete. Si el paquete incluye una cabecera de enrutamiento, esta cabecera la antecederá.
- **Cabecera de Enrutamiento (protocolo 43)**. Esta cabecera puede ser usada por un nodo origen IPv6 para obligar a un paquete a pasar a través de routers específicos en el trayecto a sus destinos. Una lista de routers intermediarios puede ser especificado dentro de esta cabecera. Esta es la forma en que el nodo origen se asegura de tener el control de la ruta por donde pasan sus paquetes para evitar que estos lleguen a routers inapropiados.
- **Cabecera de Fragmentación (protocolo 44)**. Cabecera que es utilizada por un nodo origen, que no soporta el mecanismo PMTUD cuando este debe enviar un paquete más grande que el MTU soportado en la ruta de entrega (este mecanismo es tratado más adelante en el capítulo 3). Cuando esto sucede, el nodo fragmenta el paquete y envía cada fragmento usando la cabecera de Fragmentos. Entonces el nodo de destino reensambla el paquete original al ordenar todos los fragmentos.
- **Cabecera de Autenticación (AH) (protocolo 51)**. Esta cabecera se utiliza para proporcionar autenticación además de integridad de datos, ofrece protección contra reenvío de paquetes que podrían haber sido interceptados por algún nodo. También se asegura de la protección de algunos campos de la cabecera

básica IPv6. Esta cabecera es esencialmente la misma tanto para IPv4 como para IPv6 y es mejor conocida como cabecera de autenticación IPSec, AH por sus siglas en inglés.

- **Cabecera de Encapsulación de seguridad de la información (ESP)** (protocolo 50). Esta cabecera es utilizada para permitir autenticación, integridad de datos y confidencialidad del paquete IPv6. Es muy similar a la Cabecera de Autenticación, esta cabecera es idéntica en IPv4 e IPv6. Esta también se conoce como IPSec Encapsulating Security Payload. (ESP).

Cuando un paquete IPv6 utiliza múltiples cabeceras de extensión, estas deben seguir el siguiente orden:

1. Cabecera básica IPv6
2. Opciones *Hop-by-Hop*
3. Opciones de Destino (si la cabecera de enrutamiento es usada)
4. Enrutamiento
5. Fragmento
6. Autenticación
7. Cabecera de Encapsulación de seguridad de la información
8. Opciones de Destino
9. Capas superiores (TCP, UDP, ICMPv6)

Los paquetes que incluyen múltiples cabeceras de extensión, deberán ser procesados únicamente por los nodos destino, en el estricto orden en que aparecen dentro del paquete IPv6. Los nodos que reciben los paquetes nunca deben buscar y procesar un particular tipo de cabecera de extensión dentro del paquete, antes del procesamiento de todas las cabeceras que le preceden.

Capítulo 2

Direccionamiento IPv6

2.1 Notación de las direcciones IPv6.

La longitud de una dirección IPv6 con sus 128 bits naturalmente modifica la manera en que estas se representan respecto a IPv4. Manejar 128 bits no parece una tarea sencilla, sin embargo se han creado técnicas de notación que facilitan la representación de una dirección IPv6.

2.1.1 Notación completa.

La manera formal de expresar una dirección IPv6 es la notación completa. Con esta notación los 128 bits de la dirección IPv6 se expresan mediante 8 bloques de 16 bits cada uno separados mediante el signo dos puntos “:”. Los 16 bits de cada bloque se traducen a cuatro caracteres hexadecimales, por lo tanto un bloque puede tener valores hexadecimales que van desde *0x0000* hasta *0xFFFF*. La tabla 2.1 muestra algunos ejemplos:

Direcciones IPv6 en notación completa
0000:0000:0000:0000:0000:0000:0000:0000
2001:0410:0000:FFFF:1400:5000:4545:AAAA
3FFE:0B00:0C18:0001:0000:1234:AB34:0002
FE80:0000:0000:0000:FFFF:FFFF:FFFF:FFFF

Tabla 2.1 Ejemplos de direcciones IPv6 expresadas en la forma completa

2.1.2 Notación simplificada.

En IPv6 es muy común el uso de direcciones que contienen largas cadenas de ceros, por esto se creó una sintaxis especial que simplifica valores consecutivos de ceros en dos situaciones:

1. Bloques consecutivos de ceros
2. Bloques que comienzan con uno o más ceros

Simplificando bloques consecutivos de ceros.

La simplificación de la longitud de una dirección IPv6 que presenta bloques consecutivos de ceros, se realiza al sustituir estos bloques por un par de dos puntos “::”. En una dirección IPv6 se permite el uso del par de puntos una sola vez. Cuando una dirección IPv6 presenta este par de puntos “::”, un analizador de dirección debe identificar el número de ceros omitidos. Cuando el analizador de dirección identifica la cantidad de ceros sustituidos por el signo “::”, este llena de ceros entre las dos partes de la dirección hasta que se completan los 128 bits de la dirección. Si por error una dirección presenta más de un “::”, no hay manera de que el analizador identifique el número de ceros que se intenta simplificar. La tabla 2.2 presenta ejemplos de direcciones IPv6 expresadas en la notación completa que al contener bloques consecutivos de ceros pueden simplificarse, en negritas se muestran los ceros abreviados.

Notación completa	Notación simplificada
0000:0000:0000:0000:0000:0000:0000:0000	::
FEC0: 0000:0000:0000 :1234:1010:0000:AABB	FEC0::1234:1010:0000:AABB
2001:0B00:0C18:0001: 0000 :1234:AB34:0002	2001:0B00:0C18:0001::1234:AB34:0002
FE80: 0000:0000:0000:0000:0000:0000:0000 :0009	FE80::0009

Tabla 2.2 Ejemplos de direcciones IPv6 en la forma completa que han sido simplificadas

Simplificando bloques que comienzan con uno o más ceros.

Este método es aplicable cuando uno o más ceros comienzan un bloque. Estos ceros se eliminan para simplificar la dirección. Sin embargo si todo el bloque contiene ceros, al menos un carácter 0 se debe mantener. Algunos ejemplos de este tipo de notación los muestra la tabla 2.3.

Notación completa	Notación simplificada
0000:0000:0000:0000:0000:0000:0000:0000	0:0:0:0:0:0:0:0
FEC0: 0000:0000:0000 :1234:1010: 0000 :AABB	FEC0:0:0:0:1234:1010:0:AABB
2001: 0 410: 0000 :FFFF: 00 14:5000:4545:AAAA	2001:410:0:FFFF:14:5000:4545:AAAA
FE80: 0000:0000:0000:0000:0000:0000:0000 :0009	FE80:0:0:0:0:0:0:9

Tabla 2.3 Direcciones que simplifican los 0s que inician cada bloque

Combinando ambos métodos de Simplificación.

La simplificación de bloques de 0s consecutivos, y de 0s que inician cada bloque se puede combinar. La tabla 2.4 presenta ejemplos donde se aplican ambos métodos de compresión.

Forma completa	Forma simplificada
2001:0123:BF00:AAAA:0000:0000:0002:5454	2001:123:BF00:AAAA::2:5454
FE80:0000:0000:0000:0000:0000:00AA	FE80::AA
2002:0B00:0C18:0001:0000:4321:AB12:0002	2002:B00:C18:1::4321:AB12:2
FEC0:0000:0000:001A:0BBB:4900:0000:0001	FEC0::1A:BBB:4900:0:1

Tabla 2.4 Direcciones IPv6 en forma simplificada

Los caracteres en negritas en la notación completa representan los valores que han sido eliminados en la forma simplificada.

2.2 Las subredes en IPv6.

En IPv4 existen dos formas de representar un prefijo de red:

- La notación decimal. Una máscara de red se especifica en el formato d.d.d.d. El valor de la máscara de red representa el número de bits consecutivos que está puesto a uno.
- Notación del enrutamiento interdominio sin clases (CIDR). En esta notación el prefijo de la máscara de red es especificado con un número decimal que representa el número de bits consecutivos puestos a 1. Este número se coloca después del carácter barra invertida (/).

En IPv6 la representación de máscara de red utilizando el formato largo resulta inadecuada debido a la longitud de una dirección IPv6. La única forma de representar una máscara de red IPv6 es con la notación CIDR. Aunque las direcciones IPv6 están en formato hexadecimal, el valor de la máscara de red se mantiene en notación decimal. La tabla 2.5 presenta ejemplos de direcciones IPv6 y prefijos de red utilizando la notación CIDR.

Prefijo IPv6	Descripción
2001:410:0:1:0:0:0:45FF /128	Representa una subred con sólo una dirección IPv6.
2001:410:0:1:: /64	El prefijo de red 2001:410:0:1:: /64 puede manejar 2^{64} nodos. Esta es la longitud del prefijo por defecto para una subred.
2001:410:0:: /48	El prefijo de red 2001:410:0:: /48 puede manejar 2^{16} prefijos de red de 64 bits. Esta es la longitud del prefijo por defecto para un Sitio.

Tabla 2.5 Ejemplos de prefijos IPv6 con máscaras de subred

Tanto para IPv4 como para IPv6, el número de bits puestos a 1 en la máscara de red define la longitud del prefijo de red, la parte restante es para la dirección de nodo. Esta información es fundamental para IP. Este le dice a cada nodo cuando los paquetes deben ser enviados hacia un router por defecto o hacia un nodo específico dentro de la misma subred. En IPv6 no hay direcciones reservadas dentro del rango de un prefijo de red. En IPv4, la primera y la última dirección del rango de la subred son inválidas para definir nodos debido a que son direcciones reservadas. La primera dirección de este rango es la dirección de la red y la última es la dirección broadcast. Esto implica que el número de direcciones IPv4 disponibles dentro del rango de una subred sea $2^N - 2$, donde N es el número de bits para el direccionamiento de host. Por ejemplo, con el prefijo de red 192.168.1.0/24, las direcciones 192.168.1.0 y 192.168.1.255 no deben ser asignadas a nodos debido a que están reservadas.

En IPv4 también es común utilizar diferentes máscaras de red dentro de un mismo sitio. Una subred puede usar un valor de máscara de red y la siguiente subred puede utilizar un valor diferente. IPv6 no tiene direcciones de red reservadas o de broadcast. Además el número de bits para direccionamiento de nodos dentro de un prefijo de sitio (48 bits) es tan grande que no es necesario hacer un plan de direccionamiento utilizando diferentes máscaras de red. Por lo tanto, el cálculo de máscara de red, para cada subred y el uso de VLSM no es necesario. Las subredes en IPv6 resultan más simples.

2.3 Clases de direcciones IPv6.

En IPv6, las direcciones se asignan a interfases, no a nodos y cada interfaz puede tener y utilizar múltiples direcciones IPv6 simultáneamente.

En IPv6 existen 3 clases de direcciones: Unicast, Anycast y Multicast. Cada clase de direcciones soporta una o más tipos de dirección.

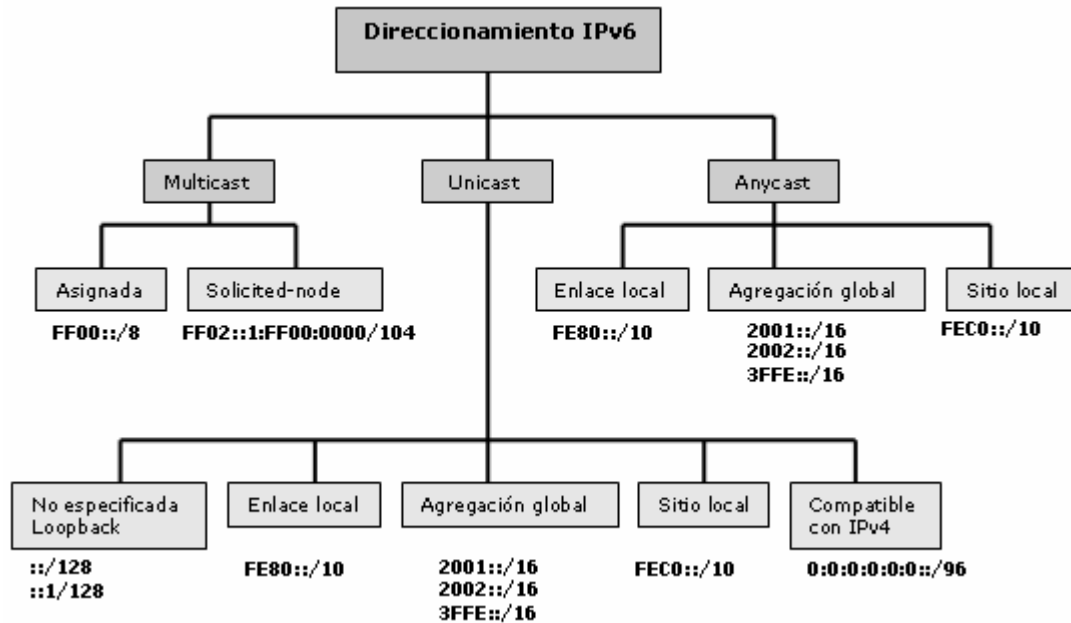


Figura 2.1 Tipos de direcciones en la arquitectura de direccionamiento IPv6

Como se presenta en la figura 2.1 bajo el ámbito de las direcciones Unicast están los siguientes tipos de dirección: Enlace local, Sitio local, de Agregación global, Loopback, no especificadas, y compatibles con IPv4. Direcciones Anycast son: de Enlace local, Sitio local y de Agregación global. Las direcciones Multicast son: Asignadas y “Solicited-node”. Cada clase de dirección se desenvuelve en ámbitos específicos, en la figura también se muestran los prefijos específicos de cada tipo de dirección.

2.3.1 Direcciones Unicast.

El unicast es el proceso donde el nodo origen envía un paquete hacia un solo destino (uno-hacia-uno). En IPv6 las direcciones unicast responden a un ámbito, esto implica que solo pueden ser usadas dentro de un contexto restringido.

2.3.1.1 Dirección de Enlace Local.

La dirección unicast de enlace local está confinada al uso entre nodos conectados al mismo enlace local, por lo tanto nunca deben ser enrutadas ni siquiera hacia las subredes dentro del sitio al que pertenecen. Cuando en un nodo se instala la pila IPv6, automáticamente se asigna una dirección de Enlace local en cada interfase del nodo. Como lo muestra la figura 2.2 una dirección de enlace local se conforma con el prefijo FE80::/10, los bits 11 hasta el 64 son puestos a 0 (54 bits), y finalmente se añade el identificador de interfase en el formato de Identificador Extendido Único (EUI-64) en los 64 bits de orden inferior de la dirección.

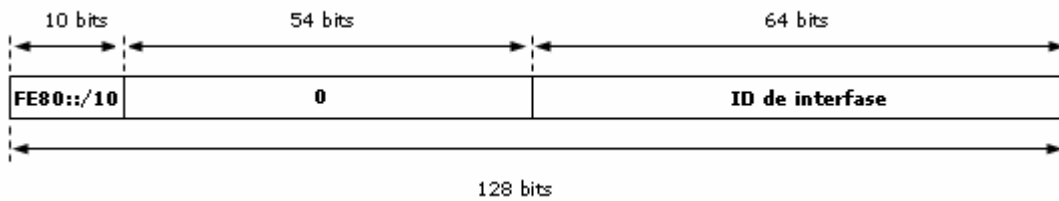


Figura 2.2 Dirección de enlace local

La tabla 2.6 presenta las diversas notaciones de una dirección de enlace local.

Representación	Valor
Forma completa	FE80:0000:0000:0000:0000:0000:0000/10
Forma abreviada	FE80::/10
Forma binaria	Los 10 bits de mayor orden puestos a 1111 1110 10

Tabla 2.6 Representaciones de una dirección de enlace local

2.3.1.2 Dirección de Sitio local.

La dirección de sitio Local es otra dirección Unicast cuyo ámbito se delimita dentro de un sitio. Las direcciones de Sitio Local no se habilitan por defecto en los nodos al instalar la pila IPv6 como sucede con las direcciones de Enlace Local, por lo que se tienen que asignar. Las direcciones de Sitio Local se utilizan en cualquier organización que aún no recibe direcciones para tráfico genérico (direcciones de Agregación global) a través de Internet IPv6. Todos los routers y nodos que son miembros de un sitio reciben una dirección de Sitio-Local. Sin embargo, las direcciones de Sitio-Local nunca deben ser enrutadas al Internet IPv6. Ilustrado en la figura 2.3, una dirección de Sitio Local contiene el prefijo FEC0::/10, un campo de 54

bits llamado Identificador de Subred, y el identificador de interfase EUI-64 localizado en los 64 bits de orden inferior.

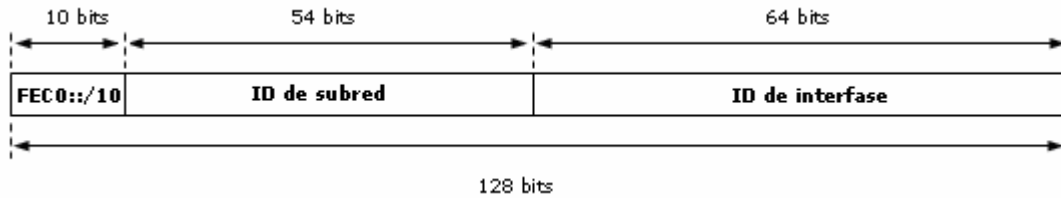


Figura 2.3 Formato de la dirección de sitio local

La tabla 2.7 muestra las representaciones de una dirección de sitio local.

Representación	Valor
Forma completa	FEC0:0000:0000:0000:0000:0000:0000/10
Forma abreviada	FEC0::/10
Forma binaria	Los 10 bits de mayor orden puestos a 1111 1110 11

Tabla 2.7 Representaciones de dirección de sitio local

El identificador de Subred de 54 bits está disponible para la construcción de subredes. Este campo le permite a un sitio crear 2^{54} diferentes subredes IPv6 con el prefijo /64. Cada subred puede usar un prefijo IPv6 diferente. Por ejemplo, un sitio con 10 subredes puede asignar prefijos de enlace de sitio como sigue:

- Subred 1- FEC0:0:0:0001::/64
- Subred 2- FEC0:0:0:0002::/64
- Subred 3- FEC0:0:0:0003::/64
- Subred 4- FEC0:0:0:0004::/64
- Subred 5- FEC0:0:0:0005::/64
- Subred 6- FEC0:0:0:0006::/64
- Subred 7- FEC0:0:0:0007::/64
- Subred 8- FEC0:0:0:0008::/64
- Subred 9- FEC0:0:0:0009::/64
- Subred 10- FEC0:0:0:000A::/64

Las direcciones de Sitio Local se designan a dispositivos que no se comunicarán con el Internet global IPv6, por lo que se utilizan en impresoras, servidores Intranet, conmutadores de red, puentes y en general cualquier tipo de servidores y routers que tengan un alcance interno para propósitos de administración. La implementación de

direcciones de Sitio-Local se recomienda para organizaciones que planean instalar IPv6 en sus redes, esto es que estén en fase de experimentación antes de dar el paso hacia Internet IPv6.

2.3.1.3 El formato EUI 64 de una dirección IPv6.

Como se acaba de describir, el procedimiento de configuración de direcciones de enlace local y de sitio local utiliza el identificador de interfase basado en 64 bits (EUI 64). Este identificador automáticamente expande la dirección Ethernet MAC basada en el formato de 48 bits a un formato de 64 bits.

La conversión de 48 a 64 bits utiliza una operación de dos pasos. El primer paso consiste en insertar el valor 0xFFFE a la mitad de la dirección MAC, justo entre el código de fabricante y el número de serie de la interfase. El siguiente paso consiste en inicializar el séptimo bit de la dirección de 64 bits. Con este bit se habilita la “singularidad” de la dirección MAC. Esta singularidad esta relacionada con la forma en que se administra la dirección MAC. Una dirección MAC puede ser administrada localmente o globalmente. La administración global implica que el usuario utiliza por defecto la dirección MAC del fabricante, asegurando la singularidad de la dirección. En cambio una dirección MAC administrada localmente significa que esta puede reescribirse manualmente o mediante software con un valor asignado por el administrador de red, por lo tanto este último método de administración no asegura la singularidad de una dirección MAC y no debe utilizarse para derivar un identificador EUI-64. El formato normal de una dirección MAC (48 bits) especifica que si el séptimo bit se inicializa a 1 se trata de una dirección administrada localmente y si se inicializa a 0 entonces es administrada globalmente. Sin embargo en el formato EUI 64, el valor es al revés: 0 para local y 1 para global. En resumen para las direcciones IPv6 que utilizan el formato EUI 64, si el séptimo bit es puesto a 1, la dirección es globalmente única de otra forma es local.

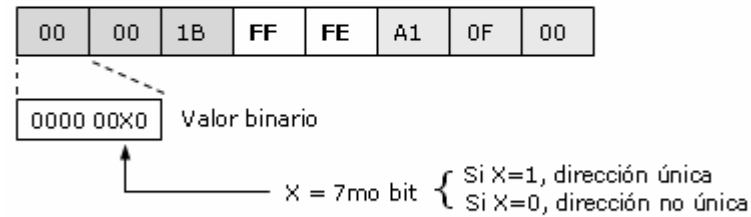
La figura 2.4 muestra como se realiza la conversión al formato EUI 64 de la dirección MAC 00:00:1B:A1:0F:00.

Paso 1: Se inserta FFFE a la mitad de la dirección MAC

Dirección MAC (48 bits) = 00:00:1B:A1:0F:00



Paso 2: Determinación del 7mo bit



Si es dirección globalmente única queda:



Figura 2.4 Conversión de una dirección MAC de 48 bits al formato EUI-64

2.3.1.4 Dirección de Agregación Global.

Las direcciones unicast de agregación global representan la parte más importante en la arquitectura de direccionamiento IPv6, estas soportan el tráfico genérico Internet IPv6. La estructura de esta clase de direcciones permite una estricta agregación de los prefijos de enrutamiento, lo que limita el tamaño de la tabla de enrutamiento global de Internet. La figura 2.5 muestra el formato de la dirección unicast de agregación global, esta contiene tres partes:

- **Un Prefijo proporcionado por un proveedor.** El prefijo que se asigna a una organización por parte de un proveedor debe tener al menos un prefijo de /48 (recomendado en el RFC 3177). El prefijo /48 representa el prefijo de la red con los 48 bits de más alto orden. Por supuesto que el prefijo asignado a la organización es parte del prefijo del proveedor.
- **Sitio.** El prefijo /48 permite habilitar 65,535 subredes dentro de la organización asignando un prefijo de 64 bits a las subredes. La organización puede usar los bits 49 hasta 64 (16 bits) del prefijo recibido para crear las subredes.

- **Host.** Llamado ID de interfase debido a que utiliza el identificador de interfaz de cada nodo. Esta parte de la dirección IPv6 representa los 64 bits de más bajo orden de la dirección.

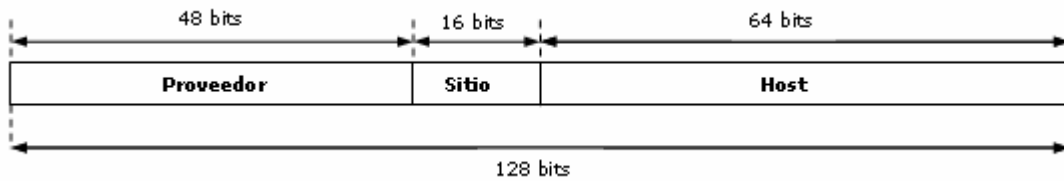


Figura 2.5 Dirección Unicast Global Agregable

2.3.1.5 Asignaciones de IANA para Prefijos Unicast de Agregación Global.

La IANA asigna un rango para el prefijo de dirección IPv6 en el espacio total de direccionamiento IPv6 para direcciones unicast globales agregables. La tabla 2.7 muestra este espacio de dirección que es caracterizado por el prefijo 2000::/3.

Representación	Valores
Rango	2xxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx /3
Primera dirección del rango	2000:0000:0000:0000:0000:0000:0000
Última dirección del rango	3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Forma binaria	Los tres bits de mayor orden puestos a 001

Tabla 2.8 Espacio de la dirección unicast de agregación global

Prefijos	Representación binaria	Descripción
2001::/16	0010 0000 0000 0001	Internet IPv6
2002::/16	0010 0000 0000 0010	Mecanismo de transición 6to4
2003::/16 hasta 3FFD::/16	0010 xxxx xxxx xxxx	Sin asignar (disponible)
3FFE::/16	0010 1111 1111 1110	6bone (obsoleto)

Tabla 2.9 Prefijos /16 del espacio de direcciones IPv6 asignados como direcciones unicast de agregación global

Del prefijo 2000::/3, tres prefijos más pequeños (/16) han sido asignados para uso público. El prefijo 2001::/16 está disponible para la producción de Internet IPv6. El prefijo 2002::/16 está reservado para nodos que utilizan el mecanismo de transición 6to4. El prefijo 3FFE::/16 era el prefijo usado en la red experimental 6bone. Desde el 2003 el IETF decidió que ya era el momento adecuado para iniciar el cierre gradual

del 6Bone. Este cierre se materializó el 6 de Junio del 2006, por lo tanto a partir de esta fecha ningún prefijo 3FFE debe utilizarse en forma alguna en Internet. Estos prefijos se presentan en la tabla 2.9.

Los prefijos 2003::/16 hasta 3FFD::/16 aún no son asignados por la IANA. Esto representa 8196 prefijos /16. Dentro de un solo prefijo /16, todo el Internet IPv4 actual puede caber billones de veces. Hasta hace poco los RFCs definían el formato de una dirección unicast de agregación global bajo una organización denominada **dirección unicast basada en proveedor**, la figura 2.6 ilustra este formato:

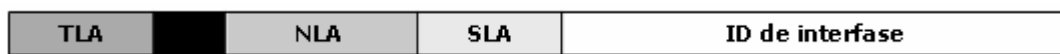


Figura 2.6 Dirección unicast de agregación global basada en proveedor

- El campo **TLA** (16 bits) contiene el identificador de agregación de nivel superior “Top Level Aggregation”, este es el bloque asignado por los Registros de Internet regionales (RIRs) a los Proveedores de Servicio Internet (ISPs).
- El siguiente campo estaba reservado (8 bits).
- El campo **NLA** (24 bits) contiene el identificador de agregación del siguiente nivel “Next Level Aggregation”, esta porción es donde los proveedores crean subredes con múltiples niveles de jerarquía para asignar bloques de direcciones a sus clientes.
- El campo **SLA** (16 bits) contiene el identificador de nivel de sitio “Site Level Aggregation”. Esta porción la utilizan los clientes para crear subredes, también pueden ser jerárquicas.

Todos estos campos conforman un prefijo /64. Finalmente está el identificador de interfase. Los términos TLA, NLA y SLA ya no se utilizan más en los RFCs, en su lugar sólo tenemos el prefijo del proveedor y el identificador de subred descritos anteriormente. Esto no afecta los principios básicos. Sin embargo como se verá mas adelante en este capítulo, la idea de direccionamiento basado en proveedor sigue siendo la misma.

2.3.2 Direcciones Multicast.

La tecnología multicast constituye el servicio de red en el cual un único flujo de datos, proveniente de un determinado nodo origen, se puede enviar simultáneamente a múltiples receptores interesados, por lo que está orientado a aplicaciones del tipo “uno para muchos”. El multicast involucra el concepto de grupo, donde:

- Cualquier nodo puede ser miembro de un grupo multicast.
- Cualquier nodo puede enviar paquetes hacia un grupo multicast.
- Todos los miembros de un grupo multicast reciben los paquetes que son enviados al grupo.

El servicio multicast optimiza la cantidad de paquetes que los nodos intercambian, lo que se refleja en un ahorro en el ancho de banda en el enlace y por lo tanto un uso más eficiente de la red. Para utilizar el servicio de multicast se deben utilizar rangos específicos de las direcciones IP. En IPv4 este rango es 224.0.0.0/3, donde los tres bits de mayor orden en la dirección IPv4 son 111. En IPv6 a la dirección multicast la define el prefijo FF00::/8.

El formato de una dirección multicast, se presenta en la figura 2.7. Este formato especifica diversos ámbitos y tipos de direcciones utilizando los campos de 4 bits **Indicador** y **Ámbito**. Estos campos están ubicados después del prefijo FF::/8. Finalmente, los 112 bits restantes de la dirección multicast conforman el identificador del grupo multicast.

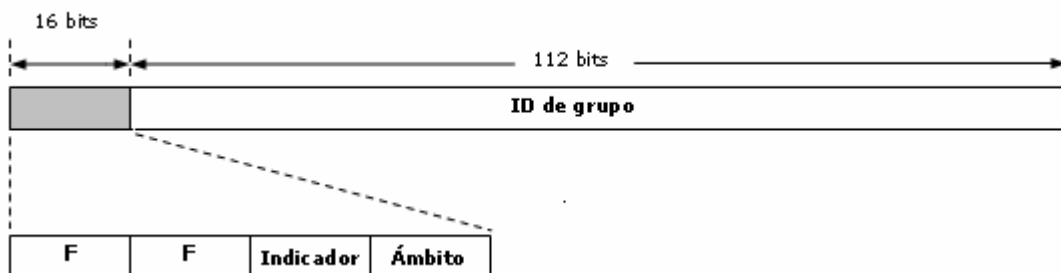


Figura 2.7 Formato de la dirección multicast con los campos Indicador y Ámbito

El campo Indicador contiene el tipo de dirección multicast, que pueden ser dos:

- Permanente. Es una dirección asignada por la IANA.
- Temporal.

