UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

DISEÑO E IMPLEMENTACION DE IPV6 EN RED UNAM

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO ELECTRICO - ELECTRONICO

P R E S E N T A N :

JUAREZ RIVAS OSCAR ALBERTO

MARIN JIMENEZ JOSE LUIS

DIRECTOR DE TESIS: ING. JUAN JOSE CARREON GRANADOS

MEXICO, D. F 2004.

A mis padres José Guadalupe Marín Jiménez y María Esther Jiménez Ibáñez
Por el apoyo y comprensión incondicional, por su cariño y la continua motivación. Gracias a todas sus enseñanzas he encontrado el más grande tesoro que existe en la vida... el estudio. Les estaré por siempre agradecido.

A mi hermano Mario Alberto Marín Jiménez
Por todo el apoyo y comprensión al realizar este trabajo y a lo largo de la carrera, espero que este logro te motive a alcanzar todas tus metas, para que no te des por vencido y te superes constantemente.

A mi abuelita Elena Ibáñez
Por todos sus enseñanzas y el apoyo incondicional que me ha brindado a lo largo de mi vida y en especial en estos momentos.

A mis compadres
Juan Adrián Rodriguez Barreto, Juan Carlos Ávila León y Arnulfo Hernández Hernández, gracias por su apoyo.

A todos mis amigos
Quisiera poder nombrarlos a todos pero sería imposible hacerlo, les agradezco todas y cada una de sus enseñanzas y su comprensión y ayuda en los momentos de la realización de este trabajo.

A mis maestros
Por contribuir con sus conocimientos y experiencias en mi formación académica, en especial a Yukihiro Minami Koyama por todas sus enseñanzas y su amistad. Gracias.

A la DGSCA
En especial a todos los que laboramos en el departamento de redes de la UNAM, en particular a los que pertenecen y han pertenecido al TAC. Quisiera agradecer especialmente al Ing. Alfredo Hernández Mendoza por creer en mí, Al Ing. Carlos Alberto Vicente Altamirano por todas sus enseñanzas y su excelente calidad humana. A Hugo Rivera Martínez por todo el apoyo brindado en todo este tiempo que he estado en la DGSCA.

A mi amigo y compañero Oscar Alberto Juárez Rivas
Por su apoyo y amistad a lo largo de toda la carrera, compartiendo conmigo momentos de felicidad y de tristeza.

Al Ing. Juan José Carreón Granados
Por la orientación que nos proporcionó durante el desarrollo de este trabajo, gracias.

José Luis Marín Jiménez

A mis padres Isidro Juárez Juárez y A. Laura Rivas Canales
Por su apoyo incondicional, con el cual pude estudiar esta carrera. Con su confianza, amor y comprensión he podido superar los momentos difíciles.

A mi hermano Víctor Javier Juárez Rivas
Quien siempre ha estado a mi lado para apoyarme y aconsejarme.

A mi hermano Alejandro Juárez Rivas
Por su valiosa amistad y apoyo en todo momento.

Mi cuñada Laura Contreras y mis hermosos sobrinos Evelyn y Daniel Juárez Contreras
Por su cariño, el cual siempre ha sido una motivación para superarme.

A la familia
Por la bella amistad que me han brindado toda la vida.

A mis amigos
Por comprenderme y apoyarme en los buenos y malos momentos.

A la Facultad de Ingeniería
Por permitirme el privilegio de estudiar y aprender en sus aulas.

A la Dirección General de Servicios de Cómputo Académico de la UNAM
En especial a la L.I. Paola Garfias Hernández y al Ing. Alfredo Hernández Mendoza por apoyarme durante mi estancia en el Departamento de Operación de la Red. A todos los compañeros de este departamento les agradezco su gran apoyo.

A mi amigo José Luis Marín Jiménez
Por todo el apoyo que me ha dado desde que entramos a la carrera, pero sobre todo por su invaluable amistad.

Al Ingeniero Juan José Carreón Granados
Por su valiosa dirección en la elaboración de este trabajo.

A la maravillosa Universidad Nacional Autónoma de México
Gracias a su riqueza humana y académica he podido continuar mi formación.

Oscar Alberto Juárez Rivas

ÍNDICE

INTRODUCCIÓN

Actualmente Internet opera con el protocolo IP (Internet Protocol) versión 4. Sin embargo esta versión ya ha alcanzado el umbral de uno de sus límites: el espacio de direcciones. La versión 6 de este protocolo (IPv6) es la solución más sólida para resolver el problema de falta de direcciones.

Por su parte, la Red UNAM, al formar parte de la comunidad de Internet, debe estudiar y planificar su migración a IPv6.

El protocolo Internet sirve para establecer comunicación entre equipos que procesan información. Estos equipos pueden estar ubicados en lugares distantes, por lo que es necesario que tengan un identificador. Este es la denominada "Dirección IP". Esta dirección consta de 32 bits, la cual permite tener aproximadamente 4 mil millones de equipos identificados globalmente. El problema es inicialmente no se contempló el crecimiento de Internet y el número de direcciones IPv4 públicas se están acabando.

En los últimos años se ha tratado de superar la falta de direcciones IPv4 con diversos mecanismos como la traducción de direcciones de red privadas en públicas. Sin embargo, estos mecanismos tienen algunos problemas que limitan los servicios disponibles de la red. IPv6 supera los problemas de IPv4 al incorporar nuevas funciones en la estructura del mismo protocolo.

El formato de la dirección en IPv6 incrementa por mucho el espacio de direcciones. Se trata de direcciones de 128 bits que permiten disponer de una gran cantidad de direcciones.

Dada la existencia del direccionamiento IP, es necesario definir como los paquetes de información viajarán de un origen a un destino. Es en este punto donde los protocolos de enrutamiento cumplen una función muy importante al mantener comunicación entre equipos de red. Ellos son los encargados de buscar la mejor ruta hacia el destino para enviar los paquetes que reciben.

Hay diversos protocolos de enrutamiento como RIP, OSPF y BGP, además del enrutamiento estático. Cada uno de tiene características muy particulares que los hace aplicables dependiendo del tipo de red. Esta puede ser muy pequeña, con simples reglas de enrutamiento estático, o puede requerir de reglas dinámicas para buscar rutas hacia un destino en Internet por medio de RIP. Si se trata de una red de un tamaño considerable puede ser necesario utilizar OSPF. BGP es el protocolo de enrutamiento necesario para redes que disponen de un número de Sistema Autónomo. Redes de este tipo generalmente proporcionan servicios de red a otras más pequeñas.

Para poder implementar IPv6 en la Red UNAM es necesario conocer las características de los protocolos de enrutamiento y sus respectivas modificaciones para cambiar de IPv4 a la nueva versión. La Red UNAM cuenta con un número AS, por lo que puede utilizar todos, o cualquiera de los protocolos de enrutamiento mencionados anteriormente dependiendo de la etapa en que se encuentre la adopción de IPv6.

La Red UNAM cuenta con un bloque de direcciones IPv6 de producción tipo Sub-TLA, es decir, de los bloques más grandes que puede proporcionar un registro regional. Con este bloque es posible plantear un esquema de direccionamiento de tipo jerárquico. Esto es posible dado el extenso espacio de direcciones del que se dispone: hasta el momento 32 bits para crear redes y 64 bits en cada una de estas redes para habilitar IPv6 en las interfaces de los equipos.

Los protocolos para aplicaciones y acceso a la red no resienten tanto el cambio de versión porque IPv6 contempla las modificaciones necesarias para adaptarse a ellos.

El cambio de versión en IP es un proceso conocido como "Transición de IPv4 a IPv6", ya que no es fácil coordinar un cambio en determinada fecha y a gran escala para mantener la comunicación en todas las redes que usan IP. La transición aprovecha la infraestructura actual de las redes, que opera con IPv4 principalmente, para permitir el transporte de paquetes IPv6 mediante mecanismos y técnicas que serán utilizadas frecuentemente. Es importante comprender estos mecanismos hasta no pasar a enlaces nativos de IPv6.

En la Red UNAM aún no se cuenta con soporte para IPv6 en los equipos de principales. Es muy probable que un futuro próximo se cuente con actualizaciones para soportar el nuevo protocolo. En caso contrario será necesario reemplazar estos equipos para permitir tráfico IPv6 sin necesidad de técnicas de transición.

Este trabajo expone un estudio detallado del Protocolo Internet versión 6. Deja en claro las características que este protocolo aprovecha de la versión 4 y da a conocer las nuevas para su futura implementación en la Red UNAM. Algunos equipos ya trabajan con IPv6, pero se espera que pronto se incorporen más.

CAPÍTULO 1

FUNDAMENTOS DEL PROTOCOLO INTERNET

1.1 Introducción a las redes de datos

Las redes de datos tienen como base el cómputo electrónico, el cual nació ante la necesidad de extender la rapidez del cerebro humano para realizar cálculos aritméticos y procedimientos repetitivos.

El esfuerzo en el cómputo electrónico se reflejó en la creación de unidades de procesamiento más rápidas conforme a los avances en la tecnología. Así tenemos cuatro generaciones bien definidas: la primera con tubos al vacío, la segunda con transistores, la tercera con circuitos integrados y la cuarta con circuitos integrados que permitieron el uso de computadoras personales y el desarrollo de las redes de datos.

Una vez resuelto el problema de extender el poder de cálculo del cerebro humano se hizo evidente la necesidad de compartir los datos y la información que ese poder de cálculo produjo; lo cual llevó a inventar la forma de compartir recursos a través de algún medio de transmisión usando una serie de reglas para acceder y manipular dichos recursos.

Las redes de computadoras permitieron reunir esfuerzos aislados en esfuerzos conjuntos para producir bienes mayores. Sin embargo, en una red la forma de acceder a dichos recursos va de la mano con conocer la manera de llegar a esos recursos y saber cómo manipularlos.

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. Al primer factor se le conoce como "Nivel físico" y al segundo "Protocolos".

En el nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido. Esas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma en que se acceden a esos paquetes es determinada por la tecnología de transmisión y se aceptan dos tipos: "Broadcast" y "Punto a punto".

Las redes de tipo broadcast se caracterizan porque todos los nodos pueden acceder a todos los paquetes que circulan por el medio de transmisión.

Las redes "Punto a punto" sólo permiten que un nodo se conecte a otro en un momento dado.

Por la extensión de las redes de tipo broadcast o de punto a punto, podemos clasificarlas de acuerdo a lo siguiente.

Distancia / CPU's	Ubicación de CPU's	Nombre
0.1 Mts.	Tarjeta Madre	Nodo
1 Mts.	Cluster,Sistema	Multicomputador
10 Mts.	Sala de Cómputo	LAN
100 Mts.	Edificio	LAN
1 Km.	Campus	LAN
10 Km.	Ciudad	MAN
100 Km.	Estado,País	WAN
1000 Km	Continente	WAN
10,000 Km	Planeta	INTERNET

Figura 1.1 Extensión de los tipos de redes

1.1.1 Redes de área local

Las redes de área local (Network Area Local "LAN") son el punto de contacto de los usuarios finales. Su finalidad principal es la de intercambiar información entre grupos de trabajo y compartir recursos tales como impresoras y discos duros. Se caracterizan por tres factores: extensión, su tecnología de transmisión y su topología.

Su extensión va de unos cuantos metros hasta algunos kilómetros. Esto permite unir nodos que se encuentran en una misma sala de cómputo, en un edificio, en un campus o una empresa mediana y grande ubicada en una misma locación.

Las redes tradicionales operan con medios de transmisión tales como cable de par trenzado (Unshielded Twisted Pair), cable coaxial (ya casi obsoleto porque presenta muchos problemas), fibra óptica (inmune a la mayoría de interferencias), portadoras de rayo infrarrojo o láser, radio y microondas en frecuencias no comerciales. Las velocidades en las redes de área local van desde 10 Mbps (Megabits por segundo) hasta 10 Gbps.

La topología de una red se refiere a la forma que ésta toma al hacer un diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico. Las topologías generales son: anillo (ring), dorsal (bus), estrella (star), árbol (tree) y mallas completas.

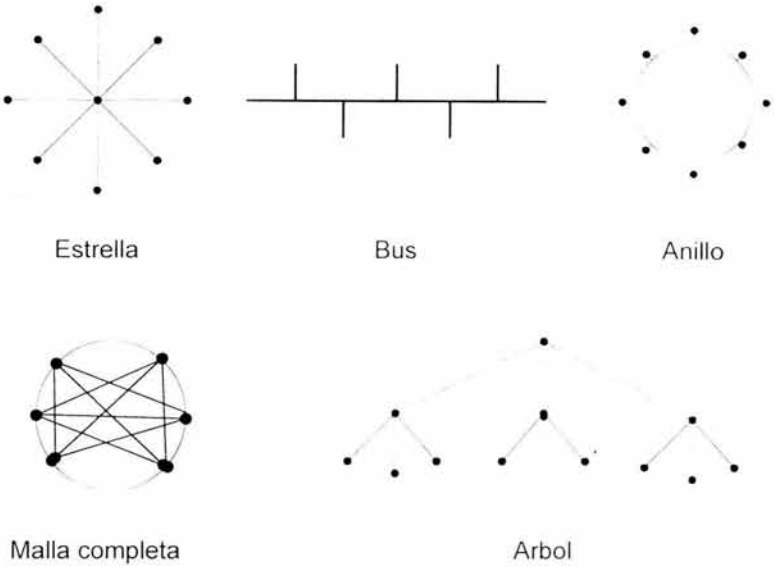


Figura 1.2: Topologías de red

Las topologías de anillo, bus y árbol se adecuan mejor para redes de tipo broadcast y el resto para redes de tipo punto a punto.

Dentro de los estándares más comunes esta el IEEE 802.3 llamado Ethernet, el cual opera entre 10 Mbps y 10 Gbps. En este estándar, todo nodo escucha todos los paquetes de está red broadcast, saca una copia y examina el destinatario. Si el destinatario es el nodo mismo, lo procesa y si no, lo deshecha para escuchar el siguiente. Para enviar un paquete escucha cuando el medio de transmisión esté libre. Si ocurre que dos nodos enviaron un paquete al mismo tiempo, se provoca una colisión y cada nodo vuelve a retransmitir su paquete después de esperar un tiempo aleatorio.

1.1.2 Red de área metropolitana

Una red de área metropolitana (MAN) es más grande que una LAN en cuanto a topología, protocolos y medios de transmisión que abarca tal vez a un conjunto de oficinas corporativas o empresas en una ciudad. Las redes de servicio de televisión por cable se pueden considerar como MANs y, en general, a cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros. El estándar IEEE 802.6 define un tipo de MAN llamado DQDB por sus siglas en inglés "Distributed Queue Dual Bus". Este estándar usa dos cables half-duplex por los cuales se recibe y transmiten voz y datos entre un conjunto de nodos.

1.1.3 Red de área amplia

Una red de área amplia (WAN) se expande en una zona geográfica de un país o continente. Los beneficiarios de estas redes son los que se ubican en nodos finales llamados también sistemas finales que corren aplicaciones de usuario. A la infraestructura que une los nodos de usuarios se le llama subred y abarca diversos dispositivos de red y líneas de comunicación que unen a las redes de área local.

En la mayoría de las redes de área amplia se utilizan una gran variedad de medios de transmisión para cubrir grandes distancias. La transmisión puede efectuarse por microondas, por cable de cobre, fibra óptica o alguna combinación de los anteriores. Sin importar el medio, los datos en algún punto se convierten e interpretan como una secuencia de unos y ceros; a partir de esta secuencia de bits se forman "Tramas"; luego estas tramas son ensambladas para formar "Paquetes", los cuales a su vez construyen archivos o registros específicos de alguna aplicación.

Las redes clásicas se caracterizan porque utilizan dispositivos de red denominados "Routers" para unir las diferentes LAN's. Como en este caso los paquetes viajan de LAN en LAN a través de ciertas rutas que los routers establecen, siendo dichos paquetes almacenados temporalmente en cada router, a la subred que usa este principio se le conoce como "Punto a punto", ya que almacena y envía.

Las topologías comunes en una red punto a punto son: de estrella, anillo, árbol, malla completa.

La posibilidad de usar el aire como medio de transmisión nos da lugar a las redes inalámbricas. Se pueden construir usando estaciones de radio o satélites que envían ondas a diferentes frecuencias para enlazar los correspondientes routers. Como el alcance de estas ondas no puede ser restringido en un cierto radio, se deben tomar algunas medidas especiales para no entrar en conflicto con otras ondas y para restringir el acceso.

Internet es la red de área amplia más grande de la tierra. Se ha derivado de un proyecto del departamento de defensa de Estados Unidos y actualmente es accesible a más de 2 millones de nodos en todo el mundo. Para abarcar la mayor parte de nuestro planeta, Internet utiliza casi todos los medios de transmisión y protocolos de red conocidos.

1.2 Modelo de referencia OSI

Al principio de su desarrollo, las LAN, MAN y WAN eran en cierto forma caóticas. En la década de los 80 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas se dieron cuenta de que podrían ahorrar mucho dinero y aumentar la productividad con tecnologías de redes, comenzaron a agregar más de éstas y a expandir las existentes casi simultáneamente con la aparición de nuevas tecnologías y productos de red.

A mediados de los 80, estas empresas debieron enfrentar problemas cada vez más serios debido a su expansión caótica. Resultaba cada vez más difícil que las redes que usaban diferentes especificaciones pudieran comunicarse entre sí. Concluyeron que era necesario dejar los sistemas propietarios.

Los sistemas propietarios se desarrollan, pertenecen y son controlados por organizaciones privadas. "Propietario" significa que un grupo de empresas controla el uso total de cierta tecnología. Por el contrario "Abierto" significa que el uso libre de la tecnología está disponible para todos.

Para enfrentar el problema de incompatibilidad de las redes y su imposibilidad de comunicarse entre sí, la Organización Internacional para la Normalización (ISO) estudió esquemas de red como DECNET, SNA y TCP/IP a fin de encontrar un conjunto de reglas. Como resultado de esta investigación, la ISO desarrolló un modelo de red que ayudaría a los fabricantes a crear redes que fueran compatibles y que pudieran operar con otras redes.

El modelo de referencia OSI, lanzado en 1984, fue el esquema descriptivo que crearon. Este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

El modelo OSI es el principal dentro de las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de dispositivos de redes relacionan sus productos con el modelo OSI, ya que es muy útil para comprender cómo se viaja la información o los paquetes de datos viajan desde los programas de aplicación, a través de un medio de red, hasta otro programa de aplicación ubicado en otro nodo de la red.

El modelo de referencia OSI se compone de siete capas, cada una de las cuales tiene una función de red específica. Si la red se divide en capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el análisis.

Las siete capas del modelo de referencia OSI se muestran en la figura 1.3:

Figura 1.3. Modelo de referencia OSI

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino.

1.2.1 Capa 7: la capa de aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, 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 y los de las terminales bancarias.

1.2.2 Capa 6: la capa de presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

1.2.3 Capa 5: la capa de sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos equipos finales o "Hosts" que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

1.2.4 Capa 4: la capa de transporte

La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte de datos entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte

1.2.5 Capa 3: la capa de red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Para ello se utiliza una arquitectura de direccionamiento lógico.

1.2.6 Capa 2: la capa de enlace de datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico, la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

1.2.7 Capa 1: la capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporizadores, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física.

1.2.8 Protocolo

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. "Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea eficiente".

Una definición técnica de un protocolo de comunicaciones de datos es: "un conjunto de reglas que determina el formato y la transmisión de datos".

1.2.9 Encapsulamiento

Si un host A desea enviar datos a otro host B, en primer lugar, los datos deben empaquetarse a través de un proceso denominado encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información[1.1].

Una vez que se envían los datos desde el origen, viajan a través de la capa de aplicación y recorren todas las demás capas en sentido descendiente. El encapsulamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus servicios a los usuarios finales. Las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

Creación de dato

Cuando un usuario envía un mensaje, los caracteres alfanuméricos se convierten en datos que pueden recorrer la red.

Encapsulamiento

Los datos se empaquetan para ser transportados por la red. La capa de transporte encapsula los datos recibidos de su capa superior y asegura que los hosts en ambos extremos del sistema de comunicación en red se puedan comunicar de forma confiable.

Encabezado de red

Los datos se colocan en un "Paquete" que contiene el encabezado de red con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

Encabezado de enlace de datos

Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

[1.1] La palabra "encabezado" o "cabecera" significa que se ha agregado la información correspondiente a la dirección.

Conversión a bits

La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio. Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la red física puede variar a lo largo de la ruta utilizada. Por ejemplo, un mensaje de correo electrónico puede originarse en una LAN, cruzar el backbone de un campus y salir por un enlace WAN hasta llegar a su destino en otra LAN remota. Los encabezados y la información final se agregan a medida que los datos se desplazan a través de las capas del modelo OSI.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicaciones de par-a-par. Durante este proceso, cada protocolo de capa intercambia información, que se conoce como unidades de datos de protocolo "PDU", entre capas iguales. Cada capa de comunicación, en el host origen, se comunica utilizando un PDU específico de la capa con la capa del mismo nivel en el host destino.

La PDU de la capa de transporte es llamada "Segmento", la de red se denomina "Paquete", y la de enlace de datos se le conoce como "Trama" o "Frame". En las capas superiores a la de transporte solo se hace referencia a los datos, mientras que en la capa física solo se ven bits codificados por medio de algún código digital. La comunicación entre capas iguales se representa en la figura 1.5.

El proceso para llegar al host destino es inverso, los datos se transportan por la red a nivel de capa uno en forma de bits; después en la capa dos, los dispositivos que forman parte de la ruta, acceden al medio para tomar y transportar las tramas hasta el host destino; con ayuda de la capa tres los paquetes van dando "saltos" por diversas redes hasta llagar la red y al host destino. Con los segmentos se tiene un mecanismo de control en la transmisión. Conforme llegan al destino, a los datos se les van quitando los encabezados de capas inferiores, ya que han dejado de prestar su servicio a las capas superiores. Finalmente los datos llegan a la capa de aplicación, listos para ser usados por el destinatario.

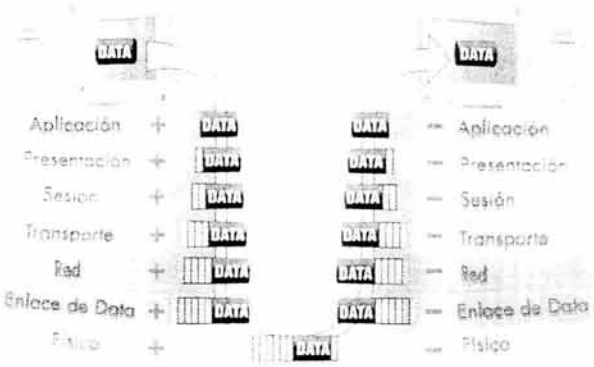


Figura 1.4: Proceso de encapsulamiento

El modelo OSI es una herramienta esencial para analizar la comunicación en las redes y en lo sucesivo se hará constante referencia a los conceptos vistos anteriormente.

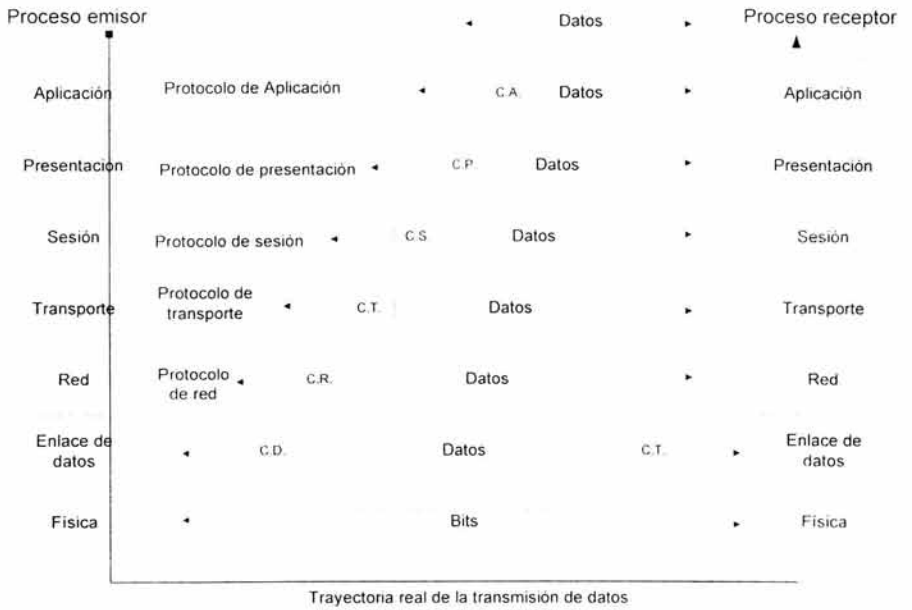


Figura 1.5: Comunicación entre capas

1.3 Pila TCP/IP

Aunque el modelo de referencia OSI es universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de transmisión/Protocolo Internet (TCP/IP). La pila de protocolo TCP/IP hace que sea posible la comunicación entre dos hosts, desde cualquier parte del mundo. El modelo TCP/IP tiene importancia histórica, al igual que las normas que permitieron el desarrollo de la industria telefónica, de energía eléctrica, el ferrocarril, la televisión y las industrias de videos.

El Departamento de Defensa de EE.UU. (DoD) creó el modelo TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. Para brindar un ejemplo más amplio, supongamos que el mundo está en estado de guerra, atravesado en todas direcciones por distintos tipos de conexiones: cables, microondas, fibras ópticas y enlaces satelitales. Imaginemos entonces que se necesita que fluya la información independientemente de la condición de cualquier nodo o red. El DoD desea que sus datos lleguen a destino siempre, bajo cualquier condición, desde un punto determinado hasta cualquier otro. Este problema de difícil solución fue lo que llevó a la creación del modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló Internet.

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI.

1.3.1 Capa 4: aplicación

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.

1.3.2 Capa 3: transporte

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Esto quiere decir que los módulos de software del protocolo en los dos sistemas extremos se comunican enviando mensajes a través de la red a fin de verificar que la transferencia esté autorizada y que ambos lados estén preparados. Después de que se haya producido toda la sincronización, se establece una conexión, y comienza la transferencia de datos. Durante la transferencia, los dos dispositivos siguen comunicándose con su software de protocolo para verificar que estén recibiendo los datos correctamente. Se mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas "Segmentos".

Una de las razones para utilizar un modelo de capas es que múltiples aplicaciones pueden compartir la misma conexión de transporte. La funcionalidad de transporte se logra segmento por segmento. Esto significa que diferentes segmentos de datos de diferentes aplicaciones que se envían al mismo destino o a varios destinos diferentes se envían según un método "el que llega primero, es atendido primero".

Cuando se envían datos desde un origen, se utiliza algún protocolo y un número de puerto asociados a la aplicación (DNS, FTP, HTTP, etc.). Los datos se encapsulan en segmentos y cuando el dispositivo destino recibe la corriente de datos, separa y clasifica los segmentos de manera tal que la capa de transporte pueda pasar los datos a la aplicación destino correspondiente. Una representación de los segmentos de datos la podemos ver en la figura 1.6.

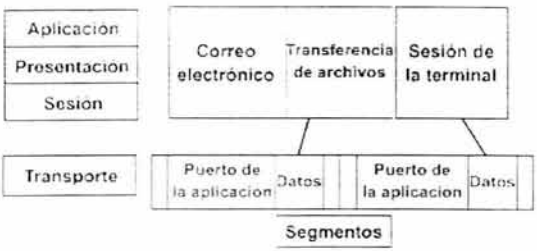


Figura 1.6: Representación de los segmentos de datos

1.3.3 Capa 2: Internet

El propósito de la capa de Internet es enviar paquetes desde cualquier red en Internet y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

Las direcciones lógicas son de gran importancia, y en el Protocolo Internet se conocen como "Direcciones IP". En el modelo de referencia OSI se ubican en la capa de red, y en el modelo TCP/IP en la capa de Internet. Al contrario de lo que ocurre con las direcciones físicas, que normalmente existen dentro de un espacio de direccionamiento plano, las direcciones IP normalmente son "jerárquicas".

1.3.4 Capa 1: acceso a la red

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de la capa física y de enlace de datos del modelo OSI.

En esta capa, que tiene su parte equivalente en el modelo OSI con la de enlace de datos, se ocupa el direccionamiento físico. Las direcciones físicas se denominan "Direcciones MAC". Para que múltiples estaciones puedan compartir los mismos medios y aún así identificarse entre sí, las direcciones MAC identifican al host para que este pueda acceder al medio y transmitir o recibir tramas de datos. Cada interfaz de LAN posee una dirección MAC exclusiva. En la mayoría de las NIC (tarjeta de interfaz de red, por sus siglas en ingles), la dirección MAC está grabada de forma indeleble en la ROM. Cuando se inicializa la NIC, esta dirección se copia en la RAM.

El diagrama que aparece en la figura 1.7 se denomina gráfico de protocolo. Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP. En la capa de aplicación aparecen protocolos que un usuario de Internet probablemente usa todos los días.

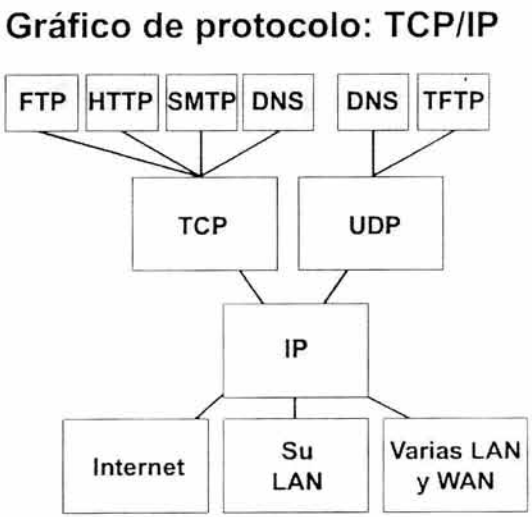


Figura 1.7

En el modelo TCP/IP existe solamente un protocolo de red: el Protocolo Internet, o 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. IP sirve como protocolo universal que permite que cualquier host en cualquier parte del mundo pueda comunicarse en cualquier momento. En la figura 1.8 podemos ver la pila del modelo TCP/IP y una comparación con el modelo OSI.

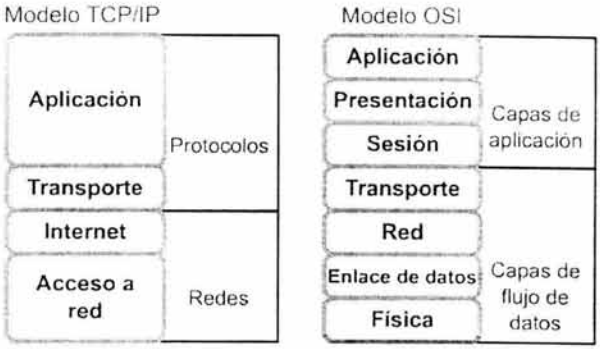


Figura 1.8: Comparación entre modelo OSI y TCP/IP

Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque este modelo se usa como guía y referencia para el análisis de la red.

1.4 Evolución del Protocolo Internet

Internet inició como una red experimental a cargo del departamento de defensa de los Estados Unidos de Norte América a finales de los años 60's, y alcanzó cierto desarrollo en los 70's. Pero fue en la década de los 80's cuando los estándares de red se fusionan para dar paso a la integración de las redes aisladas en una gran red de carácter público. El Protocolo Internet es el eje principal del funcionamiento de la "Red de redes". Este protocolo es el universalmente reconocido para comunicar dispositivos de red desde casi cualquier lugar del mundo y en ello radica su principal éxito en la industria de las comunicaciones.

1.4.1 Características del Protocolo Internet Versión 4

En la PDU de la capa de red, es decir, en los "Paquetes" se encuentra una parte fundamental del protocolo: la cabecera del protocolo Internet. En la figura 1.9 se puede ver el formato de los paquetes de capa 3, y dentro de ellos se localiza en primer lugar el agregado que realiza esta capa a los datos que vienen de capas superiores.

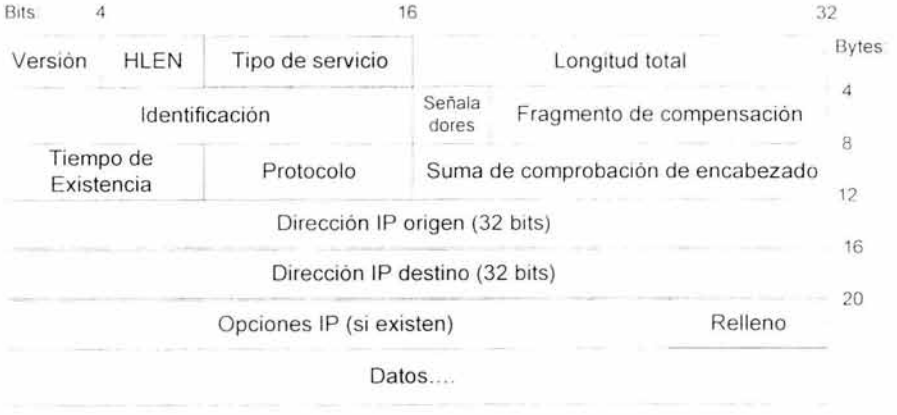


Figura 1.9: Formato del paquete IPv4

El paquete IP está formado por los datos de las capas superiores más el encabezado IP, que está formado por:

Versión

Indica la versión de IP que se usa en el momento (4 bits).

Longitud del encabezado IP (HLEN)

Indica la longitud del encabezado del paquete en palabras de 32 bits (4 bits).

Tipo de servicio

Especifica el nivel de importancia que le ha sido asignado por un protocolo de capa superior en particular (8 bits).

Longitud total

Especifica la longitud de todo el paquete IP, incluyendo datos y encabezado, en bytes (16 bits).

Identificación

Contiene un número entero que identifica el paquete actual (16 bits).

Señaladores

Un campo de 3 bits en el que los dos bits de orden inferior controlan la fragmentación; un bit que especifica si el paquete puede fragmentarse y el segundo si el paquete es el último fragmento en una serie de paquetes fragmentados.

Compensación de fragmentos

El campo que se utiliza para ayudar a reunir los fragmentos de paquetes (13 bits).

Tiempo de existencia

Mantiene un contador cuyo valor decrece, por incrementos, hasta cero. Cuando se llega a ese punto se descarta el paquete, impidiendo así que los paquetes entren en un loop interminable (8 bits).

Protocolo

Indica cuál es el protocolo de capa superior que recibe los paquetes entrantes después de que se ha completado el procesamiento IP (8 bits).

Suma de comprobación del encabezado

Ayuda a garantizar la integridad del encabezado IP (16 bits).

Dirección origen

Especifica el nodo emisor (32 bits).

Dirección destino

Especifica el nodo receptor (32 bits).

Opciones

Permite que IP soporte varias opciones, como la seguridad (longitud variable).

Datos

Contiene información de capa superior (longitud variable, máximo 64 kb).

Relleno

Se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits.

1.4.2 Direccionamiento IPv4

El direccionamiento en el Protocolo Internet tiene como base los siguientes puntos:

- Cada empresa dentro de Internet aparece como una sola red.
- Cada red de Internet se identifica con una dirección de red
- Cada host que pertenece a esa red se identifica por una dirección exclusiva.

- La ubicación de la mejor ruta se basa en la ubicación de cada dirección lógica.

Los organismos que regulan el direccionamiento en Internet son:

- IANA, Internet Assigned Numbers Authority, que es el organismo regulador para la asignación de direccionamiento IP
- Existen otros organismo regionales:
  - ARIN, American Registry for Internet Numbers para América
  - RIPE, para Europa
  - APNIC, para Asia

1.4.2.1 Direccionamiento físico

El direccionamiento físico es conocido como "Plano", es decir, todos los nodos en una red no 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 interfaz de red (NIC).
- Las direcciones físicas, en la mayoría de los casos no se pueden alterar.
- Los estándares de red más comunes hacen uso de direcciones físicas de 6 bytes a las cuales llamamos direcciones MAC (establecidas por la IEEE). Su representación es en forma Hexadecimal, y su longitud es de 48 bits.
- Las direcciones físicas solo sirven para intercomunicar equipos interconectados en una red local; ya que su nomenclatura solo hace referencia a interfaces de red.

Las direcciones MAC funcionan de esta manera. El fabricante recibe un bloque de direcciones; la primera mitad de cada dirección corresponde al código del fabricante, el resto de la dirección MAC es un número que se asigna de forma secuencial.

1.4.2.2 Direccionamiento lógico

Con el direccionamiento físico es difícil ubicar los dispositivos en otras redes ya que el formato de las direcciones no indica una forma de llegar al destino. Con el direccionamiento lógico se resuelve este problema ya que su formato es de tipo "Jerárquico". Una dirección lógica tiene una parte dedicada para ubicar la red, y otra para el "Host" destino. Las características generales de este tipo de direcciones son:

- Las direcciones lógicas, a diferencia de las físicas no se encuentran configuradas en el hardware: se configuran por software.

- Su formato varía según la arquitectura de red que se utilice (AppleTalk, Novell IPX, TCP/IP, etc.).

  - *IPX (80 bits)*

    Cinco campos en notación hexadecimal: xxxx.xxxx.xxxx.xxxx.xxxx

  - *Appletalk (24 bit)*

    Tres campos en notación decimal: yyy.yyy.yyy

  - *IP versión 4 (32 bits)*

    Cuatro campos en notación decimal: zzz.zzz.zzz.zzz

Los esquemas de direccionamiento jerárquico permiten que la información viaje por la red, así como también un método para detectar el destino de modo eficiente.

El Protocolo Internet opera con direcciones IP. Actualmente, predominan las direcciones para la versión 4, pero el nuevo formato para la versión 6 ocupará su función progresivamente.

1.4.2.3 Protocolo de Resolución de Direcciones ARP

Para que los dispositivos se puedan comunicar, los dispositivos emisores necesitan tanto las direcciones IP como las direcciones MAC de los dispositivos destino. Cuando tratan de comunicarse con dispositivos cuyas direcciones IP conocen, deben determinar las direcciones MAC. La pila TCP/IP tiene un protocolo, denominado ARP, que puede detectar automáticamente la dirección MAC. ARP permite que un nodo descubra la dirección MAC del nodo que está asociado con una dirección IP.

Los protocolos de capa 3 determinan si los datos se transportan más allá de la capa de red hacia los niveles superiores del modelo OSI. Un paquete de datos debe contener una dirección MAC destino y una dirección IP destino. Si le falta una u otra dirección, los datos no se transportan desde la capa 3 hacia las capas superiores. De esta manera, las direcciones MAC y las direcciones IP cumplen una función de equilibrio mutuo. Una vez que los dispositivos determinan las direcciones IP de los dispositivos destino, pueden agregar las direcciones MAC destino a los paquetes de datos.

Hay muchas maneras en que los dispositivos pueden determinar las direcciones MAC que se deben agregar a los datos encapsulados. Algunos mantienen tablas que contienen todas las direcciones MAC y direcciones IP de los otros dispositivos que están conectados a la misma LAN. Estas se denominan "Tablas de Protocolo de Resolución de Direcciones (ARP)", y asignan direcciones IP a las direcciones MAC correspondientes. Las tablas ARP son secciones de la memoria RAM, en las cuales la memoria caché se mantiene automáticamente en cada uno de los dispositivos. Cada nodo en una red

mantiene su propia tabla ARP. Siempre que un dispositivo de red desee enviar datos a través de una red, usa la información que le suministra su tabla ARP.

Cuando un origen determina la dirección IP de un destino, el origen consulta su tabla ARP a fin de ubicar la dirección MAC del destino. Si el origen ubica una entrada en su tabla ARP, entonces relaciona la dirección IP con la dirección MAC y la usa para encapsular los datos.

Si un host desea enviar datos, debe conocer la dirección IP destino. Si no puede ubicar una dirección MAC para el destino en su propia tabla ARP, el host inicia un proceso denominado petición ARP. La petición ARP le permite descubrir la dirección MAC destino.

Un host genera un paquete de petición ARP y lo envía a todos los dispositivos de la red. Para asegurarse de que todos los dispositivos vean la petición ARP, el origen usa una dirección de broadcast MAC. Una dirección de broadcast MAC tiene el formato FF-FF-FF-FF-FF-FF.

Como los paquetes de peticiones ARP se desplazan en un modo de broadcast, todos los dispositivos de una red local reciben los paquetes y los pasan a la capa de red donde se les analiza. Si la dirección IP de un dispositivo concuerda con la dirección IP destino de la petición ARP, ese dispositivo responde enviando su dirección MAC al origen.

1.4.2.4 Comunicación entre nodos de diferentes subredes

Para que un nodo se pueda comunicar con otro nodo de otra red, debe suministrarle un "Gateway" por defecto. Un gateway por defecto es la dirección IP de la interfaz en el router que se conecta con el segmento de red en el cual se encuentra ubicado el host origen. La dirección IP del gateway por defecto debe encontrarse en el mismo segmento de red que el host origen.

Si no se ha definido ningún gateway por defecto, la comunicación sólo se puede realizar en el propio segmento de red lógica del dispositivo. El host que envía los datos realiza una comparación entre la dirección IP destino y su propia tabla ARP. Si no encuentra coincidencias, debe tener una dirección IP por defecto que pueda utilizar. Si no hay un gateway por defecto, el host origen no tiene ninguna dirección IP destino y el mensaje no se puede enviar.

Después de que el router ubica la red, mediante la dirección IP destino, se utiliza nuevamente ARP para obtener la dirección MAC del host destino y finalmente llegar a éste.

1.4.3 Origen del Protocolo Internet Versión 6

El esfuerzo para desarrollar el protocolo sucesor de IPv4 comenzó a inicios de la década de los 90s por la "Internet Engineering Task Force (IETF)". Varios movimientos paralelos empezaron simultáneamente, todos intentando resolver el problema del limitado espacio de direcciones así como dotar de nuevas funcionalidades. La IETF comenzó el área IPng en 1993 para investigar las diferentes propuestas y hacer recomendaciones para futuros procedimientos.

Los directores del área IPng de la IETF recomendaron la creación de IPv6 en la reunión de la IETF en Toronto en 1994[1.2]. Los directores formaron un grupo de trabajo "Address Lifetime Expectation " (ALE), cuyo trabajo sirvió para determinar si el tiempo de vida esperado para IPv4 permitiría el desarrollo de un protocolo con nuevas funcionalidades o si el mismo tiempo permitiría únicamente el desarrollo de una solución al espacio de direcciones. En 1994, el grupo de trabajo ALE proyectó el agotamiento de direcciones IPv4 que ocurrirá entre los años 2005 y 2011, basados en las estadísticas que estuvieron disponibles todo el tiempo.

Hubo cuatro principales propuestas llamadas CNAT, IP Encaps, Nimrod, y CLNP. Tres propuestas más continuaron: "The P Internet Protocol " (PIP), "The Simple Internet Protocol (SIP), y TP/IX. Después en la reunión de la IETF en San Diego en marzo de 1992, Simple CLNP desarrollo en TCP y UDP con direcciones más grandes (TUBA), e IP desarrollo en la encapsulación de direcciones IP (IPAE). IPAE se unió con PIP y SIP y se llamaron "Simple Internet Protocol Plus" (SIPP). El grupo de trabajo TP/ IX cambió su nombre por "Common Architecture for the Internet" (CATNIP). Las principales propuestas fueron ahora CATNIP, TUBA, y SIPP[1.3].

"The Internet Engineering Steering Group" aprobó la recomendación de IPv6 "IPv6 recommendation" y publicó el draft con la propuesta en Noviembre 17 de 1994. El conjunto de protocolos IPv6 llegó a ser un estándar de la IETF en Agosto 10 de 1998.

1.4.3.1 Funcionalidad

IPv6 es una de las más importantes actualizaciones de redes y tecnología en la historia. Poco a poco crecerá dentro de la existente infraestructura IPv4. El desarrollo de IPv6 y sus implementaciones ya están en casi todo el mundo. IPv6 es producto de la evolución de IPv4, por lo que puede ser instalado como una actualización de software en muchos dispositivos de Internet, y puede interactuar con IPv4. IPv6 esta diseñado para trabajar bien en grandes redes con tecnología Gigabit Ethernet, ATM, y otras, así como en redes de poco ancho de banda. Además, permite una plataforma para nuevas funcionalidades de Internet que serán requeridas en un futuro cercano, tales como extensión en el direccionamiento, una mejor seguridad, y calidad de servicio (QoS).

[1.2] Su recomendación esta especificada en el RFC 1752. "The Recomendation for the IP Next Generation Protocol"
[1.3] En el RFC 1752 se tiene una discusión de estas propuestas.

1.5 La estructura del protocolo IPv6

Son muchas las funcionalidades que proporciona IPv6. Uno de los cambios más importantes en la nueva versión del protocolo IP es el formato de las direcciones. Ahora se trata de direcciones de 128 bits divididas en 8 campos de dos bytes cada uno, los cuales se representan en formato hexadecimal. Con esto se tiene que en IPv6 el espacio de direcciones es de 2^{128}, o aproximadamente $3.4x10^{38}$. En IPv4 se cuenta con tan solo 2^{32}, o 4 294 967 296 direcciones, las cuales ya se están agotando.

En IPv6 se conservan las direcciones de tipo unicast y multicast, pero además se agrega la dirección anycast. La dirección unicast da referencia de un solo nodo destino, la multicast ubica a un grupo de nodos; y la anycast busca a un nodo dentro de una grupo. Mientras que desaparece la dirección IP de broadcast, la cual se dirige a todos los nodos de un segmento de red.

1.5.1 Los campos en la cabecera de IPv6

El encabezado de un paquete IPv6 tiene una longitud fija de 40 bytes[1.4]. Al familiarizarse con los campos de la cabecera IPv6 entenderá mejor como funciona IPv6. La figura 1.10 muestra el encabezado IPv6. Los campos son discutidos en los siguientes párrafos.

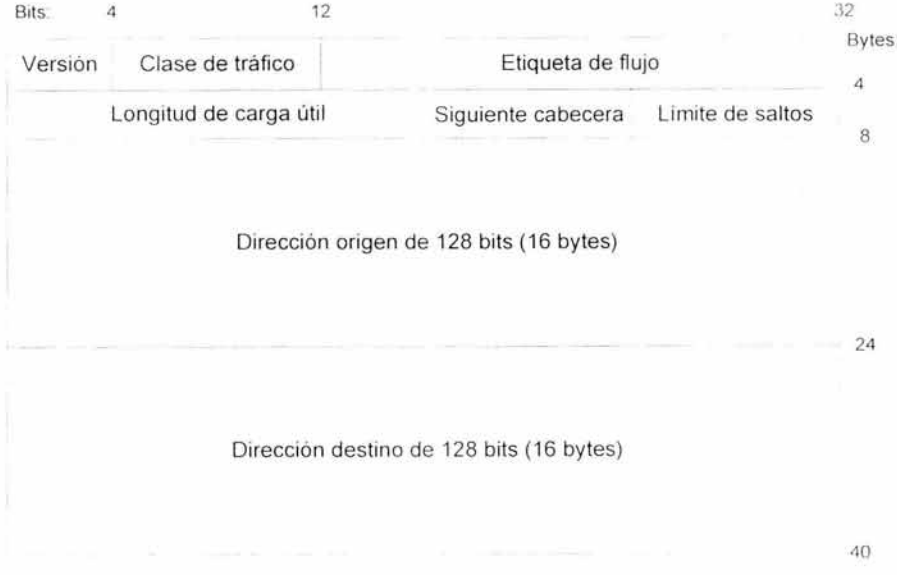


Figura 1.10: Campos de la Cabecera IPv6

[1.4] La estructura del encabezado de un paquete IPv6 esta especificado en el RFC 2460

La figura 1.10 muestra que la cabecera IPv6 tiene un tamaño total de 40 bytes, lo cual representa el doble del tamaño de una cabecera IPv4 de longitud mínima. La mayor parte del encabezado lo componen las direcciones origen y destino (32 bytes), y solo se dejan 8 bytes para otra información de cabecera.
La cabecera IPv6 esta integrada por los siguientes campos:

Versión (4 Bits)

Este es un campo de 4 bits y contiene la versión del protocolo. En el caso de IPv6, el número es 6.

Clase de tráfico (1 Byte)

Este campo reemplaza al de "Tipo de Servicio" en IPv4. Este campo facilita el manejo de "Datos en Tiempo Real" y otro tipo de datos que requieren soporte especial. Este campo puede ser usado por nodos y routers para identificar y distinguir entre diferentes clases o prioridades de paquetes Ipv6[1.5].

Etiqueta de Flujo (20 Bits)

Este campo distingue paquetes que requieren el mismo trato, en orden para facilitar el soporte de tráfico en tiempo real. Un host origen pude etiquetar secuencias de paquetes con un conjunto de opciones. Los routers guardan el registro de los flujos y pueden procesar más eficientemente paquetes que pertenecen al mismo flujo porque no tienen que volver a procesar cada cabecera de los paquetes. Un flujo únicamente es identificado por la etiqueta de flujo y dirección del nodo origen. Los nodos que no soportan las funciones del campo de etiqueta de flujo requieren pasar el campo intercambiado cuando envían un paquete e ignorar el campo cuando reciben el paquete. Todos los paquetes que pertenecen al mismo flujo deben tener las mismas direcciones origen y destino.

Longitud de carga útil (2 Bytes)

Este campo especifica el tamaño de los datos portados después del encabezado IP. El cálculo en IPv6 es distinto del que ocurre en IPv4. La longitud de la carga en IPv4 incluye a la cabecera IPv4, mientras que en IPv6 contiene únicamente los datos que siguen del encabezado IPv6. Las cabeceras de extensión son consideradas como parte de la carga y por lo tanto están incluidas en el cálculo.

El hecho de que el campo de longitud de carga útil tiene 2 bytes, limita el tamaño del paquete a un máximo de 64 KB. IPv6 tiene una cabecera de extensión "Jumbogram", la cual soporta tamaños de paquetes más grandes, si es necesario. Los "Jumbograms" son relevantes solo cuando los nodos IPv6 son agregados a enlaces que tienen una MTU de enlace más grande que 64 KB.

[1.5] El RFC 2474, "Definition of the Differentiatted Services Field (DS Field) in the IPv4 and IPv6 Headers", describe como puede ser usado el campo de "Clase de Tráfico" en IPv6.

Siguiente Cabecera (1 Byte)

En IPv4, este campo equivale al "Protocol Type". Este fue renombrado en IPv6 para reflejar la nueva organización de los paquetes IP. Si la siguiente cabecera es UDP o TCP, este campo contendrá los mismos números del protocolo que en IPv4; por ejemplo, protocolo número 6 para TCP o 17 para UDP. Pero si se usan cabeceras de extensión con IPv6, este campo contiene el tipo de la siguiente cabecera de extensión. La tabla 1.1 muestra una lista de los valores en el campo de siguiente cabecera.

Valor	*Descripción*
0	En una cabecera IPv4: reservado y no usado En una cabecera IPv6: siguiente cabecera de opción "hop by hop".
1	"Internet Control Message Protocol (ICMPv4)"
2	"Internet Group Management Protocol (IGMPv4)"
4	IP en IP (encapsulamiento)
6	TCP
8	"Exterior Gateway Protocol (EGP)"
9	IGP – alguna puerta de enlace interior privada (usada por Cisco de su IGRP)
17	UDP
41	IPv6
43	Cabecera de ruteo
44	Cabecera de fragmentación
45	"Interdomain Routing Protocol (IDRP)"
46	"Resource Reservation Protocol (RSVP)"
50	Cabecera de carga útil con seguridad de encriptación
51	Cabecera de autenticación
58	ICMPv6
59	No siguiente cabecera de IPv6
60	Cabecera de opciones de destino
88	EIGRP
89	OSPF
108	Protocolo de compresión de carga IP
115	"Layer 2 Tunneling Protocol (LTP)"
132	"Stream Control Transmission Protocol (SCTP)"
134 – 254	No asignado
255	Reservado

Tabla 1.1

Los números del tipo de cabecera derivan del mismo rango de números de protocolo por lo que no deben tener conflictos con ellos.

Limite de Saltos (1 Byte)

Este campo es análogo al de TTL en IPv4. El campo TTL contiene un número de segundos que indican cuanto puede permanecer un paquete en la red antes de ser destruido. Este campo fue renombrado a limite de saltos en IPv6. El valor en este campo ahora expresa un número de saltos y no segundos. Cada vez que un nodo envía, el valor disminuye en uno.

Dirección Origen (16 Bytes)

Esta dirección contiene únicamente la dirección del origen del paquete.

Dirección Destino (16 Bytes)

Este campo contiene la dirección IP destino del paquete.

1.5.2 Cabeceras de extensión

El encabezado en IPv4 puede extenderse desde 20 hasta 60 bytes, para especificar opciones tales como seguridad, ruteo, etc. Esta capacidad raramente se ha usado por el impacto que implica, generalmente más carga al procesador principal.

IPv6 tiene un nuevo modo de manipular las opciones que ha mejorado sustancialmente el procesamiento. Esto se traduce en cabeceras adicionales llamadas "Cabeceras de extensión", cuyo valor del campo "siguiente cabecera" se encuentra en la tabla 1.1.

Pueden ser cero, una o más cabeceras de extensión entre el encabezado IPv6 y el encabezado del protocolo de capa superior. Cada cabecera de extensión es identificada por el campo de "Siguiente Cabecera" en la cabecera que le precede.

Actualmente se tienen definidas seis cabeceras de extensión[1.6]: "Hop by hop", "Routing", Fragmentación, Opciones de destino, Autenticación y Encriptación.

Las cabeceras de extensión son procesadas o examinadas únicamente por el nodo identificado en el campo de "Dirección Destino" del encabezado IPv6. Si la dirección en el campo "Dirección Destino" es de tipo multicast, las cabeceras de extensión son examinadas y procesadas por todos los nodos que pertenecen al grupo multicast. Las cabeceras de extensión deben ser estrictamente procesadas en el orden que tienen en el paquete. Hay una excepción a la regla anterior: "solo el nodo destino procesará la cabecera de extensión". Si la cabecera de extensión es de opciones "Hop by Hop", la información que lleva debe ser analizada y procesada por cada nodo a lo largo de la ruta que sigue el paquete.

Cuando se usan cabeceras de extensión es conveniente seguir el siguiente orden: cabecera IPv6, cabeceras de extensión y cabecera de capa superior. En La figura 1.11 se muestra como se "encadenan" las cabeceras con la siguiente y la anterior (si existen).

[1.6] Las cabeceras de extensión se definen en el RFC 2460

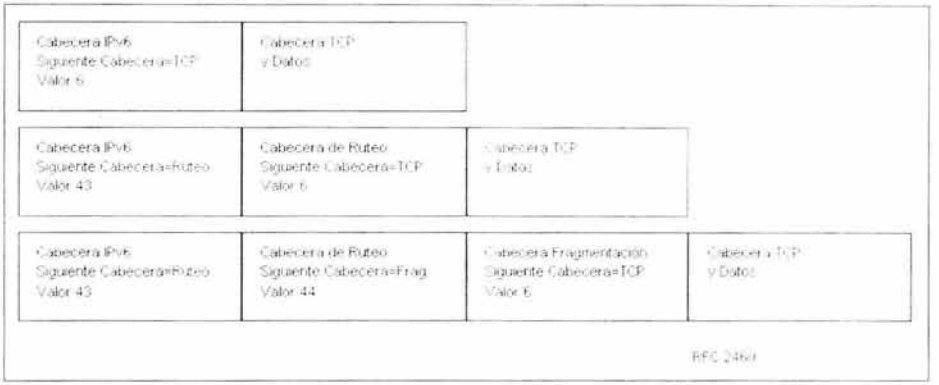


Figura 1.11: El uso de las "Cabeceras de extensión"

Cuando un host IPv6 descubre que el paquete que va a enviar a través de una ruta es más grande que la MTU disponible, debe utilizar la fragmentación[1.7]. El paquete IPv6 se clasifica en una parte que no se puede dividir y en otra que si es posible hacerlo. Con esto puede enviar la parte no divisible en distintos paquetes junto con cada uno de los fragmentos. La parte que no se puede fragmentar consiste principalmente en la cabecera IPv6 y posiblemente algunas cabeceras adicionales que deben ser procesadas por cada uno de los nodos de la ruta. La parte que se puede fragmentar incluye a los datos, cabeceras de capas superiores y algunas cabeceras de extensión que son procesadas por el host destino.

En los casos en que IPv6 es encapsulado en IPv4, la cabecera de "Capa Superior" puede ser otra cabecera IPv6 y puede contener cabeceras de extensión que siguen las mismas reglas.

1.5.3 ICMPv6

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente para IPv4, ha sido actualizado para permitir su uso bajo IPv6.

El protocolo resultante de dicha modificación es ICMPv6[1.8], y se le ha asignado un valor, para el campo de "siguiente cabecera", igual a 58. ICMPv6 es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6.

El formato genérico de los mensajes ICMPv6 es el mostrado en la figura 1.12.

[1.7] El RFC 2460 describe el proceso de fragmentación
[1.8] El Protocolo ICMPv6 esta definido en el RFC 2463

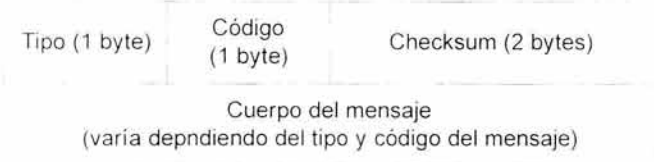


Figura 1.12: Formato de mensajes ICMPv6

El campo "codigo" depende del tipo de mensaje, y se emplea para clasificar el mensaje ICMPv6.

El "Checksum" o "Código de redundancia" nos permite detectar errores en el mensaje.

ICMPv6 maneja dos clases de mensajes: los mensajes de error y los informativos. Los mensajes de error tienen cero en el bit de mayor peso del campo "tipo", por lo que sus valores se sitúan entre 0 y 127. Los valores de los mensajes informativos oscilan entre 128 y 255.

1.5.4 Neighbor Discovery

El protocolo de resolución de direcciones ARP es sustituido por el protocolo "Neighbor Discovery" (ND)[1.9], el cual usa mensajes ICMPv6 para determinar direcciones físicas de "Vecinos" ubicados en un mismo enlace, encontrar routers, y detectar cambios de direcciones en el enlace.

Neighbor Discovery define cinco tipos de paquetes ICMPv6:

- *Solicitud de Router (Router Solicitation)*

  Generado por una interfaz cuando es activada, para pedir a los routers que se "anuncien". El tipo de paquete ICMPv6 es el 133.

- *Anunciación de Router (Router Advertisement)*

  Generado por los routers periódicamente o como consecuencia de una "solicitud de router", a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de internet, como prefijos, tiempos de vida, límite de saltos, etc. El tipo de paquete ICMPv6 es el 134.

- *Solicitud de Vecino (Neighbor Solicitation)*

  Generado por los nodos para determinar la dirección física de sus vecinos, o para verificar que el nodo vecino sigue activo, así como para detectar las direcciones duplicadas. El tipo de paquete ICMPv6 es el 135.

[1.9] Neighbor Discovery se encuentra especificado en el RFC 2461.

- *Anuncio de Vecino (Neighbor Advertisement)*

  Generado por los nodos como respuesta a la "solicitud de vecino", o bien para indicar cambios de direcciones en la capa de enlace de datos. El tipo de paquete ICMPv6 es el 136.

- *Redirección (Redirect)*

  Generado por los routers para informar a los hosts de un salto mejor para llegar a determinado destino. El tipo de paquete ICMPv6 es el 137.

Los mensajes de "solicitud de vecino" y "anunciación de vecino" permiten la resolución de direcciones de capa de enlace y la detección de vecinos inalcanzables. Si la dirección destino es multicast, entonces el origen esta resolviendo una dirección de capa de enlace. Si el origen esta verificando el alcance a un vecino, la dirección destino es unicast. Este tipo de mensaje es usado para detectar direcciones IP duplicadas. El formato del mensaje de solicitud de vecino es mostrado en la figura 1.13.

Tipo (1 byte)	135	135 = Solicitud de vecino
Código (1 byte)	0	No usado
Checksum (2 bytes)		
Reservado (4 bytes)		
Dirección objetivo (16 bytes)	.....	Usado para mensajes de detección de "inalcanzable"
Opciones (variable)		**Opciones posibles:** dirección de capa de enlace origen

Figura 1.13: Formato del mensaje de solicitud de vecino.

En la cabecera IP de este tipo de mensaje, la dirección origen puede ser la dirección de la interfaz del host que hace la solicitud o, en el caso de detección de direcciones duplicadas (DAD), la dirección no especificada (todo ceros). La dirección objetivo es usada solo si se trata de mensajes de detección de inaccesibilidad o DAD. No debe ser una dirección multicast.

El campo de opciones pude contener la dirección de capa de enlace origen solo si no es un mensaje DAD. En un mensaje DAD que usa una dirección no especificada como dirección origen, el campo de opciones es puesto en cero.

El mensaje de anuncio de vecino es enviado como respuesta al mensaje de solicitud de vecino o para propagar información rápidamente. El formato es mostrado en la figura 1.14.

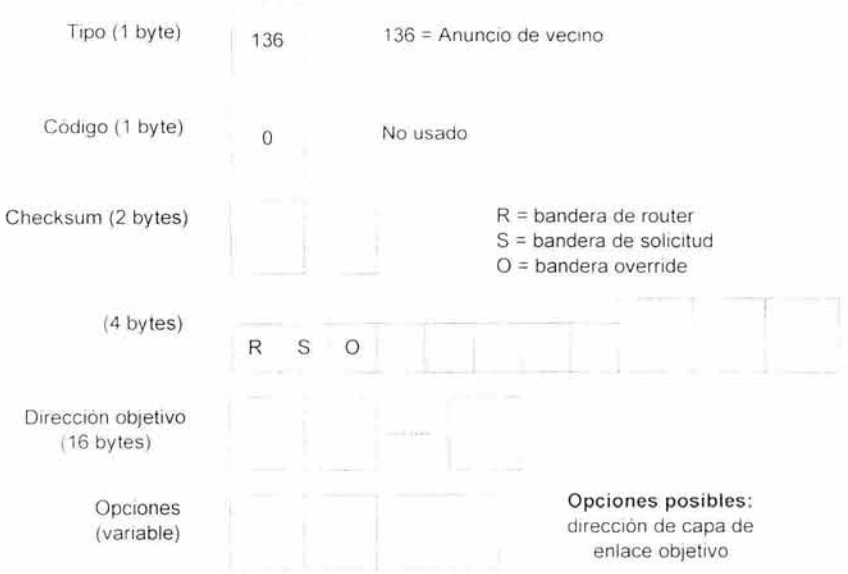


Figura 1.14: Formato del mensaje de anuncio de vecino

El tipo de dirección en la cabecera IP indica si el mensaje es una respuesta a un mensaje de solicitud. En caso de ser un mensaje solicitado, la dirección IP destino es la dirección origen de la interfaz que envio la solicitud. Si el mensaje es una respuesta a un mensaje DAD que fue originado por una dirección no especificada, la respuesta irá a la dirección multicast **FF02::1**. Esto también se usa para anuncios periódicos.

Cuando la bandera "Router" es activada, el emisor es un router. Pero cuando se trata de la bandera de "Solicitud", el mensaje es enviado como respuesta a una solicitud de vecino. Por ejemplo un host puede responder que es alcanzable al activar el bit "S" como respuesta a un mensaje de detección de "inalcanzable". La bandera "Override" indica que la información en el mensaje de anuncio debe borrar el actual cache de vecinos y actualizar las direcciones de capa de enlace. Si el bit "O" no es activado, el anuncio no actualizará el cache existente de direcciones de capa de enlace.

En anuncios solicitados, la dirección objetivo contiene la dirección de la interfaz que envió la solicitud. En anuncios no solicitados, este campo contiene la dirección de la interfaz cuya dirección de capa de enlace a cambiado. Una posible opción para el campo de opciones es la dirección de capa de enlace objetivo.

El campo de opciones tiene el formato que se muestra en la figura 1.15.

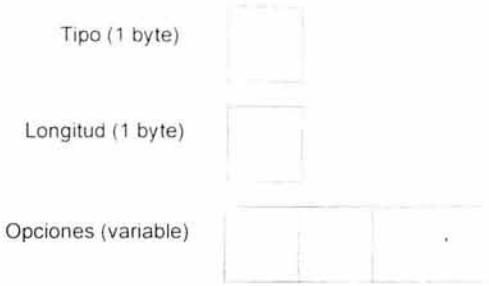


Figura 1.15: Formato del campo de opciones.

Los tipos de opciones son los siguientes:

- Tipo 1: dirección de capa de enlace origen
- Tipo 2: dirección de capa de enlace objetivo
- Tipo 3: información de prefijo
- Tipo 4: cabecera de redirección
- Tipo 5: MTU

El tamaño de la opción es indicado en el campo de longitud.

Neighbor Discovery reemplaza al protocolo ARP para adaptarse a las características de IPv6.

1.5.5 Soporte de capa 2 en IPv6

Uno de los objetivos en el desarrollo de IPv6 es que sea capaz de soportar tantas tecnologías de red como sea posible, sin cambios importantes. Esto se conoce como "IP sobre todo". Para hacer IP independiente de la capa de enlace de datos, se requiere de una interfaz para esta capa, la cual puede ser Ethernet, ATM, Token Ring, etc. La interfaz debe ser flexible y capaz de adaptarse a diferentes requerimientos. Multicast ha aumentado su campo de aplicación, mientras que el broadcast ya no es usado en IPv6.

Cuando un paquete es enviado de una red hacia otra, no se considera el tipo de medio de red que atraviesa el paquete. IP solo considera la dirección destino. Después IP pasa el paquete a la capa de enlace de datos. Cada tecnología de red define un mecanismo específico de direccionamiento[1.10]. "Neighbor Discovery" es usado para mapear las direcciones IP con las direcciones MAC.

Ethernet, tecnología LAN ampliamente utilizada[1.11], usa un esquema de direccionamiento de 48 bits. Los fabricantes de hardware Ethernet disponen de un bloque de direcciones en forma secuencial junto con el identificador de la compañía. Es por ello que dos intefaces Ethernet no pueden tener la misma dirección. Una trama Ethernet puede ser de tamaño variable, pero no más pequeña de 64 bytes ni más grande de 1518 bytes. Los paquetes sobre Ethernet tienen un MTU de 1500 bytes por defecto. El tamaño de la MTU puede ser configurado manualmente.

La cabecera Ethernet contiene las direcciones Ethernet origen y destino, y el código de "Tipo de Ethernet". El código para IPv6 es 0x86DD.

1.5.6 Relación de IPv6 con protocolos de capa superior

El Impacto de IPv6 en los protocolos de capa superior es mínimo ya que los servicios no han cambiado substancialmente. Los cambios más importantes son necesarios cuando se usa una dirección IP. Cualquier proceso o aplicación que usa una dirección IP necesita ser actualizado para ser capaz de manejar el formato de las direcciones de 128 bits.

La "Checksum" o "Suma de comprobación" se realiza en diferentes capas. La cabecera IPv6 no tiene checksum. Sin embargo, en la capa de transporte es importante una checksum para detectar malas entregas de paquetes. Otros protocolos de capa superior pueden usar checksum también. Todos los cálculos de checksum que incluyen la dirección IP deben ser modificados para soportar el formato de 128 bits.

Los protocolos de la capa de transporte TCP y UDP agregan checksum a sus paquetes. Una checksum es generada usando una pseudo-cabecera. La pseudo-cabecera de TCP y UDP para IPv6 contiene campos para las direcciones origen y destino, longitud de la carga útil, y el valor de la siguiente cabecera. Si el paquete IPv6 contiene una cabecera de ruteo, la dirección destino debe ser del destino final.

Como las direcciones IPv6 son mucho más largas que las de IPv4, la especificación de IPv6 incluye una nueva versión de pseudo-cabecera. La especificación toma en cuenta que puede existir un número desconocido de cabeceras de extensión antes de TCP o UDP, lo cual es esencial cuando se calcula la longitud de la carga útil de la pseudo-cabecera. En IPv4 la checksum para UDP era opcional, contrario a lo que sucede en IPv6, donde es obligatoria. Si el resultado de la checksum es cero, se tiene un mensaje de error y se descarta el paquete.

[1.10] En el apéndice se puede consultar la lista de RFC's donde se encuentran los que definen el formato de los paquetes IPv6 transmitidos sobre diferentes tecnologías LAN y WAN.
[1.11] EL RFC 2464 describe la transmisión de paquetes IPv6 sobre Ethernet.

El nodo origen calcula la checksum y la guarda, para que el destino la verifique. En la figura 1.16 se observa el formato de la pseudo-cabecera.

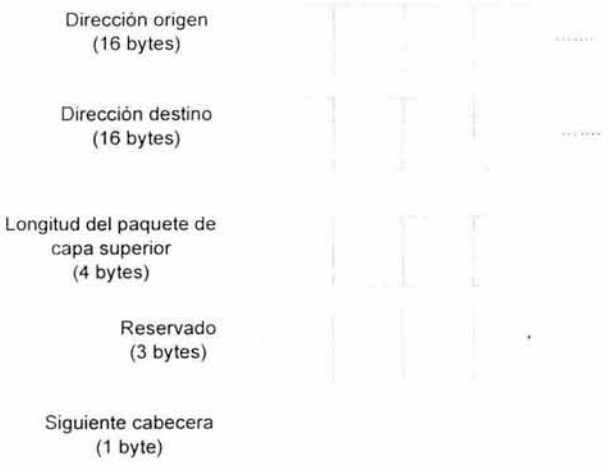


Figura 1.16: formato de pseudo-cabecera

En general IPv6 mejora las funciones que aún retiene de IPv4 e incorpora nuevas características que lo hacen un protocolo muy completo y sofisticado.

CAPÍTULO 2

PROTOCOLOS DE ENRUTAMIENTO

2.1 Introducción

El principal objetivo de la capa de red es encaminar o dirigir los paquetes desde el origen al destino. Esta es la única capa que "ve" y conoce la topología de la red, y está formada por dos tipos de nodos:

- Nodos terminales

  Generan o reciben paquetes de otros nodos, nunca encaminan paquetes dirigidos a terceros.

- Nodos intermedios o de enrutamiento

  Se utilizan para encaminar paquetes entre los nodos terminales. Suelen ser arquitecturas dedicadas y diseñadas especificamente para esa función, con sistemas operativos en tiempo real, aunque en ocasiones también se utilizan para desempeñar esta función computadoras normales.

La terminología de los dos tipos de nodos es muy diversa y varia según el tipo de red y la "cultura" de que se trate. Aunque la terminología no se puede dividir de forma estricta los nodos reflejan las denominaciones más características en algunos de los casos más habituales. Dado que la función de los nodos intermedios es interconectar redes, normalmente tienen varias interfases físicas, y los nodos terminales normalmente una. En cada interfaz física de un nodo funciona una instancia independiente del nivel físico y del nivel de enlace, y por el contrario, el nivel de red es normalmente global para todo el nodo. Por ejemplo, en el caso de IP cada interfaz física tiene, al menos, una dirección de red, independientemente de que puedan tener varias. En una LAN Ethernet, todos los nodos terminales se comunican directamente entre si usando los protocolos MAC, sin necesidad de nodos intermedios, por lo que la capa de red es innecesaria. Esto incluye el caso en que la LAN incluya bridges o switches de cualquier tipo. Debido a esto, el nivel de enlace tiene una complejidad mayor. Los bridges MAC, en especial los de enrutamiento desde el origen, desempeñan una función hasta cierto punto equivalente a la de un nodo intermedio de nivel de red pues reenvían la información entre los distintos segmentos LAN. Los servicios que ofrece el nivel de red deberán en lo posible aislar al nivel de transporte de detalles tales como tipo de tecnología física utilizada (LAN, WAN), número y topología de las subredes, etc. Las direcciones de red deberán tener un formato homogéneo, cualquiera sea el medio físico o subred utilizados.

Cuando una aplicación del host necesita enviar un paquete a un destino en una red distinta, el host direcciona la trama de enlace de datos hacia el router, utilizando la dirección de una de las interfaces del router. El proceso de la capa de red del router examina el encabezado del paquete de entrada para determinar la red destino y luego consulta la tabla de enrutamiento que asocia las redes con las interfaces de salida. El paquete se encapsula nuevamente en la trama de enlace de datos apropiada para la interfaz seleccionada y se ubica en la cola para su entrega al siguiente salto en la ruta.

Este proceso tiene lugar cada vez que el paquete se envía a través de otro router. En el router que se encuentra conectado a la red del host destino, el paquete se

encapsula en el tipo de trama de enlace de datos de la LAN destino y se entrega al host destino.

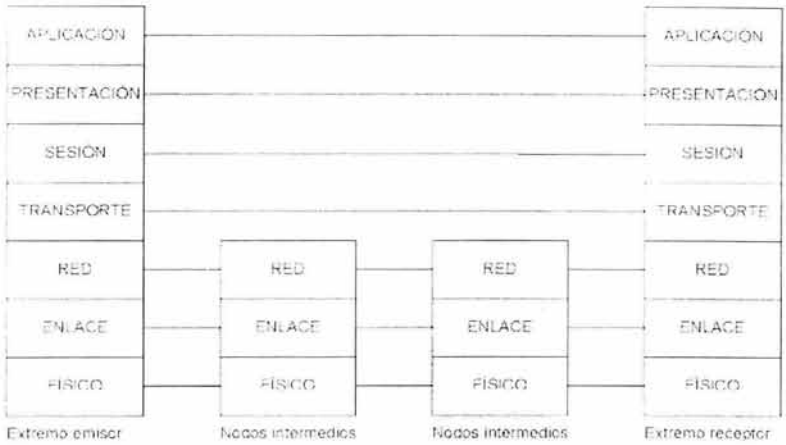


Figura 2.1

Los routers pueden soportar varios protocolos de enrutamiento independientes y mantener tablas de enrutamiento para varios protocolos enrutados. Esta capacidad le permite al router entregar paquetes desde varios protocolos enrutados a través de los mismos enlaces de datos.

2.2 Objetivos de los protocolos de enrutamiento

2.2.1 Ruta óptima

Ruta óptima se refiere a la capacidad del protocolo de enrutamiento para seleccionar la mejor ruta. La mejor ruta depende de las métricas y de las asignaciones de valor de la métrica que se usan para hacer el cálculo. Por ejemplo, un protocolo de enrutamiento puede usar el número de saltos y el retardo, pero puede asignar un valor más importante al retardo en el cálculo.

2.2.2 Simplicidad y eficiencia

El diseño de los protocolos de enrutamiento también busca que sean lo más simples y eficientes que sea posible. La eficiencia es particularmente importante cuando el protocolo de enrutamiento se debe ejecutar en un dispositivo con recursos físicos limitados.

2.2.3 Solidez

Los protocolos de enrutamiento deben ser sólidos. En otras palabras, deben ejecutarse correctamente aún ante circunstancias inusuales o imprevistas, tales como fallas del hardware, condiciones de carga elevada e implementaciones incorrectas. Como los routers están ubicados en los puntos de unión de la red, pueden provocar problemas considerables cuando fallan. Los mejores protocolos de enrutamiento a menudo son aquellos que con el tiempo han demostrado su eficiencia y que se han mantenido estables bajo una serie de diferentes condiciones de la red.

2.2.4 Convergencia rápida

Los protocolos de enrutamiento deben converger rápidamente. La convergencia es la velocidad y la capacidad de un grupo de dispositivos de red que ejecutan un protocolo de enrutamiento especifico para concordar acerca de la topología de una red después de que se produce un cambio en dicha topología. Cuando se produce un problema en la red, tal como un cambio en la topología, que hace que las rutas dejen de funcionar o queden disponibles, los routers distribuyen mensajes de actualización de enrutamiento. Los mensajes de actualización de enrutamiento se envían entre los routers, y de tal modo hacen que las rutas óptimas se vuelvan a calcular y con el tiempo hacen que todos los routers concuerden en estas rutas. Los protocolos de enrutamiento que convergen lentamente pueden provocar loops de enrutamiento o la interrupción del servicio de la red.

2.2.5 Flexibilidad

Los protocolos de enrutamiento también deben ser flexibles. En otras palabras, deben adaptarse de forma rápida y precisa a una serie de diferentes circunstancias de la red. Por ejemplo, supongamos que un segmento de red deja de funcionar. Varios protocolos de enrutamiento rápidamente seleccionan la segunda mejor ruta para todas las rutas que normalmente utilizan un segmento determinado. Los protocolos de enrutamiento se pueden programar para adaptarse a los cambios en el ancho de banda de la red, el tamaño de la cola del router, el retardo de la red y otras variables.

2.3 Loops de enrutamiento

La figura 2.2 muestra un loop de enrutamiento. En este caso, el paquete llega al Router 1 en el momento T1. El Router 1 ya se ha actualizado, de modo que sabe que la mejor ruta hacia el destino implica que la siguiente parada debe ser el Router 2. Por lo tanto, el Router 1 envía el paquete al Router 2. El Router 2 todavía no se ha actualizado y cree que el mejor salto siguiente es el Router 1. Por lo tanto, el Router 2 envía el paquete de vuelta al Router 1. El paquete continuará dando saltos para atrás y para adelante entre los dos routers hasta que el Router 2 reciba la actualización de enrutamiento o hasta que el paquete se haya conmutado la mayor cantidad de veces que esté permitido. Los distintos protocolos de enrutamiento tienen distintos números máximos; el administrador de red generalmente puede definir números máximos menores.

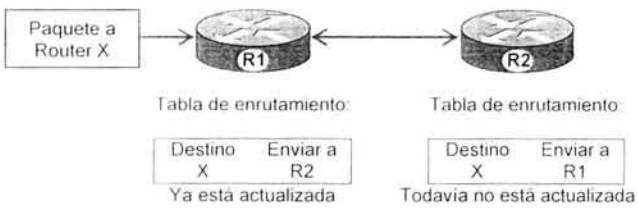


Figura 2.2. Loop de enrutamiento

2.4 Rutas estáticas versus rutas dinámicas

El conocimiento de las rutas estáticas es gestionado manualmente por el administrador de red, que lo introduce en la configuración de un router. El administrador debe actualizar manualmente esta entrada de ruta estática siempre que un cambio en la topología de la red requiera una actualización.

El conocimiento de las rutas dinámicas funciona de manera diferente. Después de que un administrador de red introduce comandos de configuración para empezar el enrutamiento dinámico, el conocimiento de la ruta se actualiza automáticamente a través de un proceso de enrutamiento siempre que se reciba nueva información de la red. Los cambios en el conocimiento dinámico se intercambian entre routers como parte del proceso de actualización.

2.4.1 Rutas estáticas

El enrutamiento estático posee varias aplicaciones útiles. Mientras que el enrutamiento dinámico tiende a revelar todo lo que se conoce acerca de la red, es posible que por razones de seguridad se desee ocultar parte de una red. El enrutamiento estático le permite especificar la información que desea revelar acerca de redes restringidas.

Cuando se puede acceder a una red a través de un solo camino, una ruta estática hacia la red puede ser suficiente. Este tipo de red se denomina red de conexión única. La configuración del enrutamiento estático para una red de conexión única (stub) evita el gasto que implica el enrutamiento dinámico.

La figura 2.3 muestra el uso de una ruta por defecto: una entrada en la tabla de enrutamiento que dirige los paquetes hacia el salto siguiente, cuando este salto no se encuentra explícitamente determinado en la tabla de enrutamiento. Se pueden establecer rutas por defecto como parte de la configuración estática.

En este ejemplo, los routers de la empresa X poseen un conocimiento específico de la topología de la red de la empresa X, pero no de las demás redes. Mantener el conocimiento de cada una de las demás redes accesibles a través de la nube de Internet es totalmente innecesario y poco razonable. En lugar de mantener un conocimiento específico de cada red, se informa a cada router de la empresa X la ruta por defecto que puede utilizar para llegar a cualquier destino desconocido direccionando el paquete hacia Internet.

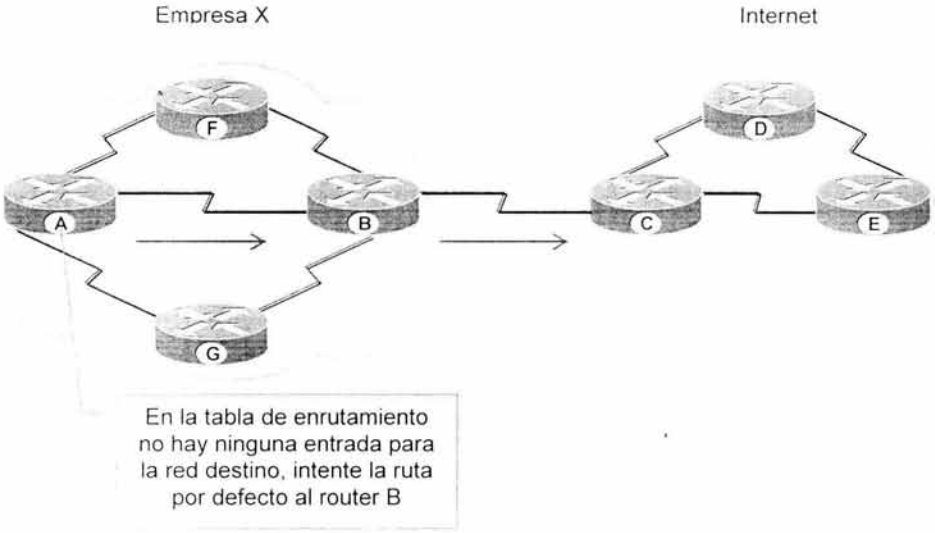


Figura 2.3: Ruta por defecto

2.4.2 Rutas dinámicas

La red que aparece en la figura 2.4 se adapta de forma diferente a los cambios de topología, según si usa la información de enrutamiento configurada de forma estática o dinámica.

El enrutamiento estático permite que los routers enruten correctamente un paquete desde una red a otra tomando como base la información configurada. El router consulta su tabla de enrutamiento y utiliza el conocimiento estático que reside allí para transferir el paquete hacia el Router D. El Router D hace lo mismo y transfiere el paquete al Router C. El Router C entrega el paquete al host destino.