Los significados del campo *Indicador* se muestran en la tabla 2.10. Los 3 bits de mayor orden del campo Indicador están reservados y deben ser 0. El bit restante indica el tipo de dirección multicast.

Representación binaria	Valor Hexadecimal	Tipo de dirección Multicast
0000	0	Permanente
0001	1	Temporal

Tabla 2.10 Valores y significados del campo Indicador

El campo **Ámbito** es el parámetro que restringe el envío de paquetes multicast hacia un determinado sector o parte de la red. La tabla 2.11 muestra los valores que puede tomar el campo **Ámbito**. Los valores que no se muestran en la tabla están reservados o no han sido asignados.

Notación Binaria	Valor hexadecimal	Ámbito
0001	1	Interfase Local
0010	2	Enlace Local
0011	3	Subred Local
0100	4	Administración Local
0101	5	Sitio Local
1000	8	Organización
1110	E	Global

Tabla 2.11 Valores y significados del campo **Ámbito**

Así por ejemplo FF02::/16 es una dirección permanente usada en un ámbito de enlace local. FF12::/16 tiene el mismo ámbito pero es una dirección temporal. FF05::/16 es una dirección permanente con un ámbito de sitio local.

Cabe señalar que cuando un nodo IPv6 envía un paquete multicast hacia una dirección multicast, la dirección origen dentro del paquete no pueden ser una dirección multicast. Además, las direcciones multicast no deben ser utilizadas como direcciones origen en ninguna cabecera de extensión de enrutamiento.

Entre las diversas aplicaciones que utilizan el uso de las direcciones multicast se encuentran: videoconferencia, cursos, distribución de software, noticias, conciertos en vivo, actualización de bases de datos, juegos, etc.

2.3.2.1 Dirección multicast asignada.

La operación del protocolo IPv6 requiere el uso de direcciones multicast especiales. Estas direcciones están reservadas y se denominan direcciones multicast asignadas. La tabla 2.12 presenta todas las direcciones multicast asignadas en IPv6.

Dirección multicast	Ámbito	Significado	Descripción
FF01::1	Nodo	Todos los nodos	Todos los nodos en la interfase local
FF01::2	Nodo	Todos los routers	Todos los routers en la interfase local
FF02::1	Enlace local	Todos los nodos	Todos los nodos en el enlace local
FF02::2	Enlace local	Todos los routers	Todos los routers en el enlace local
FF05::2	Sitio	Todos los routers	Todos los routers dentro de un sitio

Tabla 2.12 Direcciones multicast asignadas

Este tipo de direcciones las utilizan funciones específicas del protocolo IPv6. Por ejemplo, un router en una subred que necesita enviar un mensaje hacia todos los nodos pertenecientes a esa subred utilizará la dirección multicast FF02::1. Un nodo dentro de una subred que ha enviado un mensaje hacia todos los otros nodos de la misma subred también utiliza la misma dirección multicast. Todos los dispositivos IPv6 reconocen las direcciones multicast asignadas.

2.3.2.2 Dirección multicast solicited-node.

El segundo tipo de direccionamiento multicast es el direccionamiento multicast solicited-node. Por cada dirección unicast y anycast configurada en una interfase de un nodo o router, una correspondiente dirección multicast solicited-node es automáticamente habilitada. La dirección multicast solicited-node tiene un ámbito de enlace local.

Una dirección multicast solicited-node es un tipo específico de dirección usada por dos mecanismos fundamentales en IPv6:

- Reemplazo del mecanismo ARP para IPv6. Debido a que IPv6 no maneja el mecanismo ARP, los nodos ubicados dentro de un enlace local utilizan la dirección multicast solicited-node para aprender las direcciones de la capa de enlace de los nodos vecinos (dentro del mismo enlace local). Como sucede con ARP en IPv4, el conocimiento de las direcciones de la capa de enlace de nodos vecinos es obligatorio para construir tramas de la capa de enlace para entregar paquetes IPv6.
- Detección de duplicado de dirección (DAD). DAD es parte de NDP. Este le permite a un nodo verificar si una dirección IPv6 está en uso en este enlace local antes de usar tal dirección para configurar su propia dirección IPv6 con el mecanismo de autoconfiguración. La dirección multicast solicited-node se utiliza para comprobar el enlace local en busca de una dirección unicast o anycast específica ya configurada en otro nodo.

La dirección multicast solicited-node está definida por el prefijo IPv6 FF02::1:FF00:0000/104 más los 24 bits de menor orden de la dirección unicast o anycast. En la figura 2.8 se muestra como se añaden los 24 bits de menor orden de una dirección unicast o anycast al prefijo FF02::1:FF.

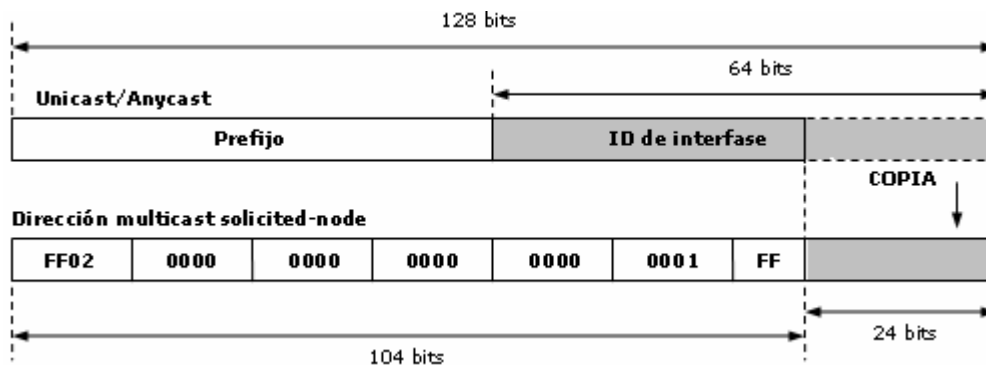


Figura 2.8 Dirección multicast solicitada-nodo

2.3.3 Dirección Anycast.

Una dirección anycast se utiliza para la comunicación tipo “uno-hacia-el más cercano”. En otras palabras es un mecanismo que entrega un paquete enviado hacia una dirección anycast al nodo más cercano que es miembro del grupo anycast. El anycast permite un tipo de mecanismo de descubrimiento para el punto más cercano.

La red por sí misma juega un papel fundamental en el anycast, al enrutar el paquete hacia el destino más cercano por medición de la distancia de la red. El mecanismo anycast está disponible tanto para IPv4 como para IPv6. Las direcciones anycast usan direcciones unicast de agregación global. Estas pueden también usar direcciones de sitio local o de enlace local. Es imposible distinguir una dirección anycast de una dirección unicast.

En general se tiene que realizar un trabajo más amplio del anycast para alcanzar beneficios reales de este tipo de dirección. Un posible uso de las direcciones anycast es el de identificar un conjunto de routers para poder acceder a Internet IPv6. Otra posibilidad sería configurar con una dirección anycast específica a todos los routers dentro de una red corporativa que proporcione acceso a Internet IPv6.

2.3.3.1 Dirección Anycast reservada.

Se ha reservado una dirección anycast para casos especiales. Como lo muestra la figura 2.9, esta dirección se conforma por el prefijo unicast de subred /64 y por los 64 bits de menor orden (65-128) puestos a 0. Esta dirección anycast reservada es también llamada dirección anycast del router de subred. Todos los routers que han incorporado IPv6 son instruidos para soportar este tipo de direcciones en cada una de sus interfaces de subred.

Un paquete enviado a esta dirección será entregado a uno de los routers de la subred. Con esta característica se pretende dar tolerancia a los fallos. También puede tener una aplicación importante en la movilidad, en situaciones donde un nodo necesite comunicarse con un router entre el conjunto de los disponibles en una subred.

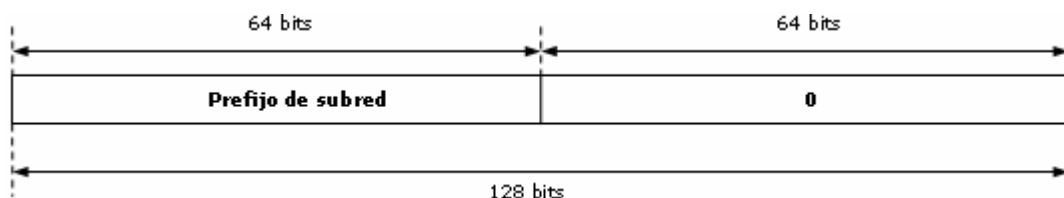


Figura 2.9 Representación de una dirección anycast reservada

2.3.4 Direcciones Especiales.

2.3.4.1 Direcciones IPv6 con direcciones IPv4 insertadas.

Este tipo de notación de dirección IPv6 es específica en entornos donde coexisten IPv4 e IPv6 y la utilizan mecanismos de transición^{2.1}. La dirección IPv4 se coloca dentro de los cuatro bytes de menor orden de la dirección IPv6, representados por los caracteres **d** (para un total de 32 bits). Los 96 bits de mayor orden conforman seis bloques de 16 bits en formato hexadecimal, representados por los caracteres **X**.

X:X:X:X:X:d.d.d.d

Dos clases de direcciones IPv6 tienen direcciones IPv4 insertadas.

- **Dirección IPv6 compatible con IPv4.** Usada para establecer un túnel automático para transportar paquetes IPv6 sobre redes IPv4. Esta dirección está relacionada con un mecanismo de transición del protocolo IPv6.
- **Dirección IPv6 mapeada con IPv4.** Usada únicamente dentro de un ámbito local con nodos que tienen ambas pilas. Los nodos usan direcciones IPv6 mapeadas con IPv4 únicamente de manera interna. Estas direcciones no conocen más allá del nodo mismo y no se deben tomar como direcciones IPv6 propiamente.

Sin embargo se maneja un diferente prefijo IPv6 para cada una de estas direcciones. El prefijo para la dirección IPv6 compatible con IPv4 se representa con los 96 de más alto orden puestos a cero, seguidos de los 32 bits de la dirección IPv4. Esto se muestra en la figura 2.10.

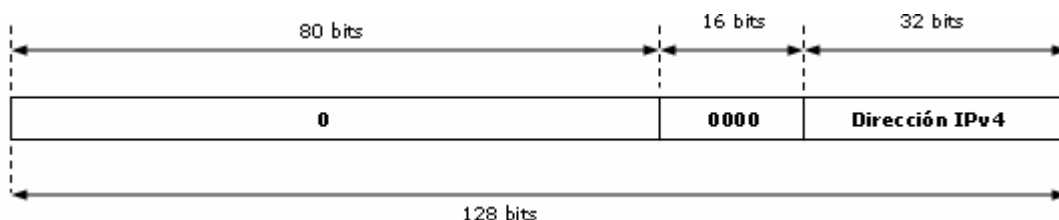


Figura 2.10 Dirección IPv6 compatible con IPv4

2.1 Los mecanismos de transición se detallan en el capítulo 5

La figura 2.11 presenta el formato de una dirección IPv6 mapeada con IPv4, esta se expresa mediante 80 bits de orden superior puestos a 0, después los siguientes 16 bits puestos a 1, y finalmente los 32 bits que representan la dirección IPv4 del nodo local.

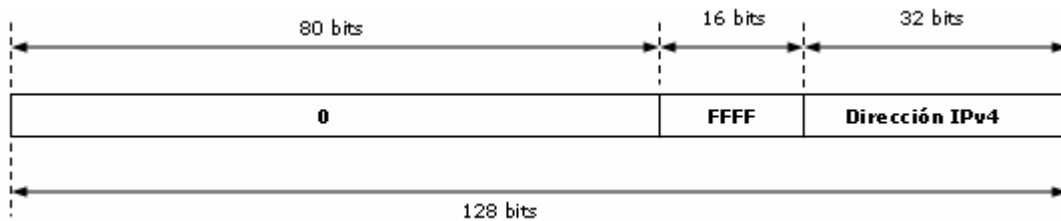


Figura 2.11 Dirección IPv6 mapeada con IPv4

2.3.4.2 Dirección Loopback.

Similar a la dirección 127.0.0.1 presentada en IPv4, cada dispositivo tiene una dirección loopback la cual es utilizada por el mismo nodo. La dirección Loopback esta definida por el prefijo ::1.

2.3.4.3 Dirección no especificada.

Indica la ausencia de una dirección válida y es usada para propósitos especiales. Por ejemplo cuando dirección origen de un host para enviar peticiones hacia el exterior para conseguir una dirección válida. La dirección no especificada se representa mediante el prefijo ::. Todos los bits son puestos a cero.

2.4 Direcciones IPv6 requeridas.

Tanto los routers como los nodos IPv6 tienen múltiples direcciones IPv6 al mismo tiempo. Sin embargo estas direcciones IPv6 son usadas en diferentes contextos.

2.4.1 Direcciones IPv6 requeridas para nodos.

La tabla 2.13 enlista las direcciones requeridas para los nodos IPv6. Tan pronto como el nodo se habilita en IPv6 este tiene una dirección de enlace local por interfase, una dirección loopback y las direcciones multicast "todos los nodos" FF01::1 y FF02::1. También puede tener direcciones de agregación global y las correspondientes direcciones multicast solicited-node. Si el nodo es un miembro de otro grupo multicast este puede tener otras direcciones multicast.

Direcciones requeridas	Representación
Dirección de enlace local por cada interfase de red	FE80::/10
Dirección Loopback	::1
Direcciones multicast "todos los nodos"	FF01::1, FF02::1
Dirección Unicast de agregación global asignada	2000::/3
Dirección multicast solicitad-node por cada dirección unicast o anycast usada	FF02::1:FFxx:xxxx
Dirección multicast de todos los grupos a los que el host pertenece	FF00::/8

Tabla 2.13 Direcciones IPv6 requeridas para nodos

2.4.2 Direcciones IPv6 requeridas para routers.

Básicamente, los routers tienen todas las direcciones requeridas por los nodos. Además tienen las direcciones multicast "todos los nodos" FF01::2, FF02:2 y FF05::2. Una dirección anycast router-subred y otras direcciones anycast configuradas son direcciones requeridas para routers. La tabla 2.14 enlista las direcciones requeridas para los routers en IPv6.

Direcciones requeridas	Representación
Todas las direcciones IPv6 requeridas para nodo	FE80::/10, ::1, FF01::1, FF02::1, 2000::/3, FF02::1:FFxx:xxxx, FF00::/8
Direcciones multicast "todos los routers"	FF01::2, FF02::2, FF05::2
Dirección anycast router de subred	Prefijo unicast :0:0:0:0
Otras direcciones anycast configuradas	2000::/3

Tabla 2.14 Direcciones IPv6 requeridas para routers

2.5 IPv6 sobre Ethernet.

De manera similar a IPv4, IPv6 corre sobre cualquier tecnología Ethernet. Sin embargo el identificador (ID) del protocolo especificado en las tramas Ethernet que transportan paquetes IPv6 son diferentes del identificador del protocolo en IPv4. El ID del protocolo dentro de las tramas Ethernet identifica el protocolo utilizado de la capa 3, como por ejemplo IPv4, IPv6 o incluso IPX, DECnet y Apple Talk entre otros.

La tabla 2.15 muestra los respectivos IDs dentro de las tramas Ethernet de los protocolos IPv4 e IPv6.

Protocolo	ID de protocolo en las tramas Ethernet
IPv4	0x0800
IPv6	0x86DD

Tabla 2.15 IDs de los protocolos IPv4, IPv6

El protocolo IPv6 utiliza de manera frecuente las direcciones multicast en muchos mecanismos dentro de el ámbito del enlace local. Por lo tanto, IPv6 tiene un mapeo especial de direcciones multicast a direcciones Ethernet (direcciones MAC Ethernet). Este mapeo se realiza al añadir los 32 bits de menor orden de una dirección multicast al prefijo 33:33, el cual se ha definido como el prefijo Ethernet multicast para IPv6. En la figura 2.12, los 32 bits de menor orden (0000:0001) de la dirección multicast “todos los nodos” (FF02::1) se añade al prefijo Ethernet multicast 33:33.

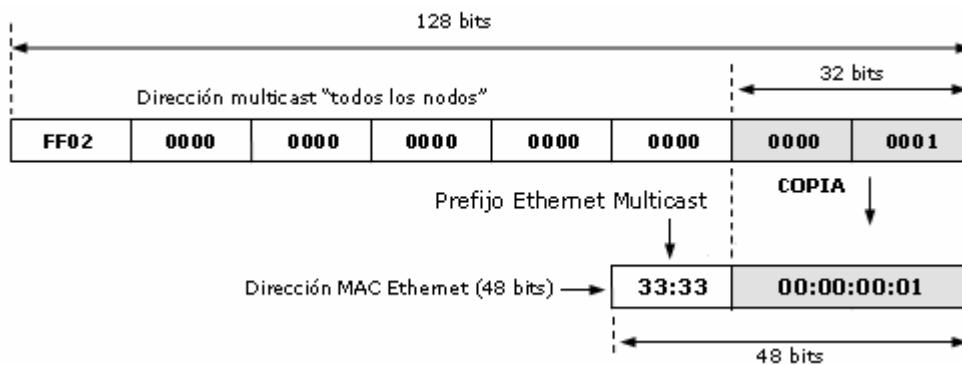


Figura 2.12 Mapeo multicast sobre una dirección Ethernet utilizando una dirección multicast “todos los nodos”

La dirección de 48 bits 33:33:00:00:00:01 representa la dirección MAC Ethernet (dirección de la capa de enlace) que se utiliza como destino en la trama Ethernet para enviar un paquete hacia la dirección multicast “todos los nodos” FF02::1. Por defecto, todos los nodos IPv6 que se han habilitado en ese enlace local escuchan y adquieren cualquier paquete IPv6 que utilice 33:33:00:00:00:01 como destino en la dirección MAC Ethernet. Este es un ejemplo enfocado a la dirección multicast “todos los nodos” pero todas las otras direcciones multicast asignadas se utilizan de manera similar.

2.6 Internet IPv6.

Para construir una producción confiable de Internet, IPv6 debe ser capaz de proporcionar espacios de direcciones IPv6 para producción a los ISPs. A partir de 1999, los RIRs comenzaron a asignar a los ISPs prefijos de producción IPv6.

La IANA asignó inicialmente el espacio de direcciones unicast de agregación global 2001::/16 para propósitos de producción de Internet IPv6. Al igual que con IPv4, este espacio de producción IPv6 es administrado por tres RIRs ubicados en diferentes regiones del mundo:

- APNIC. Asia Pacific Network Information Center. Soporta Asia y Australia.
- ARIN. American Registry for Internet numbers. Soporta al continente Americano.
- RIPE NCC. Reseaux IP Européens Network Coordination Center. Soporta Europa y Oriente medio.

Los ISPs pueden recibir su espacio de producción IPv6 solicitándolo a alguno de estos registros. Las direcciones son gratuitas pero los registros generalmente cobran por brindar este servicio.

2.6.1 Políticas de asignación de direcciones IPv6.

Las políticas de asignación de las direcciones de producción IPv6 han evolucionado, estas se han homologado para todos los registros donde la única excepción está en los precios de administración. Estas políticas fueron revisadas por el IETF y por un proceso de consulta pública. Los prefijos se asignan a ISPs no a empresas, de alguna forma se ha aprendido la lección de IPv4. La asignación inicial de prefijos de producción IPv6 se adoptó en Julio de 1999, y la actual política de asignación fue adoptada en Julio del 2002.

2.6.1.1 Política de asignación inicial.

La política de asignación inicial de direcciones IPv6 se adoptó en Julio de 1999. Esta se basó en un proceso de “lento inicio” donde los registros de Internet regionales asignaron prefijos /35 a los ISPs. Al asignar pequeñas porciones de direcciones a los ISPs, este proceso de “lento inicio” ha permitido a los registros conservar espacio de direcciones IPv6.

Posteriormente se definió un procedimiento para ayudar a nuevos ISP a cumplir el criterio inicial de esta política de asignación. El criterio se basó en la pasada experiencia de los ISPs con IPv4. Esto ayudó a que grupos de ISPs implementaran

IPv6 antes de que se aplicaran reglas permanentes. En el 2001, se comenzó a trabajar la revisión de las políticas de asignación inicial con el objetivo de establecer una política de asignación general que todos los RIRs pudieran aplicar. La política de asignación inicial se encuentra obsoleta con respecto a las nuevas políticas adoptadas en Julio de 2002.

2.6.1.2 Actual Política de asignación.

La política de asignación actual para direcciones de producción IPv6 está definida en el documento “IPv6 Address Allocation and Assignment Policy” y puede encontrarse en la página Web de ARIN usando esta dirección:

www.arin.net/policy/ipv6_policy.html

La actual política contiene los siguientes criterios iniciales:

- Ser un Registro de Internet local (LIR). Un LIR es un registro de Internet que principalmente asigna espacios de dirección a los usuarios de los servicios de red que este proporciona. Los LIRs son generalmente ISPs cuyos clientes son principalmente usuarios finales y posiblemente otros ISPs.
- No ser un sitio final. Un sitio final es un usuario final (suscriptor).
- Proyecte proporcionar conectividad IPv6 hacia otras organizaciones. El proveedor deberá asignar al menos un prefijo /48 por organización.
- Proyecte asignar 200 prefijos /48 a organizaciones dentro de un plazo de dos años.

La actual política de asignación establece que las organizaciones (ISPs) que cumplan con los criterios iniciales son elegibles para recibir una asignación mínima de /32. Organizaciones que soportaban un prefijo /35 recibido desde la inicial política de asignación son automáticamente autorizados para recibir un prefijo /32. El prefijo /32 contiene el prefijo /35 que ya les había sido asignado.

De acuerdo con esta política de asignación es posible para un proveedor calificar para una asignación inicial mayor a /32 al presentar sus justificaciones. En este caso, la asignación de direcciones se basa en el número de usuarios existentes y en la extensión de infraestructura de la organización. También es posible para un

proveedor solicitar espacio adicional de direcciones. Para este caso se ha definido el *Criterio de asignación subsecuente*. Este criterio está basado en el uso de asignaciones /48 realizada por los proveedores.

2.6.1.3 Reasignación de espacio de dirección a los clientes.

La política de asignación también define reglas para la reasignación de espacio de dirección para los clientes. La política de asignación contiene las siguientes reglas:

- Longitud del prefijo de cliente. En general, el prefijo IPv6 que le asigna un ISP a su cliente (sitio terminal) debe ser /48. Sin embargo se pueden asignar prefijos mayores a suscriptores muy grandes.
- Longitud del prefijo de subred. Se le puede asignar un prefijo /64 a una subred únicamente cuando se tiene la certeza de que una y solo una subred es necesaria en el diseño. Las redes domésticas y las pequeñas redes diseñadas con sólo una subred son ejemplos de asignaciones de prefijo /64.
- Longitud del prefijo del dispositivo. Se le asigna un prefijo /128 a un dispositivo únicamente cuando se conoce que solo este dispositivo estará conectado. Una PC, un PDA o teléfonos celulares que marcan desde una ubicación remota y usa conexiones PPP son ejemplos de asignaciones de prefijos /128.

2.6.1.4 Asignación de prefijos de producción.

La figura 2.13 muestra las asignaciones entre el prefijo 2001::/16 y los sitios terminales. El primer nivel mostrado es el prefijo de las direcciones de producción IPv6 asignado por la IANA. Es seguido por la asignación RIR. 16 bits están disponibles para el nivel RIR, así que RIR puede asignar el prefijo inicial /32 hacia cada prefijo ISP. Finalmente, los ISPs asignan el prefijo /48 a cada cliente (sitio final).

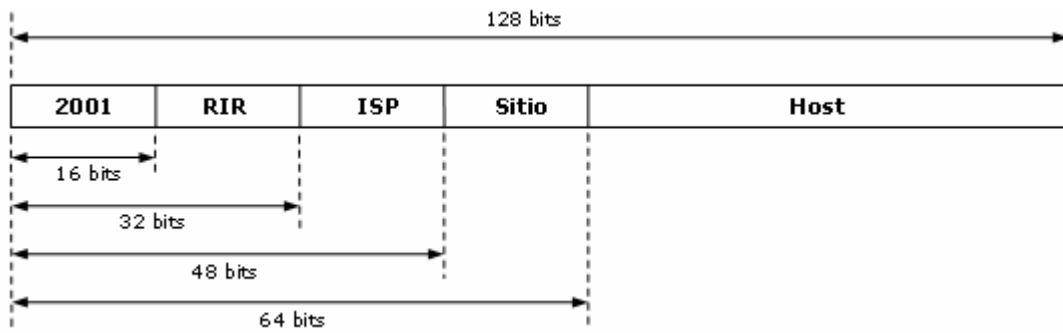


Figura 2.13 Asignaciones jerárquicas dentro del espacio de dirección IPv6 de producción 2001::/16

Por último la figura 2.14 muestra la perspectiva jerárquica de la asignación de dirección. En el nivel RIR, APNIC recibe los prefijos 2001:02xx::/23 y 2001:0cxx::/23, ARIN recibe el prefijo 2001:04xx::/23 y RIPE NCC recibe el prefijo 2001:06xx::/23. En el siguiente nivel, los prefijos /32 de los espacios de dirección recibidos por los RIRs se asignan a los ISPs y entonces los prefijos /48 son los que finalmente se asignan a los sitios (clientes).

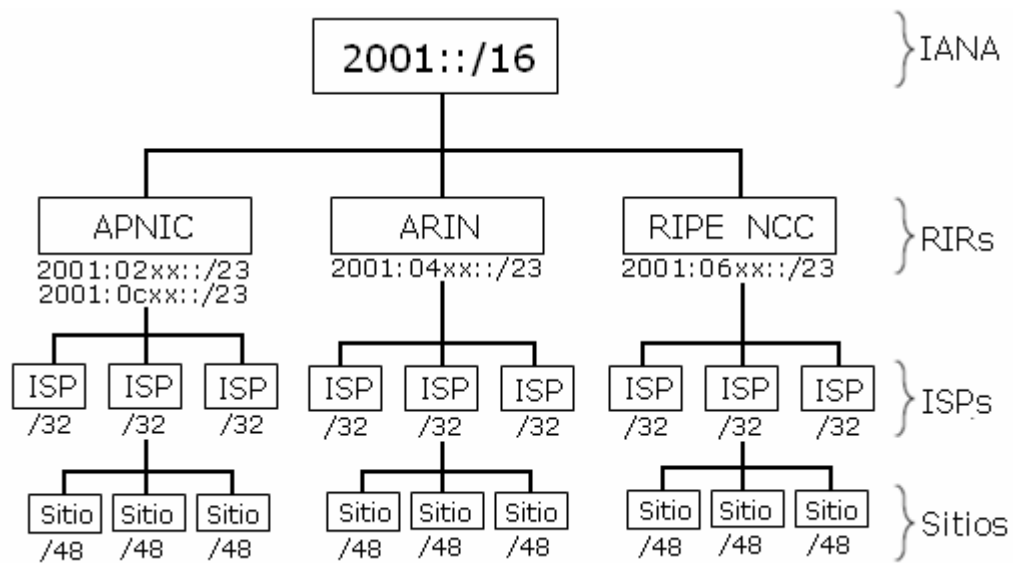


Figura 2.14 Vista jerárquica del modo en que se distribuye el espacio de direcciones IPv6 de producción

Capítulo 3

Enrutamiento

3.1 Introducción.

Las redes se han dividido en dos categorías según su alcance geográfico, tamaño y función; en Redes de Área Local (LANs) y Redes de Área Extendida (WANs). Sin embargo a medida que avanza la tecnología resulta confuso identificar a una o a otra por medio del área geográfica que abarcan. En este documento se identificará a una LAN como la red que pertenece a una sola organización y que generalmente se maneja solo a través de las capas 1 y 2 del modelo OSI, es decir trabajará solo con direccionamiento físico para identificar a los dispositivos que se están comunicando. Una WAN por el contrario implicará de una u otra forma el uso de dispositivos pertenecientes a terceros (típicamente a un ISP) dentro de una red que hace un uso extensivo del direccionamiento lógico (capa 3 del modelo OSI) para llevar a cabo la comunicación entre dispositivos.

Un router es un dispositivo de red inteligente que opera principalmente en las primeras tres capas del modelo de referencia OSI. Los routers, como cualquier host, son capaces de operar en las siete capas del modelo OSI. Las comunicaciones a través de las dos primeras capas permiten a los routers comunicarse directamente con redes de área local (LAN). Sin embargo la característica más importante de los routers, es que pueden identificar rutas a través de redes basándose en las direcciones de la capa tres. Esto permite a los routers trabajar vía Internet con múltiples redes, con independencia de que tan cerca o lejos pueden estar, usando un direccionamiento de la capa de red.

Las comunicaciones entre redes requieren que al menos una ruta física interconecte las computadoras origen y destino. Las computadoras de origen y destino deben hablar un lenguaje común (un protocolo enrutado) y los routers que residen entre estas computadoras deben hablar un lenguaje común (protocolo de enrutamiento), para poder comunicarse entre si. Los protocolos de enrutamiento permiten que los routers realicen las siguientes funciones:

- Identificar rutas potenciales a hosts y redes de destino específicas.
- Realizar una comparación matemática, conocida como cálculo para determinar la mejor ruta a cada destino.
- Monitorizar continuamente la red para detectar cualquier cambio en la topología que puedan representar rutas conocidas que no sean válidas.

3.2 Cálculo y mantenimiento de rutas.

Los protocolos de enrutamiento se pueden evaluar usando numerosos criterios específicos, algunos de los más importantes son:

Optimización.

Describe la capacidad de un protocolo de enrutamiento para seleccionar la mejor ruta disponible. Sin embargo el término “mejor ruta” resulta ambiguo. Existen diferentes modos de evaluar diferentes rutas hacia cualquier destino específico. Los criterios usados por los protocolos de enrutamiento para calcular y evaluar las rutas se conocen como métricas de enrutamiento. Existen una gran variedad de métricas de enrutamiento y varían de un protocolo de enrutamiento a otro. Las métricas más comunes se muestran en la tabla 4.1

Métrica utilizada	Descripción
Numero de saltos	El número de routers por los que debe pasar un paquete para llegar a su destino. Cuanto menor sea el número de saltos, mejor será la ruta. La longitud de ruta se utiliza para indicar el número de saltos requeridos para llegar a un destino.
Ancho de banda	La capacidad de transporte de datos de un enlace.
Retardo	La cantidad de tiempo que se requiere para mover un paquete desde un origen hasta un destino.

Carga	La cantidad de actividad en un recurso de red, como por ejemplo un router o un enlace.
Confiabilidad	La frecuencia con que se producen errores en cada enlace de la red.
Costo	Un valor arbitrario, generalmente basado en el ancho de banda, el gasto monetario y otras mediciones asignado por el administrador de red.

Tabla 4.1 Métricas de enrutamiento más comunes

Eficacia.

Otro criterio a considerar cuando se evalúan los protocolos de enrutamiento es su eficacia operativa. La eficacia operativa puede medirse examinando los recursos físicos, como por ejemplo la memoria RAM del router, el ciclo de reloj de su procesador y el ancho de banda de red requerido por un protocolo de enrutamiento dado.

Robustez.

Un protocolo de enrutamiento debe desempeñarse de manera eficaz en todas las ocasiones, no solo cuando la red es estable. Bajo condiciones de error, como los fallos en el hardware o del servicio de transmisión, los errores en la configuración del router o cargas de tráfico muy fuertes, se afecta negativamente a una red. Por lo tanto es importante que el protocolo de enrutamiento funcione adecuadamente durante estos periodos de inestabilidad.

Convergencia.

Los routers pueden detectar automáticamente cambios en la red. Cuando se detecta un cambio, todos los routers implicados deben converger en un nuevo acuerdo sobre la forma de la red y volver a calcular sus rutas a los destinos conocidos. Este proceso de mutuo acuerdo se denomina convergencia. Cada protocolo de enrutamiento utiliza diferentes mecanismos para detectar y comunicar los cambios que se producen en la red, por lo que cada uno converge en una proporción diferente. Mientras más despacio converge un protocolo de enrutamiento, mayor es la posibilidad de desestabilizar el servicio de red, porque durante ese lapso los routers no han llegado a un acuerdo colectivo acerca de la nueva topología de red, dando lugar a un enrutamiento incoherente.

Escalabilidad.

Es la capacidad de crecimiento de una red. Aunque el crecimiento no es algo necesario en todas las organizaciones, el protocolo de enrutamiento elegido debe ser capaz de crecer para alcanzar el crecimiento planeado de la red.

3.3 Tipos de enrutamiento.

Los routers pueden enrutar de dos modos básicos. Utilizando rutas estáticas preprogramadas, o pueden calcular rutas dinámicamente utilizando cualquiera de los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento dinámico son usados por los routers para descubrir rutas. Los routers programados estáticamente no pueden descubrir rutas, carecen de cualquier mecanismo para comunicar la información de enrutamiento a otros routers, es decir solo pueden enviar paquetes usando rutas definidas por un administrador de redes.

Dentro de los protocolos de enrutamiento dinámico existen dos grandes categorías:

1. Vector de distancia
2. Estado de enlace

Las diferencias entre estos tipos de protocolos de enrutamiento dinámico radican en la forma en que estos descubren y calculan nuevas rutas a los destinos. Estos se abordarán más adelante.

Muchas veces se hace referencia a los protocolos de enrutamiento por su campo de acción. En otras palabras dividirlos en categorías según el papel que desempeñan en una red. Hay dos clases funcionales de protocolos de enrutamiento dinámico: los Protocolos de Gateway Interior (IGP) y los Protocolos de Gateway Exterior (EGP).

Los IGP se utilizan “dentro” de sistemas autónomos. Un Sistema Autónomo (AS) es una red (LAN o WAN) relativa que está administrada por una sola persona o grupos de personas, que presenta un protocolo enrutado único, una arquitectura de direcciones y generalmente un solo protocolo de enrutamiento. Un sistema autónomo puede soportar conexiones con otros sistemas autónomos propiedad de la misma

organización y operados por esta. Un AS también puede tener conexiones con otras redes, como Internet aunque siempre manteniendo su autonomía operativa.

Por otro lado los EGP se utilizan “entre” los sistemas autónomos. El EGP más ampliamente usado es el Protocolo de Gateway Fronterizo (BGP), este es el protocolo utilizado para calcular rutas a través de Internet.

3.3.1 Enrutamiento estático.

La forma más simple de enrutamiento son las rutas preprogramadas, y en consecuencia, estáticas. Las tareas de descubrir rutas y propagarlas a través de la red se dejan al administrador. Un router programado para el enrutamiento estático envía paquetes a través de puertos predeterminados. Una vez configurada la relación entre una dirección de destino y un puerto de router, ya no hay necesidad de que los routers intenten descubrir la ruta o incluso comunicar información sobre rutas.

Otra ventaja es que el enrutamiento estático es un recurso mucho más eficaz. El enrutamiento estático utiliza menos ancho de banda de los servicios de transmisión, no necesita gastar recursos del CPU del router intentando calcular las rutas y requiere mucho menos memoria. Una desventaja del enrutamiento estático es que ante un fallo en la red, u otro cambio en la topología original es responsabilidad del administrador de la red ajustar manualmente el cambio. Si no se ajustan estos cambios habría un enrutamiento incoherente porque la configuración de los routers no refleja la topología real de la red. El enrutamiento estático es bueno solo para redes muy pequeñas que solo tengan una ruta concreta hacia cualquier destino. En estos casos el enrutamiento estático puede ser el mecanismo de enrutamiento más eficaz, porque no consume ancho de banda intentando descubrir rutas o comunicarse con otros routers.

3.3.2 Enrutamiento dinámico

3.3.2.1 Enrutamiento por vector de distancia.

En el enrutamiento basado en los algoritmos de vector de distancia, también llamados algoritmos Bellman Ford, los algoritmos transmiten periódicamente copias de sus tablas de enrutamiento a sus vecinos de red inmediatos. Cada receptor añade un vector de distancia (es decir su propio valor) a la tabla y lo envía a sus vecinos

inmediatos. Este proceso se produce de un modo omnidireccional entre los routers que son vecinos inmediatos. Este proceso paso a paso hace que cada router aprenda sobre otros routers y desarrolle una perspectiva acumulativa de las distancias de red. La tabla acumulativa se utiliza para actualizar las tablas de enrutamiento de los routers. Una vez completa, cada router ha aprendido una vaga información sobre las distancias a los recursos conectados a la red. No aprende nada específico sobre otros routers o de la forma real de la red.

Una de las desventajas del enrutamiento por vector de distancia es que un fallo o cualquier otro cambio en la red, implicará algún tiempo para que los routers converjan en un nuevo entendimiento de la topología de la red. Durante el proceso de convergencia, la red puede ser vulnerable al enrutamiento desordenado, por lo que el rendimiento de la red está en riesgo durante el proceso de convergencia. Por tanto, los más antiguos protocolos de vector de distancia que resultan lentos para converger pueden no ser apropiados para WAN grandes y complejas

Hablando en general los protocolos de vector de distancia son protocolos muy simples y fáciles de configurar, mantener y utilizar. En consecuencia, son muy útiles en redes muy pequeñas donde se tienen pocas rutas redundantes. El más destacado de los protocolos de enrutamiento por vector de distancia es el Protocolo de Información de Enrutamiento (RIP).

RIP.

La primera versión de este protocolo de enrutamiento fue uno de los primeros IGP que se utilizaron en redes IPv4. RIP es un protocolo de vector de distancia basado en el algoritmo Bellman Ford y busca su ruta óptima mediante el conteo de saltos, considerando que cada router que tiene que atravesar para llegar a su destino es un salto. RIP es un protocolo muy extendido en el mundo por su simplicidad en comparación a otros protocolos, además de que es un protocolo abierto, es decir no se tiene que pagar una licencia al fabricante para su uso.

RIP al utilizar como métrica de enrutamiento el conteo de saltos, no toma en cuenta otros parámetros importantes en la elección de ruta como por ejemplo el ancho de banda o el tráfico del enlace. RIP utiliza UDP para publicar información de

enrutamiento hacia otros routers RIP. RIP fue diseñado para trabajar con IPv4 e IPX en pequeñas redes. RIP tiene algunas limitaciones importantes:

- La escalabilidad de este protocolo de enrutamiento está limitado a un rango de 15 saltos máximo.
- La métrica de conteo de saltos, resulta inadecuada para elegir rutas que dependan de parámetros en tiempo real como por ejemplo los retardos o la carga de enlace.
- La velocidad de convergencia de RIP se considera lenta comparada con los protocolos de enrutamiento de estado de enlace. Los protocolos de estado de enlace se verán más adelante.

La base de datos de enrutamiento de cada uno de los hosts de la red que están utilizando el protocolo de enrutamiento RIP tiene los siguientes campos.

- Dirección de destino. Contiene la dirección de la red final a la que se desea acceder y tendrá que ser obligatoriamente "classfull", el término classfull indica que la red debe tener en cuenta la clase y por lo tanto no deberá ser compuesta por subredes.
- Siguiendo salto. Se define como el siguiente router que tiene que atravesar un paquete para llegar a su destino, este siguiente salto será necesariamente un router vecino del router origen.
- Interfaz de salida de router. La interfaz de salida que está directamente conectada al siguiente salto.
- Métrica. El conteo de saltos. Se considera cada salto como una única, independientemente de otros factores como tipo de interfaz o tráfico del enlace. A métrica total consiste en el total de saltos desde el router origen hasta el router destino, con la limitación de que 16 saltos se consideran como destino inaccesible, esto limita el tamaño máximo de red.
- Temporizador. El temporizador indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza tres tiempos importantes, el tiempo de actualización que se establece en 30 segundos, el

tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado que se establece en 300 segundos.

- El tiempo de actualización se considera el tiempo máximo que puede transcurrir entre el envío de 2 mensajes de actualización de un router vecino.
- El tiempo de desactivación se considera el tiempo máximo que puede esperar un router sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que ha caído y por lo tanto el router ya no está activo en la red, se establece la métrica a valor 16 (destino inalcanzable).
- El tiempo de borrado implica que una vez transcurrido ese tiempo, todas las rutas de ese router supuestamente caído son eliminadas de la tabla de enrutamiento.

RIPv2.

RIPv2 incorpora el siguiente conjunto de mejoras respecto a RIPv1:

- Autenticación para la transmisión de información RIP entre vecinos.
- Utilización de máscaras de subred, por lo que el mecanismo VLSM es viable.
- Utilización de máscaras de subred en la elección del siguiente salto, con lo que se permite arquitecturas de red discontinuas.
- Utilización de la dirección multicast IPv4 224.0.0.9 para el envío de actualizaciones de tablas RIP.

Aunque RIPv2 ha mejorado aún tiene una serie de limitantes importantes:

- Limitación en el tamaño máximo de la red debido a que el número de saltos máximo como en RIPv1 sigue fijado a 15 saltos, por lo que la utilización de RIPv2 en redes de tamaño grande queda descartado.
- RIPv2 al igual que RIPv1 genera mucho tráfico, porque envía toda la tabla de enrutamiento en cada actualización, con la carga de tráfico que esto implica.
- RIPv2 sólo permite una ruta por cada destino, lo que descarta realizar balanceos de carga.

La versión RIP que soporta IPv6 se denomina RIPng. RIPng evolucionó del RIPv2. El protocolo RIPng se trata más adelante.

3.3.2.2 Enrutamiento por estado de enlace.

Los algoritmos de enrutamiento por estado de enlace, mejor conocidos como Protocolos primero la ruta más corta (**SPF**), mantienen una base de datos compleja de la topología de la red. A diferencia de los protocolos de vector de distancia, los protocolos de estado de enlace desarrollan y mantienen un conocimiento completo de la red, así como del modo en que se interconectan. Esto se consigue mediante el intercambio de publicaciones del estado del enlace (**LSA**) con otros routers de una red.

Cada router que ha intercambiado LSA construye una base de datos topológica usando todas las LSA recibidas. Se utiliza entonces un algoritmo SPF para calcular la accesibilidad a los destinos en la red. Esta información se usa para actualizar la tabla de enrutamiento. Este proceso puede descubrir cambios en la topología de la red causados por el fallo de un componente o el crecimiento de la red. De hecho el intercambio de LSA es disparado por un evento de la red, en lugar de ejecutarse periódicamente, no hay necesidad de esperar a que expiren una serie de temporizadores arbitrarios para que los routers de la red puedan empezar a converger. A pesar de todas sus características y de su flexibilidad, el enrutamiento por estado de enlace tiene dos riesgos potenciales:

- Durante el proceso de descubrimiento inicial, los protocolos de enrutamiento por estado de enlace pueden inundar los servicios de transmisión de la red y por lo tanto reducir significativamente la capacidad de la red para transportar datos. Esta degradación del rendimiento es temporal, pero puede ser muy notable.
- El enrutamiento por estado de enlace es muy intensivo en cuanto a memoria y procesador. En consecuencia se necesitan routers mejor adaptados para soportar una carga de trabajo mayor que si se tratara del enrutamiento por vector de distancia. Esto por supuesto aumenta el costo de los routers configurados para un enrutamiento por estado de enlace.

El método de enrutamiento dinámico por estado de enlace puede ser muy útil en redes de cualquier tamaño. En una red bien planificada, un protocolo de enrutamiento por estado de enlace le permite a una red solucionar fácilmente los efectos de un cambio topológico inesperado. El uso de eventos como cambios para controlar las actualizaciones permite que la convergencia empiece mucho más rápidamente después de un cambio en la topología. También se evitan los excesos de consumo de las actualizaciones frecuentes, controladas por el tiempo. Esto permite utilizar más ancho de banda para el tráfico de enrutamiento en lugar de emplearla para el mantenimiento de la red.

OSPF.

Protocolo abierto al público utilizado para redes de tamaño medio a grande debido a que permite una escalabilidad muy remarcable. Entre sus muchas características es destacable que no tiene el problema de limitación de los 15 saltos de RIP, además de que los tiempos de convergencia de OSPF son mejores en todos los casos. OSPF toma en cuenta factores como el ancho de banda para el cálculo de costos y redes óptimas.

OSPF utiliza el algoritmo de estado de enlace. Los routers de estado de enlace mantienen una imagen común de la red e intercambian su información de enlaces desde un descubrimiento inicial hasta los cambios de la red. Los routers de estado de enlace no realizan broadcast de sus rutas periódicamente como los routers que utilizan vector distancia. OSPF tiene las siguientes características:

- Velocidad de convergencia. OSPF tiene un tiempo de convergencia mucho menor que el protocolo RIP ya que sólo se actualizan las rutas que han sido modificadas y que se distribuyen a través de la red de forma rápida.
- Soporta el mecanismo VLSM.
- Tamaño de red. Como OSPF no tiene la limitante de 15 saltos para alcanzar determinado destino es un protocolo adecuado para implementarse en redes de tamaño mayor. De manera concreta se recomienda que las áreas donde se implemente OSPF no deben contener un número superior a los 400 routers por área.

- Uso del ancho de banda. A diferencia de RIP que inunda con broadcast que contienen la tabla de enrutamiento actualizada la red cada 30 segundos, OSPF sólo envía actualizaciones cuando se produce un cambio en la red.
- Selección de ruta. OSPF utiliza una métrica basada en el ancho de banda y los retardos del enlace.
- Agrupación de miembros. RIP utiliza una topología plana en el cual todos los routers forman parte de la misma red. Esta característica provoca que la comunicación entre routers tenga que navegar por la totalidad de la red, de esta forma cada cambio en un router individual afectaría al resto de los equipos de la red. Sin embargo OSPF introduce el concepto de “áreas” lo que permite la segmentación de la red en porciones más pequeñas. Un área es un conjunto de redes dentro de un solo AS que se han agrupado. La topología de un área permanece oculta al resto del sistema autónomo, y cada área tiene una base de datos topológica separada. El enrutamiento en el AS se produce en dos niveles, dependiendo de si la fuente y el destino de un paquete están en la misma área (enrutamiento intra-área) o en áreas diferentes (enrutamiento Inter-áreas).
 - El enrutamiento intra-área lo determina solo la propia tecnología del área. El paquete se encamina sólo a partir de información obtenida dentro del área, no se puede utilizar información obtenida fuera de la misma.
 - El enrutamiento inter-área se hace siempre a través del backbone.

3.4 Enrutamiento IPv6.

3.4.1 Distancias administrativas.

La distancia administrativa es un valor que representa la confiabilidad del protocolo de enrutamiento. Durante el proceso de envío, los routers utilizan la distancia administrativa para seleccionar la mejor ruta cuando múltiples rutas utilizan diferentes protocolos de enrutamiento que apuntan hacia el mismo destino de red. La distancia administrativa con menor valor, es la ruta prioritaria para el router. Las distancias administrativas de los protocolos de enrutamiento soportadas por IPv6 no fueron modificadas de los protocolos equivalentes en IPv4. La siguiente tabla muestra las distancias administrativas de algunos protocolos de enrutamiento.

Protocolo de enrutamiento	Distancia administrativa (por defecto)
Interfase conectada	0
Ruta estática (hacia la interfase)	0
Ruta estática (hacia el siguiente salto)	1
BGP externo (eBGP)	20
OSPF	110
IS-IS	115
RIP	120
BGP Interno (iBGP)	200

Tabla 3.2 Distancias administrativas de los protocolos usados en IPv6

En esta tabla los protocolos de enrutamiento se han ordenado desde el más al menos confiable usando los valores de las distancias administrativas.

3.4.2 Protocolos IGP para IPv6.

Como se ha descrito Los Protocolos de Gateway Interior (IGPs) son utilizados dentro de los ASs y dominios. Los protocolos de enrutamiento IPv6 más comunes utilizados dentro de dominios, son los protocolos de información de enrutamiento (RIP), Sistema Intermediario-Sistema Intermediario (IS-IS), Primero la ruta libre más corta (OSPF), y el protocolo de enrutamiento de gateway interior mejorado (EIGRP). Se muestran a continuación los protocolos IGPs que soporta IPv6.

RIPng.

El protocolo de Información de enrutamiento con soporte para IPv6 (RIPng) tiene las siguientes capacidades heredadas de RIPv2:

- RIPng es un protocolo de vector de distancia basado en el algoritmo Bellman-Ford.
- Al igual que RIPv1/v2, RIPng continúa limitado a un radio de operación de 15 saltos.
- RIPng utiliza datagramas UDP para enviar y recibir información de enrutamiento.

- El broadcast periódico que contiene la información de enrutamiento puede ser enviado utilizando direcciones multicast para reducir tráfico en nodos que no requieren escuchar los mensajes RIP.

Debido a que IPv6 representa un nuevo protocolo que soportar, RIPng se ha actualizado para poder manejarlo. Las actualizaciones de RIP se enlistan a continuación:

- Tanto como los prefijos de destino, como las direcciones que identifican el siguiente salto, obviamente se ajustan a 128 bits en lugar de 32 bits.
- Los mensajes RIPng se envían sobre paquetes IPv6.
- El número de puerto estándar de UDP para IPv6 es 521 en lugar de 520 como en IPv4. Este puerto UDP envía y recibe información de enrutamiento entre routers RIPng.
- Las actualizaciones se envían a routers RIPng adyacentes usando la dirección de enlace local FE80::/10 como dirección origen.
- La dirección multicast estándar usada con RIPng es FF02::5, en lugar de 224.0.0.9 en IPv4. FF02::9 representa la dirección multicast “todos los routers” RIP en el ámbito de enlace local.

IS-IS.

Protocolo Sistema intermedio-Sistema intermedio (IS-IS). Este protocolo utiliza terminología OSI. IS-IS fue originalmente diseñado como un protocolo de enrutamiento OSI, que posteriormente fue adaptado para poder soportar a IPv4. IS-IS es un protocolo de estado de enlace basado en el algoritmo Dijkstra, posee una gran escalabilidad y además es jerárquico. Los routers IS-IS deben ser miembros de áreas IS-IS. IS-IS proporciona la información del costo de los enlaces (el costo por defecto de una interfase es 10) para calcular la mejor ruta y alcanzar las redes destino. El tiempo de convergencia que ofrece el protocolo IS-IS es notablemente menor en comparación al tiempo de convergencia de RIP. Las características del protocolo IS-IS lo hacen ideal para soportar IPv6 aunque para esto se requirió hacer una serie de modificaciones debido a que el protocolo IPv6 representa una nueva familia de direcciones que soportar.

Las actualizaciones se enfocan en dos nuevos “Type Length values” (TLVs), los cuales fueron añadidos para transportar información relacionada con el enrutamiento IPv6. El TLV es información de router codificada en campos de longitud variable dentro de los paquetes de estado de enlace (LSPs). Los nuevos TLVs añadidos son:

- **Accesibilidad IPv6.** Este nuevo TLV describe la accesibilidad de la red en términos del prefijo de enrutamiento IPv6, información de métrica y algunos bits de opción. Los bits de opción indican la publicación del prefijo IPv6 desde un nivel más alto, distribución del prefijo desde otros protocolos de enrutamiento (redistribución) y la existencia de sub TLVs. El valor decimal asignado al TLV de accesibilidad IPv6 es 236 (hex 0xEC).
- **Dirección de interfase IPv6.** Este TLV contiene una dirección de interfase 128 bits en lugar de una dirección de interfase IPv4 (32 bits). El valor decimal asignado al TLV es 232 (hex 0xE8).

El dominio IS-IS está basado en una estructura de dos niveles. Cualquier router IS-IS puede desempeñar los siguientes roles:

Router de nivel 1 (L1). Es el responsable del enrutamiento IPv6 intra-área.

Router de nivel 2 (L2). Responsable del enrutamiento IPv6 inter-área

Router de nivel 1-2 (L1/L2). Responsable del enrutamiento inter-área, inter-área

OSPFv3 para IPv6.

La versión 2 es la versión más avanzada de OSPF para IPv4 y es el protocolo IGP actualmente más utilizado en la mayoría de los sitios. La versión 3 de OSPF con soporte para IPv6 es la contraparte de OSPFv2. Una gran parte de las especificaciones OSPFv3 están basadas en OSPFv2 aunque si se han realizado algunas mejoras. Añadir soporte IPv6 al protocolo OSPFv2 requiere modificaciones importantes del código para eliminar la dependencia hacia IPv4. Después de haber actualizado el soporte para IPv6, OSPFv3 puede distribuir prefijos IPV6 y puede correr nativamente sobre IPv6.

Los cambios más importantes de OSPFv3 respecto a OSPFv2 son los siguientes:

- El protocolo procesa por enlace no por subred. IPv6 conecta interfaces a enlaces. Múltiples subredes IP pueden ser asignadas a un enlace simple y dos nodos pueden hablar directamente sobre un mismo enlace incluso si no comparten una subred IP en común. OSPF para IPv6 funciona por un enlace en lugar de hacerlo por subred. Los términos “Red” y “Subred” usados en OSPFv2 pueden ser reemplazados con el término “Enlace”; por ejemplo, una interfaz OSPFv3 ahora conectará a un enlace en vez de a una subred IP.
- Las direcciones IPv6 ya no son presentadas en los encabezados de los paquetes de OSPFv3. Estas son solo presentadas como información de carga útil.
- Soporte explícito para múltiples casos por enlace. Las diferentes versiones de OSPF pueden ahora funcionar sobre un mismo enlace. Una utilidad de esta característica es el que un solo enlace pertenezca a varias áreas.
- Uso de direcciones de enlace local. OSPFv3 asume que a cada interfase le ha sido asignada una dirección unicast de enlace local (fe80::). OSPFv3 utiliza las direcciones de enlace local para identificar la adyacencia OSPFv3 con sus vecinos.
- Direcciones multicast. Dos direcciones multicast específicas se utilizan en OSPFv3:
 - FF02::5. Representa a todos los routers que utilizan OSPF dentro de un enlace local. Esta dirección multicast es equivalente a 224.0.0.5 en OSPFv2.
 - FF02::6. Representa a todos los routers designados (DR) en el enlace local. La dirección equivalente en OSPFv2 es 224.0.0.6.
- Seguridad. OSPFv3 utiliza las cabeceras de extensión IPsec y ESP como un mecanismo de autenticación en lugar de una gran variedad de esquemas y procedimientos definidos para OSPFv2.

3.4.3 Protocolos EGP para IPv6.

Como se describió con anterioridad, los EGP se utilizan para la comunicación entre sistemas autónomos (AS). El EGP mas reconocido es el Border Gateway Protocol 4 (**BGP-4**) debido a que es el EGP más utilizado en interdominios por proveedores y

organizaciones para intercambiar información de enrutamiento entre AS. BGP-4 con soporte para IPv6 fue utilizado por el extinto 6bone por casi 10 años y es utilizado actualmente por el Internet IPv6. Por lo tanto BGP-4 es considerado como el protocolo de enrutamiento más importante en IPv6.

BGP4+

El estándar original BGP-4, solo puede transportar información de enrutamiento para el protocolo IPv4. Una versión mejorada llamada BGP4+, que también se conoce como multiprotocolo BGP expande las especificaciones de BGP-4 e incluye múltiples extensiones de protocolo para nuevas familias de dirección como por ejemplo IPv6 e IPX. Por lo tanto BGP4+ puede transportar información de enrutamiento para IPv6 y otros protocolos, incluyendo a IPv4. BGP4+ es un protocolo que se encarga de intercambiar información acerca del acceso a redes entre sistemas autónomos. Cada sistema autónomo se identifica por medio de un número único asignado por las autoridades de direccionamiento. Los sistemas autónomos pueden ser:

- **Sistema autónomo de tránsito.** Un AS de tránsito tiene múltiples conexiones a otros AS. Las actualizaciones de enrutamiento provenientes de cualquier AS que llegan a un AS de tránsito pueden pasar a través de este y ser distribuidas a otros AS vecinos. Un AS de tránsito puede enviar tráfico a cualquier otro AS basándose en la información de enrutamiento recibida. Los AS grandes generalmente son de este tipo.
- **Sistema autónomo terminal.** Un AS terminal tiene una sola conexión a otro AS. Todo el tráfico hacia o del AS terminal pasa a través de este enlace. Pequeños ISP's, redes corporativas o de campus utilizan este tipo de AS.
- **Sistema autónomo multihome.** Un sistema autónomo multihome tiene múltiples conexiones a uno o más AS. Las actualizaciones de enrutamiento no pasan a través de él. Por lo tanto, el tráfico que no pertenece a este AS no es reenviado. Un AS multihome permite múltiples entradas y salidas para compartir carga de tráfico de entrada y salida.

Cuando dos routers intercambian información de enrutamiento mediante BGP son llamados "BGP peers" o "BGP speakers". Estos establecen una sesión sobre TCP porque este protocolo garantiza una conexión confiable. El mensaje BGP más

importante que intercambian estos peers es el de actualización (Update), que contiene las rutas de intercambio. Una ruta BGP está definida como una unidad de información que consiste en información de ámbito de capa de red “Network layer reachability information” (NLRI) y un conjunto de atributos de ruta. Un NLRI puede representar una simple red, o más comúnmente un conjunto de destinos. Cada NLRI es acompañado por un conjunto de atributos de ruta que agregan información adicional a la ruta BGP, por ejemplo, la dirección del siguiente salto, la secuencia de sistemas autónomos a través de los cuales la ruta ha pasado durante su actualización, o su origen. Las decisiones de enrutamiento y administración de tráfico se basan frecuentemente en esos atributos de ruta.

Un atributo muy importante para la detección de bucles es el denominado “AS_PATH”. Este lleva la secuencia de números de sistemas autónomos por los que ha pasado la ruta. Si el peer receptor reconoce como suyo un número AS dentro de AS_PATH, rechaza la ruta correspondiente.

Las actualizaciones de enrutamiento BGP son intercambiadas entre dos peers. Estos están gobernados por políticas que especifican cuales NRIs son aceptadas por un peer particular. Un router solo puede anunciar la NRI que usa. Las políticas de entrada especifican cuales NRIs son aceptadas para un peer particular. Las políticas también se pueden usar para modificar un NRI y sus atributos para cambiar las características de una ruta

Si ambos routers intentan simultáneamente establecer una sesión BGP con el otro, se pueden formar dos conexiones paralelas. Para evitar una conexión de este tipo que provoca colisión, un router tiene que ceder. La conexión iniciada por el router con el mayor identificador permanece. EL identificador BGP es asignado a cada router BGP y es intercambiado durante el mensaje “Open”. Una vez que el mensaje Open es confirmado, los routers intercambian su tabla de enrutamiento completa basándose en sus políticas. Solo los cambios en la tabla de enrutamiento son intercambiados a partir de ese momento. Los mensajes “Keepalive” previenen la interrupción. La sesión TCP garantiza una entrega confiable de cada paquete.

BGP distingue entre las siguientes conexiones peer:

Conexión iBGP.