Si la ruta entre el Router A y el Router D falla, el Router A no podrá transferir el paquete al Router D utilizando esa ruta estática. Hasta que el Router A se reconfigure manualmente para enviar paquetes a través del Router B, la comunicación con la red destino es imposible.

El enrutamiento dinámico ofrece más flexibilidad. Según la tabla de enrutamiento generada por el Router A, un paquete puede llegar a destino por la ruta preferida a través del Router D. Sin embargo, una segunda ruta hacia el destino está disponible a través del Router B. Cuando el Router A reconoce que el enlace al Router D está caído, ajusta su propia tabla de enrutamiento, haciendo que la ruta a través del Router B se convierta en la ruta preferida hacia el destino. Los routers siguen enviando paquetes a través de este enlace.

Cuando se restaura la ruta entre los Routers A y D, el Router A puede nuevamente cambiar su tabla de enrutamiento para indicar una preferencia por la ruta orientada en dirección contraria a la de las agujas del reloj a través de los Routers D y C hacia la red destino. Los protocolos de enrutamiento dinámico también pueden dirigir el tráfico de una misma sesión a través de distintas rutas de una red para lograr un mejor rendimiento. Esto se conoce como carga compartida.

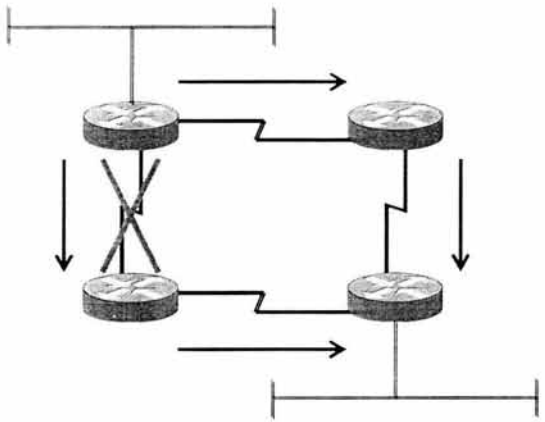


Figura 2.4

El éxito del enrutamiento dinámico depende de dos funciones básicas del router:

- El mantenimiento de una tabla de enrutamiento
- La distribución oportuna del conocimiento, bajo la forma de actualizaciones de enrutamiento, hacia otros routers

El enrutamiento dinámico se basa en un protocolo de enrutamiento para compartir el conocimiento entre los routers. Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un router cuando se comunica con los routers vecinos. Por ejemplo, un protocolo de enrutamiento describe:

- Cómo enviar actualizaciones
- Qué conocimiento contienen esas actualizaciones
- Cuándo enviar ese conocimiento
- Cómo ubicar a los destinatarios de las actualizaciones

2.5 Métricas

Existen diversos algoritmos que permiten calcular el camino más corto entre dos nodos de un grafo. Uno de los más conocidos es el algoritmo de Dijkstra, y se utiliza tanto en enrutamiento estático como dinámico. Es importante que una tabla de enrutamiento

sea actualizada y precisa, dado que su objetivo principal es incluir la mejor información para el router. Cada protocolo de enrutamiento interpreta la "mejor ruta" a su manera. El protocolo genera un valor, denominado métrica, para cada ruta a través de la red. Normalmente, cuanto menor sea la métrica, mejor será la ruta. Las tablas de enrutamiento también pueden contener información acerca de la conveniencia de una ruta. Los routers comparan las métricas para determinar las mejores rutas. Las métricas difieren según el diseño del protocolo de enrutamiento que se utiliza. Se pueden utilizar varias métricas para definir la mejor ruta. Algunos protocolos de enrutamiento, como el Protocolo de información de enrutamiento (RIP), utilizan sólo una métrica, mientras que otros, tales como IGRP, utilizan una combinación de métricas.

Las métricas que los routers utilizan más comúnmente se indican en la tabla 2.1.

Tipo de métrica	Descripción
Número 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 el origen hasta el 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.
Tictacs	El retardo en un enlace de datos que utiliza los tictacs de reloj PC de IBM (Aproximadamente 55 milisegundos).
Costo	Un valor arbitrario, generalmente basado en el ancho de banda, el gasto monetario y otras medicines, asignado por el administrador de red.

Tabla 2.1

Con esto podemos decir que la métrica es la información que se utiliza para seleccionar la mejor ruta para el enrutamiento.

2.6 Algoritmos de enrutamiento dinámico

La mayoria de los algoritmos de enrutamiento se pueden clasificar como uno de dos algoritmos básicos:

- vector distancia
- estado del enlace

El enrutamiento por vector distancia determina la dirección (vector) y la distancia hacia cualquier enlace en la red. El enrutamiento estado del enlace (también denominado primero la ruta más corta) recrea la topología exacta de toda la red (o por lo menos la porción en la que se ubica el router).

El enrutamiento híbrido balanceado combina aspectos de los algoritmos de estado del enlace y vector distancia. En las páginas siguientes se hará referencia a los procedimientos y problemas para cada uno de estos algoritmos de enrutamiento y se presentan técnicas para reducir al mínimo los problemas.

El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Siempre que la topología de una red cambia por razones de crecimiento, reconfiguración o falla, la base del conocimiento de la red también debe cambiar. El conocimiento debe reflejar una visión exacta y coherente de la nueva topología. Esta visión se denomina convergencia.

Cuando todos los routers de una red se encuentran operando con el mismo conocimiento, se dice que la red ha convergido. La convergencia rápida es una función de red deseable, ya que reduce el periodo de tiempo durante el cual los routers continúan tomando decisiones de enrutamiento incorrectas o que causan desperdicio.

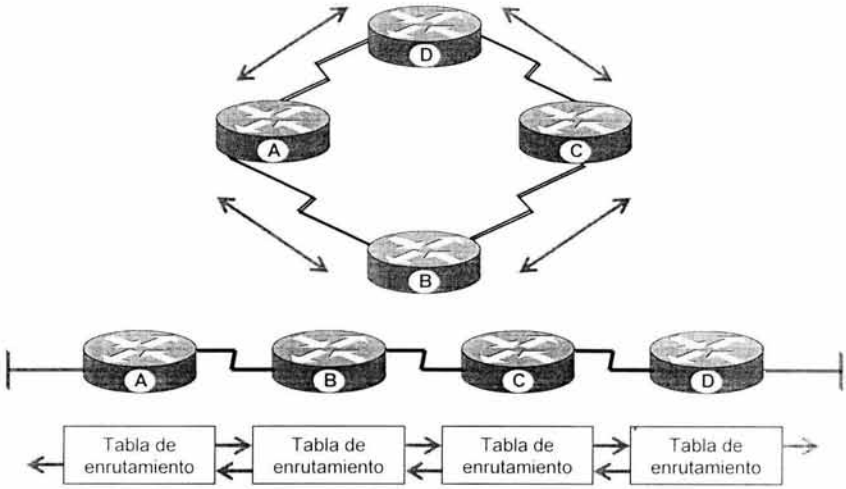
2.6.1 Enrutamiento por Vector de Distancia

Este algoritmo se aplica en diversos protocolos de enrutamiento. También se conoce como algoritmo de Bellman-Ford o Ford-Fulkerson, que fueron los autores de la idea. Fue el algoritmo original de ARPANET, se utilizó en DECNET, IPX y Appletalk. Se usa en el protocolo RIP, que hasta 1988 era el único protocolo de enrutamiento utilizado en Internet. También se utiliza en los protocolos propietarios IGRP y EIGRP de Cisco.

Los algoritmos de enrutamiento basados en vector distancia envían copias periódicas de una tabla de enrutamiento de un router a otro. Estas actualizaciones regulares entre routers comunican los cambios de topología.

Cada router recibe una tabla de enrutamiento de los routers vecinos directamente conectados. Por ejemplo, en la figura 2.5, el Router B recibe información del Router A. El Router B agrega un número de vector distancia (como, por ejemplo, el número de saltos), aumentando de esta manera el vector distancia y luego transfiere esta nueva tabla de enrutamiento a su otro vecino, el Router C. Este mismo proceso paso a paso se produce en todas las direcciones entre los routers directamente vecinos.

El algoritmo eventualmente acumula distancias de red para poder mantener una base de datos de información de topología de la red. Los algoritmos vector distancia no permiten, sin embargo, que un router conozca la topología exacta de una red.



Los routers envían copias periódicas de su tabla de enrutamiento a los routers vecinos y acumulan vectores de distancia.

Figura 2.5

Cada router que utiliza el enrutamiento vector distancia empieza identificando sus propios vecinos. En la figura, la interfaz que lleva a cada red directamente conectada tiene una distancia de 0. A medida que el proceso de descubrimiento de red vector distancia continúa, los routers descubren la mejor ruta hacia las redes destino basándose en la información que reciben de cada vecino. Por ejemplo, el Router A obtiene conocimiento acerca de otras redes tomando como base la información que recibe del Router B. Cada una de las demás entradas de red en la tabla de enrutamiento posee un vector distancia acumulado para demostrar la distancia a la que se encuentra esta red en una dirección determinada.

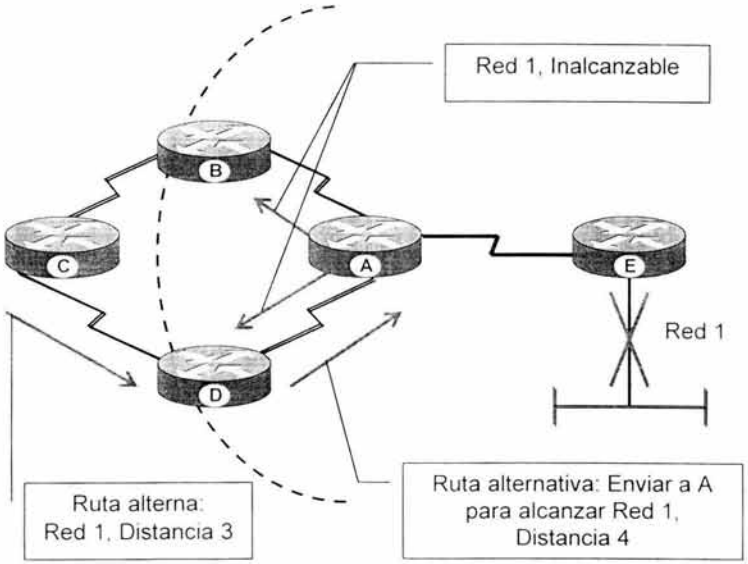
Cuando cambia la topología de una red que utiliza un protocolo vector distancia, deben producirse actualizaciones de la tabla de enrutamiento. Como en el proceso de descubrimiento de red, las actualizaciones de cambio de topología continúan paso a paso de un router a otro. Los algoritmos vector distancia requieren que cada router envíe la tabla de enrutamiento completa a cada uno de sus vecinos adyacentes. Las tablas de enrutamiento incluyen información acerca del costo de ruta total (definido por su métrica) y la dirección lógica del primer router en la ruta para cada red contenida en la tabla.

Los loops de enrutamiento se pueden producir si la convergencia lenta de una red en una nueva configuración hace que las entradas de enrutamiento sean incorrectas. La figura 2.6 ilustra cómo se puede producir un loop de enrutamiento:

Antes de la falla de la Red 1, todos los routers poseen un conocimiento coherente y tablas de enrutamiento correctas. Se dice que la red ha convergido. Supongamos, para el resto de este ejemplo, que la ruta preferida del Router C hacia la Red 1 es a través del Router B y que la distancia del Router C a la Red 1 es 3.

En el momento en que la Red 1 falla, el Router E envía una actualización al Router A. El Router A deja de enrutar paquetes hacia la Red 1, pero los Routers B, C y D siguen operando porque todavía no se les ha informado acerca de la falla. Cuando el Router A envía su actualización, los Routers B y D detienen el enrutamiento hacia la Red 1; sin embargo, el Router C no ha recibido la actualización. Para el Router C, la Red 1 todavía se puede alcanzar a través del Router B.

Ahora, el Router C envía una actualización periódica al Router D, indicando una ruta hacia la Red 1 a través del Router B. El Router D cambia su tabla de enrutamiento para introducir esta información buena pero incorrecta y transmite la información al Router A. El Router A transmite la información a los Routers B y E, etc. Cualquier paquete destinado a la Red 1 ahora realizará un loop desde el Router C al B al A al D y volverá nuevamente al C.

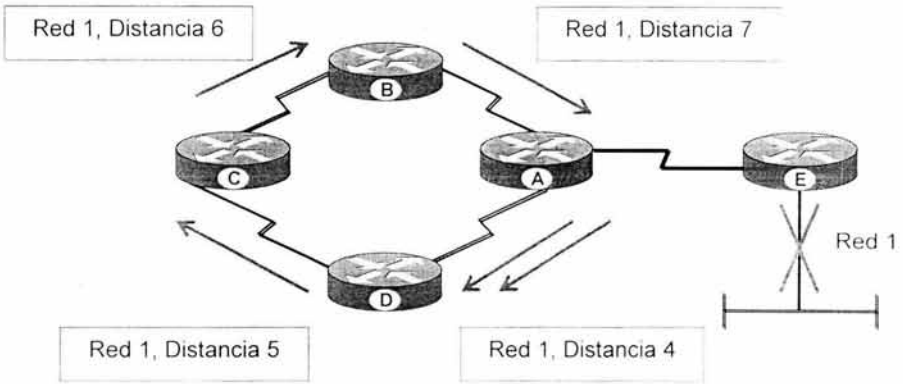


Rutas alternas, baja convergencia, enrutamiento incoherente.

Figura 2.6

Continuando con el ejemplo, las actualizaciones no válidas de la Red 1 seguirán andando en círculos hasta que algún otro proceso detenga el recorrido del loop. Esta condición, denominada conteo al infinito, hace que los paquetes recorran la red continuamente, a pesar del hecho fundamental de que la red destino, la Red 1, está caída. Mientras los routers cuentan al infinito, la información no válida permite que se produzca un loop de enrutamiento.

Si no se toman medidas para detener el proceso, el vector distancia (métrica) de número de saltos se incrementa cada vez que el paquete atraviesa otro router. Estos paquetes recorren la red formando loops (bucles) debido a la información incorrecta de las tablas de enrutamiento.



Los Loops de enrutamiento aumentan el vector de distancia

Figura 2.7

Los algoritmos de enrutamiento vector distancia se corrigen automáticamente, pero un problema de loop de enrutamiento puede requerir primero una cuenta al infinito. Para evitar que este problema se prolongue, los protocolos vector distancia definen el infinito como un número máximo especifico. Este número se refiere a la métrica de enrutamiento (por ejemplo, un número de saltos simple).

Con este enfoque, el protocolo de enrutamiento permite que el loop de enrutamiento continúe hasta que la métrica supere su máximo valor permitido. El gráfico muestra el valor de la métrica como 16 saltos, lo que supera el máximo vector distancia por defecto de 15 saltos, por lo tanto, el router descarta el paquete. En cualquiera de los casos, cuando el valor de la métrica supera el valor máximo, se considera que la Red 1 no se puede alcanzar.

Otro origen posible de un loop de enrutamiento es cuando información incorrecta que se ha enviado a un router se contradice con la información correcta que éste envió. Así es como se produce el problema:

El Router A transfiere una actualización al Router B y al Router D, indicando que la Red 1 está fuera de servicio. El Router C, sin embargo, transmite una actualización al Router B, indicando que la Red 1 está disponible a una distancia de 4, a través del Router D. Esto no infringe las reglas del split horizon.

El Router B concluye erróneamente que el Router C todavía tiene una ruta válida hacia la Red 1, aunque con una métrica mucho menos favorable. El Router B envía una actualización al Router A comunicándole al Router A la nueva ruta hacia la Red 1.

El Router A ahora determina que puede realizar los envíos a la Red 1 a través del Router B, el Router B determina que puede realizar los envíos a la Red 1 a través del Router C, y el Router C determina que puede realizar los envíos a la Red 1 a través del Router D. Cualquier paquete introducido en este entorno quedará atrapado en un loop entre los routers.

El split horizon intenta evitar esta situación, si llega una actualización de enrutamiento acerca de la Red 1 desde Router A, el Router B o D no pueden enviar información acerca de la Red 1 nuevamente hacia el Router A. El split horizon reduce así la cantidad de información de enrutamiento incorrecta y reduce también el gasto de enrutamiento.

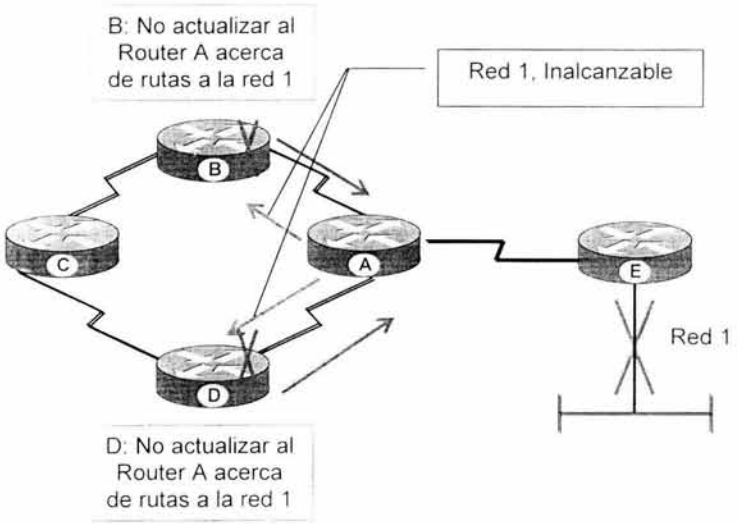


Figura 2.8

Se puede evitar el problema de cuenta al infinito mediante temporizadores de espera que funcionan de la siguiente manera:

- Cuando un router recibe una actualización por parte de un vecino que indica que una red previamente accesible ahora se encuentra inaccesible, el router marca la ruta como inaccesible e inicia un temporizador de espera. Si en algún momento, antes de que expire el temporizador de espera, se recibe una actualización por parte del mismo vecino indicando que la red se encuentra nuevamente accesible, el router marca la red como accesible y elimina el temporizador de espera.

- Si llega una actualización desde un router vecino distinto con una métrica más conveniente que la originalmente registrada para la red, el router marca la red como accesible y elimina el temporizador de espera.

- Si en algún momento antes de que expire el temporizador de espera se recibe una actualización de un router vecino diferente con una métrica inferior, se ignorará la actualización. El ignorar una actualización con una métrica inferior mientras el temporizador de espera se encuentra activado, permite ganar más tiempo para que el conocimiento de un cambio perjudicial se propague a través de toda la red.

2.6.2 Enrutamiento por Estado del Enlace

El segundo algoritmo básico utilizado para el enrutamiento es el algoritmo estado del enlace. Los algoritmos de enrutamiento basados en estado del enlace, también conocidos como algoritmos SPF (primero la ruta libre más corta), mantienen una compleja base de datos de información de topología. Mientras que el algoritmo vector distancia posee información no específica acerca de las redes distantes y ningún conocimiento acerca de los routers distantes, un algoritmo de enrutamiento estado de enlace conoce perfectamente los routers distantes y cómo se interconectan. El enrutamiento estado de enlace utiliza:

- Publicaciones estado de enlace (LSA)
- Una base de datos topológica
- El algoritmo SPF y el árbol SPF resultante
- Una tabla de enrutamiento de rutas y puertos hacia cada red

Los ingenieros han implementado este concepto de estado de enlace en el enrutamiento OSPF (Primero la ruta más corta)[2.1].

El descubrimiento de red para el enrutamiento estado del enlace utiliza los siguientes procesos:

- Los routers intercambian LSA entre sí. Cada router empieza con redes directamente conectadas para las cuales posee información directa.

- Cada router en paralelo con los demás routers genera una base de datos topológica que contiene todas las LSA de la red.

- El algoritmo SPF calcula la accesibilidad de la red. El router construye esta topología lógica como un árbol, con él mismo como raíz, y con todas las rutas posibles hacia cada red dentro de la red que usa el protocolo estado del enlace. Entonces clasifica estas rutas, colocando la ruta más corta primero (SPF).

- El router hace una lista de sus mejores rutas y de los puertos que permiten acceder a estas redes destino, dentro de la tabla de enrutamiento. También mantiene otras bases de datos con elementos de la topología y detalles de los estados.

Los algoritmos de estado del enlace se basan en el uso de las mismas actualizaciones de estado del enlace. Siempre que una topología estado del enlace cambia, el router que primero se da cuenta del cambio envía la información a los demás routers o a un router designado que todos los demás routers pueden utilizar para realizar las actualizaciones. Esto implica el envío de información de enrutamiento común a todos los routers de la red. Para lograr la convergencia, cada router debe realizar lo siguiente:

[2.1] La RFC 2328 contiene una descripción de los conceptos y operaciones de estado de enlace OSPF

- Mantener un seguimiento de los routers vecinos: el nombre de cada vecino, si se encuentra conectado o desconectado y el costo del enlace con el router vecino.

- La construcción de un paquete LSA que describa los nombres de los routers vecinos y los costos de enlace, incluyendo los nuevos vecinos, los cambios en los costos de enlace y los enlaces con los vecinos que se han desconectado.

- El envío de este paquete LSA para que todos los demás routers lo reciban

- Una vez recibido el paquete LSA, registrar el paquete LSA en la base de datos para que actualice el paquete LSA generado más recientemente por cada router.

- Completar un mapa de la red utilizando datos de los paquetes LSA acumulados y luego calcular rutas hacia todas las demás redes utilizando el algoritmo SPF.

Cada vez que un paquete LSA provoca un cambio en la base de datos estado del enlace, el algoritmo de estado del enlace (SPF) vuelve a calcular cuáles son las mejores rutas y actualiza la tabla de enrutamiento. Desde ese momento, cada router toma en cuenta el cambio de topología en el momento de determinar cuál es la ruta más corta para el enrutamiento de paquetes.

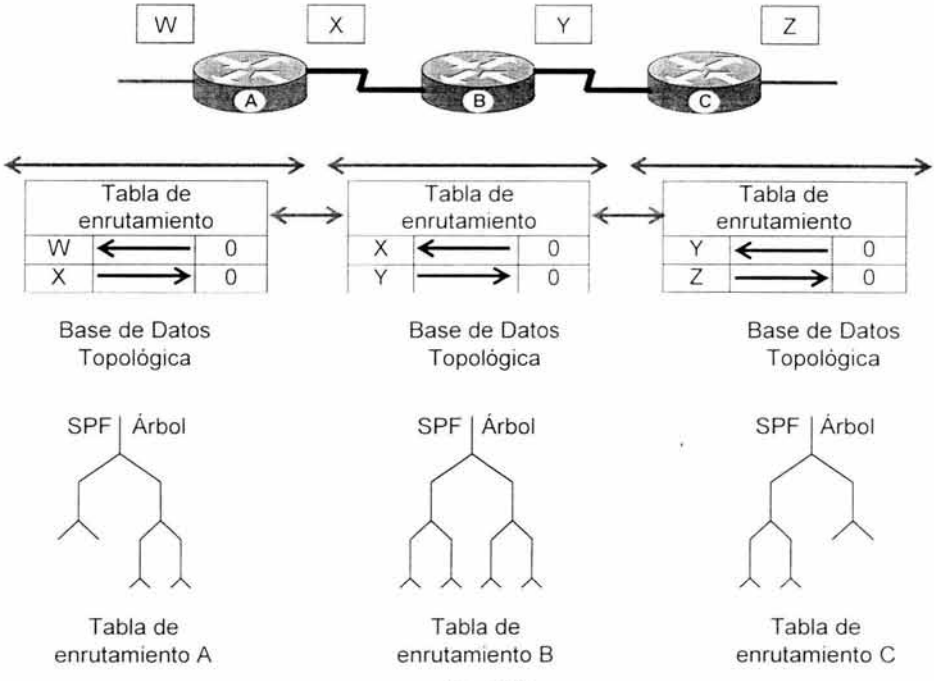


Figura 2.9

Existen dos aspectos del estado del enlace que son motivos de preocupación: los requisitos de procesamiento y memoria y los requisitos de ancho de banda.

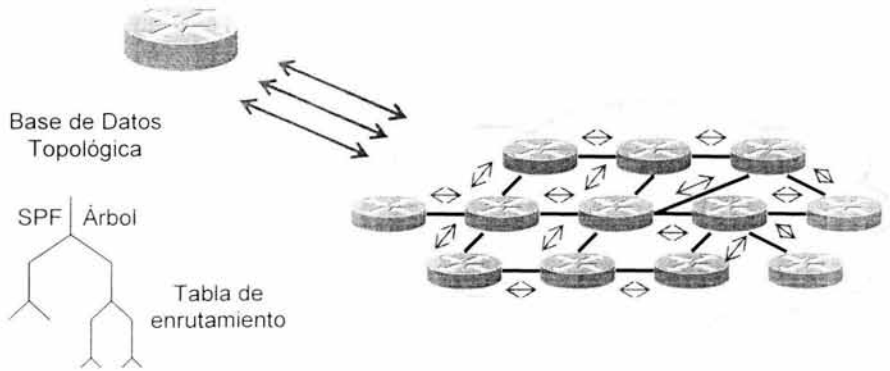
2.6.2.1 Requisitos de procesamiento y memoria

En la mayoría de los casos, ejecutar los protocolos de enrutamiento estado del enlace significa que los routers deben utilizar más memoria y realizar más procesamiento que los protocolos de enrutamiento por vector distancia. Los administradores de red deben garantizar que los routers que seleccionen sean capaces de proporcionar estos recursos necesarios.

Los routers realizan el seguimiento de todos los demás routers dentro de un mismo grupo y de las redes que cada uno puede alcanzar directamente. Para el enrutamiento estado del enlace, la memoria debe tener la capacidad de almacenar la información de varias bases de datos, del árbol de topología y de la tabla de enrutamiento. El uso del algoritmo de Dijkstra para calcular la SPF requiere una tarea de procesamiento proporcional a la cantidad de enlaces de la red, multiplicada por la cantidad de routers de la misma.

2.6.2.2 Requisitos de ancho de banda

Otro punto que puede ser motivo de preocupación es el ancho de banda que se debe utilizar para realizar la técnica de inundación inicial de paquetes de estado del enlace. Durante el proceso de descubrimiento inicial, todos los routers que utilicen protocolos de enrutamiento estado del enlace envían paquetes LSA a todos los demás routers. Esta acción inunda la red a medida que los routers demandan ancho de banda en forma masiva y reducen temporalmente el ancho de banda disponible para el tráfico enrutado que transporta los datos del usuario. Después de esta técnica de inundación inicial, los protocolos de enrutamiento estado del enlace generalmente requieren un ancho de banda mínimo para enviar paquetes LSA no frecuentes o generados por sucesos que reflejen los cambios de topología.



Un router al tener la base topológica de la red requiere de mayor procesamiento y memoria. Se debe tener en cuenta que cierto ancho de banda es consumido por la inundación inicial de estado de enlace.

Figura 2.10

El aspecto más complejo y más importante del enrutamiento estado del enlace es asegurarse de que todos los routers obtengan los paquetes LSA necesarios. Los routers con distintos conjuntos de LSA calculan las rutas tomando como base distintos datos topológicos. Entonces, las redes se vuelven inaccesibles como resultado del desacuerdo entre los routers acerca de un enlace. A continuación, presentamos un ejemplo de información de ruta incoherente:

1. Entre los Routers C y D, la Red 1 queda fuera de servicio. Ambos routers construyen un paquete LSA para reflejar este estado de inaccesibilidad.

2. Poco después, la Red 1 se activa nuevamente. Se necesita otro paquete LSA para reflejar este nuevo cambio de topología.

3. Si el mensaje "Red 1, Inaccesible" original del Router C utiliza una ruta lenta para su actualización, dicha actualización llegará tarde. Ese paquete LSA

puede llegar al Router A después del paquete LSA con el mensaje "Red 1, Nuevamente activa" del Router D.

4. Con las LSA fuera de sincronía, el Router A debe enfrentarse al dilema de qué árbol SPF debe construir. ¿Debe utilizar rutas que incluyan la Red 1 o rutas sin la Red 1, que recientemente se describió como inaccesible?

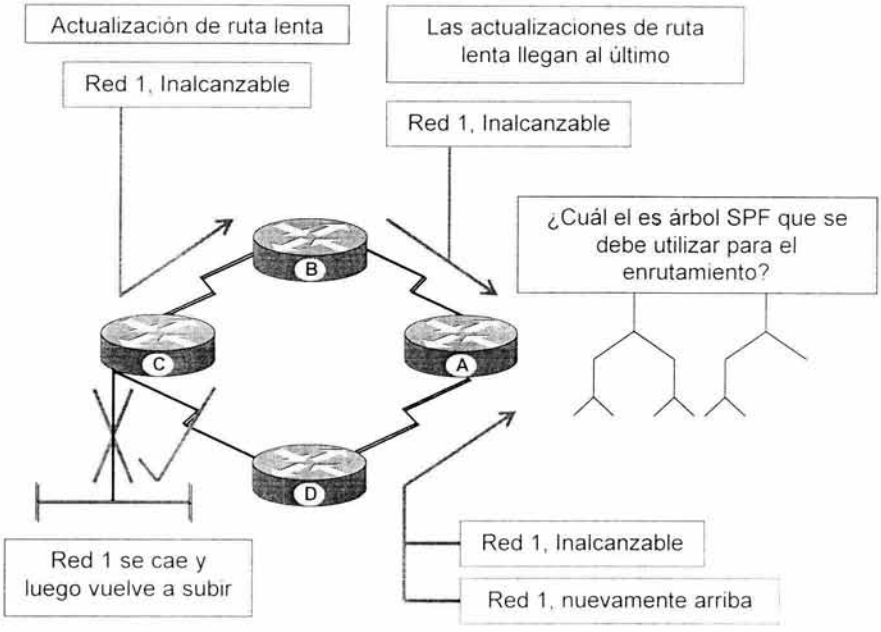
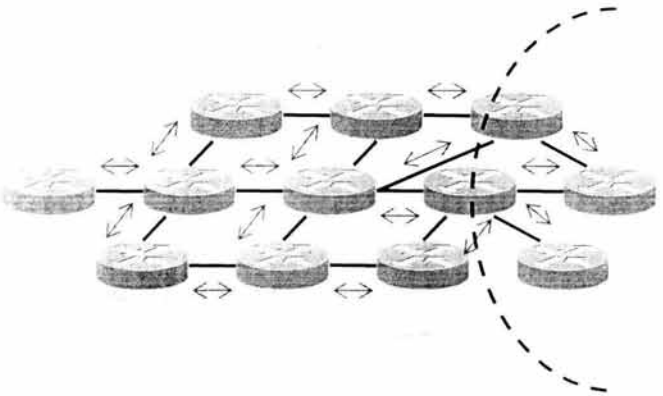


Figura 2.11

Si la distribución de los LSA's a todos los routers no se realiza correctamente, el enrutamiento por estado del enlace puede dar como resultado rutas no válidas. El escalamiento con protocolos estado del enlace en redes de gran tamaño puede agravar el problema de distribución incorrecta de paquetes LSA. Si una parte de la red se activa antes que otras partes, el orden para enviar y recibir paquetes LSA varía. Esta variación puede alterar e impedir la convergencia. Es posible que los routers obtengan distintas versiones de la topología antes de construir sus árboles SPF y tablas de enrutamiento. En una red de gran tamaño, las partes que se actualizan más rápidamente pueden provocar problemas a las partes que se actualizan con más lentitud.



La sincronización de redes extensas en ocasiones no es tan sencilla, y más si existen cambios constantes en la topología de la red. El inicio de un router modifica la topología conocida.

Figura 2.12

Entre los protocolos de enrutamiento que utilizan algoritmos basados en el estado del enlace destaca OSPF (Open Shortest Path First) que es el protocolo de enrutamiento estándar de Internet. Otro protocolo de estado del enlace también utilizado en Internet y que proviene de OSI es IS-IS (Intermediate System-Intermediate System). IS-IS es multiprotocolo, es decir, soporta múltiples protocolos de red por encima. OSPF esta basado en IS-IS, pero no es multiprotocolo. En el enrutamiento por vector distancia cada router envia información sólo a sus vecinos, pero esta información incluye a todos los nodos de la red. En cambio en el enrutamiento por el estado del enlace cada router envia su paquete de información a toda la red, pero éste solo contiene la relativa a sus vecinos más próximos. En el estado del enlace cada router puede, a partir de la información obtenida, conocer su árbol de expansión completo, mientras que esto no es posible con enrutamiento por vector distancia.

Se puede comparar el enrutamiento por vector distancia con el enrutamiento estado del enlace en varias áreas claves:

- El enrutamiento por vector distancia obtiene datos topológicos de la información de la tabla de enrutamiento de sus vecinos. El enrutamiento estado del enlace obtiene una amplia visión de la topología de red completa acumulando todos los LSA's necesarios.

- El enrutamiento por vector distancia determina la mejor ruta agregando el valor métrico que recibe a medida que la información de enrutamiento pasa de un router a otro. Para el enrutamiento estado del enlace, cada router trabaja independientemente para calcular su propia ruta más corta hacia las redes destino.

- Con la mayoría de los protocolos de enrutamiento por vector distancia, las actualizaciones para los cambios de topología consisten en actualizaciones periódicas de las tablas. La información pasa de un router a otro, dando generalmente como resultado una convergencia más lenta. Con los protocolos de enrutamiento estado del enlace, las actualizaciones son provocadas generalmente por cambios en la topología. Los LSA's relativamente pequeños que se han pasado a todos los demás routers generalmente dan como resultado tiempos más rápidos de convergencia con cualquier cambio de topología de la red.

2.7 Enrutamiento Jerárquico

A medida que una red crece la cantidad información de enrutamiento aumenta de forma exponencial, ya que cada router ha de calcular las rutas óptimas a todos los demás. Esto incrementa el tráfico, la memoria en los routers, y la complejidad de los cálculos necesarios para obtener las rutas óptimas. Como consecuencia de esto, los algoritmos de enrutamiento no son escalables. Para reducir este problema las redes se organizan en niveles jerárquicos. Se divide la red en regiones o sistemas autónomos, y sólo un número reducido de routers de cada región se puede comunicar con el exterior. Las rutas quizá no sean tan óptimas, pero se simplifica la administración y el mantenimiento de las tablas y se reduce el tráfico de la red.

2.7.1 Sistema Autónomo

Un sistema autónomo o AS será la subred que es administrada por una autoridad común, que tiene un protocolo de enrutamiento homogéneo mediante el cual intercambia información en toda la subred y que posee una política común para el intercambio de tráfico con otras redes o sistemas autónomos. Normalmente cada ISP constituye su propio sistema autónomo. Así pues, en Internet se dan, al menos, dos niveles jerárquicos de enrutamiento, el que se realiza dentro de un sistema autónomo y el que se efectúa entre sistemas autónomos. El primero es denominado enrutamiento interno o intraáreas, al segundo se le denomina enrutamiento externo o interáreas. Dado que los requerimientos en uno y otro caso son muy diferentes, se utilizan protocolos de enrutamiento distintos. Los protocolos de enrutamiento interior se denominan IGP (Interior Gateway Protocol) y los utilizados entre sistemas autónomos se llaman EGP (Exterior Gateway Protocol).

Ejemplo de protocolos IGP's:

- RIP
- OSPF

Ejemplo de protocolos EGP's:

- BGP

Los IGP's mencionados en este trabajo son abiertos, es decir, no son propietarios o en otras palabras estos pueden ser implementados en cualquier equipo que lo soporte sin importar la marca

2.8 RIPv1 - Route Information Protocol Version 1

Uno de los protocolos de enrutamiento más antiguos es el "Route Informacition Protocol" o más comúnmente llamado "RIP". RIP utiliza algoritmos de vector distancia para calcular sus rutas. Estos algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

RIP es un protocolo de enrutamiento de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de enrutamiento como por ejemplo IGRP y EIGRP propietarios de Cisco Systems.

RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto.

RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos como por ejemplo ancho de banda o congestión del enlace.

El protocolo RIPv1, al igual que sus antecesores propietarios es un protocolo de enrutamiento que fue diseñado para funcionar como protocolo vector distancia. RIPv1 fue diseñado para funcionar en redes pequeñas de tipo interior. En cuanto al protocolo tenemos que tener en cuenta las tres limitaciones:

- El protocolo no permite más de quince saltos, es decir, los dos routers más alejados de la red no pueden distar más de 15 saltos, si esto ocurriera no sería posible utilizar RIP en esta red.

- Problema del "conteo a infinito". Este problema puede surgir en situaciones atípicas en las cuales se puedan producir loops, ya que estos loops pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado.

- El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de parámetros en tiempo real como por ejemplo retardos o carga del enlace.

Además debemos que tener en cuenta que el protocolo RIPv1 es un protocolo classfull, con lo que existe el problema de la discontinuidad de redes. El problema de la discontinuidad de redes se produce en el momento que tenemos una red dividida en varias subredes, las cuales no pueden ser localizadas en una misma ruta, ya que físicamente cada una de las subredes está ubicada en un lugar que depende de una interfaz distinta de una subred a otra.

2.8.1 Tabla de enrutamiento de RIP

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
- Siguiente salto
- Interfaz de salida del router
- Métrica
- Temporizador

Para obtener esta tabla, el protocolo de enrutamiento RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de enrutamiento de cada uno de los nodos o routers de la red:

- Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia D al destino, y el siguiente salto S del router a esa red.
- Conceptualmente también debería de existir una entrada para el router mismo con métrica 0, pero esta entrada no existirá.
- Periódicamente se enviará una actualización de la tabla a cada uno de los vecinos del router mediante la dirección de broadcast. Esta actualización contendrá toda la tabla de enrutamiento.
- Cuando llegue una actualización desde un vecino S, se añadirá el coste asociado a la red de S, y el resultado será la distancia D'. Se comparará la distancia D' y si es menor que el valor actual de D a esa red entonces se sustituirá D por D'.

El protocolo de enrutamiento RIP como ya hemos dicho mantiene una tabla de enrutamiento, como cualquier protocolo de enrutamiento, ahora comentamos cada uno de los campos de la tabla.

2.8.1.1 Dirección de destino

La dirección de destino en la tabla de enrutamiento de RIP será la red de destino, es decir, la red final a la que deseamos acceder, esta red en la versión 1 del protocolo RIP tendrá que ser obligatoriamente clasfull, es decir tendrá que tener en cuenta la clase, es decir, no se permite el subneting en RIP versión 1, por ejemplo si la red de destino es la 192.168.4.0, sabemos que al ser RIP classfull la red de destino tiene 256 direcciones, de las cuales 254 son útiles, una vez descontada la dirección de red y la dirección de

broadcast, ya que la red 192.168.4.0 es de clase C, es decir que los 24 primeros bits de la dirección IP identifican la red y los 8 últimos identifican los hosts dentro de la red.

2.8.1.2 Siguiente salto

El siguiente salto lo definimos como el siguiente router por el que nuestro paquete va a pasar para llegar a su destino, este siguiente salto será necesariamente un router vecino del router origen.

2.8.1.3 Interfaz de salida del router

Se entiende por interfaz de salida del router a la interfaz que está conectada al siguiente salto.

2.8.1.4 Métrica

La métrica utilizada por RIP consiste en el conteo de saltos. Se considera cada salto como una única unidad, independientemente de otros factores como tipo de interfaz o congestión de la linea. La métrica total consiste en el total de saltos desde el router origen hasta el router destino, con la limitación de que 16 saltos se considera como destino inaccesible, esto limita el tamaño máximo de la red.

2.8.1.5 Temporizador

El temporizador nos indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza dos 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 se establece en 300 segundos.

El tiempo de actualización se considera al tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos.

El tiempo de desactivación se considera al 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 con lo cual el router no está activo en la red, se establece la métrica a valor 16, es decir 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.

2.9 RIPv2 – Route Information Protocol Version 2

RIPv2 establece una serie de mejoras muy importantes con su antecesor que son las siguientes:

- Autenticación para la transmisión de información de RIP entre vecinos.
- Utilización de mascaras de red, con lo que ya es posible utilizar VLSM.
- Utilización de máscaras de red en la elección del siguiente salto, lo cual nos puede permitir la utilización de arquitecturas de red discontinuas.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9.
- Inclusión de RIPv2 en los bloques de información de gestión (MIB).

Por supuesto además de estas mejoras RIPv2 nos permite la redistribución de rutas externas aprendidas por otros protocolos de enrutamiento.

Pero RIPv2 aunque haya tenido una serie de mejoras muy importantes desde la versión 1 del protocolo sigue teniendo una serie de carencias muy importantes como:

- Limitación en el tamaño máximo de la red. Con RIPv2 sigue existiendo la limitación de 15 saltos como tamaño máximo de la red, lo cual implica que no nos permite la utilización de RIPv2 en redes de un tamaño más grande.
- Conteo a infinito. RIPv2 sigue sin solucionar el problema del conteo hasta el infinito si se forman loops, aunque existen técnicas externas al protocolo como pueden ser el retorno envenenado y el horizonte dividido, las cuales consisten básicamente en no anunciar una ruta por el interfaz por el que se ha recibido en algún momento.
- Métricas estáticas que pueden ser cambiadas por el administrador de la red, pero que no nos dan ninguna información del estado de la red.
- RIPv2 sólo permite al igual que su antecesor una ruta por cada destino, lo cual implica la imposibilidad de realizar balanceos de carga.
- RIPv2 es un protocolo que al igual que su antecesor genera muchisimo tráfico al enviar toda la tabla de enrutamiento en cada actualización, con la carga de tráfico que ello conlleva.