Los peers están dentro del mismo sistema autónomo y se denominan peers internos. Las rutas BGP aprendidas de peers internos no deben ser enviadas de regreso a otros peers internos, solo se pueden enviar a peers externos. Cada peer interno debe tener una conexión a todos los demás peers internos. Los peers internos están en malla completa, es decir todos se conectan entre sí.

Conexión eBGP.

En este caso los peers están en sistemas autónomos diferentes y se conocen como peers externos. Las rutas aprendidas de peers externos pueden actualizar al resto de los peers. Cuando se envía una actualización a un peer externo, los atributos AS_PATH NEXT_HOP se modifican. EL router emisor, agrega el número de sistema autónomo local al AS_PATH y pone en el campo NEXT_HOP su dirección IPv6 local.

Capítulo 4

Coordinación de Redes en IPv6

4.1 ICMPv6.

La principal tarea del protocolo Internet es el de transportar datos desde su origen hasta su destino, sin embargo la función de los protocolos de la capa Internet no se limita a simplemente mover datos. Las redes se apoyan sobre la capa de Internet para coordinar muchos aspectos de su operación. Como por ejemplo el proceso de descubrimiento de vecinos, el control de la asignación de direcciones, el reporte de errores, así como servicios de diagnóstico y de administración de membresías de grupo.

Mensaje	Número	Tipo de mensaje	Definición
Destino Inalcanzable	1	Error	El puerto o la dirección IP no están activas en el host destino.
Paquete demasiado grande	2	Error	El tamaño del paquete es mayor al MTU del enlace exterior.
Tiempo excedido	3	Error	Cuando el campo Tiempo de vida (TTL) llega a 0, el paquete es eliminado y un router intermediario se lo notifica al host origen.
Petición de eco	128	Informativo	Mensaje enviado al destino solicitando un mensaje de respuesta.
Respuesta de eco	129	Informativo	Mensaje usado para responder a la petición de eco.

Tabla 4.1 Mensajes ICMP usados en IPv4 e IPv6

El protocolo responsable de todas estas funciones mínimas de la capa Internet es el protocolo ICMP, mencionado brevemente en el primer capítulo. ICMP especifica mensajes soportados para IPv4 además de mensajes adicionales para la operación de IPv6. La tabla 4.1 lista los mensajes de errores básicos e informativos que ICMPv6 hereda de ICMPv4 como por ejemplo *Destino Inalcanzable*, *Paquete demasiado grande*, *Tiempo excedido*, *Petición de eco* y *Respuesta de eco*.

ICMP está definido como el protocolo 58 por la IANA, este número de protocolo es utilizado en el campo Next Header de la cabecera básica IPv6 para especificar un paquete ICMPv6. IPv6 considera un paquete ICMPv6 como un protocolo de la capa superior, como TCP y UDP, lo que significa que este debe ser ubicado después de todas las posibles cabeceras de extensión en el paquete IPv6. Los campos dentro de un paquete ICMPv6 son los siguientes:

- **Tipo.** Este campo identifica el tipo de mensaje ICMPv6. Los mensajes de error e informativos en la tabla 4.1, son ejemplos de estos tipos de mensajes.
- **Código.** Este campo proporciona detalles específicos relacionados al tipo de mensaje enviado hacia un nodo.
- **Suma de verificación.** Procesa el valor que sirve para detectar la corrupción de datos en el mensaje durante el transporte.
- **Datos.** El uso de este campo depende del tipo de mensaje utilizado. proporciona información al nodo destino.

La figura 4.1 muestra el formato de un mensaje ICMPv6.

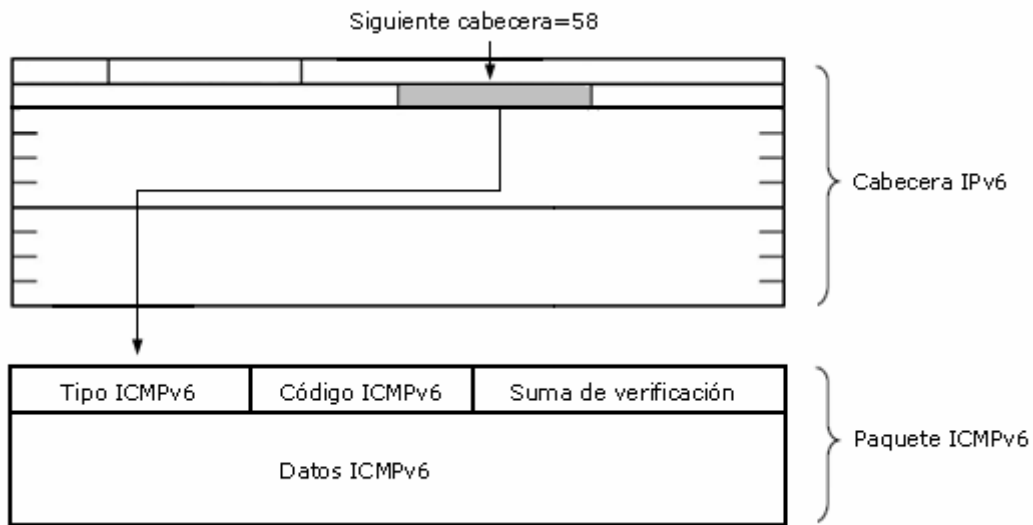


Figura 4.1 Paquete ICMPv6 utilizado después de la cabecera IPv6

Muchos de los mecanismos y funcionalidades de IPv6 utilizan los mensajes ICMPv6. Los más importantes se listan a continuación.

- **Autoconfiguración.** El mecanismo de autoconfiguración permite que los nodos configuren sus direcciones IPv6 por si mismos utilizando los prefijos que publican los routers en los enlaces locales.
- **Renumeración de prefijo.** Es el proceso que modifica el prefijo IPv6 utilizado por un cliente por uno nuevo, debido al cambio de proveedor de servicio Internet.
- **Detección de duplicación de Dirección (DAD).** Durante el proceso de autoconfiguración, cada nodo verifica que la dirección tentativa que planea utilizar no se encuentre ya en uso.
- **Descubrimiento del MTU de ruta (PMTUD).** Mecanismo donde el host origen averigua el mayor valor MTU permitido a lo largo de la ruta de entrega hacia el host destino.
- **Reemplazo de ARP.** Es el mecanismo utilizado en el ámbito de enlace local para reemplazar al mecanismo ARP, donde los nodos pueden mantener rutas hacia sus vecinos. Se han definido nuevos mensajes ICMP en IPv6 para este uso específico.

4.2 Descubrimiento MTU de ruta (PMTUD) IPv6.

PMTUD no es una nueva característica de IPv6, es una especificación incluida en IPv4. Sin embargo, el uso de PMTUD en IPv4 es opcional, por esto su práctica en entornos IPv4 no es frecuente. El principal objetivo de PMTUD es averiguar el valor del MTU a lo largo de una ruta cuando un paquete es enviado a su destino, para evitar su fragmentación. Con esta información el nodo origen puede usar la capacidad máxima del MTU encontrado para comunicarse con el nodo destino. La fragmentación ocurre en los routers intermediarios cuando un paquete es mayor al MTU soportado por la capa de enlace que se encuentra en la ruta de entrega de ese router. La fragmentación es una operación muy costosa, que se traduce en procesamiento excesivo en el CPU de los routers. Puede que en algunas circunstancias ocurra una fragmentación sobre fragmentación en muchos routers intermediarios a lo largo de la ruta de entrega, lo que provoca una considerable disminución en el rendimiento de estos.

En IPv6 la fragmentación no es una función que realicen los routers intermediarios. El nodo origen debe fragmentar los paquetes por sí mismo, esto sucede únicamente cuando el MTU de la ruta de entrega es más pequeño que el tamaño de los paquetes a entregar. El mecanismo PMTUD en IPv6 se ayuda de los mensajes de error ICMPv6 tipo 2 (Paquete demasiado grande) para esta operación. La figura 4.2 ilustra el siguiente ejemplo, en este se describe como opera el mecanismo PMTUD.

1. Un nodo origen envía un primer paquete IPv6 hacia el nodo destino utiliza un MTU de 1500 bytes.
2. El router intermediario A le contesta al nodo origen usando un mensaje ICMPv6 tipo 2 (Paquete demasiado grande), y especifica 1400 bytes como el valor más alto para el MTU en el paquete ICMPv6.
3. El nodo origen entonces envía el paquete usando los 1400 bytes como el valor MTU, el paquete pasa a través del router A.
4. Sin embargo, a través de la ruta el router intermediario B contesta al nodo origen utilizando un mensaje ICMPv6 Tipo 2 y especifica el valor MTU en 1300 bytes.

5. Finalmente, el nodo origen reenvía el paquete usando 1300 bytes como el valor MTU. El paquete pasa a través de ambos routers intermediarios y es entregado a su nodo destino.
6. La sesión es ahora establecida entre los nodos origen y destino, y todos los paquetes enviados entre estos usan un MTU de 1300 bytes.

Los valores MTU encontrados por el mecanismo PMTUD son almacenados en los nodos origen.

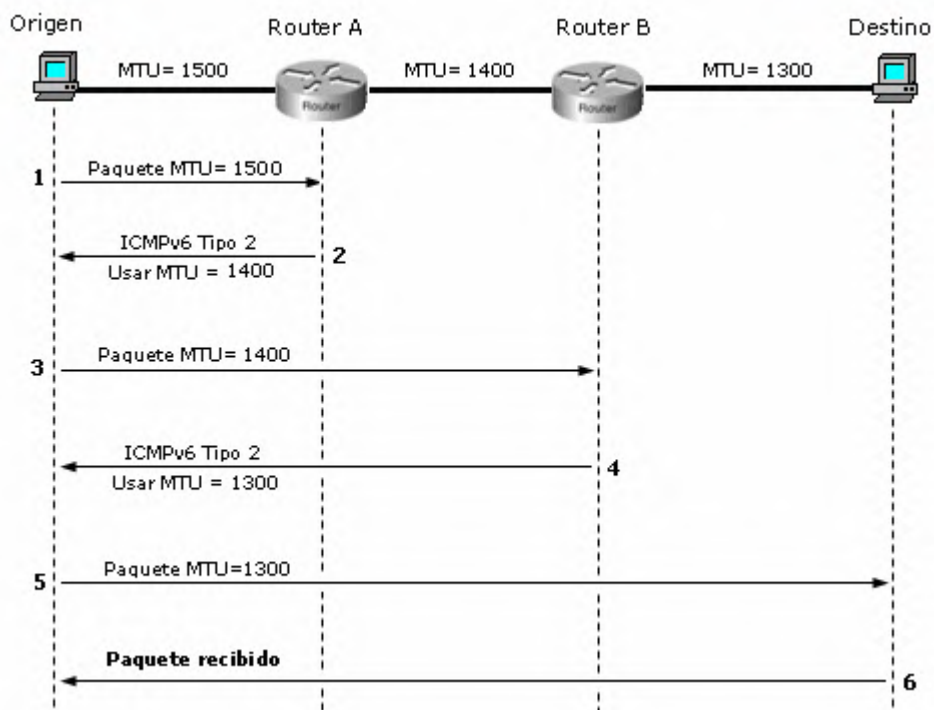


Figura 4.2 El mecanismo PMTUD utiliza mensajes ICMPv6 tipo 2

4.3 Protocolo de descubrimiento de vecinos (NDP).

Un protocolo que es fundamental para la operatividad de IPv6 es el Protocolo de descubrimiento de vecinos (NDP) y es el soporte de importantes mecanismos de IPv6 entre los que se encuentran los siguientes:

- **Reemplazo del mecanismo ARP.** Debido a que ARP ha sido eliminado en IPv6, IPv6 proporciona una nueva forma de determinar direcciones de capa de enlace de los nodos en el enlace local. Este nuevo mecanismo utiliza una mezcla de mensajes ICMPv6 y direcciones multicast.

- **Autoconfiguración.** Este mecanismo también conocido como autoconfiguración sin estado (stateless) le permite a los nodos en el enlace local configurar sus propias direcciones IPv6 por si mismos al usar una mezcla de mensajes ICMPv6 y direcciones multicast.
- **Redirección de router.** El router envía mensajes ICMPv6 hacia un nodo IPv6 para informarle de la presencia de una mejor dirección de router en el enlace local para alcanzar un destino de red.

NDP requiere nuevos tipos de mensajes ICMP y estos se definen para ámbitos específicos. Estos mensajes ICMPv6 son etiquetados en el contexto de NDP. Los nuevos mensajes ICMPv6 son Solicitud de router, Publicación de router, Solicitud de vecino, Publicación de vecino y Redirección de mensaje. La tabla 4.2 presenta estos nuevos mensajes.

Tipo de mensaje ICMPv6	Nombre del mensaje
Tipo 133	Solicitud de router (RS)
Tipo 134	Publicación de router (RA)
Tipo 135	Solicitud de vecino (NS)
Tipo 136	Publicación de vecino (NA)
Tipo 137	Redirección de mensaje

Tabla 4.2 Mensajes ICMPv6 definidos para NDP

4.3.1 Mecanismo de reemplazo de ARP en IPv6.

Recordemos que el protocolo ARP es un recurso IPv4 usado por los nodos en el enlace local para determinar las direcciones de la capa de enlace de otros nodos. Cada nodo maneja una tabla ARP, la cual contiene direcciones de la capa de enlace de nodos aprendidos con ARP. En IPv6 la determinación de las direcciones de la capa de enlace de los nodos utiliza una combinación de los mensajes solicitud de vecino (ICMPv6 tipo 135), mensajes de publicación de vecino (ICMPv6 tipo 136) y la dirección multicast solicited-node (FF02::1:FFxx:xxxx).

NDP ofrece las siguientes ventajas respecto a ARP:

- En IPv6, únicamente los nodos vecinos involucrados con este mecanismo procesan los mensajes solicitud de vecino y publicación de vecino en su pila. En IPv4, los mensajes de difusión ARP se utilizan para encontrar direcciones

de la capa de enlace de los nodos, estas difusiones ARP obligan a todos los nodos dentro del enlace local a trasladar todos los mensajes ARP hacia su pila IPv4.

- En IPv6, los hosts comunican sus direcciones de capa de enlace hacia cualquier otro host en la misma petición. En IPv4, dos mensajes de difusión ARP son necesarios para obtener el mismo resultado.
- La accesibilidad de direcciones IPv6 y direcciones de capa de enlace se verifican en la memoria del host vecino. Con ARP en IPv4, las entradas son eliminadas después de expirar (timeout).

La figura 4.3 muestra paso a paso como opera NDP para identificar la dirección de capa de enlace de un nodo en el enlace local.

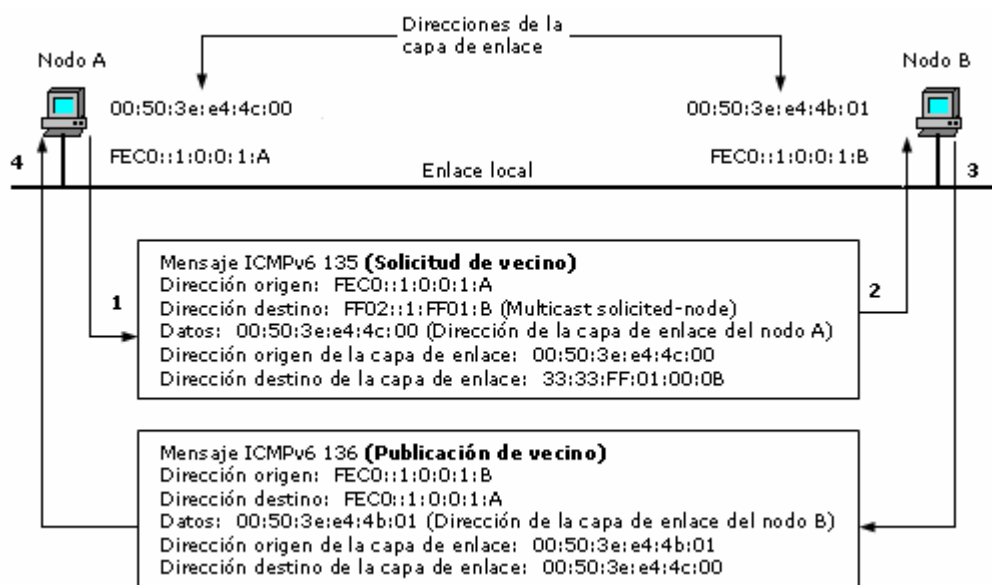


Figura 4.3 Mecanismo NDP utilizado para encontrar la dirección MAC de un nodo dentro del ámbito de enlace local.

1. El nodo A que utiliza la dirección de sitio local FEC0::1:0:0:1:A, busca entregar paquetes hacia el nodo destino B que se ubica en el mismo enlace local y que utiliza la dirección FEC0::1:0:0:1:B. Debido a que el nodo A no conoce la dirección de la capa de enlace del nodo B, envía un mensaje ICMPv6 tipo 135 (*Solicitud de vecino*) en el enlace local con los siguientes datos: su dirección de sitio local FEC0::1:0:0:1:A como dirección origen, como dirección destino utiliza la dirección multicast solicited-node FF02::1:FF01:B correspondiente a la

dirección objetivo FEC0::1:0:0:1:B. La dirección de la capa de enlace del nodo A que en este caso es 00:50:3e:e4:4c:00 actúa como dato del mensaje ICMPv6. La dirección origen de la capa de enlace de esta trama es la dirección del nodo A 00:50:3e:e4:4c:00. La dirección de la capa de enlace destino de esta trama que es 33:33:FF:01:00:0B utiliza mapeo multicast de la dirección destino IPv6 FF02::1::FF01:B. Obviamente utilizando un enlace Ethernet.

2. El nodo B, escucha el enlace local en busca de mensajes multicast, intercepta el mensaje de *Solicitud de vecino* debido a que la dirección IPv6 de destino FF02::1:FF01:B representa la dirección multicast solicited-node que corresponde con su dirección FEC0::1:0:0:1:B.
3. El nodo contesta enviando un mensaje de *Publicación de vecino* usando su dirección de sitio local FEC0::1:0:0:1:B como la dirección origen, y la dirección de sitio local FEC0::1:0:0:1:A, como la dirección destino. Este también incluye su dirección de capa de enlace 00:50:3e:e4:4b:01 en el mensaje ICMPv6.

Después de recibir los mensajes de *Solicitud de vecino* y *Publicación de vecino*, el nodo A y el nodo B conocen sus direcciones mutuas de la capa de enlace. Las direcciones de la capa 2 aprendidas se guardan en una tabla NDP, por lo tanto los nodos pueden comunicarse a través del enlace local. Cuando los nodos modifican su dirección de la capa de enlace, es posible informar a todos los nodos vecinos ubicados en el enlace local al enviar un mensaje de *Publicación de vecino* usando la dirección multicast “todos los nodos” FF02::1. Entonces la tabla NDP de todos los nodos pertenecientes al enlace local se actualiza con la nueva dirección de la capa de enlace.

Los mensajes ICMPv6 y direcciones multicast involucrados en el mecanismo que reemplaza ARP se muestran en la tabla 4.3.

Mecanismo	Dirección Multicast	Tipo de Mensaje ICMPv6
Reemplazo del mecanismo ARP	Dirección multicast solicited-node FF02::1:FFxx:xxxx	ICMPv6 Tipo 135 ICMPv6 Tipo 136

Tabla 4.3 Direcciones multicast y mensajes ICMPv6 utilizados por el mecanismo que reemplaza a ARP.

4.3.2 Autoconfiguración.

La función de Autoconfiguración *stateless* es una de las características más interesantes y de mayor utilidad de IPv6. Esta función permite que los nodos ubicados dentro de un enlace local configuren sus direcciones unicast IPv6 por si mismos apoyándose de la información que publica un router en ese enlace local. A continuación se describen los mecanismos involucrados en la autoconfiguración.

- **Publicación de prefijo.** Mecanismo que publica prefijos y parámetros en un enlace local. La información de publicación de prefijo es usada por los nodos IPv6, para configurar sus direcciones IPv6.
- **DAD.** Mecanismo que se asegura que cada dirección IPv6 configurada en una interfase adquirida mediante la Autoconfiguración *stateless*, sea única dentro del enlace local.
- **Renumeración de prefijo.** Mecanismo que publica prefijos modificados o nuevos así como parámetros en el enlace local para renumerar un prefijo ya publicado.

Es relevante señalar que los routers no pueden asignar direcciones IPv6 a sus interfaces usando la configuración *stateless*. La configuración *stateless* es una función que está diseñada únicamente para hosts.

Los mensajes de publicación de router contienen parámetros que utilizan los nodos durante y después del proceso de autoconfiguración:

- **Prefijo IPv6.** Uno de múltiples prefijos IPv6 puede ser publicado por enlace local. Por defecto, la longitud del prefijo publicado por la autoconfiguración *stateless* es de 64 bits. Los nodos adquieren el prefijo IPv6, y entonces estos añaden su dirección de la capa de enlace en el formato EUI-64 al prefijo recibido. La combinación de esta información proporciona una dirección de 128 bits a los nodos.
- **Tiempo de vida.** Un valor de tiempo de vida por cada prefijo publicado se proporciona a los nodos. Este valor puede variar desde 0 hasta el infinito. Los nodos verifican este valor para detener el uso de un prefijo después de que

este a expirado, cuando el valor es igual a 0. Hay dos tipos de valores de tiempo de vida por prefijo:

-Tiempo de vida válido. Indica cuanto tiempo en estado válido le resta a la dirección del nodo. Cuando este valor expira, la dirección del nodo se vuelve inválida.

-Tiempo de vida preferente. Indica cuanto tiempo de preferencia le resta a la dirección de un nodo, adquirida mediante la autoconfiguración *stateless* y este debe ser menor igual al tiempo de vida válido. Cuando este valor expira, todas las direcciones adquiridas mediante la autoconfiguración y que utilizan este prefijo son ignoradas. Por lo tanto los nodos no pueden establecer nuevas conexiones cuando ha expirado el tiempo de vida preferente.

- Información de router por defecto. Proporciona información acerca de la existencia y tiempo de vida de la dirección del router por defecto. En IPv6, la dirección de un router por defecto utilizada por un nodo es la dirección de enlace local del router FE80::/10. Por lo tanto, incluso si el prefijo es reenumerado, el router siempre puede ser alcanzado.
- Indicadores/Opciones. Son indicadores y opciones específicas para nodos. Se utilizan para instruir a los nodos sobre el uso de la autoconfiguración con estado (stateful) en lugar de la autoconfiguración *stateless*.

La autoconfiguración stateful le permite a los nodos adquirir sus direcciones y parámetros de configuración manualmente o desde un servidor. El servidor mantiene una base de datos que guarda las rutas de las direcciones asignadas a los nodos. DHCP es un ejemplo de la autoconfiguración stateful en IPv6.

La autoconfiguración es una funcionalidad con mucho peso en IPv6 ya que permitirá la implementación de nuevos dispositivos a una gran escala en Internet como teléfonos celulares, dispositivos inalámbricos y redes domésticas.

4.3.2.1 Publicación de prefijo.

La publicación de prefijo es el mecanismo inicial involucrado en la autoconfiguración. El mecanismo de publicación de prefijo utiliza mensajes de Publicación de router (ICMPv6 Tipo 134) y direcciones multicast “todos los nodos” FF02::1. Los mensajes de

Publicación de router se envían periódicamente a través del enlace local hacia la dirección multicast “todos los nodos”.

Con la autoconfiguración stateless, los routers IPv6 son el único tipo de dispositivos permitidos para publicar prefijos en los enlaces locales. Esta prohibido para los nodos el publicar prefijos. La longitud del prefijo usado en la autoconfiguración stateless es de 64 bits. Como se muestra en la figura 4.4, el router A envía mensajes periódicos de Publicación de router (ICMPv6 tipo 134) usando su dirección de enlace local FE80::250:3EFF:FEE4:4C00 como la dirección origen IPv6 y la dirección multicast “todos los nodos” FF02::1 como la dirección IPv6 destino. El prefijo publicado por los mensajes de publicación de router es FEC0:0:0:1::/64. Entonces los nodos A y B, los cuales escuchan la dirección multicast FF02::1 en el enlace local y obtienen los mensajes de publicación de router y pueden configurar su dirección IPv6 por ellos mismos.

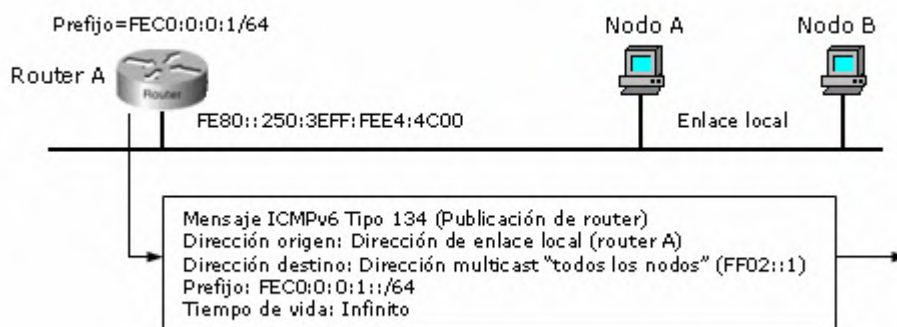


Figura 4.4 Mecanismo de autoconfiguración utilizando los mensajes de publicación de router.

4.3.2.2 Petición de publicación de router usando la solicitud de router.

Los mensajes de Publicación de router son enviados periódicamente en los enlaces locales por los routers. Sin embargo cuando se inicializa un nodo, este podría no recibir las publicaciones del router. Ante esta situación, cualquier nodo puede enviar un mensaje de solicitud de router (ICMPv6 Tipo 133) hacia la dirección multicast “todos los routers” FF02:2 en el enlace local. Cuando el mensaje de solicitud de router es recibido, un router en el enlace local responde con un mensaje de publicación de router (ICMPv6 tipo 134) usando la dirección multicast FF02::1 “todos los nodos”. La figura 4.5 ilustra este mecanismo.

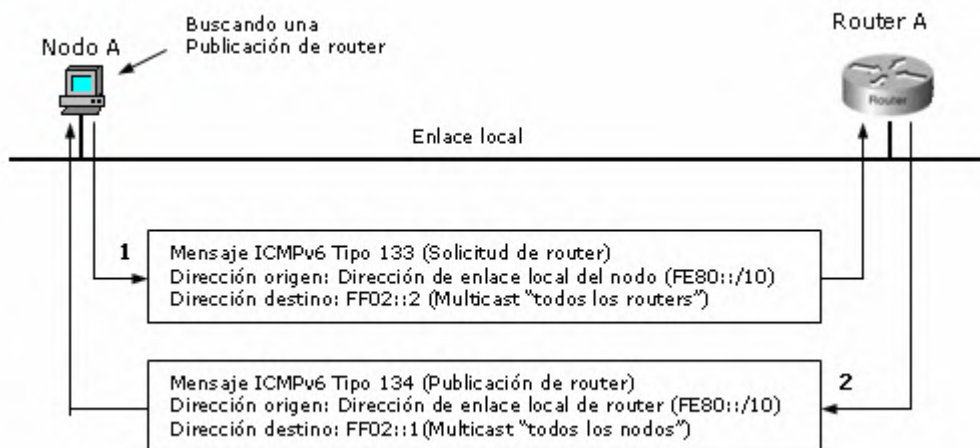


Figura 4.5 Intercambio de mensajes ICMPv6 tipo 133 y 134 entre un nodo y un router en el enlace local, para que el nodo adquiera los mensajes de publicación de router.

1. El nodo A envía un mensaje de solicitud de router usando la dirección de enlace local FE80::/10 como la dirección origen IPv6 hacia la dirección multicast "todos los routers" FF02::2. El router A que escucha el enlace en espera de paquetes multicast correspondientes a grupos al que este pertenece, detecta el mensaje de solicitud de router enviado por el nodo.
2. Usando su dirección de enlace local como dirección origen el router A responde al nodo con un mensaje de publicación de router (ICMPv6 tipo 134) enviado hacia la dirección multicast "todos los nodos" FF02::1.

Para evitar la inundación de mensajes de Solicitud de router en el enlace, cada nodo puede enviar únicamente tres mensajes de este tipo. En ausencia de un router IPv6 en el enlace, esta regla asegura que los enlaces no sean inundados con los mensajes de Solicitud del router.

En la tabla 4.4 se resumen los tipos de direcciones multicast y mensajes ICMPv6 que se utilizan en los prefijos de publicación.

Mecanismo	Dirección Multicast	Tipo de mensaje ICMPv6
Publicación de prefijo	Multicast "todos los nodos" FF02::1	Tipo 133 (Solicitud de router)
	Multicast "todos los routers" FF02::2	Tipo 134 (Publicación de router)

Tabla 4.4

4.3.2.3 Detección de Duplicado de dirección. (DAD).

DAD es un mecanismo NDP involucrado en la autoconfiguración de la dirección de un nodo. Antes de que un nodo pueda configurar su dirección Unicast IPv6 usando la autoconfiguración, este debe verificar en el enlace local que la dirección tentativa que planea utilizar sea única y no está siendo utilizada por otro nodo. El mecanismo DAD se apoya en los mensajes de Solicitud de vecino (ICMPv6 tipo 135) y direcciones multicast solicited-node, para realizar esta tarea. Esta operación requiere que el nodo envíe un mensaje de solicitud de vecino en el enlace local usando la dirección no especificada (::) como su dirección IPv6 origen y la dirección multicast solicited-node de la dirección unicast tentativa como la dirección destino IPv6. Si se descubre una dirección duplicada durante el procedimiento, la dirección tentativa no puede ser asignada a la interfase. De otro modo la dirección tentativa es configurada en la interfase.

En la figura 4.6 se muestra como opera el mecanismo DAD.

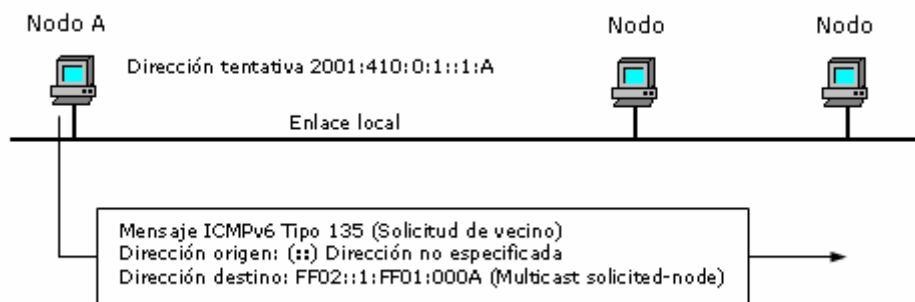


Figura 4.6

El nodo A pretende configurar la dirección unicast tentativa 2001:410:0:1::1:A en su interfase. Para asegurarse de que esa dirección es única, el nodo A envía un mensaje de solicitud de vecino, usando la dirección no especificada (::) como la dirección IPv6 origen y la dirección multicast solicited-node FF02::1:FF01:A correspondiente a su probable dirección unicast 2001:410:0:1::1:A como la dirección destino. Tan pronto como el mensaje de Solicitud de vecino se envía al enlace local, si un nodo responde a esa solicitud, eso significa que la dirección unicast tentativa del nodo A esta siendo utilizada por otro nodo. En la ausencia de una respuesta (como se muestra en la figura) el nodo A determina que la dirección unicast tentativa 2001:410:0:1::1:A es única en el enlace local, entonces puede ser asignada a su interfase.

La tabla 4.5 resume los tipos de direcciones multicast y mensajes ICMPv6 que se utilizan en el mecanismo DAD.

Mecanismo	Dirección Multicast	Tipo de Mensaje ICMPv6
DAD	Dirección Multicast solicited-node FF02::1:FFxx:xxxx	Tipo 135 (Solicitud de vecino)

Tabla 4.5

4.3.2.4 El mecanismo de reenumeración de prefijo.

Un beneficio importante del protocolo IPv6 es su capacidad de ofrecer una reenumeración transparente de la red para los usuarios finales cuando el prefijo debe ser cambiado por uno nuevo. A consecuencia de la estricta agregación del protocolo IPv6, la reenumeración del prefijo es necesaria cuando una organización decide cambiar su proveedor de servicio Internet IPv6.

El mecanismo de reenumeración de prefijo es un proceso casi imperceptible para el usuario final y se apoya en el mecanismo de Autoconfiguración para todos los nodos del sitio. Existen otros métodos que realizan el proceso de reenumeración de red, pero resultan más complejos y menos transparentes para los usuarios finales. La función de Reenumeración de prefijo es una tarea que realizan los routers que publican prefijos en el enlace local. Este mecanismo utiliza los mismos mensajes ICMPv6 y direcciones multicast que el mecanismo de publicación de prefijo.

La Reenumeración de prefijo utiliza parámetros de tiempo contenidos en los mensajes de Publicación de router descritos anteriormente. Un proceso de Reenumeración de prefijo sigue los siguientes pasos: Primero, todos los routers en el sitio continúan publicando su actual prefijo, pero los tiempos de vida válidos de este prefijo son decrementados hasta un valor cercano a 0. Entonces los routers comienzan a publicar el nuevo prefijo en el enlace local. Por lo tanto al menos dos prefijos coexisten en cada enlace local. Esto significa que los mensajes de publicación del router contienen el nuevo y el anterior prefijo IPv6. Al recibir estos mensajes de publicación del router, los nodos advierten el agotamiento del tiempo de vida del actual prefijo, por lo que también adquieren el nuevo prefijo. Durante este tiempo de transición todos los nodos usan dos direcciones unicast:

- La dirección Unicast anterior, que es la dirección basada en el prefijo anterior. Esta dirección aún es soportada por las conexiones establecidas durante este periodo de transición.
- Nueva dirección Unicast. Cuando el anterior prefijo es completamente desechado a causa de que su validez ha “caducado”, los mensajes de publicación de router (ICMPv6) incluyen únicamente el nuevo prefijo. Un prefijo es desechado cuando el valor del tiempo de vida (lifetime) válido/preferente está en 0.

4.3.3 Redirección de router.

La redirección de router es un mecanismo NDP en IPv6. Los routers usan mensajes de redirección ICMPv6 para informar a los nodos en el enlace local, que una mejor ruta existe en el enlace para enviar paquetes. El nodo que recibe el mensaje de redirección ICMPv6 puede modificar su tabla de enrutamiento local de acuerdo con la nueva dirección de router en el mensaje de redirección ICMPv6.

El mecanismo de redirección de router en IPv6 utiliza mensajes de redirección (ICMPv6 tipo 137). Este mecanismo es el equivalente al mensaje de redirección en IPv4. La figura 4.7 muestra al nodo A que busca enviar paquetes hacia la LAN ZZ. Primero, el nodo A entrega el primer paquete hacia su router por defecto (Router A). Sin embargo, después de enviar este paquete hacia la LAN ZZ, el router A reconoce que el router C es una mejor ruta para nodos en este enlace local para enviar paquetes hacia la LAN ZZ. Por lo tanto, en el segundo paso, el router A envía al nodo A un mensaje de redirección ICMPv6, que contiene la dirección IPv6 del router C. Finalmente, el nodo A envía los siguientes paquetes a enviar a la LAN ZZ a través del router C.

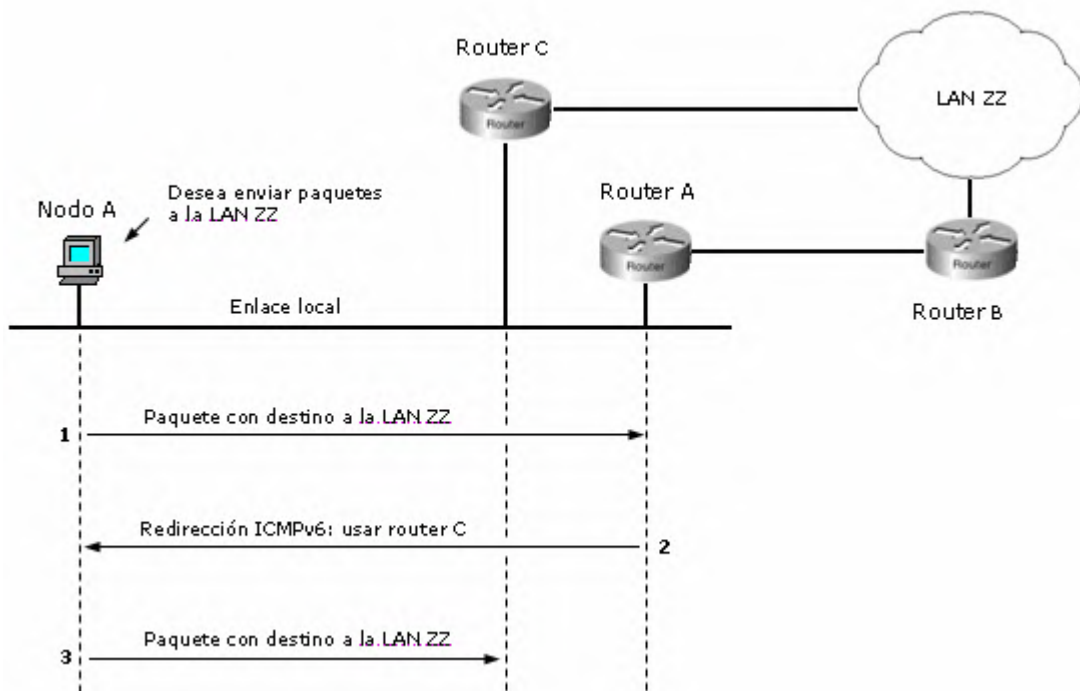


Figura 4.7 Mensajes de redireccionamiento IPv6

4.4 El servicio DNS.

Para realizar la tarea de enrutamiento TCP/IP identifica las redes mediante las direcciones IP. La inconveniencia de esta forma de identificación con IPv6 es evidente; las direcciones IPv6 requieren el manejo de 32 caracteres hexadecimales, por lo que se dificulta el proceso de escribir una dirección IPv6 y además se tiende a cometer equivocaciones. El Servicio de nombres de dominio (DNS) proporciona un servicio en el que los usuarios identifican redes mediante nombres específicos (hostnames). Los protocolos que requieren direcciones IP en lugar de nombres, utilizan el servicio DNS para traducir una forma a la otra. La función DNS no se limita solamente a proporcionar este servicio de traducción, sino que también organiza estos nombres dentro de una jerarquía.

4.4.1 Jerarquía de nombres.

Esta jerarquía tiene una estructura tipo árbol, donde en la parte más alta estarán los dominios de alto nivel (top level) de Internet, algunos de estos dominios son: .com, .org, .net, .edu, y también los códigos de país contruidos con solo dos letras: .mx (México), .jp (Japón), .uk (Inglaterra), etc.; estos códigos dividen los nombres en base a su ubicación geográfica. Por ejemplo la UNAM, que pertenece al dominio de

jerarquía .mx, tiene la dirección www.unam.mx. Esta notación separa los niveles individuales con puntos (.), esta es la forma de escribir un dominio completo.

La jerarquización permite que Internet ceda autoridad para ejercer el nombramiento de redes. Cada organismo que utiliza su porción del espacio de nombres de Internet puede subdividirlo de la forma que le parezca más conveniente, estas divisiones forman parte del propio subdominio de las organizaciones. Por ejemplo, la UNAM define múltiples subdominios entre los que se encuentran la facultad de Estudios Superiores Cuautitlán, (www.cuautitlan.unam.mx) y el proyecto IPv6 de la universidad (www.ipv6.unam.mx).

El mecanismo DNS tiene ciertas restricciones: el nombre debe comenzar con una letra ASCII y debe contener únicamente letras, dígitos y guiones. El tamaño del nombre en cualquier nivel se limita a 63 caracteres y el nombre completo incluyendo todos los niveles y los puntos de separación no deben sobrepasar los 255 caracteres. Los nombres en mayúsculas y en minúsculas son indistintos, UNAM.MX y unam.mx son equivalentes. La jerarquía DNS organiza a los servidores que proporcionan su servicio de traducción. En la parte más alta del esquema de jerarquías se encuentra el servidor raíz que en teoría tiene la responsabilidad de la traducción de todos los nombres de Internet. Este servidor raíz cede parte de esa responsabilidad a los servidores de los dominios de alto nivel.

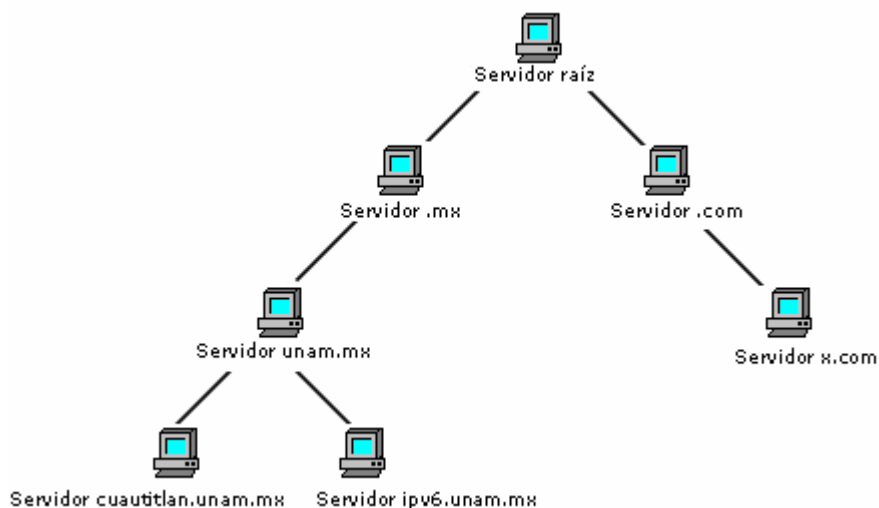


Figura 4.8 Ejemplo simple de una organización jerárquica de los servidores DNS

La figura 4.8 es un ejemplo de esta organización, que muestra a los servidores .mx y .com como servidores “hijos” del servidor raíz. Este patrón continúa hacia debajo de la jerarquía con servidores para unam.mx, cuautitlán.unam.mx y otros subdominios.

El área de responsabilidad dada a un servidor de nombre se conoce como su “zona”. En la figura anterior se simplifica a una zona por cada nivel de la jerarquía pero una zona generalmente incluye múltiples subdominios. El mecanismo DNS se inicia cuando los clientes envían peticiones hacia el servidor DNS y entonces los servidores envían su respuesta. El DNS utiliza los protocolos TCP o UDP y la mayoría de los servidores soportan ambos servicios. Cada vez que una petición llega a un servidor DNS, este responde al usuario usando el mismo servicio de transporte. Generalmente los clientes tienen una sola petición para el servidor DNS por lo tanto se utiliza UDP debido a su simplicidad. Sin embargo cuando los servidores actúan como clientes estos generalmente tienen conjuntos de peticiones para actualizar completamente su tabla de información. Bajo estas circunstancias TCP es el protocolo apropiado.

4.4.2 Formato del mensaje DNS.

DNS utiliza el mismo formato de mensaje tanto para las peticiones como para las respuestas. La figura 4.9 muestra el formato de este mensaje.

El mensaje DNS contiene los siguientes campos:

- **Identificador** (16 bits). Los clientes insertan un valor para este campo cuando envían una petición y el servidor debe reflejar el mismo valor en su respuesta. Este campo permite que los clientes tengan múltiples peticiones pendientes en un servidor. Cuando el servidor envía una respuesta, se utiliza el identificador para emparejar la respuesta con la petición original.
- **Control de bits** (16 bits). Campo que contiene indicadores del mensaje, en la tabla 4.8 se resume su significado y enlista los bits desde el más al menos significativo.

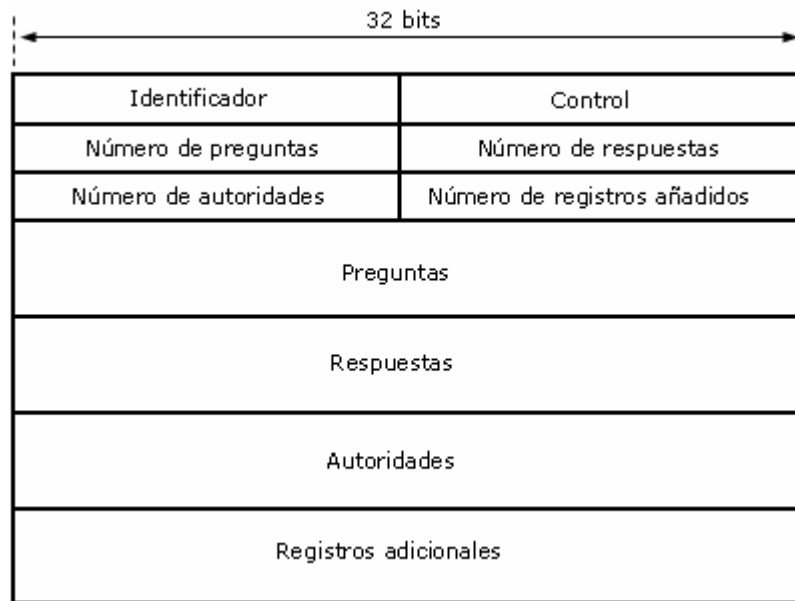


Figura 4.9 Formato del mensaje DNS

Campo	Bits	Función
QR	1	0 si el mensaje es una solicitud 1 si el mensaje es una respuesta
Opcode	4	0 si el mensaje es una solicitud estándar, 1 si es una solicitud inversa
AA	1	1 si la respuesta está autorizada
TC	1	1 si el mensaje ha sido desechado debido a restricciones de tamaño
RD	1	1 si se desea la recursión
RA	1	1 si la recursión está disponible
Z	3	Reservada (debe ser cero)
Rcode	4	Respuesta de código

Tabla 4.8 Bits del campo Control DNS

- El bit AA es 1 cuando la respuesta proviene directamente del servidor responsable del nombre en cuestión. Este no podría ser el caso cuando la respuesta es recursiva.
- El campo Rcode indica si la petición fue exitosa, si no fue así también proporciona las razones de la falla.
- El campo RD indica si se desea la recursión. La recursión es el proceso donde un servidor de nombres local a partir de una sola solicitud de un cliente, toma la responsabilidad de responder esa solicitud realizando investigación adicional a favor de su cliente.

- Los siguientes cuatro campos de 16 bits cada uno proporcionan el número de peticiones, respuestas, autoridades y registros adicionales en el resto del mensaje.
- **Preguntas.** Este campo contiene tres partes, la primera contiene el nombre de la dirección para el que se solicita su dirección IP. La segunda parte contiene el tipo de petición y tiene 16 bits. La última parte y también de 16 bits contiene la clase de petición, si tienen un valor de 1 indica información relacionada con Internet. La figura 4.10 presenta un mensaje de petición DNS sencillo.

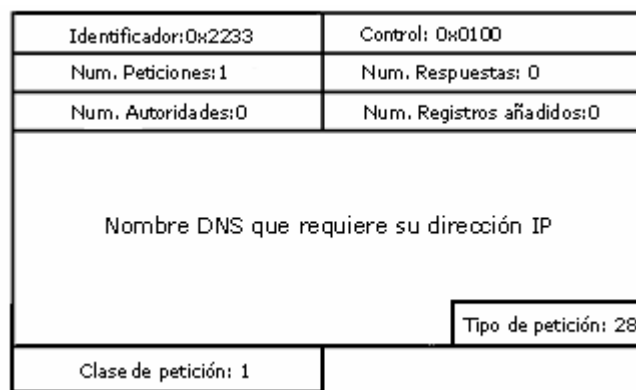


Figura 4.10 Ejemplo de un mensaje de solicitud DNS

DNS puede soportar peticiones para diferentes tipos de datos. La tabla 4.9 enlista algunos tipos comunes de solicitud para TCP/IP.

Tipo	Valor	Descripción
A	1	Dirección IPv4
NS	2	Servidor de nombres autorizado
CNAME	5	Nombre canónico
SOA	6	Inicio de una zona autorizada
PTR	12	Apuntador de dominio de nombre
MX	15	Intercambio de correo
TXT	16	Cadenas de texto
AAAA	28	Dirección IPv6
AXFR	252	Transferencia de una zona completa
*	255	Solicitud para todos los registros

Tabla 4.9 Tipos comunes de solicitud DNS

- **Respuestas.** Este campo contiene las respuestas y registros adicionales denominados recursos de registro que envía el servidor DNS. El formato de este campo es parecido al formato de Preguntas del mensaje DNS, con las partes nombre, tipo y clase de respuesta además de otros parámetros.
- Los dos últimos campos en el mensaje son las autoridades, estas no son más que los servidores DNS que tienen la autoridad sobre el nombre para el que se solicita la dirección IP.

4.5 DHCPv6.

El Protocolo de Configuración de Host Dinámico (DHCP) añade una considerable conveniencia a las redes TCP/IP. Los host generalmente necesitan configurar información antes de que estos puedan comenzar a operar dentro de una red. Con el DHCP los host pueden usar la red para obtener esta información. El DHCP se concentra en proporcionar direcciones de red a los host. Aunque un host puede siempre conformar una dirección de enlace local (FE80::/10), estas direcciones confinan el tráfico hacia su enlace local. Cuando el host obtiene su dirección unicast de agregación global por medio de la autoconfiguración stateless se tienen algunas deficiencias. Por ejemplo, todas las redes que usan la autoconfiguración deben tener un router que genere publicaciones de router y los administradores de red deben asegurarse de que todas estos routers tengan la información de prefijo correcta.

DHCP proporciona un método más flexible y más controlado de autoconfiguración de direcciones de red. El protocolo también tiene la capacidad de transferir otro tipo de información de configuración. DHCP ofrece a los administradores la flexibilidad para asignar direcciones en una de tres formas:

- **Asignación Manual.** El método más rígido es la asignación manual. Con este método el administrador explícitamente asigna direcciones específicas a host específicos. Cuando estos host usan DHCP para descubrir sus direcciones, DHCP se los proporciona con los valores manualmente asignados.
- **Asignación automática.** Similar a la autoconfiguración stateful, este método combina la dirección de enlace con un prefijo de dirección para crear una dirección de red, aunque para llegar a este resultado DHCP utiliza otro procedimiento. En lugar de esperar publicaciones de router, los host solicitan

activamente una dirección desde una computadora especial actuando como un servidor DHCP. El servidor pone la dirección de enlace junto con el prefijo de red y regresa la dirección resultante al host. Las ventajas que proporciona la asignación automática DHCP con respecto a la autoconfiguración stateless son dos:

1. DHCP no requiere la configuración y mantenimiento de routers en cada red. La administración de dirección puede ser concentrada en un único host (servidor DHCP).
 2. DHCP permite cambiar las estrategias de asignación de dirección fácilmente.
- Asignación Dinámica. La asignación dinámica representa la estrategia de asignación más flexible. Le permite a un grupo de hosts compartir un pequeño conjunto de direcciones de red. Esta estrategia es muy útil si las direcciones se dan sobre demanda y únicamente un número limitado de host necesitan una dirección a la vez.

El mecanismo DHCP sigue un modelo simple cliente-servidor. Un host que necesita una dirección de red se convierte en cliente al preguntar por su dirección. El sistema que responde la solicitud actúa como un servidor DHCP. La transacción DHCP concluye cuando el cliente acepta o rechaza la respuesta. Los clientes no conocen la dirección de su servidor DHCP. No obstante que el cliente ha enviado un mensaje hacia el servidor y que el mensaje tiene una dirección destino. Esto es posible porque DHCP confía en la ya conocida dirección multicast. La dirección FF02::C se refiere a todos los servidores DHCP. Cuando un cliente hace una petición del servicio DHCP lo hace utilizando su dirección de enlace local FE80::/10 como dirección origen y la dirección FF02::C como dirección destino. Sin embargo si un host conoce la dirección específica de un servidor DHCP este puede enviar directamente sus peticiones a ese servidor.

En algunos casos puede que no sea posible para el cliente y el servidor comunicarse directamente, esto se podría deber a factores como la topología de la red en donde reside el servidor DHCP. DHCP resuelve este problema al definir un tercer involucrado entre el servidor y cliente, este dispositivo se denomina transmisor DHCP o agente

DHCP. Si el cliente no encuentra un servidor DHCP, un transmisor DHCP acepta peticiones de un cliente, pero este no le responde directamente. En lugar de esto este transmite la solicitud hacia un verdadero servidor DHCP. Cuando un cliente requiere que el transmisor DHCP actúe como intermediario, envía un mensaje solicitando el servicio DHCP con su dirección de enlace local FE80::/10 como dirección origen, hacia la dirección multicast FF02::1:2, que es la que direcciona a todos los transmisores DHCP en el enlace local. Finalmente cuando el servidor DHCP envía la respuesta, lo hace también utilizando al agente DHCP como intermediario.

4.6 Seguridad IPv6.

La seguridad dentro del protocolo IPv6 está basada en el protocolo “IP Security” (IPSec) y aunque IPv4 también puede soportarlo, la diferencia radica en que para IPv6 el manejo de IPSec resulta obligatorio, esto significa que todas las comunicaciones IPv6 extremo-a-extremo pueden ser aseguradas. El protocolo IPSec se apoya en la cabecera de Autenticación (AH) y en la cabecera de Encapsulación de seguridad de la información (ESP), estas cabeceras de extensión IPv6 pueden ser encadenadas juntas dentro del mismo paquete IPv6. Se presenta a continuación una breve descripción de las cabeceras de extensión AH y ESP.

4.6.1 Cabecera de autenticación IPsec (AH).

La primera cabecera IPsec es la Cabecera de autenticación (AH). Esta proporciona integridad, y autenticación del nodo origen así como protección contra la duplicación. La cabecera de autenticación IPsec protege la integridad de la mayoría de los campos de la cabecera IPv6, excepto de aquellos que se modifican durante la ruta como por ejemplo el campo *Límite de saltos*. Además IPsec AH autentica el origen a través de un algoritmo basado en el cifrado.

4.6.2 Cabecera de Encapsulación de seguridad de la información (ESP).

La segunda cabecera IPsec es la cabecera de Encapsulación de seguridad de la información (ESP). Esta cabecera proporciona confidencialidad y autenticación del nodo origen, también se encarga de la integridad del paquete interior y de la protección contra la duplicación.

Capítulo 5

Mecanismos de coexistencia y transición IPv6

5.1 Introducción.

La tarea de convertir totalmente al Internet IPv4 hacia el protocolo IPv6 no es inmediata, es imposible que los millones de dispositivos que conforman Internet se actualicen a IPv6 de manera simultánea. Este cambio se dará de manera gradual y tomará varios años, lo que implica que durante ese lapso IPv4 e IPv6 deben interactuar y coexistir.

Uno de los aspectos más importantes que se tomaron en cuenta durante el desarrollo de IPv6, fue este periodo de coexistencia con IPv4. Para ello el IETF creó el grupo de trabajo llamado NGtrans, quien se encargó de diseñar herramientas, protocolos y mecanismos que permitieran a IPv4 e IPv6 interactuar a pesar de las diferencias entre existen entre estos.

Desde 1996 el NGtrans ha definido diversos mecanismos y protocolos de transición. Las técnicas de transición y coexistencia son fundamentalmente tres:

1. **Pila dual.** Mecanismo donde los nodos dentro de una red pueden manejar simultáneamente las pilas IPv4 e IPv6. Los nodos que incorporan la pila dual pueden comunicarse a través de redes que incorporan de igual forma ambos protocolos, estableciendo sesiones extremo-a-extremo, sobre infraestructura IPv4 o IPv6.
2. **Túneles.** Esta técnica permite que nodos o dominios IPv6 aislados, puedan comunicarse con otras redes IPv6 a través de infraestructura IPv4. Los nodos necesariamente deben incorporar la pila dual para habilitar este mecanismo.

3. **Protocolos de traducción.** Con este mecanismo los nodos que soportan solo a IPv6 pueden comunicarse con nodos que solo soportan IPv4, utilizando protocolos de traducción en la frontera entre los dos tipos de redes.

5.2 Pila dual.

La pila dual es una técnica donde hosts, servidores y routers de red manejan los protocolos IPv6 e IPv4 simultáneamente, a este tipo de nodos se les denomina también “nodos IPv4/IPv6”. La práctica de manejar dos pilas de protocolos ha sido aplicada con anterioridad, por ejemplo en sistemas que deben soportar simultáneamente IPv4 e IPX, o IPv4 y Apple talk.

Para utilizar la pila dual en los nodos, las aplicaciones basadas en IPv4 se deben modificar para soportar el protocolo IPv6, esto es necesario porque las aplicaciones IPv4 están instruidas solo para reconocer las direcciones de 32 bits. Estas aplicaciones modificadas que incorporan soporte para IPv6 se denominan Aplicaciones IPv4/IPv6.

Es necesario resaltar la diferencia entre una aplicación IPv4/IPv6 y un nodo IPv4/IPv6. El instalar la pila dual en un nodo no implica que automáticamente todas las aplicaciones hasta ese momento IPv4 puedan correr ahora sobre el protocolo IPv6. Si se llegara a tener tal apreciación es muy posible llegar a confundir el término “nodo IPv4/IPv6” con “Aplicación IPv4/IPv6”. En este punto también es importante mencionar que de aquí en adelante el término “IPv4/IPv6” se usará para describir que existe el manejo de ambos protocolos sea por parte de un nodo, una aplicación o una red. Si se hace referencia a un solo protocolo, como por ejemplo “nodo IPv6” esto quiere decir que solo existe soporte para ese protocolo específico, en este caso por parte del nodo.

Una típica aplicación IPv4 utiliza TCP o UDP como capa de transporte para entregar datos, después de que llegan a la pila se colocan dentro de paquetes IPv4. Después estos paquetes se envían hacia la interfase de red del nodo. Por ejemplo en una LAN Ethernet el identificador de protocolo que describe paquetes IPv4 dentro de tramas Ethernet es 0x0800.

La figura 5.1 muestra el procedimiento donde los datos de una Aplicación IPv4 pasan hacia una interfase de red a través de la pila IPv4.

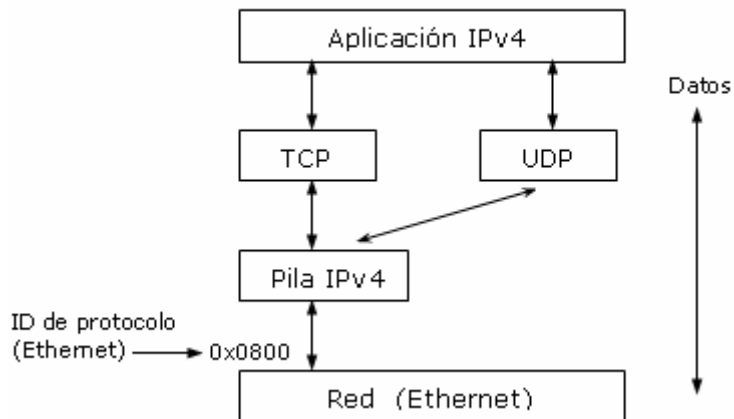


Figura 5.1 La aplicación IPv4 utiliza la pila IPv4 para enviar paquetes

Cuando una aplicación IPv4 se ha modificado para soportar simultáneamente al protocolo IPv6, se habilita una función que le permite manejar direcciones de 128 bits. Entonces la aplicación podrá seleccionar la pila para crear los paquetes de datos.