2.10 OSPF - Open Shortest Path First

El término Open en el nombre del protocolo hace referencia a que es un protocolo abierto al público y no propietario de ninguna compañía. De entre los protocolos abiertos existen varios como RIPv1, RIPv2 u OSPF; pero OSPF para redes de tamaño medio-grande es preferible, ya que permite una escalabilidad muy remarcable. Entre otras características podemos decir que OSPF no tiene el problema de la limitación de los 15 saltos de RIP, además los tiempos de convergencia de OSPF son muchisimo mejores en todos los casos. OSPF tiene en cuenta factores como el ancho de banda para el cálculo de costos y rutas óptimas.

OSPF es uno de los protocolos que sin duda están preparados para las redes actuales. OSPF también considera la capacidad de escalabilidad de la red a través de la escalabilidad que permite un modelo jerárquico que es posible conseguir mediante la utilización de distintas áreas.

OSPF utiliza el algoritmo de estado del enlace, de forma opuesta a RIP que utiliza algoritmo de vector distancia. Los router de estado del 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 del enlace no realizan broadcast de sus rutas periódicamente como los routers que utilizan vector distancia. OSPF tiene las siguientes características:

- Velocidad de convergencia

  En redes grandes, la convergencia utilizando RIP puede alargarse varios minutos, hasta que la tabla completa de enrutamiento de los routers de la red se completa y se estabiliza. En OSPF el tiempo de convergencia es muchísimo menor ya que sólo se actualizan las rutas que han sido modificadas y estás son distribuidas por la red de forma rápida.

- Soporte de VLSM

  RIPv1 es un protocolo de los denominados clasfull, y como tal no soporta VLMS, sin embargo tenemos que recordad que RIPv2 sí soporta VLMS.

- Tamaño de la red

  Por tamaño de la red nos referiremos al número de routers en una red. En un entorno de enrutamiento basado en RIP una red con más de 15 saltos no es viable, ya que más de 15 saltos se considera inalcanzable. Cabe recordar que en RIP un salto es equivalente a un router, por lo que el tamaño de la red en RIP es limitada. Sin embargo en un entorno de enrutamiento basado en OSPF no tenemos este tipo de limitación, ya que teóricamente no tenemos esta limitación de tamaño, aunque si seguimos las especificaciones de los fabricantes de routers Cisco o Lucent Technologies nos recomiendan redes en las cuales no haya más de 400 routers por área, obviamente pueden existir más áreas, pero la única limitación física, que no de protocolo sería la de los 400 routers por área. Esta característica hace de OSPF ideal para redes medianas y grandes.

- Utilización de ancho de banda

  Si utilizamos RIP estamos realizando broadcast a la red de la tabla de enrutamiento completa cada 30 segundos. Esta característica puede ser especialmente problemática sobre enlaces WAN lentos. Sin embargo OSPF utiliza multicast y sólo envía actualizaciones cuando se produce un cambio en la red.

- Selección de camino

  RIP selecciona el camino óptimo contando saltos, o distancia a otros routers. Dentro de la elección de ruta óptima no entran en consideración factores como el ancho de banda restante o los retardos en la red. Sin embargo OSPF utiliza una métrica basada en ancho de banda y retardos.

- Agrupación de miembros

  RIP utiliza una topología plana en la 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 con OSPF se introduce el concepto de "áreas", lo que permite la segmentación de la red en segmentos más pequeños. Un área es un conjunto de redes dentro de un sólo AS que se han agrupado juntas. La topología de un área permanece oculta al resto del AS, 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 (*intra-area routing*) o en áreas diferentes (*inter-area routing*).

  - El enrutamiento intra-area lo determina sólo la propia topología del área. Es decir, el paquete se encamina sólo a partir de información obtenida dentro del área; no se puede usar información de enrutamiento obtenida fuera de la misma.

  - El enrutamiento inter-area se hace siempre a través del backbone.

  La división de un sistema autónomo en áreas permite una reducción significante en el volumen del tráfico de enrutamiento requerido para gestionar la base de datos en un AS grande.

  Por ejemplo tenemos los siguientes tipos de áreas:

  - Transit Area

    Un área a través de la que se produce la conexión física de un VL (Virtual Link). Un VL o enlace virtual es parte de la backbone. Sus extremos son dos ABR que comparten un área no backbone. El VL se trata como un enlace punto a punto con métrica igual a la métrica intra-area entre los extremos. El enrutamiento a través del VL se hace usando enrutamiento "intra-area" normal.

  - Stub Area (SA)

    Un área configurada para usar el enrutamiento por defecto para el enrutamiento inter-AS. Se puede configurar en los sitios donde hay un sólo punto de salida del área, o donde se puede usar cualquier salida sin preferencia por ninguna ruta. Por defecto, las rutas inter-AS se copian a todas las áreas, por lo que el uso de SA's puede reducir las necesidades de

almacenamiento de los routers dentro de aquellas áreas donde hay definidas muchas rutas inter-AS.

Todas las áreas tienen un Area ID (AID), un número de 32 bits que identifica un área particular. El área de backbone tiene un AID de cero (0.0.0.0).

Al dividir la red en áreas se tiene que introducir el concepto de comunicación entre áreas, pero gracias a la división de la red los cambios producidos en un router de un área no afecta a la totalidad de la red, sino que sólo afecta a los routers de un área.

Ya que OSPF fue pensado y descrito para redes de un tamaño considerable al crear una red con más de 50 routers hay que tener un cuidado especial con el diseño y la planificación de la red con tal de minimizar tráfico y el montante de intercambio de información de enrutamiento.

Como protocolo de estado del enlace, OSPF opera de forma distinta a los protocolos de vector distancia como podrían ser RIP.

La información proporcionada por OSPF a los vecinos no es la tabla de enrutamiento completa. Sin embargo, los routers que utilizan OSPF les informan a sus vecinos sobre el estado de sus conexiones o enlaces. En otras palabras los routers OSPF anuncian el estado de sus enlaces. Los routers procesan esta información y generan la base de datos de estado del enlace, la cual es esencial para poder dibujar un esquema de quien está conectado con quien. Todos los routers en una misma área tienen que tener una base de datos del enlace idéntica. Cada router ejecuta independientemente el algoritmo SPF, también conocido como algoritmo de Dijkstra, en la base de datos del enlace con tal de determinar las mejores rutas a los destinos. El algoritmo SPF añade el coste (el cual está normalmente basado en el ancho de banda) a cada uno de los enlaces entre el router origen y el destino. Entonces el router escoge el camino con coste más bajo y añade el camino a su tabla de enrutamiento también conocida como base de datos de forwarding.

Los routers que utilizan OSPF mantienen información de sus vecinos y de sus bases de datos de adyacencia. Para simplificar el intercambio de información de enrutamiento sobre varios vecinos en la misma red, los routers que ejecutan OSPF tienen que escoger el Router Designado (DR) y el Router Designado de Backup (BDR) para servir de punto central para la actualización de rutas.

Los routers que ejecutan OSPF establecen relaciones, o estados, con sus vecinos para un intercambio de información de estado más eficiente. En contraste con los protocolos de vector distancia, como RIP, los cuales realizan broadcast o multicast de su tabla de enrutamiento completa por cada interfaz, esperando que los demás routers la reciban. RIP por defecto envía cada 30 segundos sólo un único tipo de mensaje, su tabla completa de enrutamiento. Sin embargo, los routers que ejecutan OSPF disponen de cinco tipos de paquetes distintos a enviar a sus vecinos para actualizar la información de estado del enlace.

Estos cinco tipos de mensajes hacen de OSPF un protocolo adecuado para comunicaciones sofisticadas y complejas.

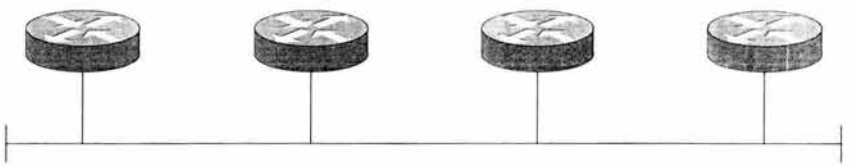
OSPF se relaciona con sus vecinos mediante siete estados distintos.

2.10.1 Topologías OSPF

En OSPF podemos encontrar distintos tipos de topologías, pero sin embargo ya se ha empezado a desarrollar soporte para otro tipo de topologías de forma propietaria.

2.10.1.1 Topología de Broadcast

Este tipo de topología se puede utilizar en entornos donde es posible que los routers tengan en común una red de broadcast, como podría ser una red Ethernet, Token Ring o FDDI. En este tipo de topologías los routers tienen en común una red que permite tráfico de multicast del DR con el resto de los routers.



2.13: Topología de broadcast

2.10.1.2 Topología punto a punto

Este tipo de topologías son las más simples, ya que en ella sólo entran dos routers conectados de forma directa formando un único enlace.

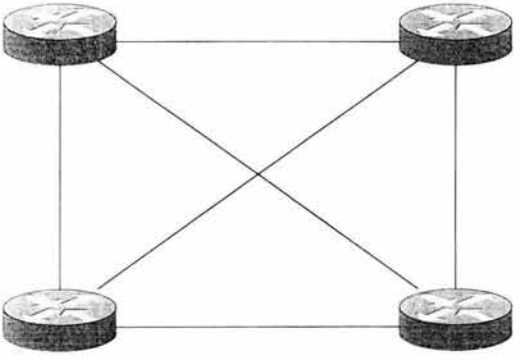
2.14: Topología punto a punto

En este tipo de topologías no es necesaria la elección de DB y BDR ya que sólo hay dos routers.

2.10.1.3 Topología NBMA

En este tipo de topologías que no son de broadcast, recordemos que NBMA son las siglas de "NoBroadcast MultiAccess networks". En este tipo de topologías nos encontramos con un problema adicional, ¿Cómo enviamos mensajes de multicast en este tipo de redes?, pues bien, esta pregunta sólo tiene una contestación posible, es decir, la contestación consiste en realizar una emulación de una red de broadcast.

La emulación de una red de broadcast en una red que no lo es sólo se puede hacer mediante la replicación de mensajes. Una red NBMA totalmente mallada, en la cual todos los routers están conectados con todos los routers tenemos que replicar un mensaje de multicast en muchos mensajes de unicast, es decir, en vez de enviar un único mensaje a la red a la dirección de multicast 224.0.0.5 tenemos que enviar el mismo mensaje por cada uno de los enlaces que tiene el router con los demás routers de la red, es decir, estamos realizando una topología que emula a una red de broadcast mediante un conjunto de redes punto a punto.



2.15: Topología NBMA totalmente mallada

2.10.2 Estados de OSPF

Para una comprensión más profunda de OSPF es necesario comprender las relaciones o estados que tienen entre si los routers que utilizan OSPF.

2.10.2.1 Estado Down

En el estado Down, el proceso OSPF no ha empezado a intercambiar información con ningún vecino. OSPF está esperando a entrar en el siguiente estado.

2.10.2.2 Estado Init

Los routers que utilizan OSPF envían paquetes de tipo 1 (Hello) en intervalos regulares para establecer relación con sus routers vecinos, cuando una interfaz recibe su primer paquete Hello entonces decimos que el router ha entrado en estado Init y está preparado para entrar en el siguiente estado.

2.10.2.3 Estado Two-Way

Utilizando paquetes Hello, cada router OSPF intenta establecer una comunicación bidireccional con cada router vecino que está ubicado en la misma red IP. Un router entra

en estado two-way en el momento que se ve en una de las actualizaciones de uno de sus vecinos. El estado two-way es la relación más básica que pueden tener los routers OSPF, pero la información de enrutamiento no se intercambia en este estado. Para aprender sobre enlaces de otros routers el router tiene que tener al menos una adyacencia completa.

2.10.2.4 Estado ExStart

Técnicamente, cuando un router y su vecino entran en estado ExStart, su conversación se caracteriza por una adyacencia, pero los routers todavía no tienen una adyacencia completa. Entre los dos routers se utilizan paquetes hello para determinar cual de los dos es el maestro y cual es el esclavo en su relación y se intercambian paquetes de tipo 2.

2.10.2.5 Estado Exchange

En el estado exchange se utilizan paquetes de tipo 2 para enviar al otro router su información de estado del enlace. En otras palabras, los routers describen sus bases de datos de estado del enlace al otro router. Si alguna de las rutas no está en la base de datos del enlace del router receptor de la información, este solicita una actualización completa, la cual se realiza en el estado Loading.

2.10.2.6 Estado Loading

Después de que todas las bases de datos han sido descritas a cada router, se tiene que solicitar una información que es más completa utilizando paquetes de tipo 3. Cuando un router recibe un paquete de tipo 3, este responde con una actualización mediante un paquete de tipo 4. Los paquetes de tipo 4 describen la información de estado del enlace que es el corazón de los protocolos de enrutamiento de estado del enlace. Los paquetes de tipo 4 con respondidos con paquetes de tipo 5.

2.10.2.7 Adyacencia Completa

Cuando termina el estado Loading, los routers están en una adyacencia completa. Cada router mantiene una lista de sus vecinos adyacentes, llamada base de datos de adyacencia. Es preciso no confundir la base de datos de adyacencia con la base de datos de estado del enlace o con la base de datos de forwarding.

Una adyacencia es una nueva relación formada entre vecinos seleccionados con el fin de intercambiar información de enrutamiento. No todos los pares de vecinos se vuelven adyacentes. En particular, no todos estos pares permanecen sincronizados. Si todos los vecinos tuvieran que estar sincronizados, el número de pares sincronizados en una red multiacceso tal como una LAN sería $n(n\text{-}1)/2$ donde n es el número de routers de la LAN. En redes grandes, el tráfico de sincronización inundaría la red, volviéndola inutilizable. El concepto de adyacencias se usa para limitar el número de pares sincronizados a 2n - 1, asegurando que el flujo de sincronización es manejable.

Ya que la adyacencia es necesaria para que los routers que utilizan OSPF puedan compartir su información de enrutamiento, un router tiene que estar adyacente con al menos otro router en la red IP a la que esté conectado. Si hay o no adyacencia depende del tipo de red que se esté utilizando, es decir, de qué tipo de red esté conectado los routers.

Las interfaces de un router que estén ejecutando OSPF tiene que reconocer tres tipos de redes: redes de broadcast (por ejemplo ethernet), NBMA (por ejemplo, frame relay totalmente mallada) y redes punto a punto (sólo dos routers). Un administrador de red podría configurar un cuarto tipo de red: red punto a multipunto.

El tipo de red en la que esté trabajando OSPF dictará el funcionamiento del protocolo, y este a su vez puede ser optimizado por el administrador de la red. Muchas redes se definen como redes de multiacceso porque no es posible predecir cuantos routers van a haber conectados.

2.10.3 Routers OSPF

Debido a que en redes de multiacceso puede existir un número significativo de routers, OSPF utiliza un método para evitar la sobrecarga de información de enrutamiento en la red, de este modo la información se centraliza en dos routers:

Router Designado (DR - Designated Router)

Para todas las redes de multiacceso IP se debe de elegir un DR. Este DR tiene dos funciones principales.
Mantener adyacencia con todos los demás routers de la red. Actuar de portavoz de todos los demás routers de la red y anunciar los cambios a las otras redes, por supuesto es el encargado de mantener la información centralizada del estado de su red.

Router Designado de Backup (BDR - Backup Designated Router)

El DR puede representar un único punto de fallo, así que se elige un BDR para proporcionar tolerancia a fallos, es decir una redundancia. Así pues el BDR también tiene que ser adyacente a todos los demás routers de la red y tiene que estar sincronizado con el DR para que en caso de caída del DR pueda este asumir la responsabilidad de la red. En redes punto a punto, en las cuales sólo existen dos nodos no tiene mucho sentido el que exista ni DR ni BDR, así que en este caso ambos routers funcionan peer-to-peer.

DR Other

La interfaz está en una red multiacceso pero el router no es el DR ni el BDR. El router forma adyacencias con el DR y el BDR.

Routers Internos (IR - Internal Router)

Los routers internos tienen todas sus interfaces en una misma área. Todos los routers de la misma área tienen las mismas bases de datos de enlaces, es decir

los routers internos de la misma área al ejecutar el algoritmo SPF utilizan los mismos routers como datos.

Routers de Backbone (BR - Backbone Routers)

Los routers de backbone están situados en los límites del área de backbone y tienen al menos una interfaz conectado al área 0.

Routers de Borde de Area (ABR - Area Border Routers)

Estos routers como indica su nombre son los routers que tienen enlaces a distintas áreas, estos routers mantienen bases de datos del enlace separadas por áreas, es decir, tienen una base de datos independiente por área y ejecutan un SPF independiente por área.

Routers de Frontera del Sistema Autónomo (ASBR - Automous System Boundary Routers)

Tienen al menos una interfaz con un AS (Sistema Autónomo) distinto. El AS distinto no tiene porque utilizar OSPF. Los ASBR distribuyen información no OSPF a la red OSPF y viceversa cuando es necesario.

Por supuesto un router puede ser de varios tipos a la vez, pero solo tienen un único Router ID (RID), un número de 32 bits que identifica un router particular. Una posible implementación es usar como RID la mayor dirección IP del router, esta es por lo regular la de loopback. Además cada router se puede configurar con un Router Priority (RP), un entero sin signo de 8 bits, configurable por medio de una interfaz que indica la selección del BDR. Un RP de cero indica que el router no se puede elegir como DR.

2.10.4 Tipos de LSA's

Los LSA's describen el estado de una red o de un router. Esta descripción cubre el estado de todas las interfaces de los routers y sus adyacencias.

En OSPF utilizamos 5 tipos de LSA's:

Tipo 1

Son llamados router link, estos LSA's describen el estado y el coste de los enlaces entre routers de área. Estos LSA's sólo se propagan dentro de una misma área, no en todo el Sistema Autónomo.

Tipo 2

Son llamados network links, estos LSA's describen todos los routers que hay en una red en particular. Estos LSA's se propagan dentro del área que contiene la red.

Tipo 3 / 4

Esos son los summary links. Estos LSA's se generan por los ABR's, y describen los enlaces entre los ABR's y los IR's del área local. Los summary links se propagan a través del área 0 o backbone a otras áreas a través de los ABR's del AS. Los LSA's de tipo 3 y de tipo 4 tiene diferencias.

Los LSA's de tipo 3 describen las rutas a las redes a través del AS y se envían por el área 0. Sin embargo los LSA's de tipo 4 describen la localización de los ASBR.

Tipo 5

Son también conocidos como external links, los cuales se crean en los ASBR's. Estos LSA's describen las rutas a destinos fuera del AS. Estos LSA's van por las áreas estándar y por el backbone.

Existen dos tipos de external links:

- External link type 1: Este se calcula añadiendo al coste externo el coste interno para alcanzar el destino.
- External link type 2: Es el coste externo sin tener en cuenta el coste interno.

Tal y como se puede observar en la descripción de los tipos de área, ningún tipo de LSA atraviesa las áreas totally stubby.

2.10.5 Funcionamiento de OSPF

Cuando un router arranca el proceso de enrutamiento OSPF en uno de sus interfaces, éste envía un paquete hello y continua enviando paquetes hello en intervalos regulares.

En el nivel 3 del modelo de referencia OSI, los paquetes hello son enviados a la dirección de multicast 224.0.0.5. Esta dirección tiene el significado de "todos los routers OSPF". Los routers que están ejecutando OSPF envían periódicamente paquetes hello para iniciar y mantener su adyacencia y para asegurarse que las adyacencias con sus vecinos no desaparecen. Los tiempos de actualización para el envío de paquetes hello son configurables, y por ejemplo fabricantes como Cisco envían por defecto paquetes hello en redes de broadcast cada 10 segundos, sin embargo en redes NBMA envían los paquetes cada 30 segundos, este sería el caso de redes Frame-Relay que utilizan OSPF como protocolo de enrutamiento.

Para el inicio de OSPF se utiliza el protocolo *Hello* para realizar un intercambio inicial en el cual se procede a conocer a los vecinos de la red, posteriormente se procede a descubrir las rutas, luego se eligen las rutas y posteriormente se mantienen la información de enrutamiento.

2.10.6 Descripción de las operaciones en OSPF

La secuencia básica de operaciones realizadas por los routers OSPF es:

1. Descubrir vecinos OSPF
2. Elegir el DR
3. Formar adyacencias
4. Sincronizar bases de datos
5. Calcular la tabla de enrutamiento
6. Anunciar los estados de los enlaces

Los routers efectuarán todos estos pasos durante su activación, y los repetirán en respuesta a eventos de red. Cada router debe ejecutar estos pasos para cada red a la que está conectado, excepto para calcular la tabla de enrutamiento. Cada router genera y mantiene una sola tabla de enrutamiento para todas las redes.

Las siguiente secciones describen estos pasos.

2.10.6.1 Descubriendo vecinos OSPF

Cuando los routers OSPF se activan, inician y mantienen relaciones con sus vecinos usando el protocolo Hello. El protocolo además asegura que la comunicación entre vecinos sea bidireccional. Los paquetes Hello se envían periódicamente al exterior por todas las interfaces de los routers. La comunicación bidireccional se indica si el propio router aparece en el paquete Hello del vecino. En una red de broadcast, los paquetes Hello se envían por multicast; los vecinos se descubren luego dinámicamente. En redes no broadcast, cada router que sea un DR potencial tiene una lista de todos los routers conectados a la red y enviará paquetes Hello a todos los demás DR's potenciales cuando su interfaz a la red sea operativa por primera vez.

2.10.6.2 Determinando el DR

Esto se hace usando el protocolo Hello. El router examina la lista de sus vecinos, desecha cualquiera que no tenga comunicación bidireccional o que tenga un RP de ver, y graba el DR, el BDR y la RP que ha declarado cada uno de ellos. El router se añade él mismo a la lista, usando el valor RP configurado para la interfaz y cero (desconocido) para el DR y el BDR, en el caso de que esté en proceso de activación.

Se emplean las siguientes reglas para determinar el BDR:

- Si uno o más routers declaran ser el BDR y no el DR, gana el que tenga un RP superior.
- En caso de empate, gana el que tenga mayor RID.
- Si ningún router declara ser el BDR, entonces el se elige el router con mayor RP a menos que se haya declarado como DR.

- De nuevo, en caso de empate gana el router con mayor RID.

Como el propio router que hace los cálculos está en la lista, puede determinar que él mismo es el BDR. Un proceso similar se sigue para el DR:

Si uno o más routers declaran ser el DR, gana el que tenga un RP superior. En caso de empate, gana el que tenga mayor RID. Si ningún router ha declarado ser el DR entonces el BDR se convierte en el DR.

El proceso real es mucho más complejo, debido a que los mensajes Hello transmitidos incluyen los cambios en los campos grabados en otros routers, y estos cambios causan eventos en los routers que a su vez podrán provocar nuevos cambio u otras acciones. La intención que se esconde tras este mecanismo es doble:

- Que cuando un router se active, no debería usurpar la posición del BDR actual aunque tenga un RP superior.

- Que la promoción de un BDR a DR debería ser ordenada y requerir que el BDR acepte sus responsabilidades.

El algoritmo no siempre da lugar a que el router de mayor prioridad sea el DR, ni tampoco que el segundo de mayor prioridad sea el BDR.

El DR tiene las siguientes responsabilidades:

- El DR genera para la red los anuncios de los estados de los enlaces, que inundan el área y describen esta red a todos los routers de todas las redes del área.

- El DR se hace adyacente a otros routers de la red. Estas adyacencias son centrales con respecto al proceso de inundación usado para asegurar que los anuncios alcanzan a todos los routers del área y que por tanto la base de datos topológica que usan todos permanece igual.

El BDR tiene la siguiente responsabilidad:

- El BDR se hace adyacente a todos los demás routers de la red. Esto asegura que cuando ocupe el puesto del DR lo pueda hacer rápidamente.

2.10.6.3 Formando adyacencias

Después de que se ha descubierto un vecino, asegurando la comunicación bidireccional, y (en una red multiacceso) elegido un DR, se toma la decisión de si se debe formar una adyacencia con uno de sus vecinos:

- En redes multiacceso, todos los routers se hacen adyacentes al DR y al BDR.

- En enlaces punto a punto (virtuales), cada router forma siempre una adyacencia con el router del otro extremo.

Si se toma la decisión de no formar una adyacencia, el estado de la comunicación con el vecino permanece en el estado "2-way".

Las adyacencias se establecen usando paquetes DD ("Database Description"), que contienen un resumen de la base de datos de estados de enlaces del emisor. Se pueden usar múltiples paquetes para describir la base de datos: con este fin se emplea un procedimiento de sondeo-respuesta. El router con mayor ID se convertirá en maestro, el otro en esclavo. Los paquetes DD enviados por el maestro (sondeos o polls) serán reconocidos por los DD's del esclavo (respuestas). El paquete contiene números de secuencia para asegurar la correspondencia entre sondeos y respuestas. Este proceso se denomina DEP ("Database Exchange Process").

2.10.6.4 Sincronización de las bases de datos

Después de que terminar el DEP ("Database Exchange Process"), cada router tiene una lista de aquellos anuncios para los que el vecino tiene más instancias actualizadas, que se solicitan por medio de paquetes LSR ("Link State Request"). La respuesta a un LSR es una LSU ("Link State Update") que contiene algunos o todos los anuncios solicitados. Si no se recibe respuesta, se repite la solicitud.

2.10.6.5 Calculando la tabla de enrutamiento

Usando como entrada las bases de datos de estados de enlaces de las áreas con las que está conectado, un router ejecuta el algoritmo SPF para construir su tabla de enrutamiento. La tabla de enrutamiento siempre se construye desde de cero: nunca se hacen actualizaciones a una tabla ya existente. Una tabla de enrutamiento vieja no se desecha hasta que se han identificado los cambios entre las dos tablas. Brevemente, el cálculo consiste en los pasos indicados abajo.

- Las rutas intra-area se calculan construyendo el árbol mínimo para cada área conectada usando el mismo router como raíz del árbol. El router calcula además si el área puede actuar como área de tránsito para enlaces virtuales.

- Las rutas inter-area se calculan examinando los LSA's. Para los ABR (que forman parte de la backbone) sólo se utilizan los anuncios correspondientes al backbone (es decir, un ABR siempre encaminará tráfico inter-area a través del backbone).

- Si el router está conectado a una o más áreas de tránsito, el router sustituye las rutas que haya calculado por rutas que pasen por áreas de tránsito si estas son mejores.

- Las rutas externas se calculan examinando los anuncios externos del AS. Las localizaciones de los ASBR ya se conocen debido a que se determinan como cualquier otra ruta intra-area o inter-area.

Cuando el algoritmo produce rutas de igual coste, OSPF puede balancear uniformemente la carga a través de ellas. El número máximo de rutas iguales admitidas depende de la implementación.

2.10.6.6 Anunciando los estados de los enlaces

Un router anuncia periódicamente el estado de su enlace, por lo que la ausencia de un anuncio reciente indica a los vecinos del router que no está activo. Todos los routers que hayan establecido comunicación bidireccional con un vecino ejecutan un contador de inactividad para detectar ese suceso. Si no se reestablece el contador, al final se desbordará y el evento asociado sitúa el estado del vecino en "down". Esto significa que la comunicación se debe establecer desde cero, incluyendo la resincronización de las bases de datos. Un router también relanza sus anuncios cuando su estado cambia.

Un router puede lanzar diversos anuncios para cada área. Estos se propagan a través del área por el procedimiento de inundación. Cada router emite un Router LSA. Si el router es además el DR para una o más de las redes del área, originará Network LSA's para estas. Los ABR generan una Network Summary LSA para cada destino inter-area conocido. Los ASBR originan un ASBR Summary LSA para cada destino externo conocido. Los destinos se anuncian uno cada vez de tal forma que el cambio de una sola ruta puede inundar la red sin tener que enviar el resto de las rutas. Durante el proceso de inundación, un sólo LSU puede llevar muchos anuncios.

2.11 BGP

Cada sistema autónomo funciona con su protocolo de enrutamiento interior (RIP, OSPF, etc.) para distribuir toda su información de enrutamiento dentro del sistema. BGP es un protocolo de enrutamiento exterior, el cual tiene como función principal intercambiar información acerca del acceso a redes entre sistemas autónomos. Cada Sistema Autónomo (AS) recibe un único número AS asignado por las autoridades de direccionamiento. La figura 2.16 muestra los diferentes tipos de sistemas autónomos que pueden estar interconectados usando BGP-4.

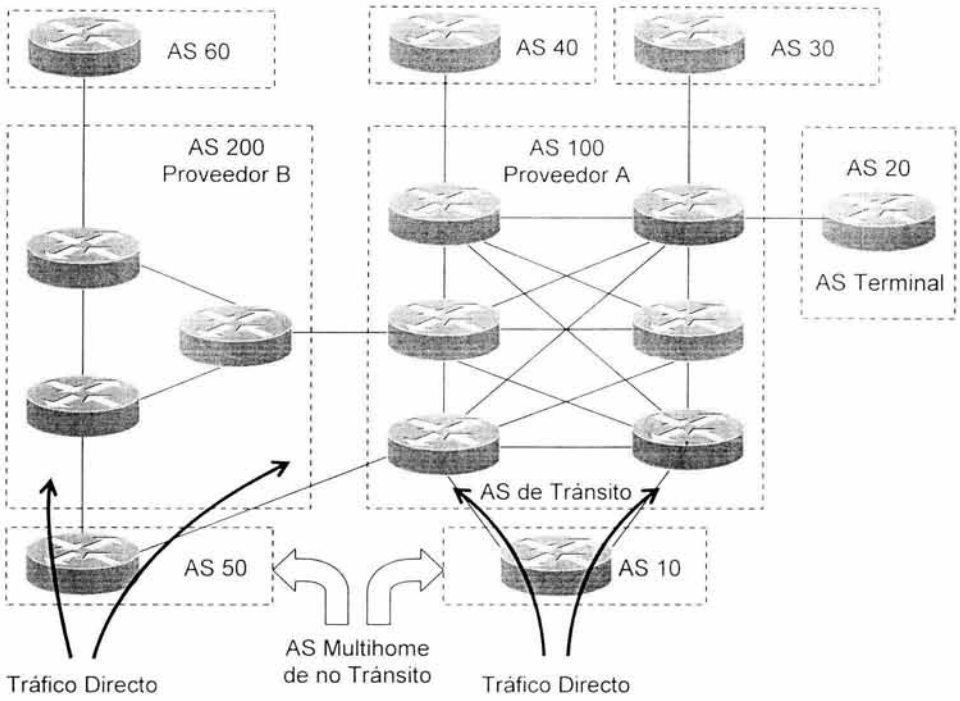


Figura 2.16: Tipos de AS y tráfico BGP

Los tipos de sistemas autónomos son los siguientes:

Sistema Autónomo de Tránsito

Un AS de tránsito tiene múltiples conexiones a otros AS's. Las actualizaciones de enrutamiento de cualquier AS que llegan a un transit AS pueden pasar a través de él 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 son generalmente de este tipo.

Sistema Autónomo Terminal (Stub)

Un As terminal tiene una sola conexión a otro AS. Todo el tráfico hacia o del AS terminal pasa a través de este enlace. ISP's pequeños, redes corporativas o de campus usan este tipo de AS.

Sistema Autónomo Multihome (De no tránsito)

Un AS 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 de salida.

Dos routers intercambiando información de enrutamiento con BGP son llamados "BGP Peers" o "BGP speakers". Ellos establecen una sesión TCP porque este protocolo garantiza una conexión confiable. Los peers realizan una conexión BGP para intercambiar mensajes BGP. El mensaje BGP más importante es el "UPDATE", el cual contiene las rutas de intercambio. Una ruta BGP esta definida como una unidad de información que consiste en información de ámbito de capa de red "Network Layer Reachabilty Information" (NLRI) y un conjunto de atributos de rutas. Un NLRI es básicamente un prefijo IPv4 con su longitud. Los conceptos de información de clase IPv4 han sido eliminados. Un NLRI puede representar una simple red, o más comúnmente, un agregado de un rango de direcciones. 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, una secuencia de sistemas autónomos a través de los cuales la ruta a pasado durante su actualización, o su origen. Las decisiones de enrutamiento y administración de tráfico frecuentemente están basadas 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 del AS_PATH, rechaza la ruta correspondiente.

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

2.11.1 Estableciendo una conexión BGP

Para intercambiar las actualizaciones de enrutamiento, dos peers primero tienen que establecer una conexión BGP. LA figura 2.17 ilustra los pasos necesarios para establecer una conexión BGP, incluyendo los diversos mensajes BGP intercambiados[2.2].

[2.2] El RFC 1771 describe este procedimiento.

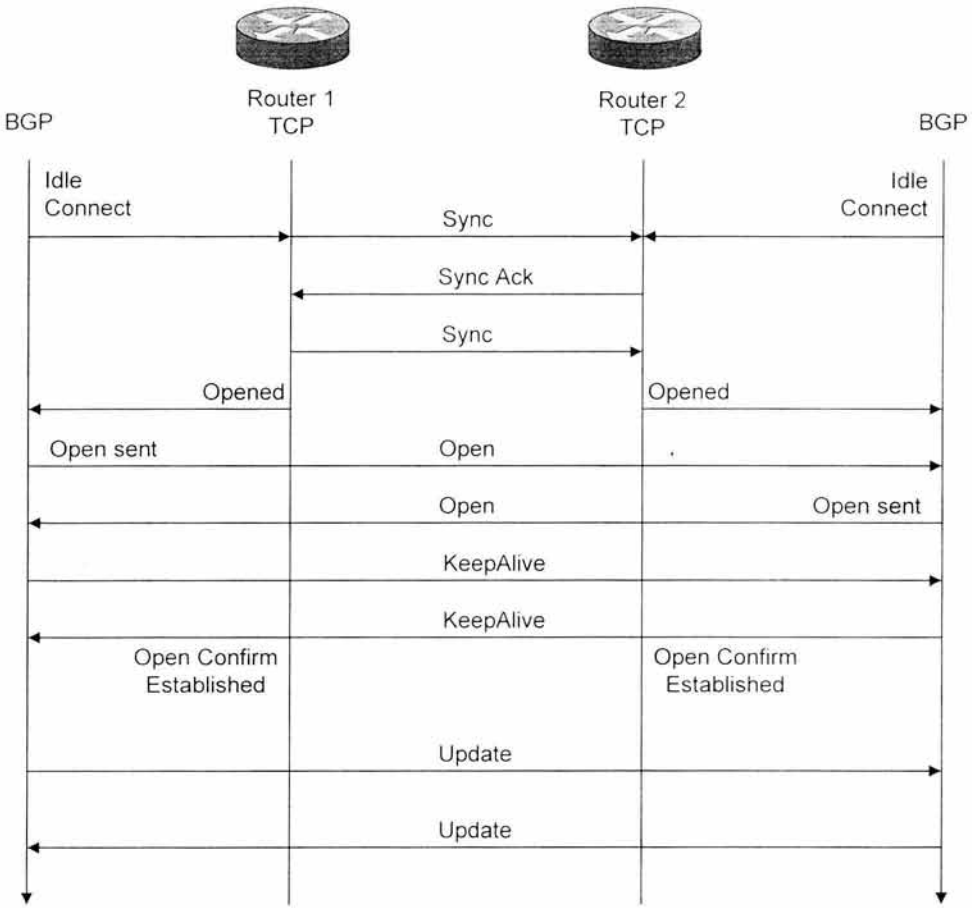


Figura 2.17: Estableciendo una conexión BGP

Si ambos routers intentan simultáneamente establecer una conexión 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 BGP 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 de enrutamiento completa basándose en sus políticas. Solo los cambios en la tabla de enrutamiento son intercambiados de ahora en adelante. 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. La introducción del "AS confederation" para BGP[2.3], o la reflexión de rutas BGP[2.4] hacen más flexible la regla anterior. Los atributos AS_PATH y NEXT_HOP no deben ser modificados cuando están pasando actualizaciones a peers internos.

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 IPv4 local.

2.11.2 Almacenamiento de Rutas y Políticas

Las rutas BGP son almacenadas en una Base de Información de Enrutamiento (RIB). La figura 2.18 muestra los tres diferentes RIB's y su interacción.

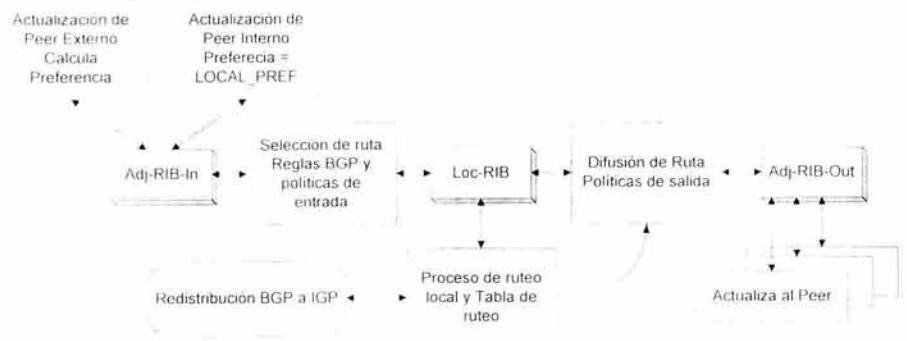


Figura 2.18: BGP RIB's y sus interacciones

Los mensajes entrantes pueden tener nuevas rutas factibles, rutas repuestas de actualizaciones iniciales, o rutas que han sido retiradas por los anuncios del peer. Todas estas rutas están ubicadas dentro del Adj-RIB-In. Por cada ruta nueva o cambiada, es calculado un grado de preferencia basado en las políticas de entrada. Esta preferencia

[2.3] Descrito en el RFC 3065
[2.4] Descrito en el RFC 2796

esta localizada dentro del atributo LOCAL_PREF. Si la ruta proviene de un peer interno, el LOCAL_PREF ya es portado en la actualización y no debe ser recalculado. Cada ruta en el Adj-RIB-In es procesada por el proceso de selección de ruta e introducida dentro del Loc-RIB. El proceso de selección primero revisa en los atributos NEXT_HOP y AS_PATH de la ruta. La dirección IP especificada por el NEXT_HOP debe ser accesible a través de una entrada en la tabla de enrutamiento local. El AS_PATH no debe contener el número AS local. Si los dos atributos cumplen, la ruta es aceptada o ignorada basándose en las políticas de entrada, de otro modo la ruta es ignorada. En caso de múltiples rutas a un mismo destino, la ruta con la preferencia más alta es aceptada. En caso de tener la misma preferencia, una compleja regla "Tie-breaking" garantiza que solo una de las rutas al mismo destino es aceptada[2.5].

Después del proceso anterior, las rutas en el Loc-RIB están ubicadas en la tabla de enrutamiento local. La dirección del salto siguiente legítima es tomada desde la entrada de ruta local a la dirección IPv4 especificada en el atributo NEXT_HOP.

Todas las rutas en el Loc-RIB y todas las rutas en la tabla de enrutamiento local son elegibles para ser anunciadas a los peers externos de este router. Solo las rutas en el Loc-RIB aprendidas de peers externos son elegibles para ser anunciadas a todos los peers internos de este router, a menos que sea habilitada la reflexión de rutas[2.6]. Las políticas de salida difunden las rutas a un Adj-RIB-Out de un peer específico. Las políticas de salida pueden ejecutar la agregación de ruta o la modificación de los atributos de ruta. Los cambios en el Adj-RIB-Out provocan que el proceso de actualización envíe una actualización al peer.

2.11.3 Cabecera del Mensaje BGP

Los mensajes BGP son transportados en las conexiones TCP, las cuales pueden ser establecidas en IPv4 o IPv6. Las direcciones IP origen y destino del datagrama dependen de la configuración del peer. Ellas siempre son del tipo unicast. Hay que recordar que solo una conexión TCP es establecida entre dos peers. Las conexiones BGP usan el puerto bien conocido 179. La figura muestra el formato de la cabecera del mensaje BGP. La cabecera tiene un tamaño fijo de 19 bytes.

[2.5] Esta regla es descrita en el RFC 1771
[2.6] Descrita en el RFC 2796.

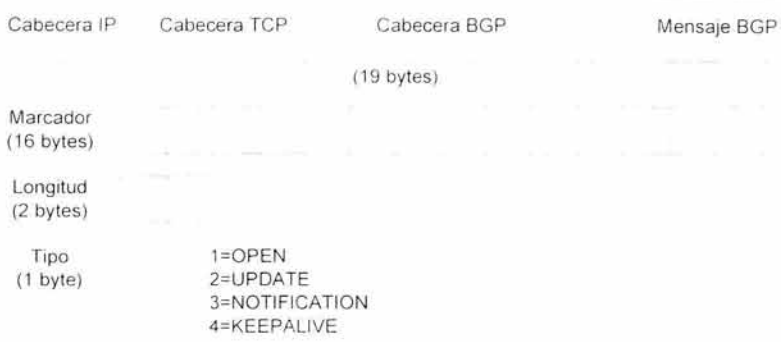


Figura 2.19: Formato de la cabecera BGP

Los campos de la cabecera son:

Marcador (16 bytes)

Contiene datos de autenticación si esta fue negociada entre los peers. Todos los bits son puestos en uno, si no se usa autenticación.