Como se presenta en la figura 5.2, una aplicación IPv4/IPv6 utiliza TCP o UDP como protocolos de transporte. Si la aplicación selecciona la pila IPv6, construye los paquetes sobre IPv6 y estos se envían a la interfase de red. Para una LAN Ethernet el identificador de protocolo que describe paquetes IPv6 dentro de tramas Ethernet es 0x86DD.

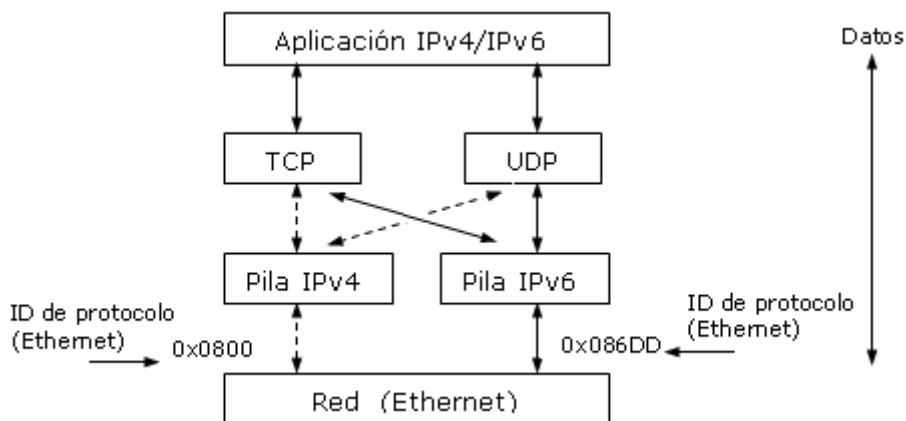


Figura 5.2 Una aplicación que soporta IPv4 e IPv6

Un nodo que soporta una aplicación IPv4/IPv6, no deja al azar la elección de la pila sobre la que ha de comunicarse. Existen dos métodos que obligan a un nodo IPv4/IPv6 a utilizar la pila IPv6 cuando se dispone de conectividad IPv6:

1. **Manual.** Si el usuario conoce la dirección IPv6 del hostname destino este puede ingresarla directamente para establecer la sesión. Esta opción a pesar de ser útil en ciertas circunstancias no resulta práctica para aplicaciones frecuentes.
2. **Servicio de nombramiento.** Esta técnica requiere configurar un Dominio totalmente calificado (FQDN) en el servicio de nombramiento (DNS) con direcciones IPv4 y con direcciones IPv6. Un FQDN es un nombre entendible, que incluye el nombre de la computadora y el nombre de dominio asociado a la misma. Por ejemplo, dada la computadora llamada “cuautitlan” y el nombre de dominio “unam.mx”, el FQDN será “cuautitlan.unam.mx”. El FQDN podría resolver direcciones IPv4 representadas por un registro A o direcciones IPv6 representadas por registros AAAA en el servidor DNS. Incluso el mismo FQDN podría estar disponible para ambos tipos de dirección.

Por lo tanto al utilizar el servicio DNS se tienen los siguientes escenarios:

- Solicitud para una dirección IPv4. La aplicación IPv4 le solicita a un servidor DNS resolver el FQDN a un registro A (dirección IPv4). Si el DNS le contesta a la aplicación con un registro A, esta se comunicará con el hostname usando la dirección IPv4 recibida.
- Solicitud para una dirección IPv6. En este caso la aplicación IPv6 le solicita a un servidor DNS resolver un FQDN a un registro AAAA (dirección IPv6). Si el DNS le contesta a la aplicación con un registro AAAA, esta se comunica con el hostname utilizando la dirección IPv6 recibida.
- Solicitud para ambos tipos de direcciones. La aplicación IPv4/IPv6 solicita al servidor DNS resolver un FQDN a direcciones IPv6 e IPv4. La aplicación primero buscará un registro AAAA, si no lo encuentra opta por buscar un registro A, para comunicarse con el hostname.

5.2.1 Solicitud de una dirección IPv4.

La figura 5.3 muestra el proceso donde la aplicación IPv4 del nodo IPv4/IPv6, solicita al servidor DNS resolver el FQDN `www.ejemplo.org`, dentro de un registro A (1). Entonces el servidor le responde al nodo especificando la dirección IPv4 que sirve de ejemplo `220.110.55.5`, como la dirección que pertenece al FQDN `www.ejemplo.org` (2). Finalmente la aplicación IPv4 obliga al nodo IPv4/IPv6 a establecer una sesión con la dirección IPv4 `220.110.55.5` como destino (3).

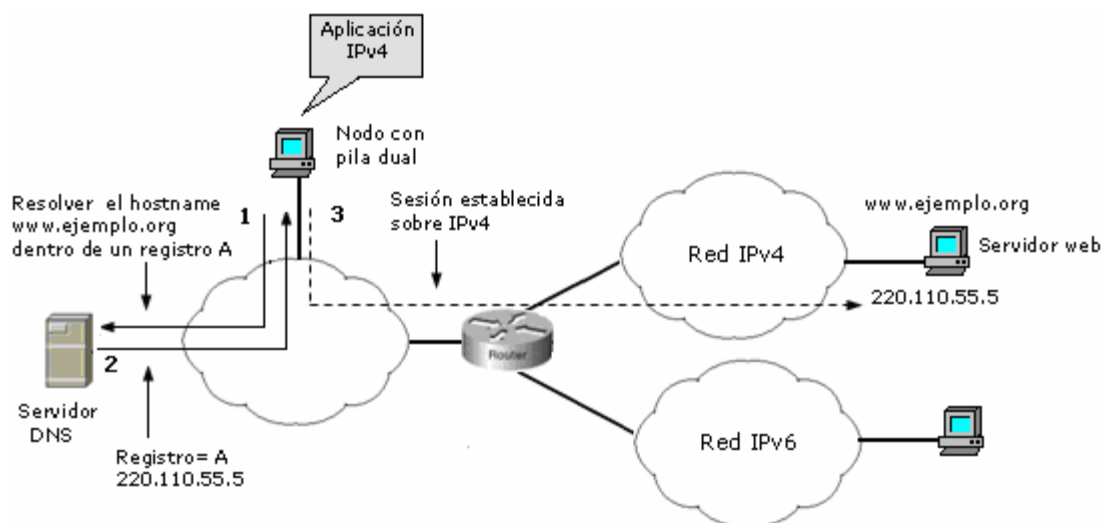


Figura 5.3 Aplicación IPv4 solicitando registros A al servidor DNS

5.2.2 Solicitud de una dirección IPv6.

Por otro lado, como se presenta en la figura 5.4 una aplicación IPv6, solicita a un servidor DNS la dirección IPv6 del FQDN con el cual se quiere comunicar. La aplicación IPv6 del nodo IPv4/IPv6 solicita a un servidor DNS resolver el FQDN `www.ejemplo.org`, a un registro AAAA (1). Después el servidor responde al nodo especificando la dirección destino `2001:b00:ffff:a::1` (2). Finalmente la aplicación IPv6 al encontrar respuesta a su solicitud obliga al nodo a establecer una sesión hacia la dirección IPv6 `2001:b00:ffff:a::1` como destino (3).

Es importante señalar que las solicitudes enviadas a los servidores DNS pueden hacerse sobre redes IPv4 o IPv6, el tipo de dirección solicitada al servidor DNS es independiente al protocolo utilizado para transportar esta solicitud.

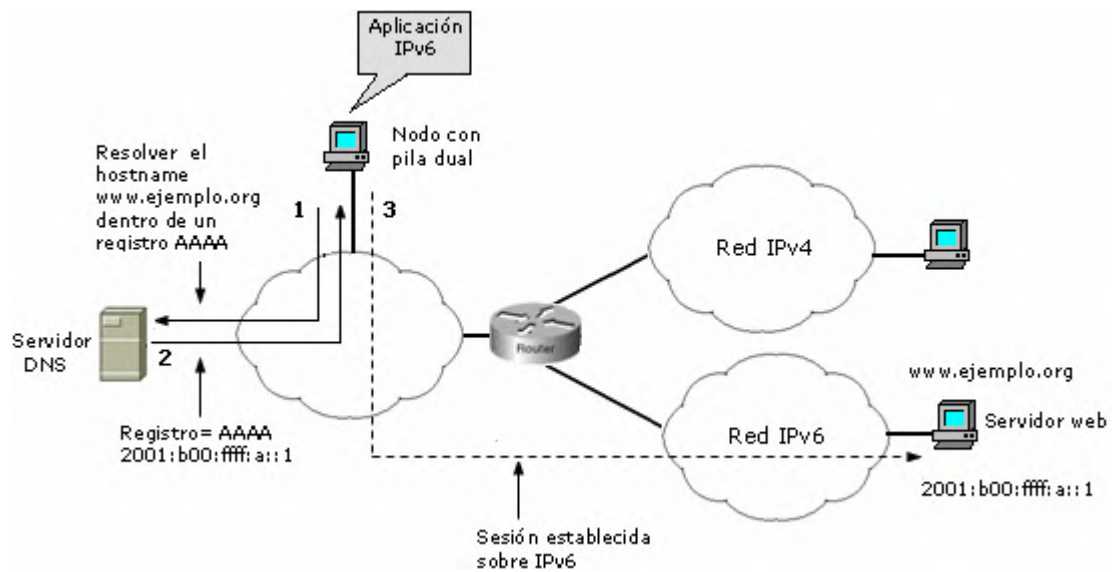


Figura 5.4 Aplicación IPv6 solicitando registros AAAA al servidor DNS

5.2.3 Solicitud de direcciones IPv4 e IPv6.

Como lo muestra la figura 5.5 una tercera posibilidad es que la aplicación del nodo sea IPv4/IPv6.

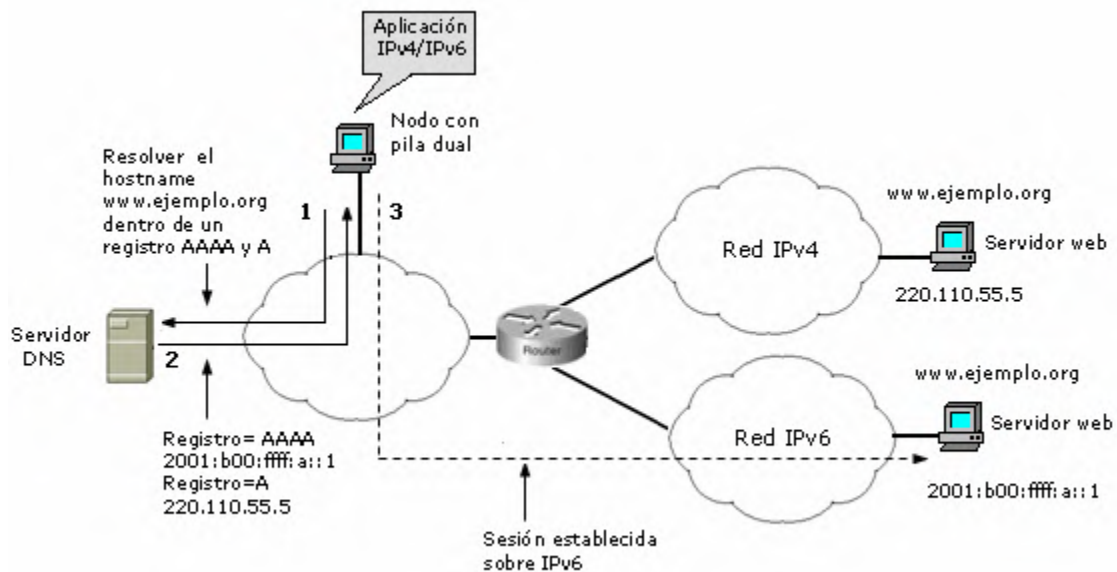


Figura 5.5 Aplicación IPv4/IPv6 solicitando registros A y AAAA al servidor DNS

5.3 Túneles IPv6.

Los túneles se utilizan por lo general para transportar, protocolos incompatibles o datos especiales sobre una red existente. El establecimiento de túneles proporciona

una forma básica para que nodos o islas IPv6 *constituidas con host, routers y servidores* IPv6 accedan a otras redes IPv6 a través de infraestructura IPv4. Como lo muestra la figura 5.6, el túnel se establece entre dos islas IPv6 a través de una red IPv4 que en este caso es Internet. Los routers ubicados en la frontera que separa a las islas IPv6 de la red IPv4 dominan el proceso de transportar paquetes IPv6 a través de infraestructura IPv4. Este mecanismo solo debe ser considerado cuando no sea posible obtener conectividad IPv6 nativa en redes, enlaces e infraestructura.

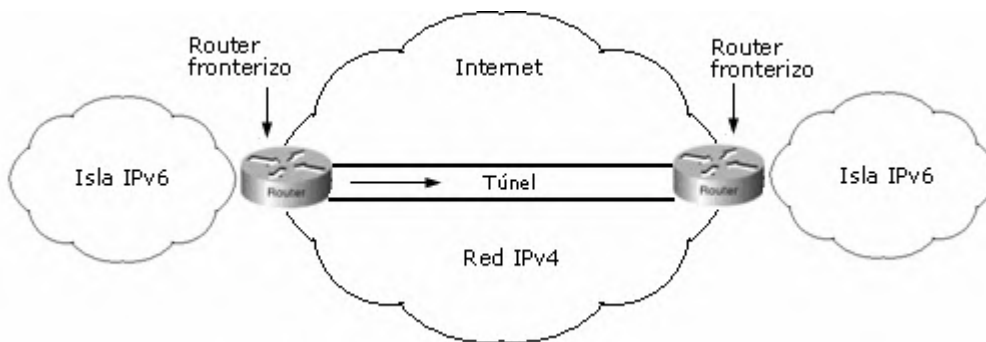


Figura 5.6 Túnel establecido entre islas de nodos IPv6 a través de infraestructura IPv4

La figura 5.7 muestra que cuando los paquetes IPv6 son transportados a través de los túneles nunca se modifica su encabezado original ni su carga útil, únicamente se encapsulan dentro de paquetes IPv4, por lo tanto la cabecera interior contiene la dirección IPv6 origen y destino de la sesión IPv6 "extremo-a-extremo" y la cabecera exterior contiene las direcciones origen y destino IPv4 de los extremos del túnel (routers fronterizos).

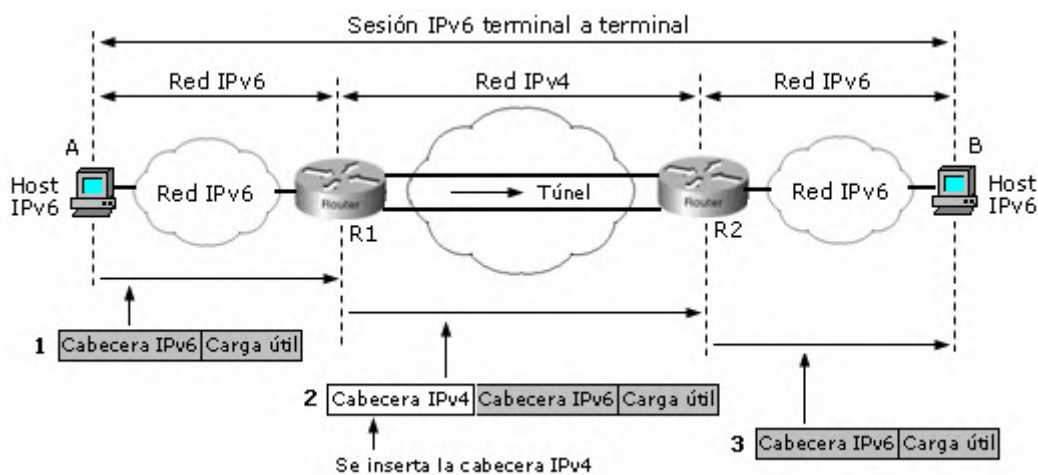


Figura 5.7 Paquetes IPv6 entregados a través de un túnel sobre IPv4

En cada extremo del túnel se realiza la encapsulación y desencapsulación de los paquetes IPv6, lo que implica que en los dispositivos ubicados en estos extremos se debe implementar la pila dual para poder realizar esta tarea.

En el ejemplo de la figura 5.7 el nodo IPv6 A conoce la dirección IPv6 del nodo B y pretende establecer una sesión IPv6 extremo-a-extremo con este. Las redes IPv6 donde residen estos nodos están aisladas pero conectadas a través de una red IPv4. Se ha establecido un túnel entre los routers R1 y R2 para poder transportar los paquetes IPv6 a través de la infraestructura IPv4 existente.

El nodo A inicia la sesión “extremo-a-extremo” enviando un paquete IPv6 hacia la dirección del nodo B. Como el nodo B está dentro de una red IPv6, el paquete que se entrega al router R1 es un paquete IPv6. El router R1 que actúa como punto de entrada del túnel, encapsula el paquete IPv6 dentro de un paquete IPv4, enviándolo hacia el router R2 a través de la red IPv4. Cuando el router R2 recibe el paquete IPv4, este actúa como el extremo final del túnel y desencapsula el paquete IPv6. Finalmente el router R2 envía el paquete IPv6 hacia el host B como destinatario. Durante este proceso el encabezado y la carga útil del paquete IPv6 permanecen intactos. El campo *Número de protocolo* dentro de la cabecera IPv4 contiene el valor 41 para especificar la encapsulación de un paquete IPv6 dentro de un paquete IPv4.

Los túneles se pueden establecer en tres contextos diferentes:

- Host a Host. Un host IPv4/IPv6 aislado dentro de una red IPv4 puede establecer un túnel hacia otro host con las mismas características. Esta arquitectura permite el establecimiento únicamente de sesiones “extremo-a-extremo” entre los host.
- Host a Router. Un host IPv4/IPv6 aislado dentro de una red IPv4 puede establecer un túnel hacia un router IPv4/IPv6. El router puede tener conectividad nativa en alguna otra de sus interfaces. Esta arquitectura proporciona el establecimiento de sesiones IPv6 extremo-a-extremo entre cualquier host destino IPv6 a través del router.

- Router a router. Un router IPv4/IPv6 dentro de una red IPv4 pueden establecer un túnel hacia otro router IPv4/IPv6. Los routers pueden interconectar islas IPv6.

Mecanismos para establecer túneles.

Existen una serie de técnicas y protocolos definidos por el IETF diseñados para el establecimiento de túneles, a continuación se enlistan algunas de estas técnicas en orden de importancia.

- Túnel configurado
- Túnel broker
- Túnel Server
- 6to4
- ISATAP
- Túnel automático compatible con IPv4^{5.1}.

Todas estas técnicas requieren que tanto los nodos y los routers que actúan como extremos del túnel incorporen la pila dual.

5.3.1 El túnel configurado.

El túnel configurado fue una de las primeras técnicas de transición soportadas por IPv6, por esa razón es el mecanismo que más se utiliza en implementaciones IPv6. Los túneles configurados son habilitados y configurados estáticamente en los nodos IPv4/IPv6. En cada extremo del túnel configurado se deben asignar las siguientes direcciones para poder configurar la interfase del túnel:

- Dirección local IPv4. Es la dirección que identifica al nodo local IPv4/IPv6 dentro de la red IPv4. La dirección local IPv4 también se utiliza como la dirección IPv4 origen del tráfico saliente.
- Dirección IPv4 far-end. Es la dirección del nodo IPv4/IPv6 que opera como el otro extremo del túnel y que identifica a este nodo dentro de la red IPv4. También se utiliza como dirección destino para el tráfico saliente.

5.1 Este mecanismo está actualmente obsoleto.

- Dirección local IPv6. Es la dirección IPv6 asignada localmente en la interfase del túnel.

Un túnel configurado es considerado un enlace punto-a-punto. En entornos IPv6 lo más recomendable para enlaces punto-a-punto es asignar las respectivas direcciones IPv6 local y far-end dentro del mismo prefijo /64, por lo tanto la longitud del prefijo recomendada para un enlace punto-a-punto es de /64 o incluso /128 cuando se está seguro de que únicamente un dispositivo es conectado. La figura 5.8 muestra el ejemplo de un túnel configurado. La red A IPv6 representada por el prefijo 2001:b00:ffff::/48 y la red B IPv6 que utiliza el prefijo 2001:420:ffff::/48 se conectan a través de un túnel configurado. La dirección IPv4 que se asigna a la interfase del router R1 el cual se desempeña como un extremo del túnel configurado es 206.123.31.200 y la dirección IPv6 asignada a la misma interfase del router es 2001:b00:ffff:2::1/64. El router R2 utiliza la dirección IPv4 132.214.1.10 y también la dirección IPv6 2001:b00:ffff:2:2/64, en la interfase que funciona como extremo final del túnel. Las direcciones IPv6 asignadas en ambos extremos del túnel configurado están dentro de la misma subred (el mismo prefijo /64).

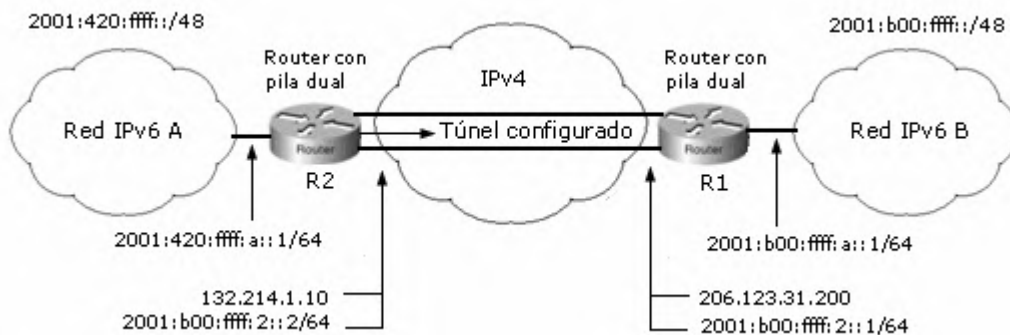


Figura 5.8 Direcciones asignadas a las interfaces de un túnel configurado

Sólo hasta que se hayan configurado apropiadamente todas las direcciones de interfase del túnel configurado y se haya habilitado el enrutamiento IPv6 en los routers es posible el envío de paquetes IPv6 entre las dos redes IPv6 en ambos extremos del túnel configurado.

5.3.2 El túnel Broker.

El túnel broker es un mecanismo que facilita la creación de túneles configurados sobre redes IPv4. El túnel broker es un sistema externo en lugar de un router que actúa como un servidor en la red IPv4, este recibe solicitudes de nodos IPv4/IPv6 para establecer túneles.

Los usuarios hacen las solicitudes al túnel broker vía HTTP, usando redes IPv4. Los usuarios generalmente llenan un registro (página web) solicitando un túnel configurado para sus host. El túnel broker envía la respuesta sobre HTTP con la información necesaria (direcciones IPv4, direcciones IPv6 y rutas IPv6 por defecto) que el usuario debe aplicar en su host para habilitar su extremo del túnel. El túnel broker puede opcionalmente proporcionar un "script" al nodo IPv4/IPv6 para facilitarle su configuración, este script es generalmente un pequeño programa que el usuario instala y que automáticamente genera la configuración que requiere el nodo para habilitar el túnel. Finalmente el túnel broker aplica remotamente instrucciones a un router IPv4/IPv6 que funciona como el otro extremo del túnel (configura la dirección far-end) para así completar la configuración en ambos extremos del túnel. Este router IPv4/IPv6 debe estar conectado a un dominio IPv6. Cuando se han configurado adecuadamente el nodo del cliente y el router, el túnel es establecido y entonces puede usarse para realizar sesiones IPv6 extremo-a-extremo sobre una red IPv4. Este proceso se ilustra en la figura 5.9.

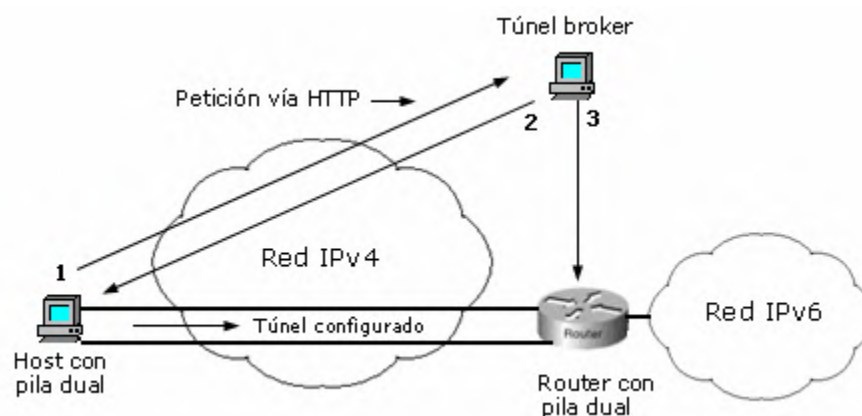


Figura 5.9 Proceso para establecer un túnel mediante el mecanismo túnel broker

El modelo del túnel broker asume que tanto el túnel broker como el router que se desempeña como extremo del túnel configurado son administrados por una misma organización y que esta cumple con los permisos necesarios para operar el router de manera segura.

5.3.3 Túnel Server.

El túnel Server es un modelo que simplifica el mecanismo del túnel broker, donde el broker y el router conforman una sola entidad o sistema, en lugar de tenerlos separadamente. La manera en la que se le solicita al túnel Server un túnel es el mismo con respecto al túnel broker, es decir usando HTTP sobre redes IPv4. La forma en que se establece un túnel mediante el túnel Server se muestra en la figura 5.10.

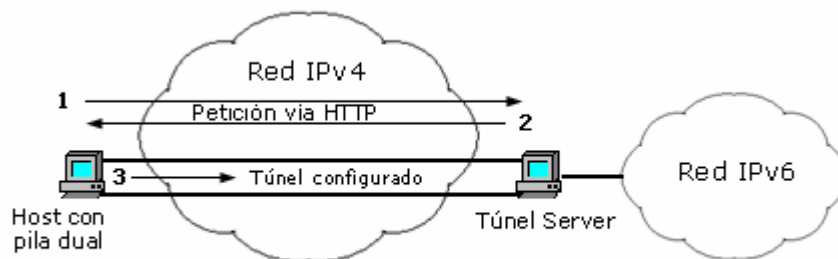


Figura 5.10 Proceso para establecer un túnel mediante el mecanismo túnel broker

Un host IPv4/IPv6 se comunica con el túnel Server sobre IPv4 utilizando el servicio HTTP, el usuario se registra llenando con sus datos una página web y entonces el túnel broker responde al usuario con la información necesaria para que este habilite a su host como un extremo del túnel. El túnel broker aplica de manera local la configuración para habilitar el extremo far-end del túnel. Cuando ambos extremos se han configurado adecuadamente, es cuando el túnel se establece.

El túnel Server y el túnel broker se consideran procedimientos que mecanizan el establecimiento de túneles configurados en nodos IPv4/IPv6 que forman parte de redes IPv4 sin manuales de operación.

5.3.4 6to4

Para algunas organizaciones el manejo de túneles configurados establecidos estáticamente no es una opción viable. El mecanismo 6to4 se creó con la finalidad de facilitar la implementación de túneles para aquellas organizaciones a las que les resulta poco conveniente el manejo estático de túneles. El mecanismo 6to4 tiene las siguientes características:

- 6to4 tiene una función que permite establecer túneles dinámicamente entre islas IPv6. No se necesita configurar manualmente las direcciones IPv4 origen y destino para habilitar los túneles. Los túneles se habilitan dinámicamente de acuerdo con las direcciones destino IPv6 de los paquetes originados desde algún nodo IPv6 ubicado dentro de un sitio 6to4. El mecanismo 6to4 también encapsula paquetes IPv6 dentro de paquetes IPv4 y utiliza redes IPv4 como medio de transporte.
- El mecanismo 6to4 es incorporado en los routers que delimitan la frontera de los sitios 6to4. Estos routers 6to4 deben ser capaces de alcanzar otros routers y sitios 6to4 utilizando infraestructura IPv4.
- El mecanismo 6to4 ofrece una gran ventaja al proporcionar automáticamente un prefijo IPv6 unicast de agregación global a cada sitio 6to4.
 - Los prefijos 6to4 están por completo basados en el espacio de dirección 2002::/16 asignado por la IANA.
 - Cada sitio 6to4 asigna al menos una dirección unicast IPv4 global a un router dentro de sus dominios. Esta dirección de 32 bits se convierte al formato hexadecimal y se añaden al prefijo 2002::/16 por lo que la representación final de la dirección es 2002:<dirección IPv4>::/48
 - Cada sitio 6to4 adquiere entonces un prefijo /48 que se basa en su direccionamiento unicast IPv4, los siguientes 16 bits al prefijo /48 son para construir subredes dentro del dominio IPv6 detrás del router 6to4, por lo que se pueden crear 65,535 subredes.

En la figura 5.11 se muestra a los routers A y B habilitados como routers 6to4.

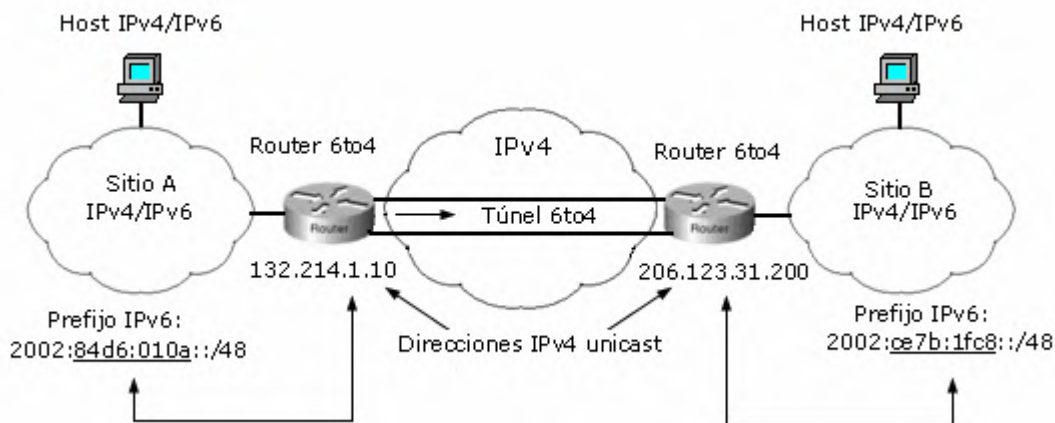


Figura 5.11

El router A usa la dirección unicast IPv4 132.214.1.10 (por ejemplo) y el router B utiliza la dirección 206.123.31.200. Por lo que el prefijo IPv6 del sitio A IPv6/IPv4 es 2002:84d6:010a::/48, donde 84d6:010A es la representación hexadecimal de 132.214.1.10. El sitio B IPv4/Pv6 utiliza el prefijo 2002:ce7b:1fc8::/48 el cual esta basado en la dirección IPv4 206.123.31.200. Cuando un host dentro del sitio A envía paquetes IPv6 hacia la dirección 2002:ce7b:1fc8::/48 como dirección destino, o cuando un host dentro del sitio B envía paquetes hacia la red destino 2002.84d6:010a::/48 se establece el túnel 6to4.

La operación del mecanismo 6to4 esta basada en el direccionamiento y en la infraestructura de enrutamiento de Internet IPv4, por lo que se tienen algunas consideraciones:

- Debido a que el prefijo IPv6 del sitio 6to4 esta basado en la dirección unicast IPv4 globalmente única del router fronterizo, cualquier cambio de esta dirección obliga la completa renumeración del sitio 6to4.
- El uso del espacio de dirección privado como 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16 está prohibido para la implementación de routers 6to4 en Internet.
- Tan pronto como un router 6to4 es habilitado como un router fronterizo, este debe aceptar paquetes encapsulados desde cualquier router 6to4 en Internet. Esta situación requiere tomar medidas en materia de seguridad como filtrar o bloquear el tráfico 6to4 entrante, basándose en la dirección IPv4 origen. La

razón de esto es que usuarios maliciosos podrían habilitar sitios 6to4 por cortos periodos de tiempo.

El mecanismo 6to4 habilitado en un router fronterizo permite el envío de paquetes IPv6 hacia cualquier destino dentro del prefijo 2002::/16 sobre la infraestructura existente IPv4. Sin embargo otros prefijos unicast de agregación global son usados en Internet IPv6 como por ejemplo 2001::/16. Estos prefijos diferentes a 2002::/16 son inalcanzables a menos que uno de los routers 6to4 en el Internet IPv4 ofrezca actuar como un intermediario para enviar tráfico 6to4 a Internet IPv6. Un router 6to4 que proporciona envío de tráfico hacia el Internet IPv6 es llamado "relay 6to4". Un relay 6to4 está generalmente entre la frontera del Internet IPv4 y el Internet IPv6. En su interfase que conecta hacia el Internet IPv6, el router 6to4 publica la ruta 2002::/16 como un participante de la red de enrutamiento unicast IPv6. La figura 5.12 muestra un ejemplo donde el router B actúa como un relay 6to4.

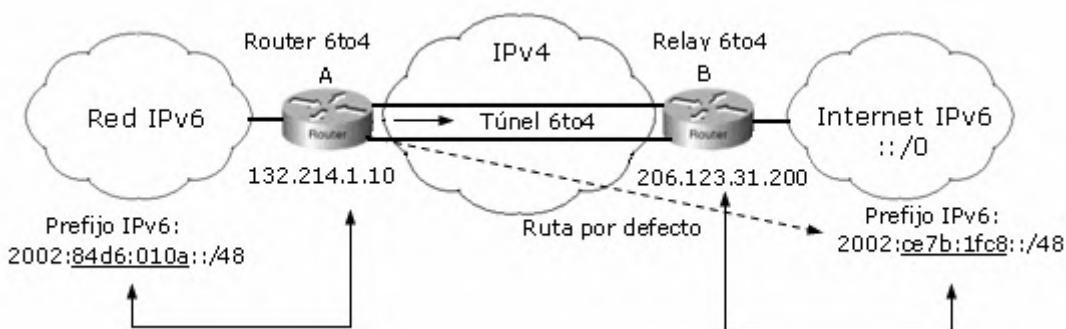


Figura 5.12

La configuración del router B es similar a la del router 6to4, excepto por la configuración de enrutamiento. El router B adquiere rutas desde el Internet IPv6 y este puede enviar los paquetes recibidos IPv6 desde los sitios 6to4 (prefijo 2002::/16) hacia el Internet IPv6. Para poder usar un relay 6to4, el router 6to4 debe añadir una ruta por defecto en su configuración apuntando hacia el relay 6to4. Por lo tanto todo el tráfico que no es 6to4 es enviado hacia el Internet IPv6 a través del relay 6to4.

El primer paso antes de habilitar una ruta por defecto hacia el Internet IPv6 a través del relay 6to4 es encontrar la dirección IPv4 de un relay 6to4 público. Para ayudar a los sitios 6to4 a encontrar un relay 6to4 en Internet se ha presentado un prefijo anycast

para el relay 6to4 desde donde los paquetes 6to4 son automáticamente enrutados hacia el relay 6to4 más cercano en el Internet IPv4.

La IANA ha asignado al relay 6to4 el prefijo anycast 192.88.99.0/24 exclusivamente para enrutar automáticamente los paquetes 6to4 hacia el relay 6to4 más cercano. La dirección IPv4 definida en este prefijo anycast para alcanzar al relay 6to4 más cercano es 192.88.99.1. Por lo tanto, la representación de esta dirección en IPv6 es 2002:c058:6301::.

5.3.5 El Túnel ISATAP.

El Protocolo de direccionamiento de túneles automáticos intrasitio (ISATAP), es un mecanismo que transporta paquetes IPv6 a través de sitios IPv4, para crear una red virtual IPv6 sobre infraestructura IPv4. Las características del mecanismo ISATAP son las siguientes:

- El túnel ISATAP se establece entre dos hosts o entre un host y un router, estos dispositivos deben soportar el protocolo ISATAP. Los túneles ISATAP son automáticos por lo tanto los nodos no requieren configuración manual adicional. La comunicación entre un host y un router ISATAP, demanda que el host inicialmente ubique la dirección IPv4 del router dentro de una lista de routers ISATAP potenciales, esta lista contiene las direcciones IPv4 que representan a todos los routers ISATAP dentro de un sitio.
- Las direcciones ISATAP que se asignan a los nodos se conforman por el prefijo unicast IPv6 de agregación global dedicado a la operación ISATAP y por el identificador de interfase.
- Un host adquiere una dirección ISATAP utilizando el prefijo de enlace local (FE80::/10). Se debe asignar un prefijo /64 de agregación global o de sitio local al sitio para habilitar la operación ISATAP. Los nodos adquieren este prefijo /64 por medio de los mensajes de publicación que envían los routers ISATAP a través de túneles ISATAP establecidos sobre IPv4.
- ISATAP obtiene el identificador de interfase a partir de la dirección IPv4 (sea esta pública o privada) asignada al dispositivo, El identificador de interfase se construye al añadir los 32 bits de la dirección IPv4 al valor 0000:5EFE, este

valor está reservado por la IANA para la operación ISATAP. Por lo tanto una dirección ISATAP tiene el siguiente formato:

[Prefijo de 64 bits]:0000:5EFE:<dirección IPv4>

- Después de que el host ISATAP es habilitado con su dirección de enlace local usando el formato ISATAP en los 64 bits de menor orden, este envía una solicitud de router hacia un router ISATAP a través de un túnel ISATAP. Después el router ISATAP responde con un mensaje de publicación de router hacia el host ISATAP, y este especifica el prefijo ISATAP definido dentro del sitio. Después de recibir el prefijo ISATAP, el host ISATAP configura su dirección IPv6 unicast de agregación global basada en este formato ISATAP. EL host ISATAP usa la dirección de enlace local del router ISATAP como la dirección por defecto del router IPV6.

5.3.6 Mecanismo Teredo.

El mecanismo para establecer túneles Teredo, también conocido como “shipworm” tiene la particularidad de que puede entregar paquetes IPv6 a los nodos IPv4/IPv6 ubicados detrás de dispositivos NAT dentro de dominios IPv4 (los túneles configurados y el mecanismo 6to4 son incompatibles con dispositivos NAT).

El tráfico IPv6 desde los hosts Teredo puede atravesar dispositivos NAT porque se encapsula dentro de mensajes UDP IPv4. Si el dispositivo NAT permite la traducción de puertos UDP, entonces puede soportar el mecanismo Teredo. La siguiente lista describe los principales componentes del mecanismo Teredo:

- Servidor Teredo. El servidor Teredo es el dispositivo que maneja la señalización del tráfico para los clientes Teredo, este se conecta al Internet IPv4 y puede ser alcanzado usando una dirección unicast global IPv4.
- Relay Teredo. Es un dispositivo que actúa como un router IPv6. El relay Teredo se conecta al Internet IPv6 y les proporciona a los clientes Teredo conectividad IPv6 por medio de paquetes UDP.

- El cliente Teredo. Un cliente Teredo es un host que puede obtener la asignación de una dirección Teredo, administrar asignaciones NAT y dirigir el tráfico IPv6 por un túnel a través de Internet IPv4.

5.3.7 Entornos específicos de cada mecanismo para establecer túneles.

Aunque existen muchos mecanismos para establecer túneles para el transporte de paquetes IPv6 sobre infraestructura IPv4 existente, se debe señalar que hay escenarios específicos para la implementación de cada uno de estos. Por ejemplo el túnel configurado y el mecanismo 6to4 debido a sus características, se utilizan para interconectar sitios. El túnel ISATAP se utiliza principalmente para interconectar a hosts con routers exteriores dentro de un dominio IPv4. El túnel Server y el túnel Broker se utilizan para establecer conectividad IPv6 a gran escala en nodos aislados que pertenecen a dominios IPv4. El túnel Teredo entrega conectividad IPv6 a nodos que se encuentran detrás de dispositivos NAT. Mientras que el túnel automático compatible con IPv4 se encuentra actualmente obsoleto.

5.4 Mecanismos de Traducción.

Se han especificado otros mecanismos de transición con los cuales se permite que los nodos pertenecientes a dominios IPv6 puedan comunicarse con nodos ubicados dentro de dominios IPv4, sin que para esto se requiera incorporar la pila dual en estos nodos. Esta interacción entre dispositivos que no son IPv4/IPv6 puede lograrse a partir de la traducción de las aplicaciones y de la traducción de direcciones IPv4-Pv6. A continuación se presentan los mecanismos de traducción más importantes.

5.4.1 Gateway de nivel de aplicación (ALGs)

El mecanismo ALG consta de una arquitectura de red en la cual un gateway que soporta la pila dual permite que nodos dentro de dominios IPv6 se comuniquen con nodos que pertenecen a dominios IPv4. La figura 5.13 muestra una arquitectura de red en la cual se ubica un ALG entre dominios IPv6 e IPv4. El host A ubicado dentro de la red IPv6 establece una sesión IP con el servidor B IPv4 a través del ALG C. El ALG C mantiene una sesión independiente con el host A utilizando IPv6 como protocolo de transporte y otra sesión independiente con el servidor B utilizando IPv4.

El ALG C que se ubica dentro de una subred que soporta la pila dual, se encarga de convertir la sesión IPv6 hacia IPv4 y viceversa. El ALG C también debe manejar la pila dual para poder realizar la traducción.

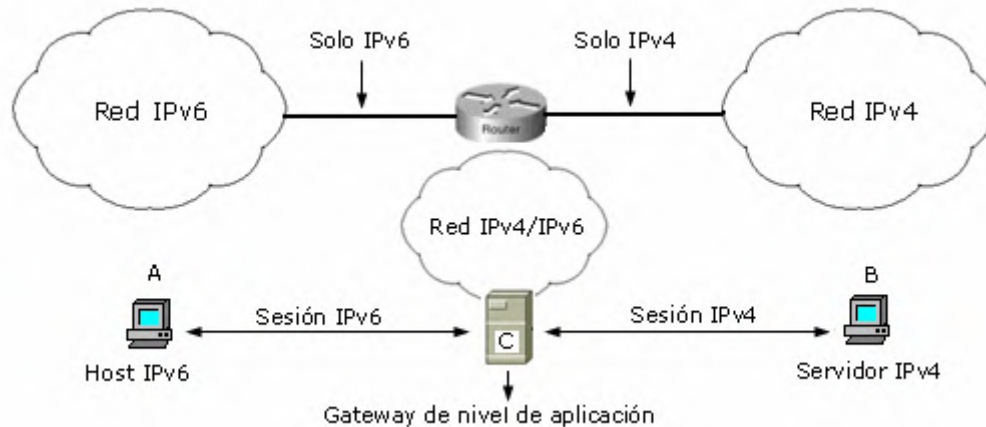


Figura 5.13 Sesión establecida entre nodos IPv6 e IPv4 utilizando un traductor de aplicación (ALG)

El método ALG se utiliza para la transición de aplicaciones Internet, como el correo electrónico, la Web entre otros:

- Correo electrónico. Los Host IPv6 pueden enviar mensajes de correo electrónico a su servidor local SMTP utilizando únicamente dominios IPv6. Después de recibir los mensajes, el servidor local SMTP que necesariamente debe ser IPv4/IPv6, se convierte en un dispositivo ALG para SMTP y envía estos mensajes hacia los servidores destino SMTP en Internet. El dispositivo ALG primero intenta alcanzar servidores SMTP destino a través de IPv6 mediante el servicio DNS. Si no encuentra ningún servidor válido dentro de dominios IPv6 opta por utilizar dominios IPv4 para entregar los mensajes, realizando la traducción correspondiente de la aplicación.
- Web. Un host IPv6 puede configurar su navegador de Internet para que a través de dominios IPv6 pueda comunicarse con cualquier sitio Web IPv4 en Internet utilizando como intermediario un servidor Web (Proxy). Este servidor Web se habilita dentro de la red local para que se desempeñe como un ALG para la aplicación HTTP. El servidor Web convertido en un ALG recibe a través de dominios IPv6 las peticiones HTTP enviadas por los hosts. El servidor Web primero intenta alcanzar a los servidores web destino a través de dominios

IPv6, utilizando el servicio DNS. Si no encuentra ningún servidor válido dentro de dominios IPv6 opta por utilizar IPv4 para entregar los mensajes realizando la traducción de aplicación.

La técnica del gateway de nivel de aplicación tiene una gran ventaja debido a que es un mecanismo transparente para los usuarios finales, es decir los usuarios no perciben que se está llevando a cabo un proceso de traducción a nivel de aplicación. Está implícito que este método de traducción requiere aplicaciones con soporte para ambos protocolos.

5.4.2 NAT-PT.

Otra técnica que permite a los nodos IPv6 comunicarse con nodos IPv4 es el “Network Address Translation Protocol Translation” (NAT-PT). NAT-PT es un mecanismo similar al NAT IPv4, que traduce direcciones IPv6 a direcciones IPv4 y viceversa. El mecanismo NAT-PT está basado en el algoritmo “Stateless IP/ICMP Traductor” (SIIT). El algoritmo SIIT traduce las cabeceras de paquete entre IPv4 e IPv6, incluyendo también a las cabeceras ICMP. De manera similar al mecanismo ALG, NAT-PT no requiere que los nodos soporten la pila dual para establecer comunicación entre estos. NAT-PT involucra traducción de direcciones de red y protocolos de traducción. La operación del mecanismo NAT-PT demanda una configuración de enrutamiento específico dentro de la red, en la cual todos los paquetes IPv6 direccionados hacia un prefijo predefinido /96 deben enrutarse hacia el dispositivo NAT-PT. Dentro del dominio IPv6 se debe reservar este prefijo /96 para habilitar la operación NAT-PT. Bajo estas condiciones, el dispositivo NAT-PT traduce las direcciones IPv6 destino contenidas dentro del prefijo /96 en direcciones IPv4 de acuerdo a sus reglas de mapeo.

En la figura 5.14 se ilustra la implementación de un dispositivo NAT-PT en la frontera de una red A IPv6 y el Internet IPv4.

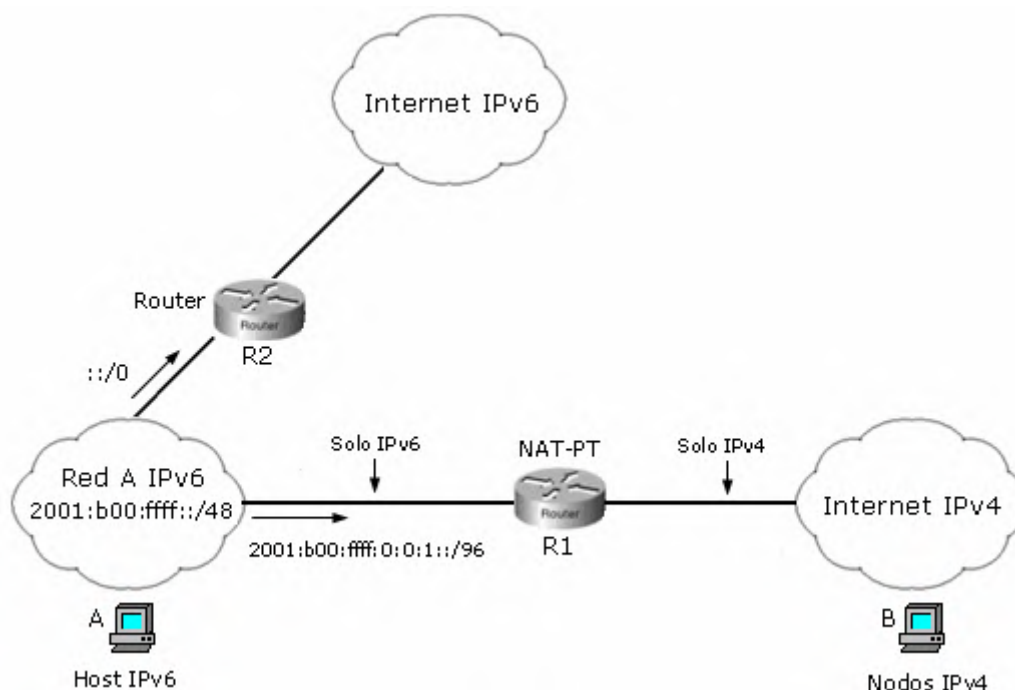


Figura 5.14 Comunicación entre nodos IPv6 e IPv4 a través del dispositivo NAT-PT

Dentro de la red A se ha configurado el prefijo 2001:b00:ffff:0:0:1::/96 para la operación NAT-PT. Los paquetes que se originan desde la red A y que utilizan direcciones destino con el prefijo 2001:b00:ffff:0:0:1::/96 se envían hacia el router R1, que desempeña el papel de dispositivo NAT-PT. Entonces las direcciones IPv6 dentro de los paquetes se traducen a direcciones IPv4 y se entregan a los nodos IPv4 a través de Internet IPv4. En este caso la red IPv6 tiene un enlace nativo IPv6 hacia el Internet IPv6. Se ha configurado una ruta IPv6 por defecto en la red IPv6 que apunta hacia el router R2 para acceder al Internet IPv6.

Los diferentes tipos de operación definidos para el mecanismo NAT-PT son los siguientes:

- NAT-PT estático. El modo estático proporciona mapeo “uno-a-uno” entre la dirección IPv6 y la dirección IPv4. Cada dirección IPv4 que debe ser alcanzada por los nodos IPv6 se debe configurar en el dispositivo NAT-PT. El destino de cada dirección IPv4 se mapea en el dispositivo NAT-PT hacia una dirección IPv6 en el prefijo predefinido NAT-PT. Este modo requiere una dirección IPv4 origen por cada mapeo IPv6 a IPv4. Este modo es muy similar al NAT estático en IPv4.

- NAT-PT dinámico. El modo dinámico también proporciona el mapeo “uno-a uno” pero utilizando un grupo de direcciones IPv4 en lugar de una sola dirección IPv4. El número de direcciones origen IPv4 dentro del conjunto determina el número máximo de traducciones simultáneas IPv6 a IPv4. Los nodos IPv6 añaden dinámicamente la dirección destino IPv4 al prefijo predefinido NAT-PT. Este modo requiere un conjunto de direcciones IPv4 para realizar la traducción dinámica. El modo dinámico NAT-PT es similar al NAT dinámico en IPv4.
- NAPT-PT. El “Network Address Port Translation- Protocol Translation” proporciona un mapeo dinámico “muchos-hacia uno”. Es decir múltiples direcciones IPv6 en el prefijo NAT-PT y una sola dirección origen IPv4. Esta traducción se realiza simultáneamente en la capa 3 (IPv6/ IPv4) y en las capas superiores (TCP/UDP). El NAPT-PT es similar al traductor de puertos NAT en IPv4 y tiene las mismas limitaciones: solamente puede traducir los protocolos ICMP, TCP y UDP.
- NAT-PT DNS ALG. EL mapeo dinámico NAT-PT puede ser combinado con un gateway de nivel de aplicación (ALG) DNS para traducir las transacciones DNS y construir automáticamente las direcciones traducidas de los nodos destino. NAT-PT puede interceptar las peticiones DNS (petición de registro A) originados desde la red IPv6, hacia la red IPv4. Un servidor DNS o incluso un nodo en la red IPv6 deben primero enviar una petición hacia un servidor DNS IPv4 a través del dispositivo NAT-PT. Entonces el NAT-PT traduce automáticamente el contenido de la respuesta DNS (registro A) hacia una dirección IPv6 (registro AAAA). El mapeo NAT-PT se configura dinámicamente entre la dirección IPv4 externa y una dirección IPv6 en el prefijo NAT-PT. Por lo tanto, el nodo Pv6 puede adquirir una dirección IPv6 para alcanzar el destino IPv4 a través del dispositivo NAT-PT.

Conclusiones.

Este trabajo presentó una descripción general del protocolo IPv6 además de la importancia que este representa para la subsistencia de Internet, IPv6 es el proceso natural ante la evolución de Internet, y aporta muchas características que sin duda resultan en mejoras en todos los aspectos.

El grupo de trabajo IPv6 del IETF ha iniciado el proceso de llevar las especificaciones de los protocolos principales de IPv6 hacia la última fase del proceso de estandarización. Los protocolos del IETF se convierten en estándares de Internet cuando tienen ya un nivel significativo de implementación y de casos con éxito operativo. IPv6 está preparado para dar ese último paso que lo lleve a su estandarización.

Quizá la razón principal por la que no se ha implementado IPv6 de manera masiva radica a que en general el usuario final no compra protocolos, sino servicios y aplicaciones. Al usuario le resulta lo mismo en teoría que su conexión a Internet sea con protocolo IP, que IPX o AppleTalk, siempre y cuando las aplicaciones y servicios que utiliza funcionen en uno o en otro. Exactamente lo mismo ocurre con IPv6 e IPv4. Lo que importa no es el protocolo que se utiliza, sino los servicios que este ofrece.

La forma en que fue diseñado y desarrollado IPv6 ha previsto un período relativamente extenso de coexistencia y transición con IPv4. Es parte integral de la propuesta que ofrece IPv6 de realizar un cambio paulatino, y sin duda, durante muchos años, seguirá habiendo dispositivos que sigan trabajando con IPv4. Es evidente por tanto, que mientras no surjan estos servicios a gran escala no podremos hablar de una “adopción masiva de IPv6”.

Sin embargo la industria informática, que es una de las más interesadas en promover a IPv6 por el mercado mundial que representa Internet, ha dado un paso decisivo con el claro objetivo de que el usuario final casi sin darse cuenta, utilice IPv6 de manera natural y es el hecho de que cada vez mas sistemas operativos utilicen la pila IPv6 por defecto (un caso particular es el Windows Vista). Esta acción a su vez obliga a los desarrolladores de aplicaciones y a los ISPs a adaptarse a las circunstancias, por lo tanto de manera paulatina habrá un número cada vez mayor tanto de aplicaciones que soporten IPv6 y de proveedores de servicio Internet que ofrezcan conectividad nativa IPv6.

Consecuentemente el uso de IPv6 ya ha empezado a modificar los porcentajes que indican que IPv4 cuenta con una participación superior al 80% del total de Internet, y no tardará en pasar a una posición opuesta, donde IPv4 cubra solo una pequeña porción de Internet.

Apéndice A. RFCs relacionados con IPv6 consultados.

Razones para IPv6.

RFC 2775, Internet Transparency, B. Carpenter, IETF, www.ietf.org/rfc/rfc2775.txt, Febrero 2000.

RFC 2993, Architectural Implications of NAT, T Hain, IETF www.normos.org/rfc/rfc2993.txt, Noviembre 2000.

Especificaciones de Protocolo.

RFC 2460, Internet Protocol, Versión 6 (IPv6) Specification, S. Deering, R. Hinden, IETF, www.ietf.org/rfc/rfc2460.txt Diciembre 1998.

RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6), a. Conta, S Deering, IETF, www.ietf.org/rfc/rfc2463.txt, Diciembre 1998.

Direccionamiento.

RFC 2373, IP version 6 Addressing Architecture, R Hinden, S. Deering, IETF, www.ietf.org/rfc/rfc2373.txt, Julio 1998.

RFC 2374, AN IPv6 Aggregatable Global Unicast Address Format, R. Hinden, S. Deering, M. O`Dell, IETF, www.ietf.org/rfc/rfc2374.txt, Julio 1998.

RFC 2375, IPv6 Multicast Address Assignments, R. Hinden, S: Deering, www.ietf.org/rfc/rfc2375.txt, Julio 1998.

RFC 2526, Reserved IPv6 Subnet Anycast Address, D. Jhonson, S Deering, IETF, www.ietf.org/rfc/rfc2526.txt, Marzo 1999.

Protocolo de Descubrimiento de vecinos: Publicación, Autoconfiguración, y reemplazo del mecanismo ARP.

RFC 2461, Neighbor Discovery for IP version 6 (IPv6) T. Narten, E. Normark, W. Simpson, IETF, www.ietf.org/rfc/rfc2461.txt, Diciembre 1998.

RFC 2462, IPv6 Stateless Autoconfiguration, S. Thomson, T. Narten, IETF, www.ietf.org/rfc/rfc2462.txt, Diciembre 1998.

RFC 3041, Privacy Extension for Stateless Address Autoconfiguration in IPv6, T. Narten, R. Dreves, IETF, www.ietf.org/rfc/rfc3041.txt, Enero 2001.

RFC 3122, Extension to IPv6 Neighbor Discovery for Inverse Discovery Specification, A. Conta, IETF, www.ietf.org/rfc/rfc3122.txt, Junio 2001.

IPv6 en Ethernet.

RFC 2464, Transmission of IPv6 Packets over Ethernet Networks, M. Crawford, IETF, www.ietf.org/rfc/rfc2464.txt, Diciembre 1998.

Internet IPv6 de producción.

RFC 3177, IAB/IESG Recommendations on IPv6 Address Allocations to Sites, IAB, IETF, www.ietf.org/rfc/rfc3177.txt Septiembre 2001.

Mecanismos de coexistencia y transición.

RFC 2529, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, B. Carpenter, C. Jung, IETF, www.ietf.org/rfc/rfc2529.txt, Marzo 1999.

RFC 2766, Network Address Translation Protocol Translation, G. Tsirtsis, P. Srisurech, IETF, www.ietf.org/rfc/rfc2766.txt, Febrero 2000.

RFC 2767, Dual Stack Hosts using the “Bump in the Stack” Technique (BIS), K. Tsuchiya, H. Higuchi, Y. Atarshi, IETF, www.ietf.org/rfc/rfc2767.txt, Febrero 2000.

RFC 2893, Transition Mechanisms for IPv6 Host and Routers, R. Guilligan, E. Nordmark, IETF, www.ietf.org/rfc/rfc2893.txt, Agosto 2000.

RFC 3053, IPv6 Tunnel Broker, A. Durand et al; IETF, www.ietf.org/rfc/rfc3053.txt, Enero 2001

RFC 3056, Connection of IPv6 Domains via IPv4 Clouds, B. Carpenter, K Moore, IETF, www.ietf.org/rfc/rfc3056.txt Febrero 2001.

RFC 3068, An Anycast Prefix for 6to4 Relay Routers, C. Huitema, IETF, www.ietf.org/rfc/rfc3068.txt, Junio 2001.

Multicast.

RFC 3306, Unicast-Prefix_based IPv6 Multicast Addresses, B. Haberman, D. Thaler, IETF, www.ietf.org/rfc/rfc3306.txt. Agosto 2002.

RFC 3307, Allocation Guidelines for IPv6 Multicast Addresses, B. Habermann, IETF, www.ietf.org/rfc/rfc3307.txt, Agosto 2002.

PMTUD.