Longitud (2 bytes)

La longitud total del mensaje BGP, incluyendo las cabeceras. El valor debe estar entre 19 y 4096. El tamaño máximo de un mensaje BGP es 4096 bytes.

Tipo (1 byte)

Indica el tipo de mensaje BGP.

2.11.4 Tipos de mensaje BGP

Tipo	Nombre	Descripción
1	OPEN	Inicializa la conexión BGP y negocia los parámetros de sesión.
2	UPDATE	Intercambia rutas BGP remotas y factibles.
3	NOTIFICATION	Reporta errores o termina conexiones BGP.
4	KEEPALIVE	Conserva la conexión BGP a partir de la expiración.

Tabla 2.2

2.11.5 Mensaje OPEN

Tan pronto como la conexión entre dos peers BGP ha sido establecida, los routers envían mensajes OPEN para inicializar la conexión BGP. Este mensaje verifica la validez del peer y negocia los parámetros usados en la sesión. Para verificar la validez de un

peer, en cada lado de la conexión se debe configurar la dirección IP y el número de AS del peer.

Los campos del mensaje OPEN son los siguientes:

Versión (1byte)

Indica la versión BGP usada por el peer emisor. La versión actual es 4. Ambos peers deben tener la misma versión. La versión no puede ser negociada. Cada peer generalmente indica la versión más reciente que soporta. Si el peer receptor no soporta esta versión, se notifica y termina la sesión.

My Autonomous System (2 bytes)

Indica el número de sistema autónomo del router emisor. El router receptor debe verificar que este número es el número AS del peer. Si es incorrecto, el peer es notificado y la sesión termina. Si el número AS es el mismo que el del router receptor, el peer es interno (IBGP), de otro modo, el peer es externo.

Hold Time (2 bytes)

Propone un tiempo máximo en segundos que puede pasar antes que cualquier mensaje BGP llegue a esta interfaz. El "Hold timer" es negociado al valor más pequeño anunciado por cualquiera de los peers. Para conservar una conexión BGP a partir expiración, los peers envian mensajes KEEPALIVE una vez cada HoldTime/3 segundos. Un hold time de cero indica que no es necesario enviar mensajes KEEPALIVE. El valor del hold time es cero 0 o mayor que 2.

Identificador BGP (4 bytes)

Cada router debe estar identificado por un único y globalmente asignado identificador BGP. Al comenzar, el identificador BGP es puesto a una dirección IPv4 de una interfaz local. Esto significa que el router debe tener por lo menos una dirección IPv4 configurada localmente, aún en un ambiente IPv6. El mensaje es rechazado si el identificador BGP es igual al identificador BGP del router receptor, o si el identificador BGP es ilegal.

Longitud de Parámetros Opcionales (1 byte)

Indica la longitud o tamaño de los parámetros opcionales que serán negociados. Una longitud de cero indica que no hay parámetros opcionales.

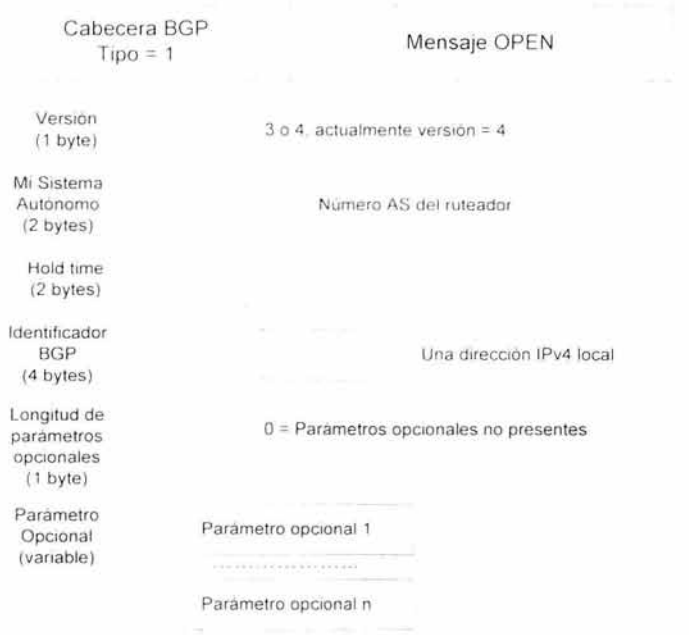


Figura 2.20: El mensaje OPEN

Parámetros Opcionales

Cada parámetro opcional consiste en una tripleta TLV: tipo, longitud, valor. Ambos routers deben conocer y estar de acuerdo en los parámetros opcionales; de otra forma, el peer es notificado del rechazo del parámetro. Esto podría conducir al final de la sesión. Por el momento, solo revisaremos dos parámetros. El parámetro opcional "Capacidad BGP" es muy importante para el soporte de IPv6.

Tipo	Nombre	Descripción
1	Autenticación	El parámetro consiste en dos campos: Código de autenticación y Datos de autenticación. El primero define el mecanismo de autenticación usado y como están el marcador y el campo de datos de autenticación para ser procesados.
2	Capacidad BGP	El parámetro consiste en una o más tripletas: código, longitud, valor. Las cuales indican diferentes capacidades de BGP[2.7]. El parámetro de capacidad puede aparecer más de una vez en el mensaje OPEN. El código de capacidad puesto en 1 indica la capacidad de extensión multiprotocolo[2.8].

Tabla 2.3

[2.7] En el RFC 2842 se define este mecanismo.
[2.8] Definido en el RFC 2858.

La capacidad de extensión multiprotocolo tiene un campo de 4 bytes. Los primeros 2 bytes identifican al "Address Family Identifier (AFI)", el byte 3 esta reservado, y el cuarto byte define el "Subsequent Address Family Identifier (SAFI)". El AFI define el protocolo de capa de red usado en la extensión multiprotocolo. El SAFI define información adicional acerca del protocolo: si el protocolo utiliza "envío unicast (SAFI=1)", "envío multicast (SAFI=2)", o ambos (SAFI=3). Para soportar IPv6, la capacidad de extensión multiprotocolo es puesta en: Código=1, Longitud=4, Valor=hexadecimal 0x0002 0001.

2.11.6 Mensaje UPDATE

Un mensaje UPDATE transporta rutas BGP anunciadas por el peer origen. Es dividido en tres secciones. La primera sección especifica el NLRI IPv4 que el peer emisor esta retirando. La segunda sección define todos los atributos asociados con el NLRI IPv4 factible seguido en la tercera sección. Múltiples NLRI con el mismo conjunto de atributos de ruta pueden ser ubicados en un simple mensaje UPDATE.

Los campos del mensaje UPDATE son detallados en la siguiente lista:

Unfeasible Routes length (2 bytes)

Define la longitud del campo de rutas retiradas. Puesto en cero indica que el peer origen no tiene una ruta que retirar con este mensaje.

Withdrawn Routes

Una lista de NLRI's IPv4 que ya no son válidos. Cada NLRI es codificado como <longitud, prefijo> y representa un prefijo IPv4. El primer byte (longitud) define la longitud correspondiente del campo prefijo. El campo de longitud de un byte define la longitud del correspondiente campo "Prefijo". El campo "Prefijo" es aumentado hasta llenar el octeto con bits cero. Como los NLRI's son prefijos IPv4, este campo puede no ser utilizado para retirar rutas IPv6.

Longitud total de atributos de ruta (2 bytes)

Define la longitud del campo de atributos de ruta.

Atributos de ruta

Contiene una lista de los atributos de ruta que pertenecen al NLRI factible anunciado.

Network Layer Reachability Information (NLRI)

Una lista de NRLI's IPv4 que son anunciados con esta actualización. Cada NLRI es codificado como <longitud, prefijo> y representa un prefijo IPv4. El campo con longitud de un byte define la longitud del correspondiente campo "Prefijo". El campo del "Prefijo" es aumentado hasta llenar el octeto con bits cero. Como los NLRI's son prefijos IPv4, este campo puede nunca ser utilizado para anunciar rutas IPv6.

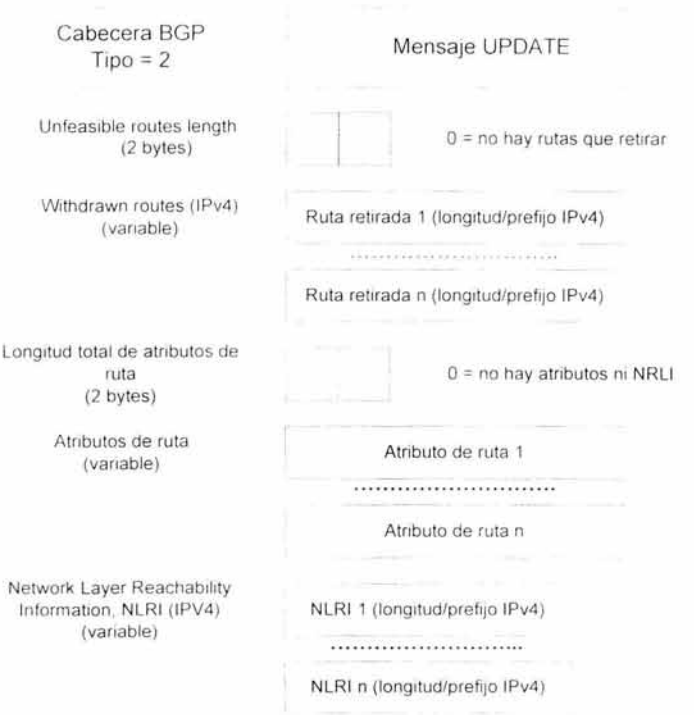


Figura 2.21: El mensaje UPDATE de BGP.

2.11.7 Atributos BGP

Los atributos de ruta proporcionan información adicional acerca del NLRI anunciado. Cada atributo de ruta tiene una cabecera de atributo de 2 bytes.

Figura 2.22: Los atributos de ruta.

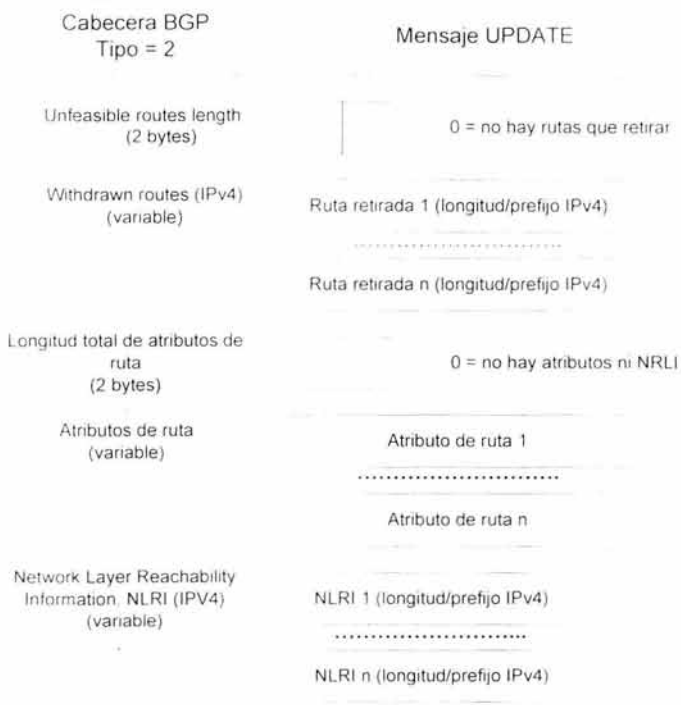


Figura 2.21. El mensaje UPDATE de BGP.

2.11.7 Atributos BGP

Los atributos de ruta proporcionan información adicional acerca del NLRI anunciado. Cada atributo de ruta tiene una cabecera de atributo de 2 bytes.

Figura 2.22. Los atributos de ruta.

La cabecera de atributo de ruta esta formada por:

Bit Opcional (O bit)

Define si el atributo es opcional (se pone en uno) o reconocido (puesto en cero). Un atributo reconocido debe ser reconocido y soportado por cada router BGP. Los atributos opcionales pueden no ser reconocidos por algunos routers.

Bit Transitivo (T bit)

Define si el atributo es transitivo (puesto en uno), o no lo es (puesto en cero). Los atributos transitivos siempre deben ser pasados cuando el NLRI es anunciado a otro peer. Los atributos reconocidos siempre deben ser transitivos.

Bit Parcial (P bit)

Aplica solo a atributos transitivos opcionales. Si un router a lo largo de la ruta actualizada no reconoce el atributo transitivo opcional, debe poner el bit parcial (P) en uno. Esto indica que al menos un router de la ruta no reconoce este atributo. Este bit siempre se debe poner en cero para opciones no transitivas o atributos reconocidos.

Bit de longitud extendida (E bit)

Define si el campo "longitud de atributo" es de 1 byte (puesto a cero) o 2 bytes (puesto en uno). La longitud extendida puede ser usada si los datos del atributo son más de 255 bytes.

Código de atributo (1byte)

Define el tipo de atributo. La siguiente lista que explica algunos de los atributos más comunes[2.9].

Tipo	Nombre/Bandera	Descripción
1	ORIGIN (reconocido)	Define el origen de esta ruta. 0=IGP,1=EGP, 2=Incompleta
2	AS_PATH (reconocido)	Una secuencia de números AS que esta ruta a pasado durante su actualización. El número más a la derecha indica el AS origen. Previene bucles y puede ser usado junto con políticas.
3	NEXT_HOP (reconocido)	Especifica la dirección IPv4 del siguiente salto. No puede ser usado en IPv6.
4	MED (opcional no transitivo)	El MULTI_EXIT_DISC (MED) indica una preferencia deseada (4 bytes) de esta ruta al peer. El más bajo es el mejor. Diseñado para múltiples conexiones EBGP entre dos sistemas autónomos para compartir carga de tráfico entrante.

[2.9] El RFC 1771 u otros de extensión BGP describen detalladamente estos atributos

La cabecera de atributo de ruta esta formada por:

Bit Opcional (O bit)

Define si el atributo es opcional (se pone en uno) o reconocido (puesto en cero). Un atributo reconocido debe ser reconocido y soportado por cada router BGP. Los atributos opcionales pueden no ser reconocidos por algunos routers.

Bit Transitivo (T bit)

Define si el atributo es transitivo (puesto en uno), o no lo es (puesto en cero). Los atributos transitivos siempre deben ser pasados cuando el NLRI es anunciado a otro peer. Los atributos reconocidos siempre deben ser transitivos.

Bit Parcial (P bit)

Aplica solo a atributos transitivos opcionales. Si un router a lo largo de la ruta actualizada no reconoce el atributo transitivo opcional, debe poner el bit parcial (P) en uno. Esto indica que al menos un router de la ruta no reconoce este atributo. Este bit siempre se debe poner en cero para opciones no transitivas o atributos reconocidos.

Bit de longitud extendida (E bit)

Define si el campo "longitud de atributo" es de 1 byte (puesto a cero) o 2 bytes (puesto en uno). La longitud extendida puede ser usada si los datos del atributo son más de 255 bytes.

Código de atributo (1byte)

Define el tipo de atributo. La siguiente lista que explica algunos de los atributos más comunes[2.9].

Tipo	Nombre/Bandera	Descripción
1	ORIGIN (reconocido)	Define el origen de esta ruta. 0=IGP, 1=EGP, 2=Incompleta
2	AS_PATH (reconocido)	Una secuencia de números AS que esta ruta a pasado durante su actualización. El número más a la derecha indica el AS origen. Previene bucles y puede ser usado junto con políticas.
3	NEXT_HOP (reconocido)	Especifica la dirección IPv4 del siguiente salto. No puede ser usado en IPv6.
4	MED (opcional no transitivo)	El MULTI_EXIT_DISC (MED) indica una preferencia deseada (4 bytes) de esta ruta al peer. El más bajo es el mejor. Diseñado para múltiples conexiones EBGP entre dos sistemas autónomos para compartir carga de tráfico entrante.

[2.9] El RFC 1771 u otros de extensión BGP describen detalladamente estos atributos

5	LOCAL_PREF (reconocido)	Define una preferencia local (4 bytes) de esta ruta. La más alta es la mejor. Generalmente es calculada de rutas que llegan de peers externos y conservan a peers internos. Esta diseñado para compartir carga de tráfico saliente.
6	ATOMIC_AGGREGATE (reconocido)	Especifica que uno de los routers ha seleccionado esta ruta menos especifica sobre otra ruta más especifica.
7	AGGREGATOR (opcional transitivo)	El identificador BGP del router que ha agregado rutas dentro de esta ruta.
8	COMMUNITY (opcional transitivo)	Lleva una etiqueta de 4 bytes con información. Puede ser usada por el proceso de selección de ruta[2.10].
9	MP_REACH_NLRI (opcional no transitivo)	Anuncia el multiprotocolo NLRI. Usado por prefijos IPV6.
10	MP_UNREACH_NLR (opcional no transitivo)I	Retira el multiprotocolo NLRI. Usado por prefijos IPV6.

Tabla 2.4

2.11.8 Mensajes NOTIFICATION y KEEPALIVE

Los mensajes NOTIFICATION son usados para reportar errores. Un campo de 1 byte para el Código de Error especifica la categoria del error[2.11].

Los mensajes KEEPALIVE no contienen datos de ninguna clase, solo la cabecera de mensaje BGP con el mensaje tipo 4. Son usados para prevenir una conexión BGP de interrupción.

[2.10] Descrito en el RFC 1997.
[2.11] La sección 4.5 del RFC 1771 tiene todos los codigos de error. Para IPv6 los codigos de error son especificados en el RFC 2858.

CAPÍTULO 3

ESQUEMA DE DIRECCIONAMIENTO Y ENRUTAMIENTO PARA RED UNAM

3.1 Direccionamiento IPv6

En IPv4 las direcciones son de 32 bits, mientras que en IPv6 son de 128 bits. Extender el espacio de direcciones fue una de las razones para desarrollar IPv6, además de optimizar las tablas de enrutamiento, especialmente en Internet.

3.1.1 Tipos de direcciones

En IPv4 tenemos las direcciones tipo "Unicast", "Broadcast", y "Multicast"[3.1]. Con IPv6 ya no se usa el broadcast, por lo que ya no hay direcciones de este tipo. Las direcciones multicast sustituyen la función de las direcciones de broadcast.

La dirección ***Unicast*** identifica únicamente a una interfaz de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada con esta dirección.

La dirección ***Multicast*** identifica a un grupo de interfaces. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.

La dirección ***Anycast*** es asignada a múltiples interfaces que, generalmente, se encuentran en múltiples nodos[3.2]. Un paquete enviado a una dirección anycast es entregado solo a una de las interfaces, generalmente la más "cercana", de acuerdo a la distancia del protocolo de enrutamiento empleado.

3.1.2 Reglas generales

Las direcciones IPv6 se asignan a interfaces, por lo que cada interfaz de un nodo necesita por lo menos una dirección unicast. Una interfaz puede tener asignadas múltiples direcciones IPv6 de los diferentes tipos: unicast, multicast, o anycast. Un nodo puede, por lo tanto, estar identificado por la dirección de cualquiera de sus interfaces. También es posible asignar una dirección unicast a múltiples interfaces por razones de balanceo de carga. En IPv6 todos los ceros y unos son válidos para cualquier campo en una dirección, excluyendo algunas combinaciones especiales dependiendo del tipo de dirección. Una dirección IPv6 consiste en tres partes: el prefijo global de enrutamiento, el identificador ID de subred, y el identificador ID de la interfaz, como se muestra en la siguiente figura.

El prefijo global de enrutamiento se usa para identificar el tipo de dirección. El identificador de subred se usa para identificar un enlace dentro de un sitio. Un identificador de subred se asocia con un enlace. Múltiples identificadores de subred pueden ser asignados a un enlace. Un identificador de interfaz se usa para identificar una interfaz en un enlace y necesita ser único en ese enlace.

[3.1] La arquitectura de direccionamiento IPv6 esta definida en el RFC 2373, el cual sustituye al 1884.
[3.2] La dirección "Anycast" es un tipo de dirección introducida en el RFC 1546. Ahora se usa en IPv6.

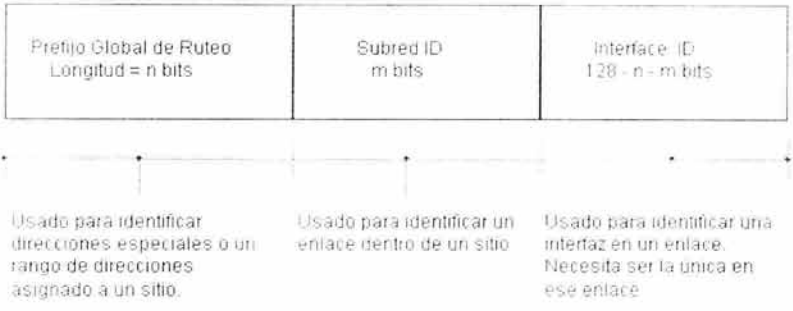


Figura 3.1: Formato general de las direcciones IPv6

3.1.3 Notación de direcciones

Una dirección IPv6 tiene un tamaño de 128 bits, o 16 bytes. Las direcciones están divididas en ocho bloques, cada uno de 16 bits, y están en notación hexadecimal. Los bloques están separados por dos puntos. Por ejemplo:

FF80:0000:0000:0000:0202:B3FF:FE1E:8329

Para hacer más fácil el manejo de las direcciones IPv6, es posible hacer algunas abreviaciones. Un caso muy común es omitir los primeros ceros de cada bloque. Por ejemplo, la dirección anterior se puede escribir simplemente como:

FF80:0:0:0:202:B3FF:FE1E:8329

Un par de dos puntos puede reemplazar ceros consecutivos. Por ejemplo, la dirección anterior puede representarse simplemente como:

FF80::0202:B3FF:FE1E:8329

Con un par de dos puntos podemos sustituir los bloques de ceros. El par de dos puntos solo puede usarse una vez en cada dirección. La razón de esto es porque que los procesadores usan una representación de 128 bits; si al procesar la dirección se encuentra un par de dos puntos, se expande con los ceros necesarios para completar el formato de 128 bits. En el caso de tener una dirección con dos o más pares de dos puntos el procesador no podría resolver cuantos ceros agregar por cada uno. En caso de tener una dirección **CAFF:CA01:0000:0056:0000:ABCD:EF12:1243**, se puede representar de la siguiente forma:

CAFF:CA01::56:0:ABCD:EF12:1243

también:

CAFF:CA01:0:56::ABCD:EF12:1243

Vemos que solo es posible aplicar un par de dos puntos. Si se quieren omitir ceros de bloques no consecutivos, se deja un solo par de dos puntos y el resto debe abreviarse

con un cero por bloque adicional. Si se omiten todos los ceros de otros bloques, entonces, se estarían creando más pares de dos puntos, lo cual no esta permitido.

En ambientes donde IPv4 e IPv6 están mezclados, otra notación conveniente en IPv6 es poner la dirección IPv4 dentro de los 4 bytes de menor orden de una dirección IPv6. Una dirección IPv4 **192.168.0.2** puede ser representada en IPv6 como **X:X:X:X:X:X:192.168.0.2**. Por lo tanto, una dirección **0:0:0:0:0:0:192.168.0.2** puede ser escrita como **::192.168.0.2**, o en formato hexadecimal: **::C0A8:2** .

3.1.4 Notación de prefijos

El formato de un "Prefijo" se refiere a los bits de mayor orden de una dirección IP y se usa para identificar la subred o un tipo de dirección especifico[3.3]. La notación añade la longitud del prefijo, escrita como un número de bits con una barra invertida:

Dirección IPv6 / longitud del prefijo

La longitud del prefijo especifica cuantos son los bits más a la izquierda que comprenden el prefijo de la dirección especificada antes de la barra invertida. Esta es otra forma de representar una máscara de subred. Recordemos que una máscara de subred indica cuantos bits de la dirección IPv4 pertenecen al identificador de red. El prefijo se usa para identificar la subred a la que pertenece una interfaz y es usado por los routers para enviar los paquetes.

Podemos revisar el ejemplo de la sección anterior, donde, estamos interesados en el prefijo de la dirección **CAFF:CA01:0000:0056:0000:ABCD:EF12:1234 /64**. Si comprimimos a la forma **CAFF:CA01::0056 /64** y, después expandimos esta última con las reglas de notación vistas anteriormente, tendremos **CAFF:CA01:0000:0000:0000:0000:0000:0056**, con **CAFF:CA01:0000:0000** para el prefijo de 64 bits. Esta no es la misma dirección que la original ni el mismo prefijo. Para evitar estos conflictos, podemos usar la notación **CAFF:CA01:0:56:: / 64**.

3.1.5 Formato de prefijos

La tabla 3.1 muestra la asignación inicial de prefijos[3.4]. La mayor parte del espacio de direcciones (cerca del 85%) no esta asignado, lo cual permite futuras asignaciones.

Asignación	Prefijo binario	Prefijo hexadecimal	Fracción del espacio de direcciones
Reservado	0000 0000	::0 / 128	1 / 256
Reservado para asignación NSAP	0000 0001		1 / 128
Reservado para IPX	0000 010		1 / 128

[3.3] La notación de los prefijos también se ha especificado en el RFC 2373. En los drafts más recientes es llamado prefijo global de ruteo "Global routing prefix".

[3.4] EL RFC 2373 tiene una lista de formatos de prefijos "Global Routing Prefixes" que se usan para identificar direcciones especiales, tales como direcciones de enlace-local o direcciones multicast.

Direcciones unicast globales agregables	001		1 / 8
Direcciones unicast de enlace local	1111 1110 10	FE80:: / 10	1 / 1024
Direcciones unicast de sitio local	1111 1110 11	FECO:: / 10	1 / 1024
Direcciones multicast	1111 1111	FF00:: / 8	1 / 256

Tabla 3.1: Lista de prefijos asignados

Algunas direcciones especiales son asignadas fuera del espacio de direcciones reservado con el prefijo binario 0000 0000. Estas incluyen a las direcciones no especificadas, las de loopback, y direcciones IPv6 con direcciones IPv4 insertadas.

Las direcciones unicast pueden ser distinguidas de las multicast por su prefijo. Globalmente, solo las direcciones unicast tienen el byte de mayor orden comenzando con 001. Una dirección con el byte de mayor orden que comienza con 1111 1111 (FF en hexadecimal) es siempre de tipo multicast.

Las direcciones anycast son tomadas del espacio de direcciones unicast, por lo que no se pueden identificar como anycast solo por el prefijo. Si se asigna y configura una dirección unicast a múltiples interfaces adquiere la función anycast.

Las direcciones dentro del rango de prefijos 001 a 111 pueden usar un identificador de interfaz de 64 bits que sigue el formato EUI-64 para auto configuración[3.5], excepto las direcciones multicast.

Las dirección de enlace local de un nodo es la combinación del prefijo **FE80:: /64** y un identificador de interfaz de 64 bits expresado en notación hexadecimal[3.6].

3.1.6 Privacidad de direcciones

Es necesario considerar la privacidad de las direcciones IPv6 autoconfiguradas usando el identificador de interfaz. Si una dirección IPv6 esta construida usando la dirección MAC, el acceso a Internet puede ser trazado porque este identificador es globalmente único para la interfaz. Sin embargo, no es indispensable que un nodo IPv6 tenga una dirección basada en el identificador de la interfaz. El nodo IPv6 puede tener una dirección estática y manualmente configurada o dinámicamente asignada por un servidor DHCP. También es posible obtener, solo en IPv6 y de manera temporal, la dirección a partir de un número aleatorio en lugar del número serial asignado de fábrica[3.7].

[3.5] El EUI-64 es el único identificador definido por la IEEE (Institute of Electrical and Electronics Engineers), más información al respecto se puede ver en http://standards.ieee.org/regauth/oui/tutorials/EUI64.html. En el apéndice de este trabajo se puede encontrar una descripción de la autoconfiguración usando el identificador EUI-64.

[3.6] El proceso de configuración de direcciones de enlace local se describe en el RFC 2464.

[3.7] A inicios del año 2001 fue publicado el RFC 3041, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", el cual definió un nuevo tipo de direcciones, disponibles solo para IPv6.

Un dispositivo de Internet que es objeto de comunicación con IP y proporciona algún servicio, necesita una dirección IP única y estable; mientras que un host que actúa como cliente no necesita tener la misma dirección cada vez que se conecta a Internet. Con la arquitectura IPv6 se puede tener dos tipos de direcciones:

Direcciones IP únicas estables

Asignadas por configuración manual, servidor DHCP, o auto-configuración.

Direcciones IP temporales

Asignadas usando un número aleatorio en lugar del identificador de interfaz.

3.1.7 Direcciones locales de sitio y de enlace

En IPv4 las organizaciones frecuentemente usan direcciones dentro de los rangos privados[3.8]. Las direcciones reservadas para uso privado no son transmitidas por los routers de Internet, pero si pueden hacerlo dentro de la red de una organización. Para conectar las direcciones privadas con las direcciones públicas de Internet se utiliza NAT, mecanismo que hace la "Traducción" entre los dos tipos de direcciones.

IPv6 adjudica dos espacios de direcciones para sitio local y enlace local, ambos identificados por su prefijo. Una dirección de enlace local se usa en un enlace y no debe ser enrutada. Esta puede ser usada para mecanismos de auto-configuración y en redes sin routers, por lo que es útil para crear redes temporales. Permite reunir hosts en una sala de conferencia y compartir información. Las direcciones de sitio local contienen información de la subred y pueden ser transmitidas por routers dentro de un sitio, pero no fuera de él.

En notación hexadecimal, una dirección de enlace local es identificada por el prefijo **FE80**; una dirección de sitio local es identificada por el prefijo **FEC0**.

[3.8] El RFC 1918 especifica el uso de direcciones privadas.

Dirección de Enlace Local

1111 1110 10	0	ID de Interfaz
10 bits hex: FE80	54 bits	64 bits

Dirección de Sitio Local

1111 1110 11	0	ID de Subred	ID de Interfaz
10 bits hex: FEC0	38 bits	16 bits	64 bits

Figura 3.2: Formato de Direcciones Locales de Sitio y de Enlace

3.1.8 Direcciones Unicast Globales Agregables

Las direcciones Unicast Globales Agregables están identificadas por el prefijo **001**[3.9].

Prefijo 001	TLA ID	Res	NLA ID	SLA ID	ID de Interfaz
3 bits	13 bits	8 bits	24 bits	16 bits	64 bits

Figura 3.3: Formato de Direcciones Unicast Globales Agregables

Al prefijo le siguen cinco componentes más:

Prefijo

001, prefijo de las direcciones unicast globales agregables.

TLA ID

Identificador de agregación de nivel superior "Top-level aggregation identifier"

[3.9] La especificación inicial de las direcciones las definió como "Provider-based Address"; el nombre se ha cambiado por "Aggregatable Global Unicast Address". El cambio de nombre refleja la adición de un ISP independiente, significado de agregación denominado: agregación basado en intercambio "Exchange-based Aggregation".

RES

Reservado para uso futuro

NLA ID

Identificador de agregación del siguiente nivel "Next-level aggregation identifier"

SLA ID

Identificador de agregación de nivel de sitio "Site-level aggregation identifier"

Interfaz ID

Identificador de interfaz

El identificador de agregación de nivel superior (TLA) contiene el nivel más alto de la información de enrutamiento acerca de la dirección. El tamaño de 13 bits limita el número de rutas top-level a 8192[3.10]. El objetivo de este identificador es la optimización del enrutamiento. En el "Core" de Internet, las tablas de enrutamiento necesitan solo una ruta de entrada por TLA, aunque pueden tener más, por lo que los trece bits son bastantes.

Las adjudicaciones TLA que se muestran en la siguiente tabla.

Prefijo	Adjudicación	RFC
2001:: /16	Asignaciones Sub-TLA	2450
	ARIN 2001:0400:: /29	
	RIPE NCC 2001:0600:: /29	
	APNIC 2001:0200:: /29	
2002:: /16	6to4	3056
3FFE:: /16	6Bone para pruebas	2471

Tabla 3.2: Adjudicaciones TLA

Los grandes proveedores pueden consultar con su correspondiente registro regional acerca de la asignación de direcciones IPv6. Los registros regionales son ARIN, RIPE, y APNIC; para América, Europa, y Asia respectivamente.

Proveedores y puntos de intercambio usan el siguiente nivel de agregación "Next-Level Aggregation Identifier" (NLA). Estos proveedores de acceso a la red son generalmente públicos, y son los que promoverán la estructura del espacio de direcciones asignado por los TLA con la optimización en la topologia de rutas como una prioridad. Después de identificador NLA se puede disponer de los bits a la derecha para dar servicio a otros sitios, lo cual es representado por "Site ID". En este nivel es posible crear más de un nivel de agregación NLA para optimizar el enrutamiento:

[3.10] En la especificación inicial, el TLA fue un identificador basado en proveedor. Este fue asignado a la "American Registry for Internet Numbers" (ARIN) en Norte América, RIPE en Europa, y "Asia Pacific Network Information Center" (APNIC) en Asia. Con el cambio en la especificación, el motivo comercial de los TLA ha sido desplazado por la optimización del enrutamiento.

Figura 3.4

En este nivel es posible crear más de un nivel de agregación NLA, esto es, las organizaciones que reciben un NLA ID pueden utilizar la parte del Site ID para crear más NLA's de acuerdo a sus necesidades.

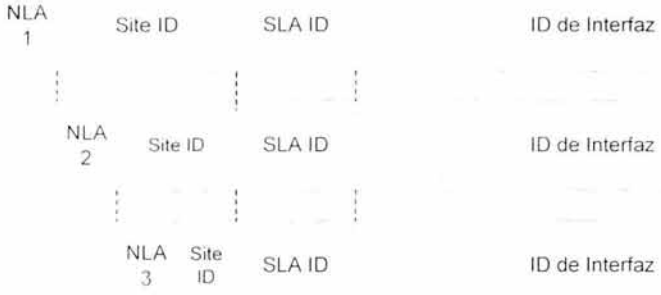


Figura 3.5

El identificador de agregación de nivel de sitio "Site-Level Aggregation Identifier" (SLA) es el espacio de direcciones asignado a organizaciones para que puedan crear su jerarquía de direccionamiento local. Es análogo al concepto de subredes en IPV4 excepto que cada organización tiene un número mayor de subredes. El número de subredes soportadas en este formato debería ser suficiente, salvo para organizaciones muy grandes. Las organizaciones que necesiten subredes adicionales pueden solicitar otros identificadores SLA.

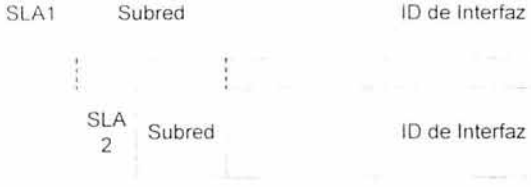


Figura 3.6

La última parte de las direcciones unicast es usado por el identificador de 64 bits de la interfaz.

3.1.9 Direcciones especiales

Hay algunas direcciones especiales que es necesario discutir. La primera parte del espacio de direcciones IPv6 con el prefijo de **0000 0000** esta reservado. Fuera de este prefijo, se han definido las siguientes direcciones especiales:

Dirección no especificada

Las dirección no especificada tiene un valor de **0:0:0:0:0:0:0:0**, por lo que también se conoce como dirección todo-ceros. Es comparable con **0.0.0.0** en IPv4. Indica la ausencia de una dirección válida, y puede, por ejemplo, ser usada como una dirección origen por un host en el proceso de arranque cuando envía peticiones al exterior para conseguir una dirección válida. Esta dirección puede representarse por **::** . Nunca debe ser asignada estática o dinámicamente a una interfaz, y no debe aparecer como una dirección IP destino o dentro de un encabezado de enrutamiento IPv6.

Dirección de loopback

La dirección de loopback es útil para probar la pila IP, ya que puede ser usada para enviar un paquete a la pila del protocolo sin enviarla a la subred. Se representa por **0:0:0:0:0:0:0:1**, o en forma abreviada **::1**. Nunca debe configurarse estática o dinámicamente a una interfaz.

En los siguientes párrafos se describen tres tipos de direcciones que se han especificado para ser usadas por los mecanismos de transición. Estas son utilizadas para crear interfaces virtuales llamadas pseudo-interfaces.

3.1.9.1 Direcciones IPv6 con direcciones IPv4 insertadas

Como la transición a IPv6 será gradual, hay dos tipos de direcciones que se han definido para ser compatibles con IPv4[3.11].

Dirección IPv6 compatible con IPv4

Este tipo de dirección se usa para hacer túneles con paquetes IPv6 dinámicamente sobre una infraestructura IPv4. Los nodos IPv6 que usan esta técnica emplean una dirección unicast IPv6 especial que lleva una dirección IPv4 en los 32 bits de menor orden.

[3.11] Las direcciones IPv6 con direcciones IPv4 insertadas son descritas en el RFC 2373.

Dirección IPv6 mapeada con IPv4

Este tipo de dirección se utiliza para representar las direcciones de nodos que solo tienen el protocolo IPv4. Esta dirección puede ser usada por un nodo IPv6 para enviar un paquete a un nodo que funciona con el protocolo IPv4 únicamente. La dirección IPv6 lleva la dirección IPv4 en los 32 bits de menor orden.

Figura 3.7: Formato de direcciones IPv6 con direcciones IPv4 insertadas

La diferencia entre estos dos tipos de direcciones es el formato: cuando los 16 bits antes de la dirección IPv4 son ceros, se trata de una dirección IPv6 compatible con IPv4; si los bits son unos, entonces se trata de una dirección IPv6 mapeada con IPv4.

3.1.9.2 Direcciones 6to4

IANA ha asignado permanentemente un identificador TLA de 13 bits para operaciones 6to4 dentro del rango de las direcciones unicast globales agregables. 6to4 es uno de los mecanismos definidos que permiten a los hosts y redes IPv6 comunicarse sobre una infraestructura IPv4[3.12]. El formato de la dirección es mostrado en la figura 3.8.

El prefijo tiene una longitud total de 48 bits. La dirección IPv4 en el prefijo debe ser una dirección IPv4 pública en notación hexadecimal. Por ejemplo la dirección 6to4 de **62.2.84.115** es **2002:3E02:5473:: /48**. Por medio de esta interfaz, todos los hosts IPv6 en este enlace pueden transmitir paquetes por túnel sobre una infraestructura IPv4.

[12] 6to4 es descrito a detalle en el capítulo de mecanismos de transición y en el RFC 3056

3 bits	13 bits	32 bits	16 bits	64 bits
FP 001	TLA 0x0002	Dirección IPv4 (hex)	SLA ID	ID de Interfaz

Longitud de prefijo: 48 bits (/48)

Figura 3.8: Formato de la dirección 6to4

3.1.10 Direcciones Anycast

Las direcciones anycast están en el mismo rango que las unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, todos los nodos a los que dicha dirección ha sido asignada, deben estar configurados para que reconozcan que se trata de una dirección anycast. Hasta no conseguir más experiencia en el manejo de las direcciones unicast, se tiene las siguientes restricciones[3.13]:

- La dirección anycast no debe ser usada como la dirección origen de un paquete IPv6.
- La dirección anycast no debe ser asignada a un host IPv6. Solo puede ser asignada a un router IPv6.

Un uso esperado de las direcciones anycast es para identificar un conjunto de routers que den acceso a la red IPv6[3.14]. Otra posibilidad es configurar con una dirección anycast específica a todos los routers dentro de una red corporativa que proporciona acceso a Internet.

Existe una dirección anycast, requerida para cada subred, que se denomina "Dirección anycast del router de subred"[3.15]. El formato de esta dirección consiste en un prefijo que especifica la subred y un identificador que es puesto todo en ceros. Un paquete enviado a esta dirección será entregado a uno de los routers de la subred.

Con esta característica se pretende dar tolerancia a fallos. También puede tener una aplicación importante en la movilidad, esto es, cuando un nodo necesite comunicarse con un router entre el conjunto de los disponibles en su subred.

Prefijo de Subred longitud = n bits	Longitud = 128 - n bits 0000 0000 ...

Figura 3.9: Formato de direcciones anycast del router de subred

[3.13] Las direcciones anycast y sus restricciones están definidas en el RFC 2373. En el apendice hay más información acerca de este tipo de direcciones

[3.14] Una función esperada de dirección anycast es la "6to4 Relay", la cual esta especificada en el RFC 3068

[3.15] La "Dirección anycast del router de subred" está definida en el RFC 2373

3.1.11 Direcciones Multicast

Una dirección multicast es un identificador para un grupo de nodos. Este tipo de dirección se distingue por el byte de mayor orden FF, o 1111 1111 en notación binaria. El formato de las direcciones multicast se muestra en la figura 3.10.

El primer byte identifica a la dirección como multicast. Los siguientes 4 bits son para banderas, las cuales se definen como sigue: los primeros tres bits del campo de bandera deben ser cero; ellos están reservados para uso futuro. El último bit del campo de banderas indica si esta dirección es una de las bien conocidas direcciones multicast asignadas por IANA, o es una dirección multicast temporal. Un valor cero del último bit define a una como dirección bien conocida; un valor de uno indica una dirección temporal. El campo de ámbito o alcance es usado para limitar el alcance de las direcciones multicast. Los posibles valores se listan en la tabla 3.3.