RFC 1981, Path MTU Discovery for IP version 6, J. McCann et al. IETF, www.ietf.org/rfc/rfc1981.txt, Agosto 1996.

Historia.

RFC 1550, IP: Next Generation (IPng) White Paper Solicitation. S. Brander, A. Mankin., IETF, www.ietf.org/rfc/rfc1550.txt, Diciembre 1993.

RFC 1752, The Recommendation for the IP Next Generation Protocol, S. Bradner, A. Mankin, IETF, www.ietf.org/rfc/rfc1752.txt, Enero 1995.

Apéndice B. Obtener conectividad IPv6 mediante un servicio Túnel Broker.

Como se ha descrito en el capítulo 5 de este trabajo, uno de los métodos más factibles para crear túneles configurados a través de redes IPv4 y conectarse a redes IPv6 es el mecanismo del túnel Broker. La finalidad de este apartado es el de mostrar de manera general la manera en que un usuario IPv4 puede obtener conectividad IPv6 de manera sencilla.

Existen varios servicios túnel Broker gratuitos en la red, entre los que se encuentran:

Página de Eurosix

<http://tb4.consulintel.euro6ix.org/in/index.php#>

Página Hurricane Electric Internet Services

<http://ipv6tb.he.net>

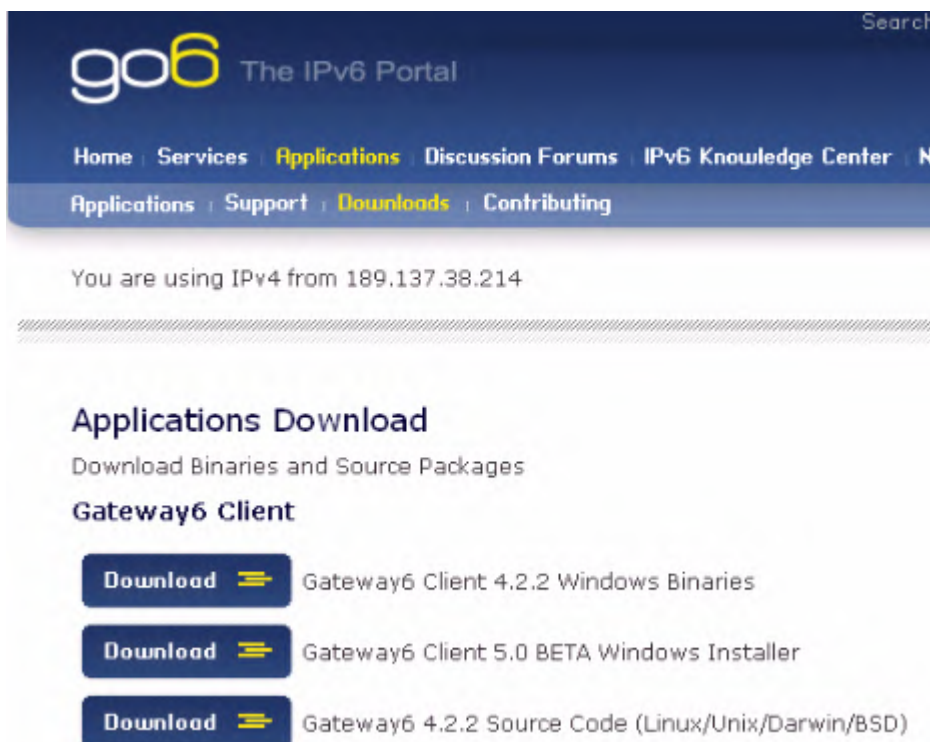
Página T6 chile

<http://t6.nxs.cl>

Página Hexago

<http://www.go6.net>

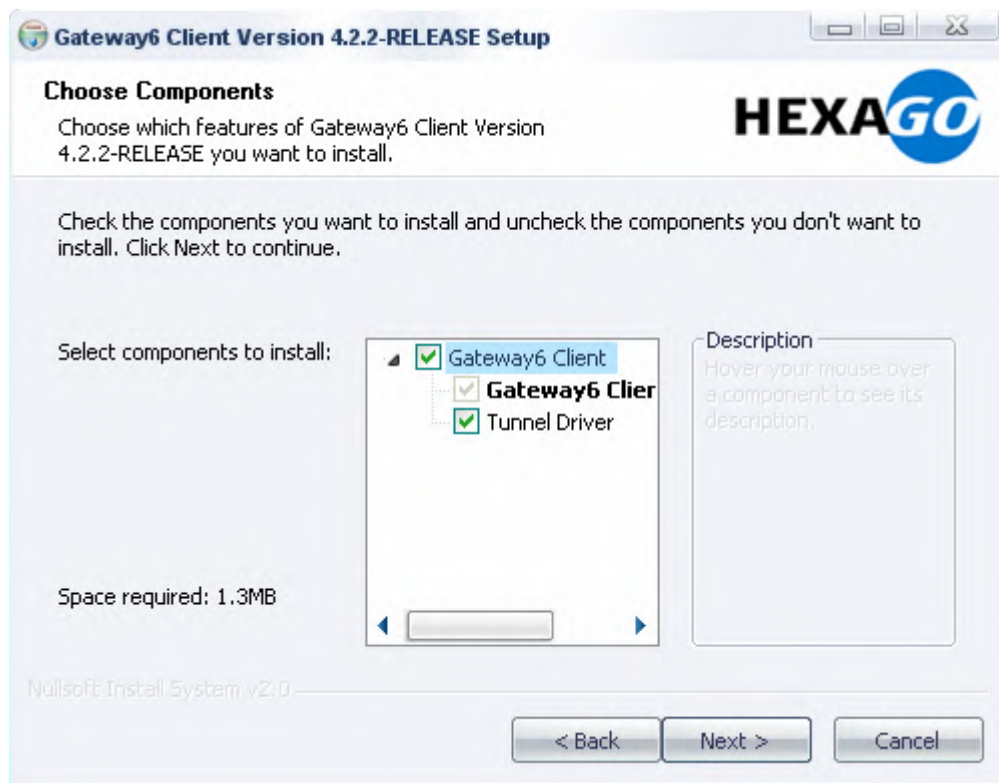
Para nuestros propósitos se optó por el servicio que ofrece Hexago, y se ha utilizado el sistema operativo Windows XP que es el más comúnmente usado.



The screenshot shows the go6 website interface. At the top, there is a search bar and the go6 logo with the tagline 'The IPv6 Portal'. Below this is a navigation menu with links for Home, Services, Applications (highlighted), Discussion Forums, IPv6 Knowledge Center, and News. A secondary menu includes Applications, Support, Downloads (highlighted), and Contributing. A status message indicates 'You are using IPv4 from 189.137.38.214'. The main content area is titled 'Applications Download' and 'Download Binaries and Source Packages'. Under the heading 'Gateway6 Client', there are three download buttons: 'Gateway6 Client 4.2.2 Windows Binaries', 'Gateway6 Client 5.0 BETA Windows Installer', and 'Gateway6 4.2.2 Source Code (Linux/Unix/Darwin/BSD)'.

El Software (script) que descargaremos desde la página de hexago se llama Cliente Gateway6 versión 4.2.2 para Windows. Cabe señalar que Hexago pone también a disposición software para los sistemas operativos Linux y FreeBSD.

El cliente Gateway6 viene con su programa de instalación. Al correr la instalación habrá que aceptar el contrato de uso, los componentes a instalar y el fólдер destinatario del cliente Gateway6.



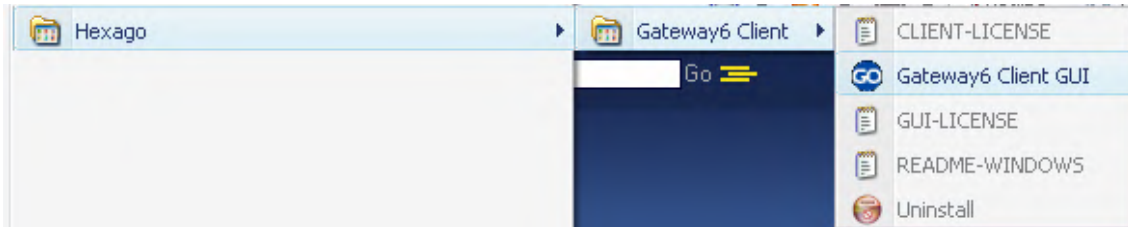
Como siguiente paso y una vez instalado se nos invita a abrir la interfase gráfica para añadir nuestra información personal. Para la mayoría de los usuarios cambiando el identificador de usuario, el password y el servidor resultará suficiente

Estas configuraciones crean los archivos apropiados en un fólдер destinatario, añaden un icono en el menú de inicio y también crea una nueva “conexión de red”. Si nosotros ingresamos a Panel de control -> Conexiones de red podremos ver un nuevo tipo de conexión: “Hexago virtual multi-tunnel Adapter”.

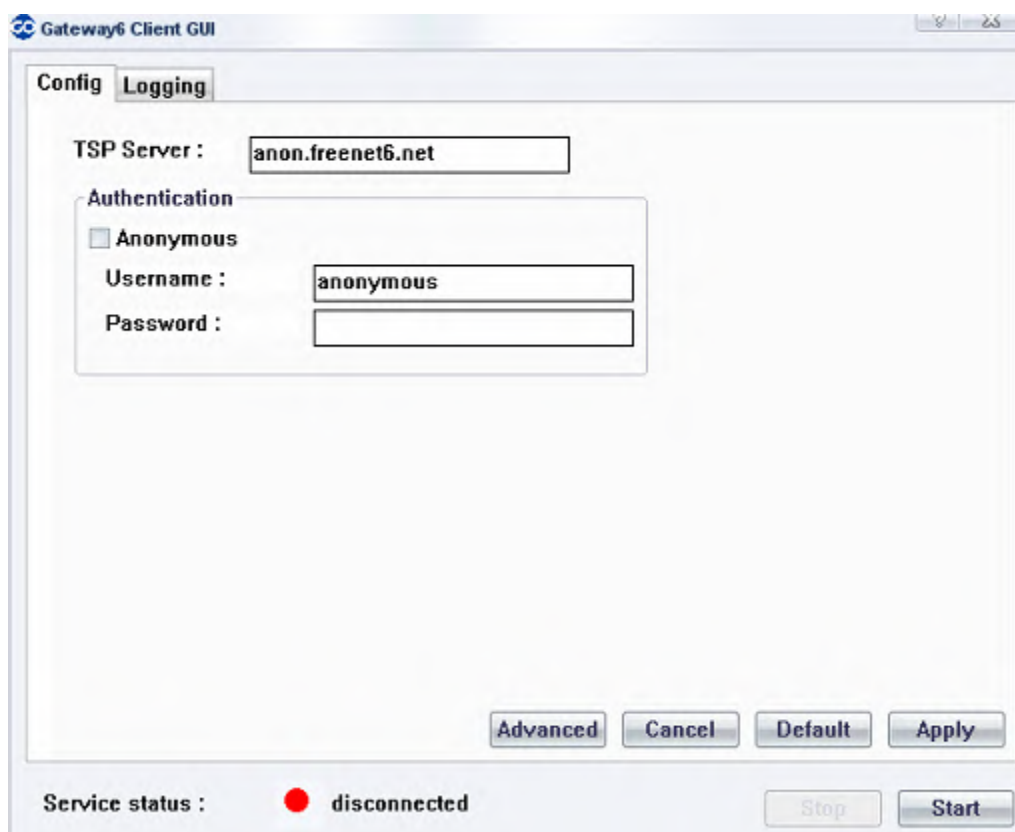
LAN o Internet de alta velocidad



El cliente Gateway6 es configurado utilizando una Interfaz de usuario gráfica (GUI), con el que podremos modificar nuestras opciones de conexión como son el ID de usuario, el Password, autenticación etc. El GUI es llamado desde el icono de Hexago en la barra de inicio.

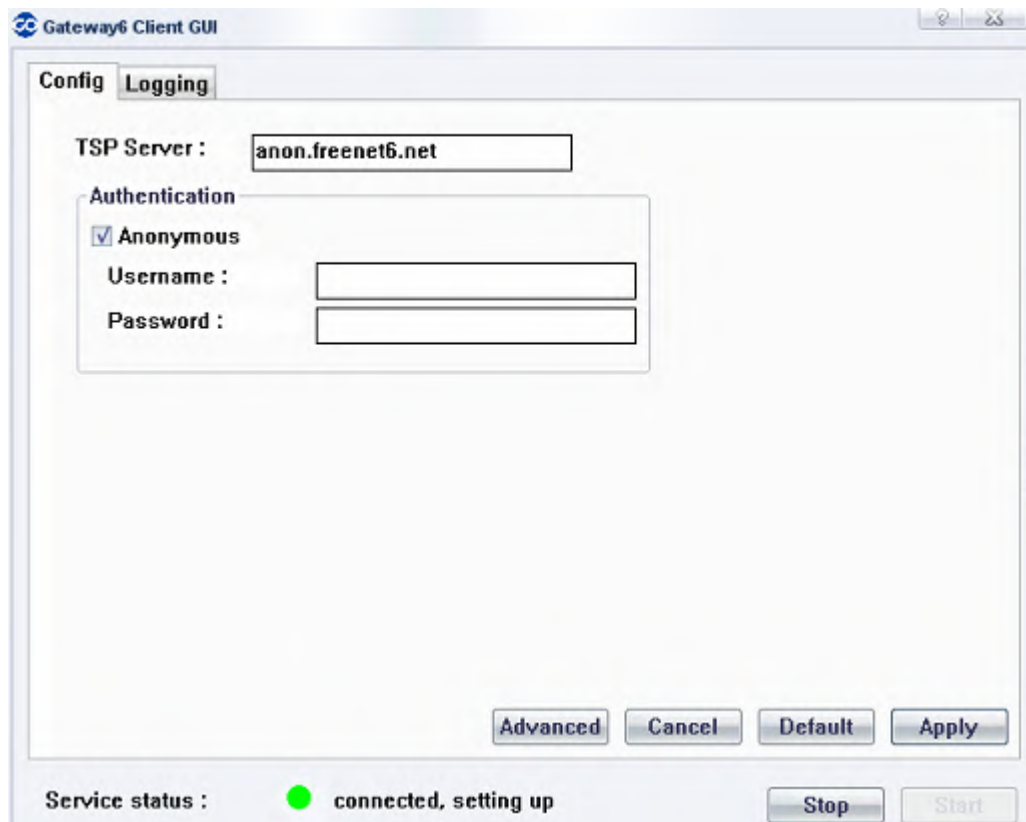


Una vez en el GUI, en la pestaña “Config” se muestran algunos de los parámetros a configurar como el modo de autenticación y la dirección del servidor que nos va a proporcionar el servicio (predeterminada). Si se desean hacer modificaciones más avanzadas está el botón “Advanced “. Para mayor referencia sobre las opciones disponibles, se dispone de una guía de usuario incluido en el cliente Gateway6.

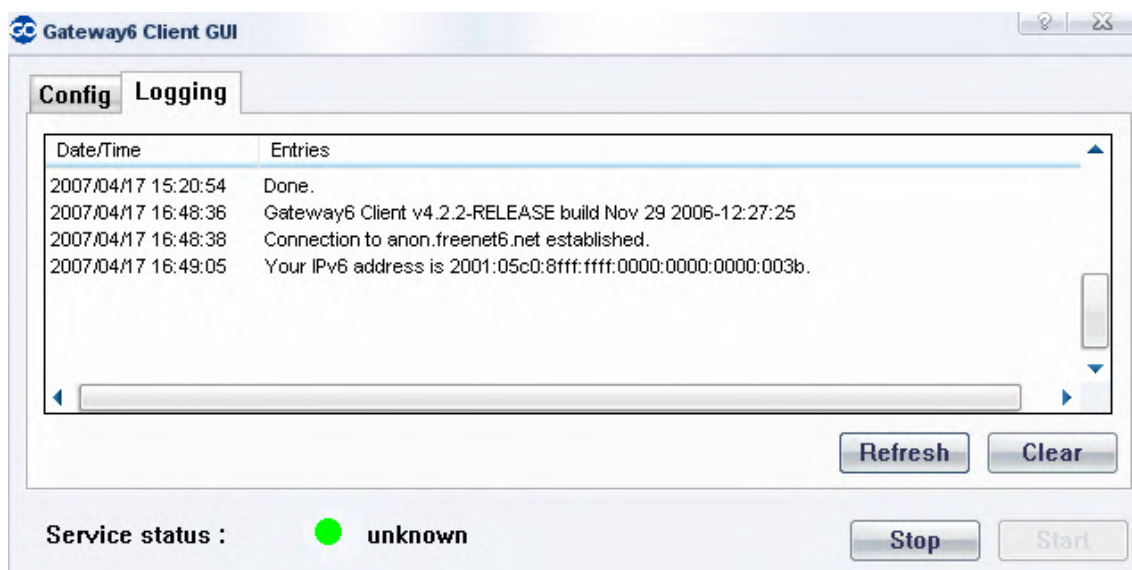


La pestaña “Logging” nos mostrará los sucesos que ocurran una vez que intentemos conectividad IPv6

Una vez configurado el cliente Gateway6 mediante el GUI haremos click en el botón “Apply” y después “Start”.



En la figura, en la parte inferior izquierda se observa un círculo, que ha modo de semáforo nos indica el estado del servicio. Con la leyenda “Connected, setting up” asumiremos que se ha podido establecer conexión con el servidor TSP, y por lo tanto tener conectividad IPv6. Haremos click en la pestaña Logging para ver los sucesos ocurridos, así como nuestra dirección IPv6.



Finalmente, probaremos nuestra conectividad IPv6 al ingresar a páginas accesibles solo desde redes IPv6. En este caso por ejemplo la página del Proyecto Kame (<http://www.kame.net>), donde la animación de la tortuga nos indicará tenemos conectividad IPv6.

The KAME project

1998.4 - 2006.3



Dancing kame by [atelier momonga](#)



También está la página del proyecto JOIN (<http://www.ipv6.uni-muenster.de/>) donde se indica nuestra dirección IPv6 desde la que estamos accediendo.


IPv6-Referenzzentrum

JOIN - Das IPv6-Projekt am Zentrum Informationsverarbeitung der Westfälischen Wilhelms-Universität

JOIN Projekt wurde beendet. Es gibt hier keine Neuigkeiten mehr.

↓

Ihre IPv6-Adresse lautet **2001:5c0:8ff:fff::3b**

Team | Kontakt: join@uni-muenster.de | IPv4: <http://www.join.uni-muenster.de> | IPv6: <http://www.ipv6.uni-muenster.de>
[Impressum](#) | Letzte Änderung: 21.12.2006, 18:36 Uhr | Switch language to 
Falls nicht anders angegeben: sämtliche Inhalte und Bilder sind Copyright © 1994-2005 by JOIN

Glosario de términos.

Anycast: Un nodo origen enviando un solo paquete hacia el destino más cercano. Al igual que el multicast, el anycast implica el concepto de grupo.

APNIC: Centro de Información de red Asia Pacífico. Uno de los tres registros regionales de Internet en el mundo que puede asignar bloques de direcciones IPv6 de producción a los ISPs. APNIC cubre Asia y Australia.

ARIN: Registro americano para números de Internet. Uno de los tres registros regionales de Internet en el mundo que puede asignar bloques de direcciones IPv6 de producción a los ISPs. ARIN cubre el continente americano.

ARP: Protocolo de resolución de dirección. Protocolo de la arquitectura Internet utilizado para traducir direcciones de protocolo de alto nivel dentro de direcciones de hardware físicas. Comúnmente utilizado en el Internet para mapear direcciones IP dentro de direcciones Ethernet.

ARPA: Agencia de proyectos de investigación avanzados. Una de las organizaciones de investigación y desarrollo dentro del Departamento de defensa de los E. U. Responsable de la fundación de ARPANET y del desarrollo del Internet TCP/IP.

ARPANET: Red fundada por ARPA a finales de los años 60, la cual se convirtió en el backbone para desarrollar Internet.

Autenticación: Protocolo de seguridad en el cual dos partes sospechosas se proporcionan mutuamente la información que verifica que ellos son quienes claman ser.

Autoconfiguración stateless: Un mecanismo IPv6 que le permite a los nodos configurar sus direcciones IPv6 por ellos mismos utilizando los mensajes de publicación de router recibidos.

Bellman Ford: nombre para el protocolo de enrutamiento de vector de distancia con los nombres de los inventores.

BGP: Protocolo de Gateway Fronterizo. Protocolo de enrutamiento interdominio por el cual el sistema autónomo intercambia información de accesibilidad. La versión más importante es BGP4+.

Broadcast: Un método para la entrega de un paquete hacia cada host dentro de una red particular. Puede ser implementada en hardware (por ejemplo Ethernet) o software (por ejemplo broadcast IP).

CIDR: Enrutamiento interdominio si clases. Método de agregación de rutas que trata a un bloque continuo de direcciones de clase C como una sola red.

Ciente: El solicitante de un servicio en un sistema distribuido.

DAD: Detección de duplicado de dirección. Un mecanismo IPv6 que verifica la existencia de una dirección IPv6 en el enlace local antes de configurar una dirección IPv6 en una interfase de red.

Dirección Unicast de agregación global: Una dirección unicast IPv6 utilizada para el tráfico genérico en el Internet IPv6. Esta representa la parte más importante del espacio de direccionamiento IPv6. La dirección unicast de agregación global habilita la estricta agregación de los prefijos de enrutamiento para limitar el tamaño de la tabla de enrutamiento global de Internet.

Datagrama: La entidad de transmisión básica en a arquitectura de Internet. Un datagrama contiene todo sobre la información necesaria para enviarse hacia su destino. Los datagramas de Internet son no orientados a la conexión.

DHCP: Protocolo de configuración dinámica de host. Protocolo utilizado por los hosts para inicialmente aprender múltiple información de red, como su dirección IP.

DNS: Sistema de dominios de nombre. El sistema de nombramiento distribuido de Internet utilizado para resolver nombres a direcciones IP y viceversa. El DNS se implementa por una jerarquía de servidores de nombres.

dominio: Puede referirse tanto al contexto del espacio de nombres jerárquicos del DNS (por ejemplo dominio .mx) , así como a una región de Internet que es tratada como una sola entidad para propósitos de enrutamiento jerárquico, esto último es equivalente a un sistema autónomo.

EGP: Protocolo de Gateway exterior. Protocolo de enrutamiento interdominio con varios años en el mercado, el cuál fué utilizado por los gateways exteriores (routers) de los sistemas autónomos para intercambiar información de enrutamiento con otros Ass. Fue reemplazado por el protocolo BGP.

Enlace: Conexión física entre dos nodos de una red, puede ser implementado sobre cobre, o cable de fibra óptica o puede ser un enlace sin cable (por ejemplo las microondas).

Ethernet: Tecnología de la capa 1 y 2 d modelo OSI que utiliza CSMA/CD y un ancho de banda que va en aumento conforme se va mejorando la tecnología (ha pasado de 10 Mbps a 10000 Mbps). Un ethernet por sí mismo es sólo un cable pasivo, todos los aspectos de transmisión Ethernet son completamente implementados por los adaptadores de host.

EUI-64: Dirección del nivel de enlace de 64 bits que se utiliza como base para la generación de identificadores de interfaz en IPv6.

FTP: Protocolo de transferencia de archivos. El protocolo estándar de la arquitectura Internet para transferir archivos entre host. Está construido sobre el protocolo TCP.

Host: computadora conectada a una o más redes que soporta usuarios y corre programas de aplicación.

HTTP: Protocolo de transporte de hipertexto. Un protocolo de nivel de aplicación basado en el modelo solicitud/respuesta utilizado en la web. HTTP utiliza conexiones TCP para la transferencia de datos.

ICMP: Protocolo de mensajes de control Internet. Protocolo que forma parte integral de IP. Este permite que un router o host destino comunicarse con el origen generalmente para reportar un error en el procesamiento de un datagrama.

IETF: Grupo de Ingeniería de Internet. Equipo de trabajo responsable de proveer soluciones de desarrollo a corto plazo para Internet.

Internet: El Internet global basado en la arquitectura TCP/IP conectado a millones de hosts a nivel mundial.

IP: Protocolo Internet (también conocido como IPv4). Protocolo que ofrece servicio de entrega no orientado a la conexión con el menor esfuerzo de datagramas cruzando Internet.

ISP: Proveedor del servicio de Internet. Una compañía que proporciona conectividad a Internet y espacio de direcciones IP a compañías, organizaciones e individuos.

IPSec: Seguridad IP. Una arquitectura para autenticación, privacidad y mensajes de integridad entre otros servicios de seguridad para la arquitectura Internet.

IS-IS: protocolo de enrutamiento de estado de enlace, similar a OSPF.

ISO: Organismo Internacional de estandarización. Organismo que prueba la arquitectura de siete capas del modelo OSI y su conjunto de protocolos que aún no consiguen éxito comercial.

LAN: red de área local. Una red basada en cualquier tecnología de red física que está diseñada para implementarse en distancias arriba de unos pocos cientos de metros (por ejemplo Ethernet).

MTU: Unidad de transmisión máxima. El tamaño del paquete más grande que puede enviarse sobre una red física.

Multicast: Forma especial de broadcast en la cual los paquetes son entregados hacia un subgrupo de host de red específicos.

NAT: Traducción de direcciones de red. Técnica para extender el espacio de direcciones IP que involucra traducciones entre direcciones IP unicast globales y direcciones privadas en la frontera de una red o un sitio.

Ngtrans: Grupo de trabajo del IETF que ha diseñado herramientas, protocolos, y estrategias que permiten la transición de redes IPv4 hacia IPv6.

Nodo: Término genérico utilizado por computadoras individuales que conforman una red. Los nodos incluyen computadoras de propósito general, switches y routers.

OSI: Interconexión de Sistemas abiertos. El modelo de referencia de siete capas desarrollado por ISO. Dirige el diseño de los protocolos estándar ISO.

Paquete: Una unidad de datos enviada sobre una red de paquetes conmutados.

PDU: Unidad de datos de protocolo. Otro nombre para paquete o trama.

Pila dual: Nodos que tienen habilitada la pila IPv4 e IPv6 simultáneamente. La pila dual es una estrategia de transición y coexistencia que permite a los nodos recibir y enviar tráfico IPv4 e IPv6.

Protocolo no orientado a la conexión: Protocolo en el cual los datos pueden ser enviados sin ningún avance adelante de instalación. IP es un ejemplo de este protocolo.

RFC: Petición de comentarios. Reportes de Internet que contienen entre otras cosas especificaciones para protocolos como TCP/IP.

RIP: Protocolo de Información de enrutamiento. Protocolo de enrutamiento intradominio.

RIPE NCC: Réseaux IP Européens Network Coordination Center. Uno de los tres registros regionales de Internet en el mundo que puede asignar direcciones Ipv6 de producción a ISPs. RIPE NCC cubre Europa y oriente medio.

Router: Un nodo de red conectado a dos o más redes y que envía paquetes desde una red a otra.

Servidor: El proveedor de un servicio en un sistema distribuido cliente/servidor.

Sistema Autónomo (AS): Grupo de redes y routers, sujetos a una autoridad común y que además utilizan el mismo protocolo de enrutamiento intradominio.

SMTP: Protocolo de transferencia de correo simple. El protocolo de correo electrónico de Internet.

SNMP: Protocolo de administración de red simple. Protocolo de Internet que permite el monitoreo de host, redes y routers.

TCP: Protocolo de control de transmisión. Protocolo de transporte orientado a la conexión de la arquitectura Internet. TCP proporciona un servicio de entrega confiable.

Telnet: Protocolo de terminal remota de la arquitectura Internet. Telnet permite a un dispositivo interactuar con otro dispositivo remoto si entre estos existe una conexión directa.

Trama: Otro nombre para un paquete generalmente utilizado en referencia a los paquetes enviados a un solo enlace en lugar de a la red completa.

Túnel configurado: Un túnel IPv6 sobre infraestructura IPv4 (enlace punto a punto) definido estáticamente entre nodos IPv4/IPv6. El túnel configurado es un mecanismo de coexistencia y transición que permite transportar paquetes IPv6 sobre redes IPv4.

UDP: Protocolo de datagrama de usuario. Protocolo de transporte de la arquitectura Internet que proporciona servicio de datagramas sin conexión a procesos de nivel de aplicación.

Unicast: Envío de un paquete hacia un único host de destino.

VLSM: Máscara de Subred de Longitud Variable. Posibilidad de especificar una máscara de subred diferente para el mismo número de red en diferentes subredes. VLSM ayuda a optimizar el espacio de direcciones disponible.

WAN: Red de área amplia. Cualquier tecnología de red física capaz de cubrir grandes distancias (por ejemplo un país).

Zona: Partición del dominio de jerarquías de nombres correspondiente a una autoridad administrativa que es responsable de esa parte de la jerarquía. Cada zona debe tener al menos dos servidores de nombre para cubrir las peticiones DNS para la zona.

Bibliografía.

Thomas A. Stephen.
**IPng and the TCP/IP protocols :
implementing the next generation Internet**
Ed. J. Wiley, 1996.

Desmeules, Regis.
**Cisco self-study :
implementing IPv6 networks (IPV6)**
Ed. Cisco Press, 2003.

Salus H. Peter.
Understanding IPv6 Addressing
Ed. AP Professional, 1999.

Huitema Christian.
IPv6: the new Internet Protocol
Ed. Prentice Hall, 1997.

Fourazan A. Behrouz.
TCP/IP Protocol Suite
Ed. McGraw-Hill, 2000.