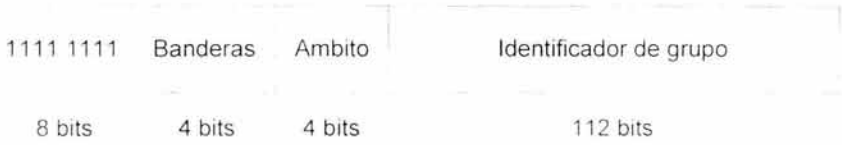


Figura 3.10: Formato de direcciones multicast

Banderas: *bit 0 – 3* *Reservado, deben ser ceros*
bit 4 *0 = se trata de una bien conocida dirección multicast*
1 = se trata de una dirección multicast temporal

Ámbito: *Revisar la tabla 3.3 para ver los valores.*

Valor	Descripción
0	Reservado
1	Ámbito de interfaz local
2	Ámbito de enlace local
3, 4	No asignado
5	Ámbito de sitio local
6, 7	No asignado
8	Ámbito de organización local
9, A, B, C, D	No asignado
E	Ámbito global
F	Reservado

Tabla 3.3: Valores del campo de ámbito

El identificador de grupo se refiere al grupo multicast, ya sea permanente o temporal, dentro de un determinado ámbito.

Los últimos 112 bits de la dirección portan el identificador ID del grupo multicast[3.16]

3.1.12 Direcciones requeridas

El estándar especifica que cada host debe tener las siguientes direcciones para identificarse en la red:

- Una dirección de enlace local por cada interfaz.
- Una o más direcciones unicast.
- La dirección de loopback.
- La dirección multicast a todos los nodos.
- Dirección multicast de nodo solicitado por cada una de sus direcciones unicast y anycast. Esta dirección se usa en el proceso de detección de direcciones duplicadas.
- Direcciones multicast de todos los demás grupos a los cuales pertenece el host.

Un router necesita todo lo anterior además de lo siguiente:

- La dirección anycast del router de subred para las interfaces en las cuales esta habilitado como tal.
- Todas las direcciones anycast con las que el router ha sido configurado.
- Las direcciones multicast para todos los routers.
- Direcciones multicast de todos los otros grupos a los que pertenece el router.

3.2 Direccionamiento en Red UNAM

Actualmente en la UNAM se tiene un modelo de red jerárquica y redundante, el cual nos permite un diseño de red en niveles:

- Core: proporciona transporte óptimo entre sitios.
- Distribución: proporciona conectividad de acuerdo a políticas de acceso.
- Acceso: proporciona acceso a usuarios o grupos de trabajo a la red.

El nivel de Core es la parte de backbone de la red que tiene conmutación de alta velocidad, que es crucial para permitir la comunicación dentro del Sistema Autónomo. Este nivel debe de tener las siguientes características:

[3.16] El RFC 2375 define la asignación inicial de direcciones multicast de manera permanente. En el apéndice se puede consultar la lista que define los valores de las "Bien conocidas direcciones multicast".

- Ofrecer alta confiabilidad.
- Proporcionar redundancia.
- Proporcionar tolerancia a fallos.
- Adaptarse a los cambios rápidamente.
- Ofrecer baja latencia y buena operación.
- Evitar la lenta manipulación de paquetes causada por filtros u otros procesos.
- Diámetro consistente y limitado (El número de saltos de router de extremo a extremo, es llamado diámetro).

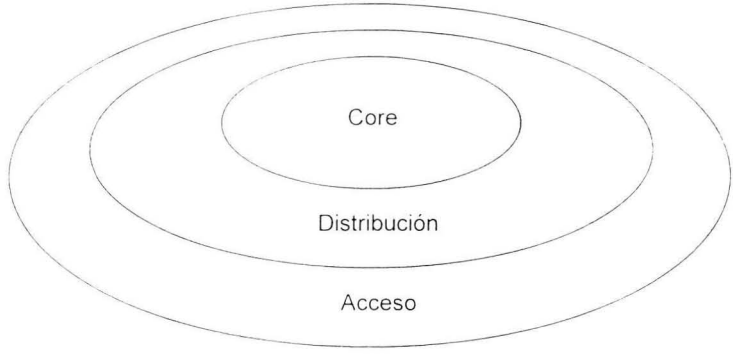


Figura 3.11

El nivel de Distribución de la red es un punto delimitador entre los niveles de acceso y de Core de la red. Este nivel puede tener muchos roles, incluyendo la implementación de las siguientes funciones:

- Políticas (por ejemplo, asegurar que el tráfico enviado de una red particular debe de ser enviado por cierta interfaz, mientras que todo el demás trafico sea enviado por otra interfaz).
- Seguridad.
- Agregación de dirección o área.
- Acceso a departamentos o grupos de trabajo.
- Definición de dominios de broadcast/multicast.
- Enrutamiento entre VLAN's.
- Translación de medios (por ejemplo entre Ethernet y Token Ring).
- Redistribución entre dominios de enrutamiento (por ejemplo entre dos diferentes protocolos de enrutamiento).
- Delimitación entre protocolos de enrutamiento estático y dinámico.

El nivel de Acceso es la conexión al segmento de red local. Este nivel esta caracterizado por una LAN de medio compartido o segmentado por switches. La micro-segmentación, usada por los switches de LAN proporciona gran ancho de banda a los grupos de trabajo.

3.2.1 Objetivos de direccionamiento en Red UNAM

Las políticas que rigen, según los últimos acuerdos de los Registros Regionales de Internet (RIR's), proponen tres partes lógicas para la arquitectura jerárquica de direcciones unicast IPv6[3.17]:

La Red Pública

Comprende los 48 bits de la izquierda. Esta parte la adjudican los Registros Regionales, los Registros Locales, o los Proveedores de Servicios de Internet, éstos últimos bajo la autoridad de los primeros.

La Red de Sitio

Los 16 bits que siguen después de los 48 primeros identifican a la subred. En esta parte se tiene el esquema de direccionamiento local para las organizaciones.

La Interfaz

Los 64 bits de más a la derecha corresponden al identificador de interfaz.

Las direcciones unicast IPv6 desempeñarán progresivamente la función que actualmente tienen las direcciones IPv4. En la Red UNAM se asignarán direcciones de este tipo para producción. Los otros tipos de direcciones complementarán la operación eficiente de las de tipo unicast.

La Universidad Nacional Autónoma de México actualmente dispone de un bloque de direcciones IPv6 unicast globales agregables para producción, el cual fue adjudicado por ARIN. La dirección de la red es **2001:0448:: /32** del tipo TLA. Hay otro bloque de direcciones adicional para la red IPv6 de pruebas, sin embargo el análisis lo haremos solo para el bloque de producción.

Dentro del plan de direccionamiento IPv6 en la Red UNAM se tienen dos objetivos:

Objetivo General de Direccionamiento

Proponer un esquema de direccionamiento IPv6 jerárquico en Red UNAM para tener tablas de enrutamiento pequeñas, lo que implica un enrutamiento más eficiente, ya que la toma de decisiones en equipos de capa 3 es más rápida.

Objetivo Particular Direccionamiento

Proponer un esquema de direccionamiento IPv6 para backbone, dependencias internas, escuelas y facultades que actualmente están bajo administración de Red UNAM.

[3.17] La administración del espacio de direcciones IPv6 es según los acuerdos de los registros regionales de Internet. Documentación al respecto se puede encontrar en los sitios web de los mismos.

3.2.2 IPv6 jerárquico

El Core de Internet trabaja con protocolos de enrutamiento exterior, generalmente BGP, entre sistemas autónomos. A partir del Core de Internet en IPv6 se derivan las redes Sub-TLA, NLA's, SLA's y equipos finales. La UNAM se integra a la red IPv6 con su red de producción **2001:448:: /32** como Sub-TLA. Esta condición puede variar en el futuro, principalmente en la adjudicación de más espacio de direccionamiento IPv6.

Dada la dirección de red de producción de la UNAM se tiene una versión modificada del formato de dirección unicast original. Una de las características de IPv6 es poder modificar la longitud de los campos en la dirección unicast IPv6. Esto se realiza en base a las necesidades de la red. La tendencia es ir reduciendo el prefijo TLA y aumentar los campos sTLA y NLA para que los proveedores de servicios puedan manipular el espacio de direcciones y crear esquemas jerárquicos que hagan más eficiente el enrutamiento.

De acuerdo a la arquitectura jerárquica de direcciones en IPv6, existen tres partes lógicas en una dirección: la porción pública, la de sitio y la correspondiente a las interfaces. La primera comprende los primeros 48 bits (TLA, NLA), es decir un /48. La segunda corresponde al sitio local y utiliza los siguientes 16 bits: del /48 al /64. Finalmente los últimos 64 bits son dedicados a las interfaces.

Las tres partes lógicas mencionadas en al párrafo anterior tendrán su campo de acción en la implementación de las redes. Para ello nos referiremos a ellas como "Topología Pública", "Topología de Sitio", e "Interfaces" respectivamente. Con "Topología", en este caso, nos referimos a la estructura lógica de la red.

El espacio de direcciones IPv6 permite tener subdivisiones o subredes (como en IPv4) en cada una de estas topologías. Se pueden crear más NLA's o SLA's con el objeto de optimizar el enrutamiento y la administración de la red.

Por lo tanto, con las topologías, y las subdivisiones en cada una estas, se tiene un modo de operación jerárquico en los equipos de capa 3. Con esta forma de operar, switches de capa 3 y routers, adoptaran los protocolos de enrutamiento más indicados para la ubicación que tengan dentro de las topologías. En la parte pública los routers trabajarán con el protocolo BGP para IPv6, mientras que en la porción de sitio se podrá rutear con protocolos de carácter interior: OSPF y RIP para IPv6. Se puede tomar parte del campo de topología pública para incrementar la estructura interna de la red si se trata del mismo Sistema Autónomo. Por el momento se recomienda respetar los campos de las topologías públicas y de sitio como tales hasta no adquirir más experiencia en el manejo de IPv6.

Los protocolos de enrutamiento junto con las rutas estáticas conservan características de IPv4 pero con las extensiones necesarias para aprovechar las características de IPv6.

Ahora pasaremos a la revisión del objetivo general. Para ello analizaremos las topologías pública y de sito.

3.2.3 Prefijo de Red UNAM

De los primeros 16 bits (2001), 3 pertenecen al prefijo que identifica al tipo de dirección unicast (010), y 13 identifican a la parte TLA como parte del troncal de Internet. Los siguientes 13 bits los ha adjudicado IANA para los Registros Regionales, para el caso del Registro de América (ARIN) el prefijo completo es **2001:0400 /29**. Por su parte ARIN ha adjudicado el prefijo **2001:0448:: /32** para la UNAM.

Después de los primeros 32 bits, la Red UNAM dispone de 96 bits. En el siguiente bloque de 16 bits a la derecha se puede crear el siguiente nivel de agregación, por ejemplo NLA1. Este nivel será utilizado por los ISP's más grandes, como otros sistemas autónomos que reciban una adjudicación de direcciones por parte de la UNAM. Si este es el caso, la conexión será por BGP, ya que este es el protocolo para sistemas autónomos. Para crear este nivel de inicio solo utilizarán 8 bits (/40), lo que da como máximo 256 entradas en las tablas de enrutamiento. Como ya mencionamos la longitud de este bloque y las entradas en las tablas de enrutamiento pueden variar en el futuro:

- Hacia la izquierda: al disminuir el tamaño del prefijo TLA, esto es pasar de /32 a /28 por ejemplo. En caso de que esto suceda, se pueden crear mas niveles de agregación para mantener las tablas de enrutamiento pequeñas.

- Hacia la izquierda: al tomar parte del siguiente nivel de agregación (NLA2) que abarca hasta los 48 bits, es decir, integrar y manipular la parte entre /40 y /48 para satisfacer alguna necesidad de diseño futura.

En este nivel de agregación habrá otros ISP's que deseen utilizar el prefijo de la Red UNAM con IPv6. En este caso, los proveedores lo podrán hacer como sistemas autónomos y por conexión BGP.

Dentro de este nivel se pueden reservar 2 ó más prefijos para darle redundancia lógica y física a la Red de Backbone y dependencias internas, que es nuestro objetivo particular.

Con 2 o más prefijos se puede aprovechar otra de las características de IPv6: asignación de múltiples direcciones a cada interfaz. Con esto, cada equipo puede salir a red por diferentes equipos de capa 3. En el futuro, se puede hacer más eficiente el flujo de información en la red, ya que con diferentes opciones de salida a Internet, habrá posibilidad de balancear carga, dar redundancia y rutas más seguras.

Lo anterior forma parte del "Multi-homig", esto es, cada sitio de la Red UNAM puede salir a Internet por varias rutas. Estas pueden ser parte de la Red UNAM o de otro proveedor.

Los sitios multi-homing tendrán 2 o más prefijos de red para igual número de proveedores de nivel superior que tengan. El problema de cada sitio multi-homig para decidir que proveedor de nivel superior elegir, en determinado momento, dependerá de sus propias necesidades.

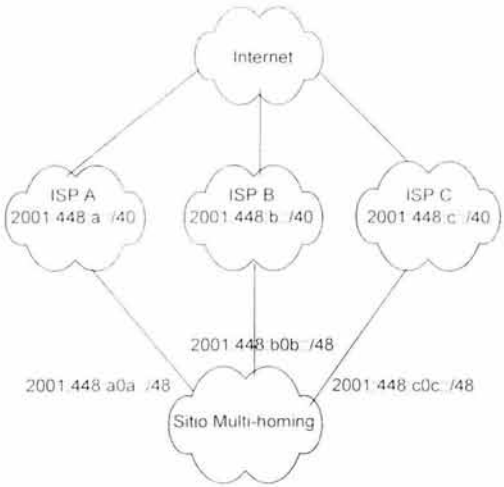


Figura 3.12. Sitios Multi-homing

La combinación del direccionamiento jerárquico, junto con los "Intercambiadores" es lo que harán el enrutamiento más eficiente. Se pueden reservar algunos prefijos para intercambiadores dentro de Red UNAM. Su trabajo será cambiar entre proveedores de Internet, sean de la UNAM o no, para sus clientes sin necesidad de renumeración. Con este mecanismo los sitios multi-homing no requieren tener prefijos para cada uno de sus proveedores, ya que los intercambiadores serán los encargados de cambiar los prefijos según sea necesario. Este es un tema que requiere de discusión para definir políticas y métodos de intercambio. Por ahora nos concentraremos en el direccionamiento jerárquico.

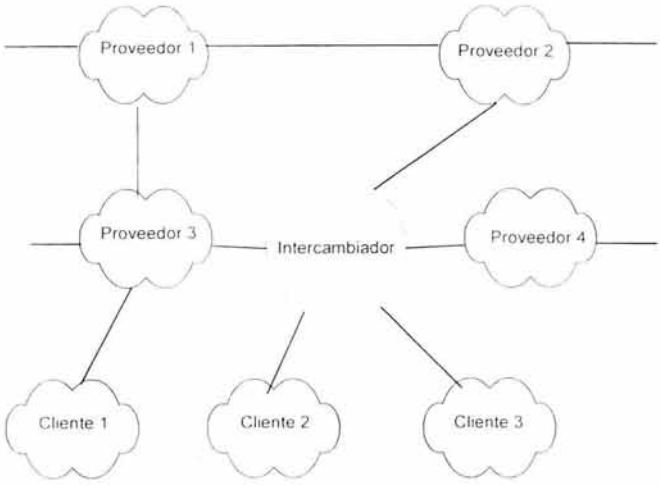


Figura 3.13. Intercambiadores

Para cumplir con el objetivo particular de direccionamiento en Red UNAM hay que reservar uno o más prefijos /40 para las redes de backbone y de dependencias en el campus principal. A este conjunto lo llamaremos simplemente "Backbone de Red UNAM". Esta es la red principal de la Universidad Nacional Autónoma de México. Los prefijos de red propuestos para este fin son:

2001:0448:01:: /40	**Prefijo NLA1 Principal del Backbone de Red UNAM**
2001:0448:02:: /40	**Prefijo NLA1 Secundario del Backbone de Red UNAM**

Es posible adjudicar más prefijos para el Backbone y Dependencias de Red UNAM. Con ello aprovecharemos las opciones de rutas más seguras, balanceo de carga y redundancia que se mencionaron anteriormente.

Dentro de los primeros 40 bits el protocolo de enrutamiento será preferentemente BGP, con carácter de exterior (EBGP).

Dentro de la región NLA, pero ahora en los siguientes 8 bits después del prefijo /40 es donde tendrán más proveedores de menor extensión.

Para la Red UNAM de backbone es posible reservar espacio para operar en futuro con el protocolo OSPF para IPv6 (OSPFv3), aunque por el momento se hará con BGP4+ de acuerdo a la función pública de la región NLA. Los prefijos propuestos en este nivel son:

2001:0448:0101:: /48	**Prefijo NLA2 Principal del Backbone de Red UNAM**
2001:0448:0102:: /48	**Prefijo NLA2 Secundario del Backbone de Red UNAM**

Se puede ver que es posible adjudicar más prefijos secundarios para dar alternativas al Backbone de Red UNAM en lo que se refiere a seguridad, balanceo y redundancia. En los prefijos anteriores solo se uso el prefijo principal de la región NLA 1, pero se puede hacer lo mismo para el prefijo secundario.

Dentro de la región NLA2, en cada prefijo, se tendrá un máximo de 256 entradas en las tablas de enrutamiento de los equipos que operan en capa 3.

Los prefijos destinados a ser secundarios del principal **2001:0448:01:: /40** para el Backbone de Red UNAM serán utilizados de acuerdo a los criterios de operación de los administradores de la Red UNAM. Por ejemplo, si se quiere balancear carga, el tráfico de información debido a los equipos de jerarquía inferior, será desviado a los equipos de jerarquía superior con prefijo secundario. Otro caso sería que los equipos de jerarquía superior con prefijo **2001:0448:01:: /40** dejaran de dar servicio por falla, entonces el tráfico de los equipos de jerarquía inferior sería desviado al equipo con el prefijo **2001:0448:02:: /40** ó a otros secundarios como **2001:0448:03:: /40**, etc.

Después de este análisis, ya hablamos de la región NLA, que representa otra perspectiva en Red UNAM, ya que habrá un nuevo troncal en esta Red. El Backbone de Red UNAM que hemos mencionado, y que actualmente se encuentra en operación en el campus de la UNAM, será un Backbone Local de Red UNAM.

De acuerdo a lo anterior, la región NLA podemos ubicarla, en buena parte por su posible extensión geográfica, dentro de una red de área metropolitana, o incluso, en una red de área amplia. Ahora podemos analizar el objetivo particular del direccionamiento de Red UNAM: el "Backbone de Red UNAM".

3.2.4 Backbone de Red UNAM

Después de destinar un prefijo principal y otros secundarios para el Backbone Local de Red UNAM, podemos iniciar el análisis del direccionamiento en esta Red.

Iniciando con el prefijo principal para la red de Backbone **2001:0448:0101: /48,** de forma similar y con las consideraciones descritas anteriormente, los prefijos secundarios pueden dar servicio a esta red. Considerándolo de esta forma, los prefijos quedarían como sigue:

2001:0448:0101: /48	**Prefijo Principal del Backbone de Red UNAM**
2001:0448:0102: /48	**Prefijo Secundario del Backbone de Red UNAM**
2001:0448:0201: /48	**Prefijo Secundario del Backbone de Red UNAM**
2001:0448:0202: /48	**Prefijo Secundario del Backbone de Red UNAM**

Con esto podemos darle posibilidades de "Red multi-homing" y una gran flexibilidad a la Red UNAM.

Sin embargo, es necesario dar la estructura interna de esta red. Tenemos que ubicar las direcciones para las dependencias, facultades, escuelas e institutos que actualmente poseen una infraestructura de red.

Además, debemos ver que en el futuro las dependencias seguramente tendrán un crecimiento interno de acuerdo al progreso tecnológico. Muchos dispositivos novedosos serán accesibles y controlados por red. Con esta consideración, queremos reservar un espacio de direcciones para que las escuelas, dependencias, facultades, centros de investigación e institutos tengan la posibilidad de crear su propia infraestructura de red. Cada una de ellas será la responsable de la operación interna de sus redes locales de acuerdo a sus necesidades.

Después del prefijo NLA **2001:0448:0101: /48** se tiene la topología de sitio, es decir, de forma local. En este nivel se pretende continuar con la optimización del enrutamiento, por lo que se puede jerarquizar al tomar 8 bits de los 16 disponibles antes de llegar al identificador de interfaz, con esto tendremos un máximo de 256 rutas posibles dentro de un nivel SLA1 (nivel de agregación de sitio uno).

En este punto es conveniente mencionar que la Red UNAM actual bajo el protocolo IPv4 tiene dos direcciones de red clase B, es decir, dos bloques de 16 bits para subredes y hosts.

Considerando lo anterior se tiene que reservar espacio de direcciones de red para cuando todas las dependencias que existen y las nuevas operen sus redes con IPv6. Con esto queda la posibilidad de crear más subredes o niveles de agregación de sitio: SLA2, SLA3, etc. En esta propuesta de direccionamiento del Backbone Local de Red UNAM mostraremos para el prefijo principal, asumiendo una estructura similar en los prefijos secundarios:

2001:0448:0101:: /48	**Prefijo Principal del Backbone de Red UNAM**
2001:0448:0101:0100:: /64	**Prefijo Principal de Equipos de Backbone de Red UNAM**
2001:0448:0101:0200:: /64	**Prefijo Secundario de Equipos de Backbone de Red UNAM**
2001:0448:0101:0300:: /64	**Prefijo de la Primera Dependencia, Escuela o Facultad de Red UNAM**
.	
.	
.	
2001:0448:0101:MN00:: /64	**Prefijo de la MN-esima Dependencia, Escuela o Facultad de Red UNAM**
2001:0448:0101:FF00:: /64	**Último Prefijo para esta Red UNAM**

Con estos prefijos dejamos 8 bits de reserva representados por los dos últimos ceros de los prefijos anteriores. Estos bits están destinados para cada dependencia, instituto, escuela o facultad. Aunque inicialmente se les dará un prefijo **/64**, si justifican el uso de más direcciones de red se les puede entregar más bits, por ejemplo, un prefijo **/60**, o incluso **/56**. Con estos prefijos o direcciones de red, cada dependencia puede crear una infraestructura de red local. 4 bits les permite a las dependencias crear hasta 16 subredes, y con 8, hasta 256. Si aún así, no se satisfacen las necesidades de alguna dependencia, entonces se le asignará un prefijo de nivel de agregación superior: por ejemplo un /48.

Para este nivel de sitio se deja la posibilidad de operar con el protocolo de enrutamiento OSPF para IPv6, dado que su funcionamiento es jerárquico.

Finalmente se tiene la parte final del direccionamiento IPv6 en el Backbone Local de Red UNAM: las interfaces de los equipos. El direccionamiento en las interfaces de los equipos de escuelas, facultades y dependencias dependerá de la administración de red local en cada caso.

Los equipos del Backbone Local de la Red UNAM recibirán un prefijo **2001:0448:0101:0100:: /64**, por lo que las direcciones para la administración de los equipos de acuerdo al grado de importancia puede ser el siguiente:

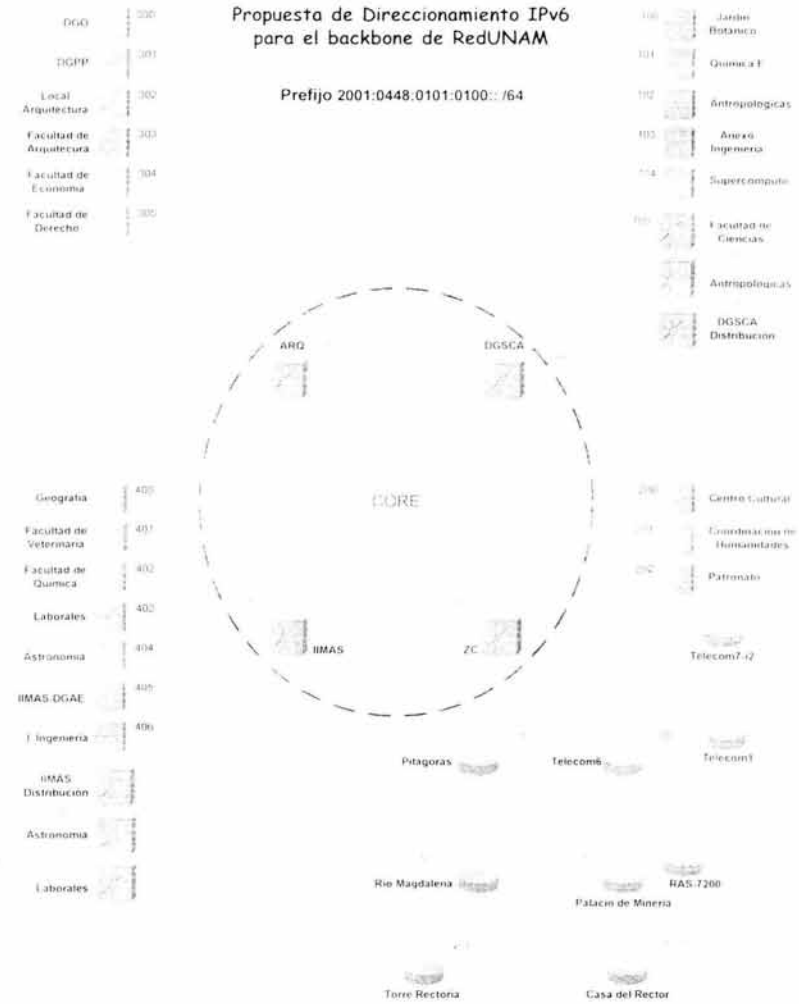
2001:0448:0101:0100:: /64	**Prefijo Principal de los Equipos de Backbone de Red UNAM**

A partir de este prefijo se tiene el direccionamiento en los equipos de backbone, quedando 8 bits de reserva representados por los dos últimos ceros.

2001:0448:0101:0100::1	**Primer Equipo de "Core" de Backbone de Red UNAM**
2001:0448:0101:0100::2	**Segundo Equipo de "Core" de Backbone de Red UNAM**
.	
.	
.	
2001:0448:0101:0100::n	**n-esimo Equipo de "Core" de Backbone de Red UNAM**
2001:0448:0101:0100::n+1	**Primer Equipo de Distribución de Backbone de Red UNAM**
2001:0448:0101:0100::n+2	**Segundo Equipo de Distribución de Backbone de Red UNAM**
.	
.	
.	
2001:0448:0101:0100::n+m	**m-esimo Equipo de Distribución de Backbone de Red UNAM**

Los últimos 64 bits, por lo tanto, serán destinados para la configuración de las interfaces de los equipos. "n" y "m" son números hexadecimales.

En la siguiente sección describiremos la operación de los equipos de capa 3 en IPv6. Principalmente abordaremos las extensiones que se hicieron en los protocolos de enrutamiento para IPv4, ya que la parte fundamental de los mismos aún se conserva.


Propuesta de Direccionamiento IPv6
para el backbone de RedUNAM
Prefijo 2001:0448:0101:0100:: /64
DGO
DGPP
Local Arquitectura
Facultad de Arquitecura
Facultad de Economia
Facultad de Derecho
Jardin Botanico
Quimica I
Antropologicas
Anexo Ingenieria
Supercomputo
Facultad de Ciencias
Antropologicas
DGSCA Distribucion
ARQ
DGSCA
CORE
IIMAS
ZC
Geografia
Facultad de Veterinaria
Facultad de Quimica
Laborales
Astronomia
IIMAS-DGAE
I. Ingenieria
IIMAS Distribución
Astronomia
Laborales
Centro Cultural
Coordinacion de Humanidades
Patronato
Telecom7-/2
Telecom1
Pitagoras
Telecom6
Rio Magdalena
RAS-7200
Palacio de Mineria
Torre Rectoria
Casa del Rector

3.3 Protocolos de enrutamiento en IPv6

Enviar un paquete IPv6 fuera del medio local requiere un dispositivo de capa 3. Los routers ven la dirección IPv6 destino que se encuentra en paquete y buscan una correspondencia con un prefijo de su tabla de enrutamiento (la tabla de enrutamiento es una lista de los destinos IPv6). Una vez que el router ha encontrado correspondencia con un destino, el paquete es enviado de acuerdo a la información asociada al siguiente salto en la tabla de enrutamiento. Si no se encuentra correspondencia, el paquete es desechado, por lo que es muy importante que el router tenga los destinos relevantes en su tabla de enrutamiento. Esta tabla puede ser creada manualmente en todos los routers, pero esto no es muy práctico. Los protocolos de enrutamiento o de enrutamiento definen procedimientos de intercambio para sincronizar las tablas de rutas entre los routers en forma dinámica. Además la información de enrutamiento requiere ser distribuida dentro de un sistema autónomo (AS) o entre sistemas autónomos. Un sistema autónomo se define como un conjunto de redes bajo una administración común. Los protocolos de enrutamiento que distribuyen información dentro de un sistema autónomo se denominan "Interior Gateway Protocols" (IGP), mientras que los que distribuyen información entre sistemas autónomos se denominan "Exterior Gateway Protocolos" (EGP). RIPng, OSPF para IPv6 pertenecen a la primera categoria; BGP4 y su extensión para IPv6 entran en la segunda. En esta sección veremos estos protocolos.

3.4 RIPng

RIPng es un protocolo de enrutamiento basado en el algoritmo vector distancia, o también conocido como algoritmo Bellman-Ford[3.18].

3.4.1 Algoritmo Vector Distancia en RIPng

Cada router tiene una lista de las mejores rutas para cada destino IPv6. La siguiente es un ejemplo de una tabla de enrutamiento:

```
Prefix                                                  Protocol    Next Hop
                                                                    Interface
-------------------------------------------------------------------------------
FEC0::0008:0000 /112                                    DIRECT      3
RIPv6       Metric:     3,    Prefix on a directly attached link
Last Updated 3865 seconds ago

FEC0::0005:0000:0000:0000:0000 /64                      RIPv6       1
RIPv6       Metric:     2,    Nexthop:    FE80::0280:2DFF:FE41:C90B
Last Updated 10 seconds ago
```

Por cada ruta, el router guarda las siguientes entradas en su tabla de enrutamiento:

[3.18] La mayoria de los conceptos de RIPng han sido tomados de RIPv1 y RIPv2. Para detalles del algoritmo vector distancia podemos consultar los RFCs 1058 (RIPv1) y 2453 (RIPv3). RIPng esta definido en el RFC 2080.

IPv6 route

El prefijo IPv6 y la longitud del prefijo de la dirección destino.

Dirección del siguiente salto (next hop address)

La dirección IPv6 del primer router, generalmente de enlace local, en la ruta hacia la red destino IPv6. Si el destino esta directamente conectado al router no se necesita esta dirección.

Interfaz del siguiente salto (next hop interface)

La interfaz física usada para alcanzar el siguiente salto.

Métrica

Un número que indica la distancia total hacia el destino. En RIP, la métrica consiste en el número de saltos hacia el destino. Los routers directamente conectados generalmente tienen una métrica de cero. RIPng anuncia las redes directamente conectadas con la métrica del enlace, normalmente 1.

Temporizador (Timer)

El tiempo transcurrido desde la última actualización.

Bandera de cambio de ruta

Es una bandera que indica que la información acerca de una ruta ha cambiado recientemente. Es necesaria para controlar las actualizaciones de enrutamiento.

Origen de la ruta (Route source)

Indica la entidad que proporcionó el conocimiento de una ruta, la cuál puede ser una entrada estática, estar directamente conectada, u originada por algún protocolo de enrutamiento.

El router distribuye información periódicamente acerca de las rutas que conoce a sus vecinos directamente conectados usando mensajes de actualización RIPng. Al recibir los mensajes de actualización de su vecino, el router agrega la distancia entre el vecino y el mismo a la métrica de cada ruta recibida. Esta distancia generalmente es uno. Después el router procesa la ruta recibida usando el algoritmo Bellman-Ford.

Un router A recibe una actualización de enrutamiento de un router B y agrega la distancia de 1 a cada ruta r_i anunciada por B. Para cada ruta r_i el router ejecuta el algoritmo Bellman-Ford. La tabla de enrutamiento será actualizada si los siguientes criterios son verdaderos, en caso contrario la ruta r_i será descartada:

La ruta r_i es nueva y la métrica es alcanzable.

La ruta, métrica, y el siguiente salto son agregados como una nueva entrada en la tabla de enrutamiento. El temporizador es puesto en cero, y la bandera de cambio es activada.

La ruta r_i ya es conocida y el siguiente salto es el mismo que uno que esta en la tabla de enrutamiento.

Si la métrica ha cambiado, entonces es actualizada y es activada la bandera de cambio. El temporizador es reposicionado a cero en cualquier caso.

La ruta r_i ya es conocida, pero el siguiente salto es diferente y la métrica es más pequeña que la entrada en la tabla de enrutamiento.

La métrica y el siguiente salto son actualizados. El temporizador es puesto en cero y es activada la bandera de cambio.

La ruta r_i ya es conocida, pero el salto siguiente es diferente y la métrica es igual a una de la tabla de enrutamiento.

Si el proceso de enrutamiento permite múltiples rutas de costos similares al mismo destino en la tabla de enrutamiento, la ruta destino es tratada como una nueva entrada. Si el proceso no permite múltiples rutas de costo equivalente, la ruta r_i es descartada. Múltiples rutas de costo equivalente permiten compartir carga de tráfico IPv6.

El siguiente salto de r_i es tomado de la información que viene en los mensajes de actualización de enrutamiento o de la dirección IPv6 origen del paquete RIPng.

Cuando los routers son inicializados por primera vez, solo conocen las redes directamente conectadas. Esta información es pasada a todos los vecinos, procesada, y luego distribuida a los vecinos de los vecinos. Eventualmente, todas las redes IPv6 son conocidas por todos los routers. Los routers continúan enviando mensajes de actualización periódicamente para prevenir la expiración de rutas válidas.

3.4.2 Limitaciones del protocolo

RIPng, como las versiones anteriores de RIP, esta diseñado para actuar como IGP dentro de una pequeña red. Las principales limitaciones son:

El campo de acción de RIPng es limitado.

La ruta más larga a un destino IPv6 esta limitada por la métrica de 15. Generalmente la métrica es igual al número de saltos, asumiendo un costo de 1 por cada enlace cruzado.

Los loops de enrutamiento causan elevados tiempos de convergencia.

Cuando rutas IPv6 no válidas son propagadas hasta formar loops, RIPng depende de "La cuenta al infinito" para eliminar esas rutas.

La métrica no refleja la velocidad del enlace

RIPng usa una métrica fija normalmente puesta en 1 por cada enlace que cruza. Una ruta no puede ser escogida por su ancho de banda, o parámetros de tiempo real como el retardo, la carga o la confiabilidad.

3.4.3 Cambios en la topología

Los cambios en la topología se deben a la aparición de una nueva ruta o a la caída de alguna. Cuando hay una nueva ruta hacia una red, esta es anunciada en el siguiente mensaje de actualización del router que esta conectado directamente a dicha red. Los vecinos procesan la nueva ruta y la anuncian a más vecinos. Después de la convergencia, todos los routers saben de la nueva ruta. El tiempo de convergencia es aquel que toma a todos los routers de la red aprender algún cambio en la topología de la red. Lo importante de este parámetro es saber si su duración es aceptable para la operación de la red. Para reducir el tiempo de convergencia al mínimo y evitar loops de enrutamiento es necesario utilizar los mecanismos descritos en el capítulo 2 (Split Horizon y Poison Reverse).

3.4.4 Formato de los mensajes

RIPng es un protocolo basado en UDP y su puerto bien conocido es el 521, el "Puerto RIPng". El proceso de enrutamiento RIPng siempre "escucha" mensajes que llegan a este puerto. Con excepción de peticiones específicas, todos los mensajes RIPng ponen a este puerto como origen y destino.

Los campos del mensaje RIPng son:

Command

El valor de 1 indica un mensaje que pide a un receptor que envíe toda o parte de su tabla de enrutamiento.

Un valor de 2 envía un mensaje de actualización que contiene toda o parte de la tabla de enrutamiento del emisor. El mensaje puede ser una respuesta a una solicitud previa o una actualización periódica no solicitada.

Versión

Este campo es puesto en 1.

Entrada a la Tabla de Enrutamiento (RTE) (20 bytes cada una)

La cabecera RIPng es seguida por una o más RTE's, usando el formato de la figura 3.15.

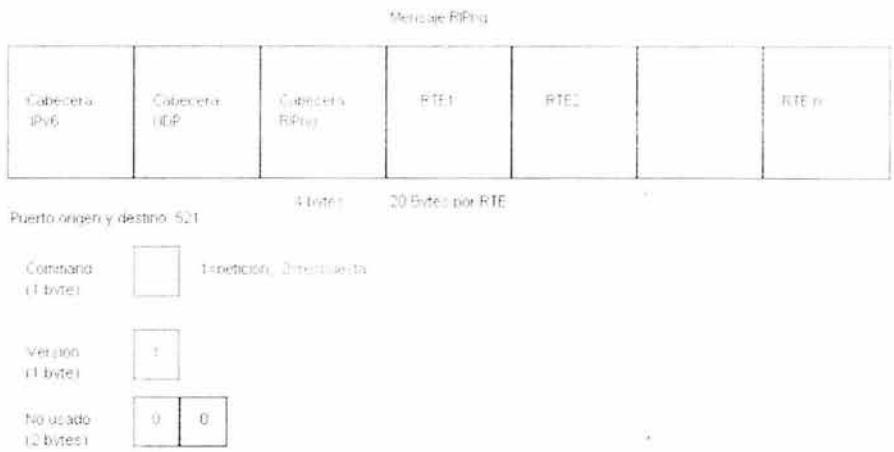


Figura 3.14 Formato de los mensajes RIPng

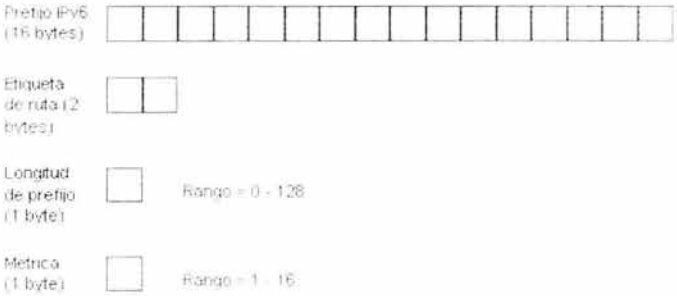


Figura 3.15: Formato de una Entrada de Tabla de Enrutamiento

Cada RTE describe la ruta que será anunciada usando el prefijo IPv6 y la longitud de su prefijo. El campo de métrica contiene la métrica usada por el emisor para esta ruta. Una métrica válida tiene un valor entre 1 y 15. Una métrica de 16 indica una ruta inalcanzable.

Cada RTE contiene un campo de etiqueta de la ruta, el cual puede ser usado para agregar información adicional acerca de una ruta aprendida por otro protocolo de enrutamiento, por ejemplo BGP. Un router que importa rutas externas dentro de RIPng, puede usar esta etiqueta. RIPng conservará y distribuirá esta etiqueta dentro de su dominio de rutas. La información contenida en esta etiqueta puede servir para redistribuir una ruta fuera del dominio RIP.

El número de RTE's en los mensajes depende de la MTU del medio entre dos routers vecinos. La relación es la siguiente:

Número de RTE's = (MTU – longitud de cabeceras IPv6 – longitud de cabecera UDP – longitud de cabecera RIPng) / tamaño de la RTE

3.4.5 Consideraciones de direccionamiento y de ruta por defecto

El prefijo 0:0:0:0:0:0:0:0 con longitud cero es usado como ruta por defecto. Una ruta por defecto es usada si la ruta a un destino no esta listada en la tabla de enrutamiento. El router del siguiente salto en la ruta por defecto es denominado "Default router". Al enviar tráfico al default router se asume que éste conoce todas las rutas o el mismo tiene una ruta por defecto. Este mecanismo generalmente es usado para enviar tráfico hacia fuera de un sistema autónomo, o de sitios remotos a uno central. La ventaja de introducir una ruta por defecto es disminuir el número de actualizaciones de enrutamiento que son distribuidas en la red. Una métrica es asignada a la ruta por defecto en su origen para establecer precedencia entre múltiples default routers. RIPng maneja una ruta por defecto de la misma forma que otros destinos.

3.4.5.1 Temporizadores

RIPng implementa diversos temporizadores para controlar las actualizaciones de la información de enrutamiento. El nombre y propósito de ellos es el siguiente:

Temporizador de Actualización

Por defecto, cada 30 segundos el proceso RIPng envía anuncios no solicitados a sus routers vecinos. Estos anuncios contienen la tabla de enrutamiento completa excepto rutas que siguen la regla del horizonte dividido.

Temporizador Timeout

Cada vez que una ruta es actualizada, el temporizador timeout es puesto en cero. Si la entrada de una ruta alcanza cierto tiempo (180 segundos por defecto), sin otra actualización, se considera que ha expirado. La métrica se pone en 16 y el proceso hold-down comienza. Además se activa la bandera de actualización de la ruta para indicar el cambio. El proceso de salida usa esta bandera para mandar una actualización.

Temporizador Hold-down

Este temporizador es puesto a 120 segundos para cada entrada de ruta que ha cumplido con el temporizador timeout, o ha sido recibida con una métrica de 16. Solo hasta la culminación de este temporizador la entrada de una ruta será removida de la tabla de enrutamiento. Si una nueva actualización de esta ruta llega antes de que el temporizador hold-down termine, la ruta es repuesta y el temporizador hold-down es limpiado.

3.4.6 Procesamiento de paquetes

Veamos como el router procesa la entrada y salida de paquetes RIPng.

3.4.6.1 Mensaje de petición

Un mensaje de petición pide al router una respuesta con toda o parte de su tabla de enrutamiento. La petición es procesada como sigue.

Si hay exactamente una RTE con un prefijo cero, un prefijo de longitud cero, y una métrica de 16, la petición es por la tabla de enrutamiento completa; entonces el router responde enviando su tabla de enrutamiento.

De otro modo, el mensaje de petición es procesado con un RTE a la vez. Si el prefijo de la RTE se encuentra en la tabla de enrutamiento, la métrica del RTE es puesta dentro del campo de métrica de la RTE; una métrica de 16 es puesta dentro del campo de métrica, indicando que la ruta es desconocida. Una vez que todas las RTEs han sido procesadas, el campo "command" en la cabecera RIPng es cambiado para responder y el mensaje de respuesta formado es enviado a aquel que hizo la petición.

Hay dos tipos de mensajes de petición, generales y específicos, los cuales son manejados de forma diferente por el router receptor.

Una petición general es enviada por un router que ha empezado a funcionar y quiere llenar su tabla de enrutamiento rápidamente. El router envía un mensaje de petición general, pidiendo a todos los vecinos directamente conectados que envíen su tabla de enrutamiento completa. Cada vecino responde con un mensaje de respuesta que contiene su tabla de enrutamiento completa y usando la regla del horizonte dividido.

Un mensaje de petición específico es enviado por una estación de monitoreo preguntando por toda o parte de la tabla de enrutamiento. El router consultado responde enviando la información requerida de su tabla de enrutamiento. La técnica del horizonte dividido no es usada por que se asume que el que pide la información la usa solo con propósitos de diagnóstico.

3.4.6.2 Mensaje de respuesta

Un mensaje de respuesta lleva información de enrutamiento que es procesada por el router receptor usando el algoritmo Bellman-Ford. Un mensaje de respuesta es aceptado por un router solo si la dirección origen IPv6 es una dirección de enlace local de un vecino directamente conectado y los puertos origen y destino utilizan el puerto UDP dedicado a RIPng. Además el contador de saltos debe ponerse en 255 para garantizar que la respuesta no ha viajado sobre un nodo intermedio.

Una vez que el mensaje de respuesta es aceptado, cada RTE debe ser verificado. La verificación incluye su prefijo, que no sea una dirección de enlace local o multicast, la longitud del prefijo, y la métrica. Si la RTE es aceptada, la métrica de la interfaz entrante es agregada a la métrica del RTE. Después la RTE pasa por el proceso Bellman-Ford.

Las reglas de anteriores para validar un mensaje de respuesta no aplican para una consulta específica. La cuenta de saltos puede ser menor que 255, y la dirección origen IPv6 puede no ser de enlace local. Una estación de diagnóstico puede usar la RTE recibida solo para probar software y no para enrutamiento.

Hay dos tipos de mensaje de respuesta: el solicitado y el no solicitado. Este último es enviado periódicamente por un proceso de actualización. El proceso de actualización periódico examina la tabla de enrutamiento entera cuando expira el temporizador de actualización en alguna interfaz. El proceso de actualización comienza tan pronto se activa la bandera de cambio en la ruta, y examina solo las rutas que tienen la bandera activada. Ambos procesos siguen con lo siguiente: si la entrada de la ruta examinada tiene una dirección de enlace local o no debe ser usada por causa del horizonte dividido, entonces lo ignora. De otro modo, pone el prefijo, la longitud del prefijo, y la métrica dentro de la RTE, y pone la RTE dentro del mensaje de respuesta. Si se alcanza el máximo tamaño de la MTU, envía el paquete y construye uno nuevo.

Enviar un mensaje no solicitado a la dirección multicast **FF02::9** garantiza que el mensaje de respuesta alcance a todos los vecinos en una red directamente conectada.

3.5 OSPF para IPv6

OSPF para IPv6 (OSPFv3) modifica el existente OSPF para IPv4 para soportar IPv6. Los fundamentos de OSPF para IPv4 permanecen sin cambios. Algunos cambios han sido necesarios para acomodar el incremento del tamaño de la dirección en IPv6 y los cambios de la semántica en el protocolo entre IPv4 e IPv6.

3.5.1 Revisión de OSPF para IPv6

3.5.1.1 Diferencias entre OSPF para IPv4 y OSPF para IPv6

La mayoría de los conceptos de OSPF para IPv4 han sido conservados; lo siguiente es un breve vistazo de los cambios:

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, inclusive si no comparten una subred IP en común. OSPF para IPv6 funciona por enlace en vez de por subred. Los términos "Red (Network)" y "Subred (Subnet)" usados en OSPF para IPv4 pueden ser remplazados con el termino "Enlace (Link)"; por ejemplo, una interfaz OSPF ahora conecta a un enlace en vez de a una subred IP.

Traslado de la semántica del direccionamiento.

> Las direcciones IPv6 ya no son presentadas en los encabezados de los paquetes de OSPF. Estas son solo presentadas como información de carga útil. Los Router-LSA y Network-LSA no contienen direcciones IPv6. Router ID, area ID y Link State ID permanecen con 32 bits, así que estas ya no pueden tomar el valor de una dirección IPv6. Designated Routers (DR's) y Backup Designated Routers (BDR's) ahora son siempre identificados por su Router ID y ya no por su dirección IP.

Campos de inundación.

Cada tipo de LSA contiene un código para especificar su campo de inundación. Este código es fijado en el campo del tipo de LS. Tres campos de inundación han sido introducidos: link-local, area y AS.

Soporte explícito para múltiples casos por enlace.

Múltiples ejemplos del protocolo OSPF pueden ahora funcionar sobre un mismo enlace, esto permite a AS's separados, cada uno corriendo un proceso OSPF, usar un enlace en común. Otro uso de esta característica es que un solo enlace pertenezca a varias areas.

Uso de direcciones link-local.

OSPF asume que a cada interfaz le ha sido asignada una dirección de tipo unicast link-local. Todos los paquetes usan la dirección como dirección origen. Los routers aprenden la dirección link-local de todos sus vecinos y usan esta dirección como dirección del siguiente salto. Los paquetes enviados en un enlace virtual, sin embargo, deben usar ambas, la dirección IP global o la site-local como el origen para los paquetes OSPF.

Autenticación

La autenticación ha sido eliminada de OSPF para IPv6, dado que se confía en la autenticación de OSPF.

Cambio en el formato LSA.

Tipo 3 (Summary Link) ha sido renombrado como Inter-area-Prefix-LSA. Tipo 4 (AS Summary Link) ha sido renombrado como Inter-area-Router-LSA. Dos nuevos LSA's llevan prefijos de información IPv6 en su carga útil. Link-LSA (Tipo 8) lleva información de la dirección IPv6 de los enlaces locales, e Inter-area-Prefix-LSA (Tipo 9) lleva información de los prefijos IPv6 del router y enlaces de red.

Manejo de LSA's de tipo desconocido.

En lugar de simplemente descartarlos, OSPF introduce una forma flexible para el manejo de LSA's de tipo desconocido. Un nuevo bit manejable ha sido agregado al campo LS Type para permitir el inundamiento de LSA's de tipo desconocido.

Soporte para Areas Stub.

El concepto de areas stub se ha conservado den la versión de OSPF para IPv6, una regla adicional especifica el inundamiento de LSA's desconocidos dentro del area stub.

3.5.1.2 Protocolos basados en estado de enlace

Cada router mantiene una base de datos describiendo los estados de los enlaces dentro del sistema autónomo(AS). Esta base de datos esta siendo construida con el intercambio de los LSA's (Anuncios de estado de enlace - Link State Advertisement) entre routers vecinos. Dependiendo de su contenido, un LSA es inundado a todos los routers en el sistema autónomo (campo de inundamiento AS ó AS flooding scope), a todos los routers dentro de la misma area (campo de inundamiento de area o area flooding scope), o simplemente a sus vecinos. El flooding siempre ocurre a lo largo del camino de los routers, de esta manera una amistad entre vecinos es extremadamente importante para OSPF para trabajar con propiedad. La amistad entre vecinos es llamada adyacencia.

Cada router origina LSA's anunciando el estado local de sus interfaces a todos los routers dentro de la misma área. También los LSA's son originados para identificar enlaces con múltiples Routers (redes multi-acceso), las rutas de IPv6 de otras areas, o las rutas IPv6 externas a el sistema autónomo. Cada router coloca los LSA's recibidos en su base de datos LSA, llamada LSDB (Link-State Database).

Usando la LSDB como entrada, cada router ejecuta el mismo algoritmo para construir el árbol con el camino de menor costo (SPF tree) para cada router. La LSDB es como tener un mapa de la red usado para graficar el camino mas corto a cada destino. El costo es descrito como una métrica adimensional, que es configurable en cada interfaz del router. La métrica asociada a la interfaz es usualmente inversamente proporcional al ancho de banda del enlace, esto es, que a mayor ancho de banda menor costo. Una formula muy común, de acuerdo al RFC, es dividir 10^8 entre el ancho de banda del enlace en bits por segundo (bps), sin embargo se pueden modificar esta métrica con respecto a nuestras necesidades.

OSPF puede poner múltiples caminos de igual costo a la ruta en la tabla de enrutamiento, el algoritmo para la distribución del trafico de esos caminos queda a en manos del propio proceso de enrutamiento, normalmente basado en la dirección IPv6 origen y destino.

3.5.1.3 Áreas OSPF y rutas externas

La LSDB puede hacerse un poco grande y esto puede hacer intensivo el uso de CPU y la memoria, dado que los cambios en la base de datos afectan a todos los routers dentro del AS. OSPF permite que el AS sea dividido en áreas, para reducir el procesamiento, también OSPF puede importar rutas derivadas de fuentes externas al proceso de OSPF, como por ejemplo rutas estáticas o inclusive otros protocolos de enrutamiento como RIP o BGP.

3.5.1.4 Autenticación y seguridad

Dado que OSPFv3 corre bajo IPv6, este confía en la autenticación IP de la cabecera y el encapsulamiento de seguridad IP de la carga útil o datos para asegurar la integridad y autenticación de los intercambios de enrutamiento. La autenticación de OSPFv2 ha sido removida, solo una verificación de la integridad ha sido conservada, que vienen en la forma del checksum, que es calculada a todo el paquete OSPF.

3.5.2 Áreas de OSPF y rutas externas

Dentro del sistema autónomo, los routers pueden ser agrupados para formar areas, a cada area le es asignado un único Area ID, que es un entero de 32 bits, tipicamente es escrito como 4 números decimales separados por puntos, este no tiene significado de direccionamiento, solamente es para identificar el area. Un LSA con un campo de inundamiento de area, nunca será inundado fuera de esta. Juntos forman la estructura de datos del area, también conocida como el LSDB del area. Los Router-LSA y Network-LSA pertenecen a esta categoria. Routers y redes forman un area y son escondidos para otras areas. Esto es como dividir el mapa total de la red en múltiples mapas más pequeños, en los cuales cada una representa la topologia de su area. Cada router dentro de un area calcula el árbol SPF a todos los routers del area. Esos routers son llamados routers intra-area. Los routers que tienen todas sus interfaces perteneciendo a la misma area son llamados routers internos. Los routers de borde de area (ABR) proveen de rutas que se encuentran fuera del area a la que pertenecen. Cada area debe de ser agregada a una area en común llamada "Area de Backbone" o area 0. El ABR anuncia todas las rutas del area de backbone al area local a la que pertenece, de esta manera todas las rutas son distribuidas dentro del AS.

El enrutamiento dentro del AS toma lugar en 2 niveles, si la dirección IP origen y destino del paquete pertenecen a la misma área, el paquete será enviado a su destino solamente usando la información obtenida de la LSDB del área, este enrutamiento es llamado intra-area.

La ventaja de dividir el AS en área es la reducción en el uso del CPU y memoria en los routers, dado que la topologia de un área es mucha más pequeña que la del AS total, de esta manera el cálculo del árbol SPF lleva menos tiempo. Esto da como resultado que los cambios en la topologia afectan de manera local y solo los routers de la misma area necesitan recalcular el árbol SPF, los routers en otras areas resultan menos afectados, dado que la topologia de su propia area no cambio y no necesitan recalcular el árbol SPF. Los routers internos son los más beneficiados en la división del AS en areas pues su LSDB es mucho más pequeña.

3.5.2.1 El área de backbone

El área de backbone es una area especial que usa el Área ID 0.0.0.0 (area 0), esta contiene a todos los ABR's del AS. Si el AS no esta dividido en areas, esta seria la única area configurada. Si el AS esta dividido en areas, el backbone será una colección de rutas provenientes de todas las demás areas. El area de backbone debe de ser contigua, esto es, que cada router dentro de la misma area 0 debe de tener por lo menos un enlace directo a otro router de la misma area, y este enlace debe pertenecer a el area 0. Sin embargo, con la introducción de los enlaces virtuales, el area de backbone no necesariamente debe de tener una contiguidad física. Un area de transito puede ser usada para crear un túnel (un enlace virtual) perteneciente al área 0.

3.5.2.2 Áreas

Las áreas reciben un único Área ID diferente de 0.0.0.0, estas deben ser físicamente contiguas. Cada area debe de tener un ABR conectado al area de backbone,

usando ya sea un enlace físico o un enlace virtual. Un ABR anuncia todas las rutas del area a la cual pertenece al area de backbone y al revés, el ABR anuncia todas las redes conocidas del area de backbone al area que pertenece. Normalmente el ABR usa un LSA (llamado Inter-Area-prefix-LSA) por cada ruta anunciada. El ABR puede ser configurado para sumarizar las rutas usando un prefijo corto IPv6, representando parte o la totalidad de las rutas anunciadas, esto reduce el número de anuncios y los requerimientos de memoria y procesador. Es muy importante el planeamiento de los prefijos IPv6 dentro del area para lograr los máximos beneficios de la sumarización. Un area puede tener múltiples ABR's.

3.5.2.3 Enlaces virtuales

Un enlace virtual (virtual link) es un enlace lógico que funciona de túnel para el trafico de backbone a través de un area, este puede ser configurado entre dos ABR's que usan un area en común llamada area de transito. Un enlace virtual pertenece a el backbone y puede cruzar solo un area de transito, el area de transito no debe de ser un area stub. Un area remota sin una interfaz física al area de backbone puede ser conectada a al area de backbone mediante el uso de enlaces virtuales. Los enlaces virtuales pueden ser usados también para crear conexiones redundantes al backbone. OSPF considera a un enlace virtual como un enlace punto a punto. El camino mas corto entre los ABR's a través del area de transito determina la dirección del túnel en el otro extremo, esa dirección debe ser global o una dirección unicast IPv6 del site local.

3.5.2.4 Rutas externas

Un router puede aprender rutas Ipv6 externas de diferentes fuentes, tales como rutas estáticas programadas por el administrador, protocolos de enrutamiento tanto internos como externos como RIP, BGP, etc. Todas las rutas provenientes de una fuente ajena a OSPF son consideradas a ser rutas externas a OSPF y pueden ser importadas al proceso. Para importar rutas externas al proceso de OSPF, un router debe de tener al menos una interfaz configurada con OSPF y aprender por lo menos una ruta por otro medio que no sea OSPF. Este tipo de routers son llamados ASBR (Autonomus System Border Router), las rutas externas son importadas por medio de un AS-External-LSA por cada ruta externa. Dependiendo de la implementación, un ASBR puede sumarizar un rango de rutas externas en un LSA externo.

Los AS-External-LSA's deben ser inundados a todo el AS, cualquier router dentro del AS reenviara los paquetes de las redes externas a el ASBR o a una dirección opcional de reenvío que apunte al ASBR, en consecuencia debe haber una entrada del ASBR en la Area-LSDB o la dirección de reenvío debe de estar en la tabla de enrutamiento local. Si el ASBR no esta dentro del área local, el ABR es responsable de anunciar la existencia del ASBR al área local, esto se hace usando un Inter-Area-Router-LSA.

Las métricas de las rutas externas no son compatibles con las métricas de OSPF. Los ASBR's anuncian rutas externas usando uno o dos tipos de métricas, external-1 y external-2. Las rutas external-1 son consideradas a estar cerca del ASBR. Las rutas dentro del AS agregan el costo OSPF para alcanzar el ASBR o la dirección de reenvío a la métrica de la ruta external-1. Las rutas external-2 son consideradas a estar lejos del

ASBR, en consecuencia una métrica mayor que el costo de cualquier ruta intra-AS será agregada a la métrica de la ruta.

Si una misma ruta es anunciada en una ruta interna OSPF y también en una ruta externa, el camino a la ruta interna OSPF es siempre elegido. Esto puede pasar si existen varios ASBR's conectados a la misma red externa. Un ASBR anuncia una ruta OSPF al protocolo de enrutamiento y otro ASBR importa la misma ruta al proceso de OSPF.

3.5.3 Formato del mensaje OSPFv3

3.5.3.1 Encapsulamiento en paquetes IP

Los paquetes OSPF IPv6 son directamente encapsulados como lo especifica el protocolo numero 89, este número puede estar en el campo "Next Header" de la cabecera de encapsulamiento IPv6.

OSPF no usa fragmentación, de modo que confía plenamente en la fragmentación IP cuando envía paquetes mayores que el MTU. La fragmentación debe ser ignorada siempre que sea posible. Los paquetes potencialmente grandes como los paquetes DD (Database Description) o los paquetes LSU (Link State Update) pueden ser fácilmente divididos en varios paquetes por el propio proceso de OSPF.

Los mensajes OSPF normalmente usan la dirección IPv6 del link-local (de la interfaz por donde son enviados los datos) como su dirección origen, a excepción de los mensajes enviados en un enlace virtual. Estos usan direcciones link-local o unicast globales del enlace virtual como su origen. Dependiendo de la situación, los mensajes OSPF pueden ser enviados como un mensaje unicast (a un vecino en especifico) o multicast (a varios vecinos). Las siguientes direcciones han sido apartadas para este propósito:

AllSPFRouters (FF02::5)

> Todos los routers corriendo OSPF deben "escuchar" a esta dirección multicast. Los paquetes Hello son siempre enviados a esta dirección. Esta dirección es usada también por algunos paquetes durante el flooding.

AllDRouters (FF02::6)

> DR y BDR en un medio multiacceso deben "escuchar" a esta dirección. Esta dirección es usada por algunos paquetes durante el flooding.

Los paquetes OSPF enviados a la dirección multicast tienen un campo local y su límite de saltos se establece en 1. Este nunca será enviado en múltiples saltos.

3.5.3.2 Cabecera OSPF

Existen cinco diferentes tipos de paquetes usados en OSPF, todos los paquetes comienzan con una cabecera estándar de 16 bytes, como se muestra en el diagrama:

Figura 3.16. Cabecera del paquete OSPF para IPv6

En este caso nuestro interés esta dirigido al los tipos de paquetes, pero primero daremos una breve descripción de los demás campos.

Versión

La versión de OSPF, en este caso 3.

Packet length

Este es el tamaño del paquete OSPF en bytes, incluyendo la cabecera.

Router ID

Este es el Router ID del router que origino el paquete.

Area ID

Este es el Area ID de la interfaz que origino el paquete.

Checksum

OSPF usa el cálculo estándar del checksum para las aplicaciones IPv6.

Caso ID

Este identifica el caso OSPF a el cual pertenece el paquete.

Type

Este campo representa el tipo de mensajes del router.

Tipo de paquete	Nombre	Descripción
1	Hello	Inicializa y mantiene las adyacencias. Elige DR y BDR.
2	Database Description	Intercambia la descripción de la base de datos durante la formación de adyacencias.
3	Link State Request	Petición de LSA's anticuados o perdidos.
4	Link State Update	Intercambio de LSA's cada uno respondiendo a peticiones cuando se están formando las adyacencias o durante el flooding de LSA's.
5	Link State Acknowledgment	Acuses de recepción de un LSA. Todos los LSA's deben ser acusados de recibidos.

Tabla 3.4: Tipos de paquetes

3.5.3.3 Procesando los paquetes OSPF

Cuando un router envia un paquete del protocolo OSPF, este llena los campos de la cabecera como se ha descrito anteriormente. El Area ID y el Caso ID son tomados de la estructura de datos de la interfaz por la que salen los paquetes, si es requerida la autenticación, esta será responsabilidad de IPv6 para agregar las cabeceras necesarias.

Cuando un router recibe un paquete del protocolo OSPF, IPv6 lo valida primero comparando sus cabeceras (dirección IPv6, campos del protocolo y autenticación). Una vez hecho esto el paquete es dado al proceso de OSPF, OSPF checa la versión (que debe de ser 3), el checksum y el Area ID configurada en la interfaz de entrada. Si no hay una concordancia, pero el Area ID es 0, la interfaz de entrada debe ser el extremo de un enlace virtual. El Caso ID del paquete debe de coincidir con el Caso ID de la interfaz. Si la dirección IPv6 destino del paquete es la dirección multicast AllDRouters, el router debe de ser ya sea el DR o el BDR en este enlace. Si el paquete pasa por todo el proceso mencionado, este pasa al proceso de OSPF apropiado para un procesamiento más, de otra manera este debe ser ignorado.

En OSPFv3 se conservan sin alteraciones la formación de adyacencias, la elección de un DR y un BDR y el paquete Hello, estos han sido explicados a detalle para OSPFv2, por lo tanto no serán mencionados, pero cabe recordar que estos elementos son parte fundamental del protocolo OSPF. Parte fundamental es también la LSDB (Link State Database), por lo que será mencionada con mas profundidad que el la versión anteriormente mencionada.

3.5.4 La LSDB

La LSDB (Link State Database) es el componente más importante de OSPF. La LSDB es una estructura de datos que consiste en el intercambio de LSA's en el AS. La información del estado del enlace es estructurada para permitir la construcción de un árbol cuyas ramas y hojas representen el camino mas corto a todos los routers dentro del AS. Cada router construye un árbol desde su punto de vista, con él como la raiz. Mas comúnmente, el router usa el algoritmo desarrollado por Dijkstra para construir ese árbol de el camino mas corto (SPF tree). Primero el router construye el árbol de la intra-area para todos los destinos dentro del área. Inter-area y rutas externas son entonces agregadas a las ramas representando un ABR o un ASBR, al final cada ruta dentro del árbol es agregada a una de las cuatro secciones de la tabla de enrutamiento de OSPF: rutas intra-area, rutas inter-area, rutas external-1 o rutas external-2. El próximo salto es siempre a la dirección link-local del primer router en el camino mas corto para la ruta.

3.5.4.1 Contenido de la LSDB

El SPF es un sistema de direcciones gráficas usando vértices para construir un árbol[3.19]. Este básicamente describe la topología de la red como un conjunto de apuntadores construyendo un árbol. Existen cuatro apuntadores básicos dentro del árbol:

Router a Router

Describe una interfaz punto a punto del router identificando el Router ID del router vecino en un enlace punto a punto. En la terminología de la LSDB, este apunta de un Router-LSA a otro Router-LSA.

Router a enlace de transito

Describe la interfaz de un router a un enlace de transito mediante la identificación de la Interfaz ID del DR para su enlace de transito. En la terminología de la LSDB, este apunta de un Router-LSA a un Network-LSA.

Enlace de transito a routers

Describe un enlace de transito y apunta a todos sus routers agregados. En la terminología de la LSDB, este apunta de un Network-LSA a uno o muchos Router-LSA's.

[3.19] El RFC 2328 especifica el algoritmo SPF.

Informativo

Asocia información a su creador (por ejemplo, direcciones IPv6, prefijos IPv6, etc.), usando la terminología del árbol, esto es como agregar hojas a las ramas. Sin parecerse a los apuntadores previos, que construyen el árbol actual, este apuntador solo agrega información al árbol. Los LSA's pertenecientes a este tipo de apuntador son: Inter-Area-Prefix-LSA, Inter-Area-Router-LSA, AS-External-LSA, Type-7-LSA, Link-LSA e Intra-Area-Prefix-LSA.

3.5.4.2 LSA's

Cada LSA dentro de la LSDB incorpora uno o más de los apuntadores previamente mencionados, esto consiste en una cabecera LSA y un cuerpo LSA. La cabecera LSA identifica cada LSA únicamente.

3.5.4.3 Cabecera LSA

Cada LSA comienza con una cabecera en común de 20 bytes. La figura muestra a detalle esta cabecera. El estado de enlace (Link State (LS)), el LS ID y los anuncios del router (Advertising Router) juntos únicamente identifican el LSA.

Los campos de la cabecera LSA son detallados en la siguiente lista:

LS Age (2 bytes)

LS Age es el tiempo en segundos desde que el LSA fue originado, si este ha alcanzado el MaxAge (3600 segundos), el LSA ya no es considerado para el calculo del árbol SPF. El router que origino este LSA debe renovar el LSA e incrementar el numero de secuencia antes de que el MaxAge sea alcanzado para evitar que el LSA envejezca. Esto es recomendado para renovar un LSA después de MaxAge/2.

LS Type (2 bytes)

Este es el tipo de LSA anunciado. Los primeros tres bits del campo del tipo de LSA indican propiedades especiales del LSA.

- Bit U (manejo de tipo de LS desconocido)

  Identifica el manejo de los tipos de LSA desconocidos por los routers. Si el bit es puesto, el LSA debe ser guardado e inundado como si el tipo fuera entendido. De otra forma, si el bit es cero, el LSA tiene que ser tratado como si este tuviera un campo de inundamiento link-local.

- Bit S2 y S1 (campo de inundamiento)

  Define el campo de inundamiento del LSA. Los cuatro valores son:

- 00 = Link-local, inundamiento solo en el enlace en el cual fue originado.
- 01 = Area, inundamiento a todos los routers del área de donde fue originado.
- 10 = AS, inundamiento a todos los routers en el AS.
- 11 = Reservado.

Los últimos 13 bits representan el actual código de función del LSA. El tipo de LS es representado en hexadecimal para reflejar el campo de inundamiento.

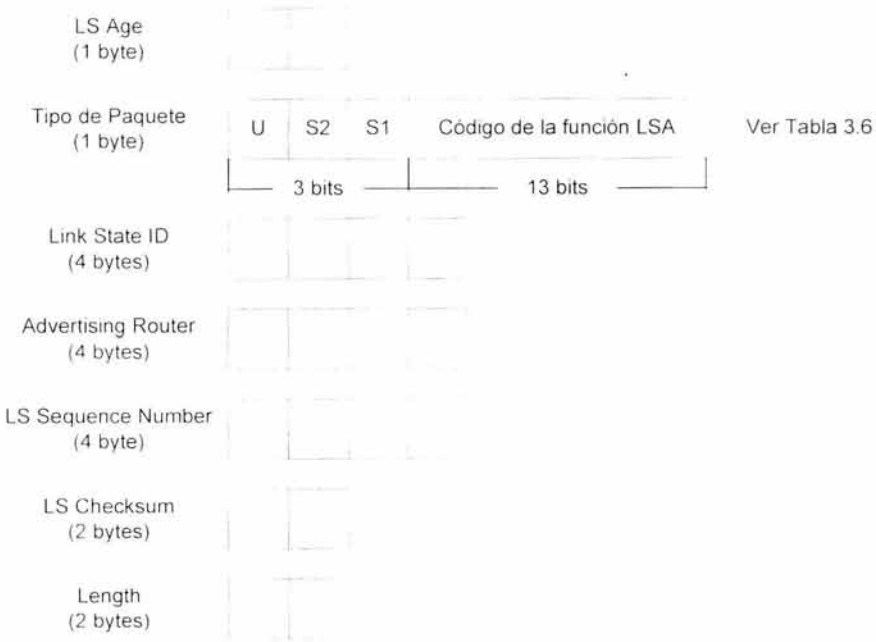


Figura 3.17: Cabecera LSA

La siguiente tabla muestra los nueve tipos de LSA's que existen:

Tipo LSA	Nombre	Campo de inundamiento
0x2001	Router-LSA	Area
0x2002	Network-LSA	Area
0x2003	Inter-Area-Prefix-LSA	Area
0x2004	Inter-Area-Router-LSA	Area
0x2005	AS-External-LSA	AS

0x2006	Group-Membership-LSA	Area
0x2007	Type-7-LSA	Area
0x2008	Link-LSA	Enlace
0x2009	Intra-Area-Prefix-LSA	Area

Tabla 3.5: Tipos de LSA's

Link State ID (4 bytes)

El Link State ID es la parte de la identificación del estado del enlace. Con el Router-LSA y el Network-LSA, el Link State ID sirve como un valor para un apuntador en el árbol para identificar ese router o esa red. Para todos los otros LSA, el router que lo origina usa un único ID localmente.

Advertising Router (4 bytes)

El Link State ID es el Router ID del router que origina el LSA.

LS Sequense Number (4 bytes)

El LS Sequense Number identifica el caso en el que se encuentra este LSA. Este es usado para determinar cual LSA es mas reciente en el caso de múltiples ocurrencias del mismo LSA. El LS Sequense Number mas alto es el mas reciente, este siempre comienza con el numero 0x80000000 y el máximo posible es 0x7FFFFFFF. Si este numero ha sido alcanzado el LSA es envejecido (LS Age es igual a MaxAge) e inundado, antes un nuevo caso de LSA (ahora usando 0x80000000) es publicado.

Checksum (2 bytes)

Este es el fichero checksum que contiene el LSA completo, incluyendo las cabeceras LSA pero excluyendo el campo LS Age.

Length (2 bytes)

Esta es la longitud completa del LSA en bytes.

A continuación se explican todos los tipos de LSA's, con la excepción de Group-Membership-LSA y Type-7-LSA[3.20].

3.5.4.4 "Router-LSA" (Type-0x2001)

Router links describe los enlaces punto a punto, virtuales o de transito del router. Básicamente, este incluye a todos los enlaces que tienen por lo menos un vecino. A diferencia de OSPF para Ipv4, los enlaces stub ya no son anunciados dentro del Router Link. Un ABR debe originar Router Links separados para cada área que tenga agregada,

[3.20] Los Group-Membership-LSA y Type-7-LSA están definidos en los RFC's 1584 y 1587 respectivamente, pero que aun no han sido actualizados para Ipv6

conteniendo solo enlaces pertenecientes a esa área en particular. Los enlaces virtuales siempre pertenecen a el área 0 son solo anunciados por el ABR.

Los campos del Router-LSA son mencionados a detalle a continuación:

Flags (1 byte)

El campo de Flags indica la función especial en este router.

Bit	Nombre
W bit	Este es una wildcard de multicast
V bit	Este es el extremo de un enlace virtual, usando esta área como área de transito
E bit	Este es un ASBR
B bit	Este es un ABR

Tabla 3.6

Options (3 bytes)

Este campo describe las opciones de las capacidades soportadas por este router.

Bit	Nombre	Descripción
0-17	No usados	Reservados para usos futuros
18	DC	Manejo de demanda de circuitos
19	E	Capacidades de ese router para External-routes. Todos los miembros de un area deben estar de acuerdo con la capacidad externa. En un area Stub, a todos los routers se les debe de poner en cero este bit para lograr una adyacencia, este bit es solo significativo para los paquetes Hello.
20	MC	Capacidad de multicast
21	N	A todos los routers dentro de un area NSSA se les debe de poner en uno este bit, además de que el E-bit debe de ser cero.
22	R	Indica que el router que origino el paquete Hello es un router activo. Si el bit es puesto en cero, el que lo origino no reenviara paquetes.
23	V6	Indica que ese router soporta OSPF para IPv6. Si es puesto en cero, este router o enlace podria ser excluido del cálculo de la tabla de enrutamiento.

Tabla 3.7

Link Entry (16 bytes por enlace)

En la siguiente tabla veremos los posibles tipos de enlaces y sus correspondientes campos. Cada enlace tiene una métrica asignada a este, basado en las caracteristicas de la interfaz. El Neighbor ID y el Router ID son aprendidos mediante el protocolo Hello. Las entradas de los enlaces son usadas como

apuntadores para construir el árbol intra-area. Los tipos de interfaz 1 y 4 apuntan al Router-LSA, especificado en el Neighbor Router ID (LS-ID y Advertised Router). Interfaz tipo 2 apunta a el Network-LSA como especificado en el "Neighbor Interface ID" (LS-ID) y "Neighbor Router ID" (Advertised Router).

Tipo de enlace	Nombre	Neighbor Interface ID	Neighbor Router ID
1	Punto a punto	Interfaz ID del vecino en el otro extremo del enlace punto a punto	Router ID del vecino en el otro extremo del enlace punto a punto
2	Transito	Interfaz ID del DR en ese enlace	Router ID del DR en ese enlace
3	Reservado		
4	Virtual	Interfaz ID del vecino en el otro extremo del enlace virtual	Router ID del vecino en el otro extremo del enlace virtual

Tabla 3.8

3.5.4.5 Network-LSA (Type 0x2002)

El router designado (DR) de cada enlace de transito en el área origina un Network-LSA. Al "Link State ID" le es puesto el "Interface ID" de la interfaz del DR al enlace de transito.

Este simplemente contiene el campo de opciones que fue mencionado anteriormente, seguido de una lista de Router ID's identificando a todos los routers agregados a ese particular enlace de transito. Este representa un apuntador a todos los routers agregados a ese enlace de transito.

3.5.4.6 Inter-Area-Prefix-LSA (Tipo 0x2003)

Los "Inter-Area-Prefix-LSA" son originados por el ABR para anunciar prefijos IPv6 de otras areas al area de este LSA. Un Inter-Area-Prefix-LSA separado es originado para cada ruta. Un ABR podria sumarizar un rango contiguo de prefijos IPv6 en un anuncio. Para un area Stub, el ABR anuncia la ruta por default usando este LSA. Inter-Area-Prefix-LSA es el equivalente al "Summary-LSA" de OSPF para IPv4.

En el proceso de la construcción del árbol, este LSA representa un apuntador informativo asociado con el ABR que agrega rutas al inter-area al árbol SPF. Los campos Inter-Area-Prefix-LSA son detallados como sigue:

Metric (20 bits)

Define el costo del ABR al prefijo anunciado de la dirección IPv6 con este Inter-Area-Prefix-LSA. Si esa ruta representa un resumen, la métrica podria ser tomada de la métrica más alta de los prefijos miembros.

IPv6 Prefix Representation (0 a 20 bytes, en múltiplos de cuatro)

Define el anuncio actual del prefijo IPv6. Este consiste de cuatro campos: la longitud del prefijo, las opciones del prefijo, un campo sin uso (puesto en cero) y el prefijo actual de la dirección IPv6. La longitud del prefijo define la longitud de la dirección del prefijo. La ruta por default es representada por un prefijo de longitud cero.

La siguiente tabla explica las opciones del campo prefix options, los prefijos de la dirección representan la dirección IPv6, si es necesario pueden ser puesta en cero la siguiente palabra de 32 bits.

Bit	Nombre	Descripción
0-3	Reservado	
4	Bit P	Bit de propagación, si es puesto, el NSSA ABR anunciará el prefijo al Backbone, este es solo usado en el Type-7-LSA
5	Bit MC	Bit de multicast, si esta puesto, el prefijo debe ser incluido en los cálculos de enrutamiento de multicast.
6	Bit LA	Bit de dirección local (Local Address), si esta puesto, el prefijo es actualmente una dirección local IPv6 del router que lo genera.
7	Bit UN	Bit No Unicast, si esta puesto, el prefijo debe de ser excluido de los cálculos unicast

Tabla 3.9

3.5.4.7 Inter-Area-Router-LSA (Tipo 0x2004)

Los "Inter-Area-Router-LSA's" son originados por los ABR's para anunciar ASBR's de otras áreas a esa área. Un Inter-Area-Router-LSA es originado por separado para cada ASBR, esto es necesario para informar a todos los routers en esa área de la existencia de un ASBR fuera de la misma. El Inter-Area-Router-LSA es el equivalente al AS-Summary-LSA para OSPFv2. El Inter-Area-Router-LSA contiene el campo de opciones (al cual ya nos referimos con detalle anteriormente), el campo de la métrica y el Router ID del ASBR. El campo de la métrica representa el costo del ABR al ASBR.

En el proceso de la construcción del árbol, este LSA representa un apuntador informativo asociado con el ABR que agrega un ASBR al árbol SPF.

3.5.4.8 AS-External-LSA (Tipo 0x4005)

Los "AS-External-LSA" son anunciados por los ASBR's para importar prefijos IPv6 Externos al área. Cada AS-External-LSA representa un prefijo IPv6 externo para OSPF (por ejemplo, los aprendidos mediante RIP, BGP, rutas estáticas, etc.). Estos son inundados a todo el AS y son de esta forma conocidos por todos los routers, excepto los routers en áreas Stub.

En el proceso de la construcción del árbol, este LSA representa un apuntador informativo asociado con el ABR que agrega rutas externas al árbol SPF.

3.5.4.9 Link-LSA (0x0008)

Los Link-LSA son generados por cada router, uno por cada enlace del router. Estos nunca son inundados más allá de este enlace. El Link State ID es puesto al Interface ID del enlace. El Link-LSA tiene tres propósitos:

- Este provee la dirección link-local del router a todos los otros routers agregados a este enlace.
- Este provee de una lista de prefijos IPv6 asociados con este enlace.
- Este provee de una lista de opciones usadas por el DR para este enlace.

En el proceso de la construcción del árbol, este LSA representa un apuntador informativo asociado con cada enlace o a un Router-LSA. Este agrega la dirección link-local del enlace al árbol SPF.

3.5.4.10 Intra-Area-Prefix-LSA (Tipo 0x2009)

Un router usa los Intra-Area-Prefix-LSA para anunciar uno o más prefijos IPv6 asociados con el router o un Network-LSA. Como OSPFv3 ha removido toda la semántica de direccionamiento de los Router-LSAs y los Network-LSAs, el Intra-Area-Prefix-LSA provee esta información. Cada prefijo anunciado es asociado con un Router-LSA o un Network-LSA.

En el proceso de la construcción del árbol, este LSA representa un apuntador informativo asociado con un router, que agrega prefijos IPv6 a sus interfaces locales del árbol SPF. Este puede ser también asociado con un enlace de transito, agregando sus prefijos IPv6 a el árbol SPF.

3.6 Extensiones BGP para IPv6

No hay una versión de BGP para IPv6. El soporte de IPv6 deriva de la capacidad de BGP-4 para intercambiar información con otros protocolos de capa de red además de IPv4[3.21]. En lo que sigue veremos la parte de IPv6 en BGP-4[3.22].

BGP-4 tiene solo tres partes de información que son especificas de IPv4:

- El NLRI en el mensaje UPDATE contiene un prefijo IPv4.

[3.21] Estas extensiones multiprotocolo de BGP-4 están definidas en el RFC 2858, el cual sustituye al RFC 2283. Este ultimo es mencionado por que es el documento base del RFC 2545, el cual define las extensiones IPv6 para BGP-4.
[3.22] El RFC 2545 define las extensiones IPv6 para BGP-4.

- El atributo de ruta NEXT_HOP en el mensaje UPDATE contiene una dirección IPv4.

- El identificador BGP esta en el mensaje OPEN y en el atributo AGGREGATOR.

Para hacer BGP-4 compatible con otros protocolos de red, debe ser agregado el NLRI multiprotocolo y su información del siguiente salto[3.23]. Para soportar más protocolos, BGP-4 agrega dos nuevos atributos para anunciar y retirar el multiprotocolo NRLI. El identificador BGP permanece sin cambios. Por lo tanto los routers BGP con extensiones para IPv6, aún necesitan una dirección IPv4 local. Para establecer una conexión BGP intercambiando prefijos IPv6, los routers peers necesitan anunciar el parámetro opcional de "Capacidad BGP" para indicar el soporte IPv6. Las conexiones BGP y la selección de ruta continúan sin cambios. Cada implementación necesita extender el RIB para introducir rutas IPv6. Las políticas necesitan tomar el NLRI IPv6 y la información del siguiente salto dentro de las consideraciones para la selección de la ruta.

Un mensaje UPDATE anunciando solo NLRI IPv6 pone el campo de longitud de ruta inaccesible en cero y no transporta NLRI IPv4. Todos los anuncios o retiros de rutas IPv6 son portados dentro del MP_REACH_NLRI y el MP_UNREACH_NLRI. El UPDATE debe llevar los atributos de ruta ORIGIN y AS_PATH; en conexiones IBGP; también debe llevar el LOCAL_PREF. El atributo NEXT_HOP no debería ser transportado. Si el mensaje UPDATE contiene el atributo NEXT_HOP, el peer receptor debe ignorarlo. Todos los demás atributos pueden ser portados y reconocidos.

Un mensaje UPDATE podría anunciar los NLRI IPv6 y NLRI IPv4 con los mismos atributos de ruta. En este caso todos los campos pueden ser usados. Para el NLRI IPv6, el atributo NEXT_HOP debería, sin embargo, ser ignorado. Los NLRI IPv4 e IPv6 están separados en el RIB correspondiente.

3.6.1 Atributo de ruta MP_REACH_NLRI

Este atributo opcional no transitivo permite al peer el intercambio de NLRI IPv6, con su dirección IPv6 de siguiente salto. El NLRI y el siguiente salto son entregados en un atributo como se ve en la figura.

[3.23] El RFC 2858 extiende BGP para soportar múltiples protocolos de la capa de red.

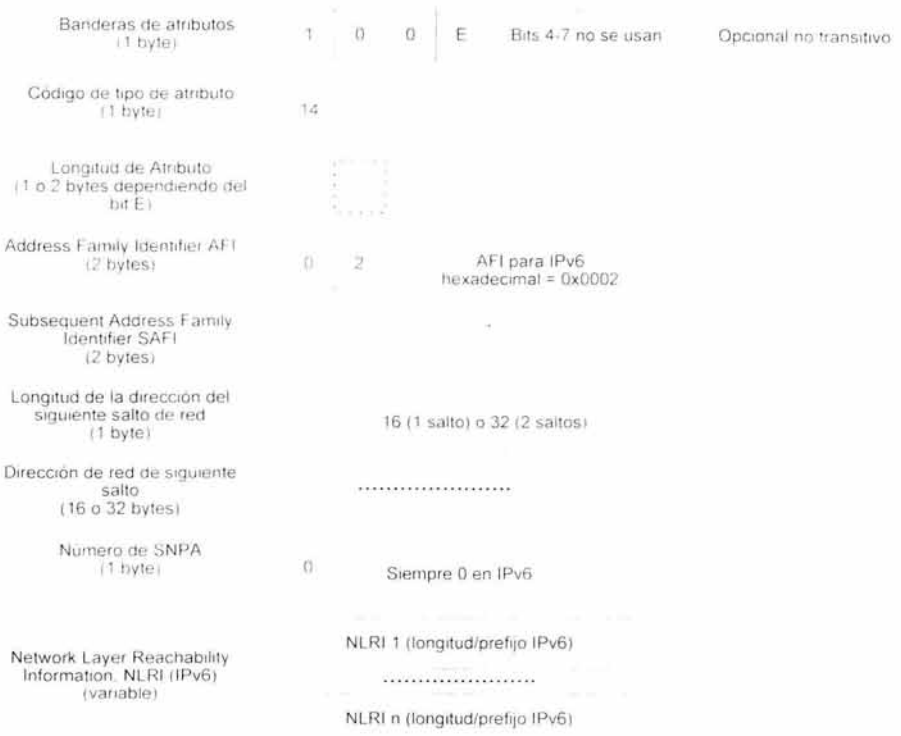


Figura 3.18: El atributo de ruta MP_REACH_NLRI para IPv6

Los campos del atributo de ruta MP_REACH_NLRI para IPv6 son los siguientes:

Address Family Identifier (AFI) (2 bytes)

Define el protocolo de capa de red. IPv6 usa el valor hexadecimal 0x0002[3.24]

Subsequent Address Family Identifier (SAFI) (1 byte)

Define si el protocolo utiliza envío unicast (SAFI=1), multicast (SAFI=2), o ambos (SAFI=3).

Longitud de la dirección del siguiente salto de red (1 byte)

Define el número de bytes usados para el campo "Dirección del siguiente salto". IPv6 pone este valor en 16 o 32 dependiendo de la dirección del siguiente salto proporcionada.

[3.24] El identificador AFI esta especificado en el RFC 1700.

Dirección de red del siguiente salto

Contiene la dirección IPv6 del siguiente salto de esta ruta IPv6. Este campo es actualizado cuando se anuncia esta ruta a un peer externo. El router elige su propia dirección IPv6-global/sitio-local del enlace al peer externo. Este campo generalmente no es actualizado cuando anuncia esta ruta a un peer interno. Si la dirección IPv6 del siguiente salto y la dirección IPv6 del peer comparten un enlace común, por ejemplo, un enlace entre dos peers externos, la dirección de enlace local del enlace compartido debe ser agregada como una segunda dirección del salto siguiente. En cambio, cuando se anuncia esta ruta a un peer interno, la dirección de enlace local recibida de un peer externo necesita ser removida.

Número de SNPA (1 byte)

Define el número "Subnetwork Points of Attachment" que sigue a la derecha después este campo. SNPA lleva información adicional del router asociado con la dirección del siguiente salto. IPv6 no usa este campo y lo pone en cero.

Network Layer Reachability Information (NLRI)

Una lista de NLRI IPv6 que son anunciados con este atributo. Cada NLRI es codificado como <longitud, prefijo>. El campo de longitud de 1 byte define la longitud del correspondiente campo "Prefijo". El campo Prefijo es llenado hasta completar el octeto con bits cero.

3.6.2 Atributo de ruta MP_UNREACH_NLRI

Este atributo opcional no transitivo permite al peer emisor retirar rutas que ya no son válidas IPv6. Como se ve en la figura, básicamente contiene una lista de prefijos IPv6 que el peer debería quitar de su RIB.

Figura 3.19: El atributo de ruta MP_UNREACH_NLRI para IPv6

Los campos del atributo de ruta MP_REACH_NLRI para IPv6 son los siguientes:

Address Family Identifier (AFI) (2 bytes)

Define el protocolo de capa de red. IPv6 usa el valor hexadecimal 0x0002.

Subsequent Address Family Identifier (SAFI) (1byte)

Define si el protocolo usa envio unicast (SAFI=1), envio multicast (SAFI=2) o ambos (SAFI=3).

Withdrawn routes

Una lista de NLRI IPv6 que son retiradas del servicio. Cada NLRI es codificada como <longitud, prefijo>. El campo de longitud de un byte define el tamaño del correspondiente campo "Prefijo". El campo de prefijo es aumentado hasta llenar el octeto con bits cero.

CAPÍTULO 4

MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6

4.1 Introducción

IPv6 e IPv4 coexistirán por muchos años. Se ha definido un amplio rango de técnicas para permitir esta coexistencia y proporcionar una transición fácil. Hay principalmente tres categorías:

- Pila dual

  Permite a los equipos soportar al mismo tiempo los protocolos IPv4 e IPv6.

- Túnel

  Esta técnica permite el transporte del tráfico IPv6 sobre una infraestructura IPv4.

- Traducción.

  Los nodos IPv6 pueden comunicarse con nodos IPv4 mediante la traducción de direcciones.

Estas técnicas se pueden usar en combinación. La migración a IPv6 puede ser hecha paso a paso, comenzando con una simple subred. Se puede migrar una red corporativa, o partes de ella, mientras el ISP correspondiente aún opera con IPv4 únicamente. Otro caso, es lo contrario, que el ISP se actualice a IPv6 mientras el cliente trabaja bajo IPv4. En este capítulo describiremos las técnicas de transición disponibles actualmente[4.1]. Mientras que IPv6 continué creciendo dentro de las redes, nuevos mecanismos serán definidos.

Los mecanismos de transición descritos en las siguientes secciones serán utilizados de acuerdo a las características de cada red.

4.2 Capa Dual

Un nodo con capa dual soporta ambas versiones del protocolo IP. Este tipo de nodo frecuentemente es denominado "Nodo IPv6/IPv4". Dentro de la comunicación con un nodo IPv6, el nodo IPv6/IPv4 se comporta como nodo IPv6 y, en comunicación con un nodo IPv4, se comporta como un nodo IPv4. En este tipo de nodo se tiene una función de conmutación que habilita o deshabilita alguna de las pilas en un momento dado. Es así como este tipo de nodo puede tener tres tipos de operación. Cuando la pila IPv4 es habilitada, y la pila IPv6 es deshabilitada, el nodo se comporta como un nodo IPv4 únicamente. Cuando la pila IPv6 es habilitada, y la pila IPv4 es deshabilitada, se comporta como un nodo IPv6. Cuando los protocolos IPv4 e IPv6 son habilitados, el nodo puede usar ambos.

Una red con pila dual es una infraestructura en la cual ambos protocolos, IPv4 e IPv6, están habilitados en los equipos de capa 3. La desventaja de esta técnica es que se debe ejecutar software adicional en la red para operar ambas pilas por separado. Esto

[4.1] El RFC 2893, "Transition Mechanisms for IPv6 Hosts and Routers", define el conjunto inicial de mecanismos de transición.

significa que todas las tablas de enrutamiento son almacenadas simultáneamente, estando configurados ambos protocolos. Esto implica mayor procesamiento en los equipos, y más complejidad en la administración de la red.

4.3 Túneles

Los mecanismos de túneles pueden ser usados para desarrollar IPv6 mientras la infraestructura IPv4 esta activa. Los túneles pueden transportar tráfico IPv6 encapsulado dentro de paquetes IPv4, usando una infraestructura IPv4 existente. Por ejemplo, si el proveedor de servicios de red tiene opera con IPv4, los túneles le permiten tener clientes con redes IPv6 usando la infraestructura IPv4 para comunicarse con otras redes IPv6[4.2]. Actualmente hay dos tipos de túnel:

Túneles IPv6 configurados sobre IPv4

Los paquetes IPv6 son encapsulados en paquetes IPv4 para ser transportados sobre infraestructuras IPv4. Estos túneles son punto a punto.

Túneles IPv6 automáticos sobre IPv4

Los nodos IPv6 pueden usar diferentes tipos de direcciones, tales como direcciones IPv6 compatibles con IPv4 o direcciones 6to4, para pasar paquetes IPv6 a través de los túneles sobre una red IPv4. Estas direcciones unicast especiales transportan la dirección IPv4 en alguno de los campos de la dirección IPv6.

4.3.1 Como funcionan los túneles

Los conceptos discutidos en este apartado son aplicables a los túneles en general, más adelante se discutirá la diferencia entre los túneles configurados y los túneles automáticos. La figura 4.1 muestra dos redes IPv6 conectadas a través de una red IPv4.

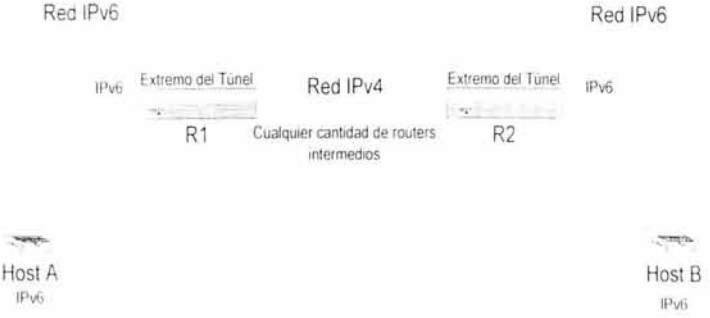


Figura 4.1: El funcionamiento de los túneles

[4.2] Las tecnicas de túneles y de encapsulamiento de paquetes IPv6 en paquetes IPv4 se han definido en varios RFC's, como el RFC 2473, 2893, y el 3056.

El host A esta en una red IPv6 y quiere enviar paquetes IPv6 a un host B que se encuentra en otra red IPv6. La red entre el router R1 y el router R2 funciona con IPv4. R1 es el punto de entrada al túnel. El host A envía el paquete IPv6 a R1. Cuando R1 recibe el paquete destinado a B, encapsula el paquete con una cabecera IPv4 y lo envía a R2, el cual es punto de salida del túnel. R2 desencapsula el paquete y lo envía a su destino final. No hay un límite definido en la cantidad de routers IPV4 entre R1 y R2.

Un túnel tiene dos nodos extremos: el de entrada y el de salida. En la figura 4.1 vemos que los extremos son dos routers. El túnel puede ser implementado router a router, host a router, host a host, o router a host. Dependiendo del caso, los extremos pueden ser host o router. Si la salida del túnel es un host, la dirección IPv6 destino del paquete original es idéntica a la de salida del túnel y puede ser tomada de la cabecera IPv6 en el paquete original. Si la salida del túnel es un router, la dirección destino original del paquete IPv6 no es igual a la dirección de salida del túnel. En este caso la entrada del túnel debe proporcionar la información de la dirección de la salida del túnel.

Los paquetes IPv6 son encapsulados de acuerdo a lo siguiente: .

1. La entrada del túnel disminuye en uno el límite de saltos IPv6, encapsula el paquete IPv6 con una cabecera IPv4, y transmite el paquete encapsulado a través del túnel. Si es necesario el paquete IPv4 es fragmentado.

2. La salida del túnel recibe el paquete encapsulado. Si el paquete fue fragmentado, en este punto es reensamblado. Entonces el nodo de salida remueve la cabecera IPv4 y procesa el paquete IPv6 a su destino original.

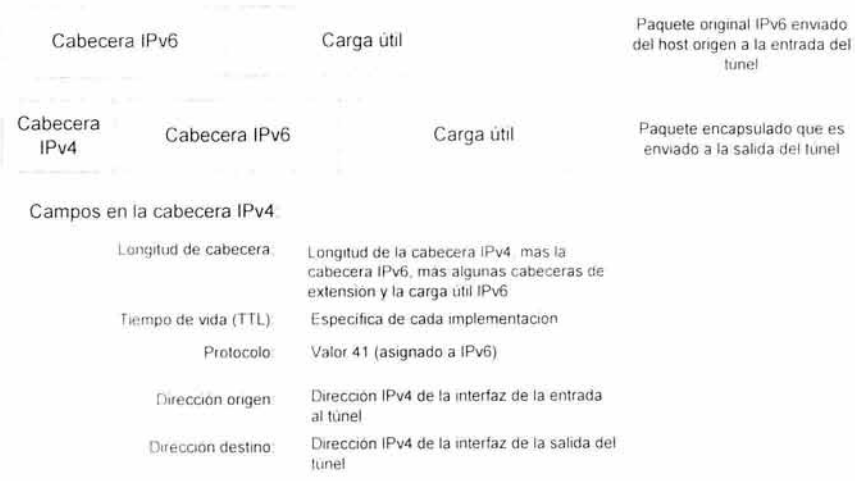


Figura 4.2: Paquete IPv6 encapsulado en un paquete IPv4.

El campo "Longitud de cabecera" contiene la longitud de la cabecera IPv4, la longitud de la cabecera IPv6, algunas cabeceras de extensión y el tamaño de la carga útil

IPv6. Si el paquete encapsulado ha sido fragmentado, se tendrán los valores correspondientes en el campo de banderas y en el de fragmentación. El valor del campo "Tiempo de vida" (TTL) depende de la implementación usada. El número del protocolo es puesto en 41, el cual es el valor asignado a IPv6. De esta forma, si se quiere analizar el tráfico IPv6 en túnel, se puede poner un filtro en un analizador para mostrar los paquetes que contienen el valor 41 en el campo del número de protocolo. La dirección IPv4 origen es la dirección de la interfaz de la entrada del túnel, y la dirección destino IPv4 es la dirección de la interfaz de la salida del túnel. El túnel IPv6 sobre IPv4 se considera como un salto, por lo que el campo "Límite de saltos" en la cabecera IPv6 es disminuido en uno; esto oculta la existencia del túnel al usuario final y no es detectable por herramientas de administración de red como "traceroute".

Cuando la salida del túnel recibe un datagrama IPv4 con un valor de protocolo de 41, sabe que el paquete se ha encapsulado. En caso de fragmentación, reensambla los paquetes, retira la cabecera IPv4, y entrega el paquete IPv6 al destino final.

Los dos extremos del túnel requieren de una dirección IPv6 de enlace local, la cual se forma con el prefijo de enlace local y la dirección IPv4 de la interfaz. Por ejemplo, un host con una dirección IPv4 de **192.168.0.2** tiene una dirección de enlace local **FE80::192.168.0.2 /64** .

Antes de enviar un paquete IPv6 desencapsulado, la salida del túnel debe verificar que la dirección origen del túnel es válida. De esta forma, se puede evitar un ingreso no válido a la red. Si el túnel es bidireccional, la verificación se hace al comparar la dirección origen del paquete encapsulado con la dirección configurada en el otro extremo del túnel. Para túneles unidireccionales, el túnel debe ser configurado con una lista de prefijos con direcciones IPv4 válidas.

4.3.2 Túneles Automáticos

Los túneles automáticos permiten a nodos IPv6/IPv4 comunicarse sobre una infraestructura IPv4 sin la necesidad de una configuración previa del extremo final del túnel[4.3]. La dirección de éste último es determinada por la dirección destino compatible IPv4. Este tipo de direcciones IPv6 son asignadas exclusivamente a nodos que usan túneles automáticos.

La dirección IPv4 compatible es creada al tomar la dirección IPv4 y colocando un prefijo de 96 bits todo ceros. La interfaz a la cual es asignada esta dirección es denominada "Psedo-interface". Por ejemplo, tenemos la dirección IPv4 compatible con IPv6: **::62.2.84.115** . Si la dirección IPv4 no es de un rango privado, la dirección IPv4 compatible es globalmente única.

Se puede usar una entrada especial en la tabla de enrutamiento para dirigir paquetes a través del túnel. La entrada puede ser simplemente una ruta al prefijo todos ceros con una máscara de 96 bits. Todos los paquetes con una dirección IPv4 compatible que tienen como destino una dirección IPv6 harán correspondencia con este prefijo y serán enviados por el túnel automático. La dirección IPv4 destino es tomada de los 32 bits

[4.3] El RFC 2893 define el mecanismo de tunel automatico

de menor orden de la dirección IPv6 destino. El túnel automático no envía paquetes IPv4 de broadcast, multicast, loopback, o direcciones no especificadas.

4.3.3 Túneles Configurados

En los túneles configurados, la dirección del extremo de salida del túnel es configurada en el extremo de entrada al túnel. Cuando el paquete IPv6 es encapsulado, la entrada al túnel usa esta dirección como destino en la cabecera IPv4[4.4]

Hosts IPv6/IPv4 conectados a segmentos de red con routers sin IPv6 pueden ser configurados con una ruta estática a un router IPv6 en Internet en el otro extremo del túnel IPv4; este habilita la comunicación con una red IPv6 remota. En este caso, la dirección IPv6 de un router IPv6/IPv4 en el otro extremo del túnel se agrega en de la tabla de enrutamiento como ruta por defecto. Así, todas las direcciones IPv6 destino corresponderán a la ruta y pueden pasar por el túnel a través de la infraestructura IPv4. La ruta por defecto tiene una máscara de cero y se usa solo si no hay otras rutas con una máscara de correspondencia más específica.

4.3.4 Combinación de Túneles Configurados y Automáticos

También es posible combinar las dos técnicas anteriores para hosts conectados a segmentos sin un router IPv6. Un host puede tener dos entradas de enrutamiento para túneles. Una entrada apunta al prefijo todos ceros de 96 bits (**:: /96**). Todos los paquetes con direcciones destino IPv6 compatible con IPv4 serán enviados a través de esta ruta. La otra entrada de enrutamiento apunta a un router IPv6 que también ejecuta túneles automáticos. Todos los paquetes con direcciones destino IPv6 nativas serán dirigidos a través del túnel configurado. Los paquetes de respuesta de los hosts IPv6 nativos serán enviados al router IPv6, el cual los entrega de regreso al host original a través del túnel automático.

Si un host que envía un paquete que tiene las direcciones IPv6 compatible con IPv4 y la IPv6 nativa global, este host debe usar la dirección compatible con IPv4 como la dirección origen de los paquetes que tienen como destino direcciones IPv6 compatibles con IPv4; y debe usar la dirección IPv6 nativa como el origen de los paquetes con direcciones destino IPv6 nativas.

4.3.5 Paquetes encapsulados con IPv6

La mayoría de las reglas discutidas aquí acerca de los túneles en IPv4 aplican a los túneles en IPv6. La principal diferencia es que en un túnel sobre IPv6, los paquetes son encapsulados con una cabecera IPv6 y enviados a través de una red IPv6. El paquete encapsulado puede ser un paquete IPv4 o de algún otro protocolo[4.5]. A la entrada del túnel se coloca la cabecera IPv6, y si es necesario, una o un conjunto de cabeceras de extensión delante de la cabecera original del paquete. Estas cabeceras se denominan "Cabeceras del Túnel IPv6".

[4.4] El RFC 2893 define el mecanismo de túnel configurado.
[4.5] El RFC 2473 especifica el modelo y los mecanismos genéricos de encapsulamiento con IPV6

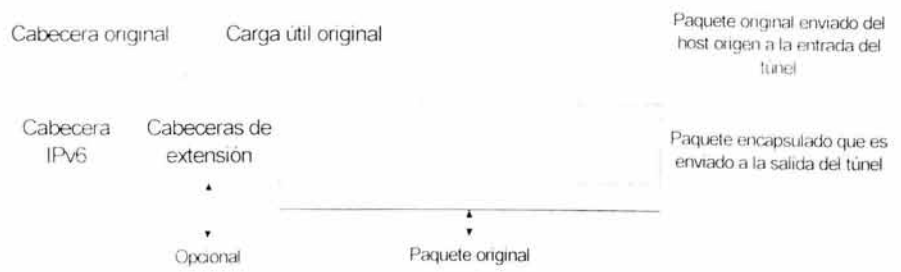


Figura 4.3: Cabeceras del Túnel IPv6.

En la cabecera IPv6 aplicada a la entrada del túnel, la dirección origen es la dirección del nodo de entrada al túnel, y la dirección destino es la dirección del nodo de salida del túnel. El nodo origen del paquete original puede ser el mismo de entrada al túnel. El paquete original, incluyendo su cabecera, se convierte la carga del paquete encapsulado. La cabecera del paquete original es procesada de acuerdo a las reglas de envío estándar. Si es una cabecera IPv4, el campo TTL es disminuido en uno, ya que la red entre la entrada al túnel y su salida es virtualmente un salto.

La cabecera del túnel IPv6 es procesada de acuerdo a las reglas del protocolo IPv6. Las cabeceras de extensión, si están presentes, son procesadas como un paquete estándar. Por ejemplo, una cabecera de extensión "Hop by hop" puede ser procesada por cada nodo listado en el campo de opciones "Hop by hop". La cabecera de "Opciones de destino" puede ser procesada por el host destino, el cual puede ser la salida del túnel. Un ejemplo del uso de la cabecera de "Opciones de destino" es la configuración de una opción de límite de encapsulamientos[4.6]. Esta opción puede usarse cuando se intercalan túneles. Cuando un salto en un túnel es la entrada a otro túnel, se dice que los túneles se intercalan. El primer túnel se denomina "Túnel exterior" y el segundo "Túnel interior". La entrada al túnel interior trata a todo el paquete recibido del túnel exterior como el paquete original y aplica las mismas reglas mostradas en la figura 4.3. El único límite natural para el número de túneles intercalados es el tamaño máximo del paquete IPv6. Cada encapsulamiento agrega el tamaño de las cabeceras del túnel IPv6. Esto permitiría alrededor de 1600 túneles intercalados, algo que remotamente ocurre. También hay que considerar el caso en que el paquete tiene que ser fragmentado. Si tiene que ser fragmentado por que las cabeceras adicionales del túnel IPv6 han incrementado el tamaño del paquete, el número de fragmentos es duplicado. Es por ello que se requiere de un mecanismo que limite el número de túneles intercalados[4.7]. Este mecanismo se lleva a cabo en la cabecera de opciones de destino y tiene el formato mostrado en la figura 4.4.

[4.6] El RFC 2473 especifica el límite de encapsulamientos.
[4.7] El RFC 2473 especifica el mecanismo para el límite de encapsulamiento: "Option Limit Encapsulation Tunel".

Tipo de opción (1 byte)	4	Valor decimal 4 que especifica la opción de límite de túneles encapsulados
Longitud de datos de la opción (1 byte)	1	Valor decimal 1
Datos de la opción (1 byte)		Valor del límite de túneles encapsulados que especifica cuántos niveles de encapsulamiento son permitidos

Figura 4.4. Formato de la opción de límite de encapsulamiento de túneles.

El campo de tipo de opción tiene 1 byte y un valor decimal de 4 que indica la opción del límite de encapsulamiento de túneles. El campo "Longitud de datos de la opción" tiene el valor decimal de 1, el cual especifica la longitud del siguiente campo de la opción. En este caso el campo "Datos de la opción" tiene un tamaño de 1 byte y contiene el valor del límite de encapsulamiento de túneles. El valor de este campo especifica cuantos niveles de encapsulamiento son permitidos. Si el valor es cero, el paquete es descartado. Si el valor no es cero, el paquete es encapsulado y enviado. En este caso una nueva opción de límite de encapsulamiento de túneles tiene que ser aplicada con un valor de uno menos que el límite recibido en el paquete encapsulado. Si el paquete recibido no tiene un límite de encapsulamiento de túneles, pero esta entrada de túnel tiene configurada una, la entrada del túnel debe aplicar una cabecera de opciones de destino e incluir el valor configurado.

El encapsulamiento de Loopback debe ser evitado. Este encapsulamiento sucede cuando un nodo encapsula un paquete originado desde él y destinado hacia él. Al implementar IPv6 se debe prevenir esto y rechazar configuraciones de túneles donde las entradas y salidas pertenecen al mismo host. Otra situación indeseable es la encapsulamiento dentro de un loop de enrutamiento. Esto ocurre si el paquete de un túnel interior reingresa a un túnel exterior del cual aún no ha salido. Esto solo puede ser controlado por una combinación del límite de saltos del paquete original más la configuración de límites de encapsulamiento de túneles.

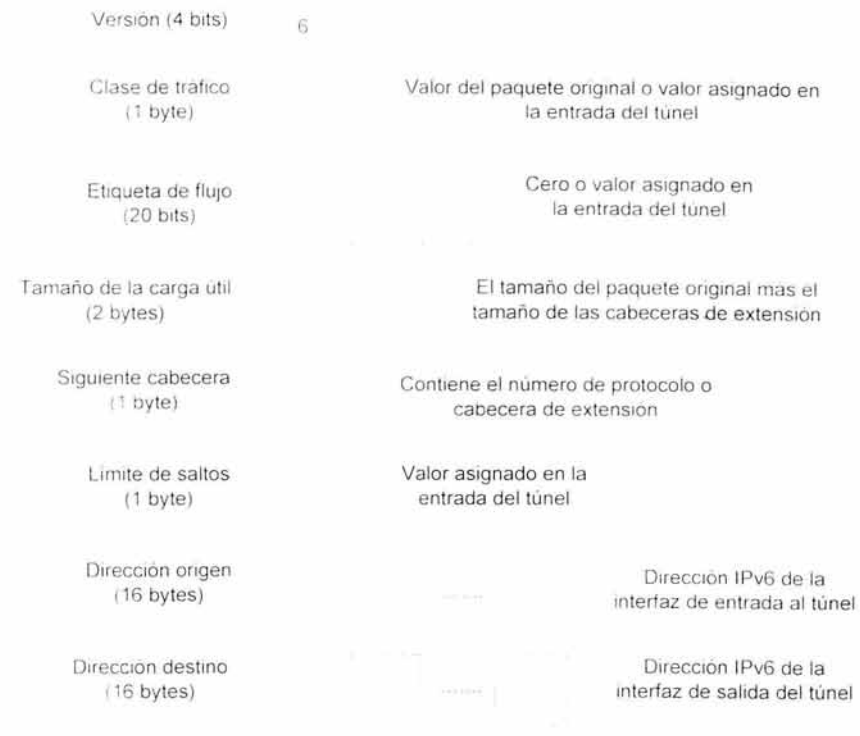


Figura 4.5: La Cabecera del Túnel IPv6

Los campos de la cabecera IPv6 estándar fueron discutidos en el capitulo 1. Los valores que nos interesan en este punto son: clase de tráfico, etiqueta de flujo y límite de saltos, los cuales pueden ser configurados a la entrada de un túnel. La longitud de la carga tiene el valor de la longitud del paquete original más el tamaño de las cabeceras de extensión colocadas a la entrada del túnel. Las direcciones origen y destino de la cabecera del túnel IPv6 contienen las direcciones IPv6 de la entrada y salida del túnel respectivamente. Un host que es la entrada de un túnel debe soportar la fragmentación de los paquetes que encapsula. Los paquetes encapsulados pueden exceder la MTU del túnel. Como la entrada del túnel se considera el origen del paquete encapsulado, entonces debe fragmentar si es necesario. El nodo de salida del túnel reensamblará el paquete. Si el paquete original es un paquete IPv4 con el bit de "No fragmentación" habilitado, la entrada del túnel descarta el paquete.

4.3.6 6to4

Hay otro mecanismo para sitios IPv6 que se comunican sobre una infraestructura IPv4 que se conoce como 6to4[4.8]. La red IPv4 de área amplia es tratada como un enlace

[4.8] El RFC 3056 "Connection of IPV6 Domains via IPv4 Clouds" especifica el mecanismo 6to4

punto a punto, y los dominios nativos IPv6 se comunican via routers 6to4. Estos últimos son denominados "Gateways 6to4". Este mecanismo de transición ha sido y continuará siendo útil durante la coexistencia de IPv4 con IPv6, sin embargo no es una solución permanente.

Los paquetes IPv6 son encapsulados con la cabecera IPv4 en el gateway 6to4, por que al menos se requiere de una dirección unicast IPv4 global para esta configuración. IANA ha asignado un prefijo especial TLA para el esquema 6to4. Este prefijo es el **2002:: /16** . La figura 4.6 muestra el formato de la dirección 6to4 a detalle.

3 bits	13 bits	32 bits	16 bits	64 bits
FP 001	TLA 0x0002	Dirección IPv4	SLA ID	ID de Interfaz

Longitud de prefijo: 48 bits (/48)

Figura 4.6: Formato del prefijo 6to4.

Los 32 bits después del prefijo **2002:: /16** son la dirección IPv4 del gateway 6to4 en representación hexadecimal. Por ejemplo la dirección IPv4 62.2.84.115 se convierte en 2002:3E02:5473:: /48 . Esto deja 80 bits de espacio para las redes locales IPv6. Después de los 48 bits, con los 16 siguientes se pueden crear hasta 65,536 redes; y los 64 bits restantes son para los nodos de cada red.

Si hosts IPv6 quieren comunicarse con otros que se encuentran en redes remotas IPv6, como el 6Bone, se requiere de un "6to4 relay router". Este router conecta a la red 6to4 con redes nativas de IPv6[4.9].

Para tener una red 6to4, se puede escoger el mejor relay router dentro del sitio para usarlo como gateway 6to4, esto es, la ruta IPv6 por defecto.

Los gateways 6to4 necesitan una ruta para encontrar un 6to4 relay router en Internet[4.10]. IANA ha asignado un prefijo anycast 6to4 en IPv4: **192.88.99.0 /24**. La dirección anycast asignada corresponde al primer nodo en el prefijo, por ejemplo, **192.88.99.1**. Los routers 6to4 deben tener una ruta por defecto apuntando a esta dirección anycast. Al Usar esta dirección, los paquetes 6to4 son dirigidos al 6to4 relay router disponible y más cercano de forma automática. Si un 6to4 realay router no esta disponible, no se necesita reconfigurar el gateway 6to4, ya que los paquetes serán dirigidos automáticamente al siguiente relay router disponible. Con el desarrollo de las redes IPv6 comerciales, el número de routers 6to4 públicos se incrementará. Si un host desea comunicarse con otro en una red IPv6 nativa, por ejemplo la dirección **3FFE:B00:C18:1::10**, la dirección destino en la cabecera IPv4 será la dirección anycast reservada **192.88.99.1** y, será entregada al 6to4 relay router más cercano. El otro caso: un host nativo IPv6 que quiere enviar paquetes a un host que se encuentra en una red

[4.9] Hay una lista de 6to4 relay routers públicos de Internet, en http://www.kfu.com/~nsayer/6to4/

[4.10] El RFC 3068 define una dirección anycast para los 6to4 relay routers que simplifica la configuración de los gateway 6to4 que necesitan una ruta por defecto para encontrar un 6to4 relay router en Internet

6to4 dirigirá sus paquetes al 6to4 relay router más cercano que anuncia el prefijo **2002:: /16**.

Cuando los paquetes IPv6 dejan un sitio 6to4 para entrar a una zona IPv4, son encapsulados en paquetes IPv4 por el gateway 6to4.

Cuando dos hots están en comunicación, uno con solo una dirección 6to4 y el otro con una dirección 6to4 más una dirección IPv6 nativa, deben usar las direcciones 6to4. Si ambos hosts tienen una dirección 6to4 más una nativa, entonces pueden usar cualquiera de las dos direcciones, aunque los dos deben usar el mismo tipo de dirección.

4.4 Diseño de una Red

Veamos como diseñar una red utilizando túneles. Se puede comenzar a desarrollar IPv6 con algunos hots y subredes que no requieren cambios importantes en la infraestructura de red IPv4.

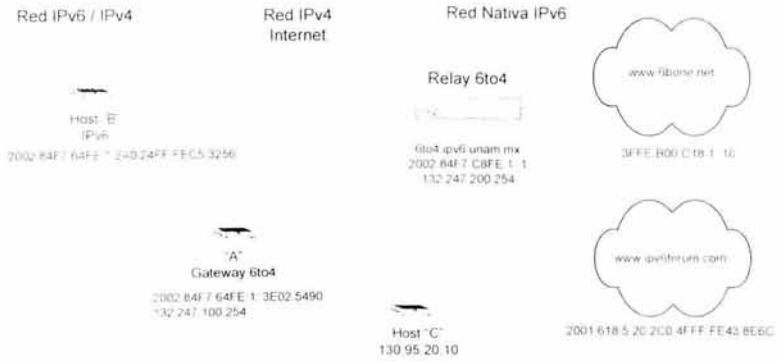


Figura 4.7: Diseño de una red 6to4

"A" es el gateway 6to4 de la "Red 1", el cual tiene una dirección IPv4 global **132.247.100.254**, una interfaz lógica IPv6 dentro de la Red 1, y anuncia el prefijo **2002:84F7:64FE:: /48** para la ruta 6to4. Además tiene configurada una dirección IPv4 de un 6to4 relay router, que puede ser el equipo con nombre **6to4.ipv6.unam.mx.** El gateway A proporciona transito IPv6 para todas las máquinas IPv6 que se encuentran dentro de la Red 1. "B" es una máquina con IPv6 dentro de la Red 1, que tiene una dirección **2002:84F7:64FE:1:2A0:24FF:FEC5:3256** que utiliza el prefijo anunciado por A. El 6to4 relay router conecta a sitios 6to4 con redes nativas de IPv6, por ejemplo el 6Bone. El relay router es una máquina con pila dual, cuyas interfaces tienen las direcciones **132.247.200.254** y **2002:84F7:C8FE:1::1,** para IPv4 e IPv6 respectivamente. En la figura 4.7 se muestra como el host B, que es 6to4, puede acceder a dos hosts IPv6 nativos:

3FFE:B00:C18:1::10 y **2001:618:5:20:2C0:4FFF:FE43:8E6C.** "C" es solo un host IPv4 de otra red conectada a Internet con dirección 130.95.20.10

El host B solo tiene el protocolo IPv6 habilitado. Puede estar sobre una red 6to4, o en una red IPv4/IPv6. Si B quiere comunicarse con otros sitios 6to4, debe usar el gateway A; y si quiere comunicarse con nodos que solo tienen IPv6, debe usar el 6to4 relay router. Cuando el gateway A obtiene un paquete para un host del 6Bone, lo encapsula con una cabecera IPv4 y lo envía al otro extremo del túnel, es decir, hacia el 6to4 relay router. Este quita la cabecera IPv4 y envía el paquete IPv6 nativo al 6Bone. Si hosts del 6Bone envían paquetes a sitios 6to4, estos paquetes tendrán una dirección destino con el prefijo **2002::/16**. De esta forma, el relay router sabe que tiene que encapsular el paquete en IPv4, y puede derivar la dirección IPv4 de la dirección que viene del gateway 6to4. El gateway desencapsula el paquete y lo envía hacia el host B. Si B quiere comunicarse con otro host de su mismo segmento, lo puede hacer sin usar el gateway A. Si el host B quiere comunicarse con el host C, el cual no tiene la pila IPv6, solo lo puede hacer con algún mecanismo de traducción de direcciones. Sin este mecanismo, el host C es incapaz de interpretar la información de la cabecera IPv6.

El diseño anterior es un muestra de lo que se puede hacer con los túneles. Estas técnicas proporcionan una migración ordenada y flexible. Además permiten la actualización gradual de los hosts y routers. No hay que olvidar que estos mecanismos agregan carga en los routers y hacen el procesamiento más complejo. Los routers requieren de tiempo, recursos de CPU y memoria para encapsular y desencapsular los paquetes. La cuenta de los saltos, tamaño de MTU y problemas de fragmentación pueden aparecer en las especificaciones de ambos protocolos.

4.5 Traducción de Dirección y de Protocolo

La traducción proporciona enrutamiento transparente para los nodos en redes IPv6 que se comunican con nodos en redes IPv4 y viceversa[4.11]. Un gateway NAT usa direcciones IPv4 globalmente únicas y las vincula con direcciones IPv6. No son necesarios cambios en los nodos finales. En la traducción de direcciones y de protocolo tenemos las siguientes abreviaciones:

Network Address Translation (NAT)

Traduce direcciones IP.

Network Address Port Translation (NAPT)

Además de la traducción hecha por NAT, cambia algunos identificadores como los números de puerto TCP, UDP.

Network Address Translation and Protocol Translation (NAT-PT)

Traduce paquetes IPv6 a su equivalente en IPv4 y viceversa.

[4.11] Las técnicas de traducción de direcciones y de protocolo están definidas en los RFCs 2765 y 2766

Network Address Port Translation and Protocol Translation (NAPT-PT)

Además de la traducción realizada por NAT-PT, cambia algunos identificadores como los números de puerto TCP, UDP.

4.5.1 NAT

NAT se ha usado ampliamente, especialmente para cubrir la limitación del espacio de direcciones IPv4. Las redes corporativas usan direcciones IPv4 del rango privado junto con un router NAT en el borde de la red para traducir estas direcciones en una o un limitado número de direcciones públicas. NAT, como es descrito aquí, proporciona enrutamiento entre una red IPv6 y una red IPv4. Esto permite a un conjunto de hosts IPv6 compartir una simple dirección IPv4.

4.5.2 Como son traducidos los paquetes

Para comprender como son traducidos los paquetes, seguiremos un paquete desde que es enviado por un host IPv6 a través de un gateway NAPT y después se dirige hacia un host IPv4, y luego regresa.

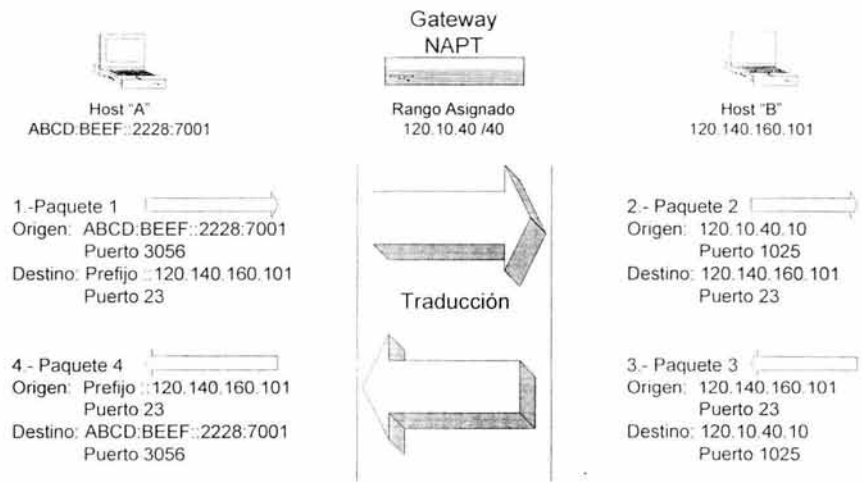


Figura 4.8: Flujo de comunicación sobre NAPT

"A" es un host IPv6 que tiene una dirección **ABCD:BEEF::2228:7001**. El host "B" se encuentra del otro lado del router NAPT y tiene una dirección IPv4 **120.140.160.101**. El gateway NAPT tiene asignado un rango de direcciones para realizar la traducción: **120.10.40.0 /24** . El host A inicia una sesión con el host B al enviar un paquete a la dirección destino **::120.140.160.101** por el puerto 23. El gateway NAPT anuncia el prefijo **::/96** en la red IPv6. Cuando es enviado un paquete hacia este prefijo, el paquete será enrutado a través de NAPT. El host A usa su dirección IPv6 como dirección origen con el

número de puerto 3056. El gateway NAPT asigna al paquete una dirección IPv4 y un número de puerto hacia el exterior. El paquete nuevo con dirección origen **120.10.40.10** y puerto 1025 sale de NAPT hacia el host B que tiene una dirección destino **120.140.160.101**, puerto 23. Cuando el host B responde, envía un paquete con dirección origen **120.140.160.101**, puerto 23 hacia la dirección destino **120.10.40.10**, puerto 1025. NAPT traduce el paquete de acuerdo a los parámetros que ha almacenado en su memoria cache durante la sesión y lo envía con la dirección origen **::120.140.160.101**, puerto 23, hacia la dirección destino **ABCD:BEEF::2228:7001**, puerto 3056.

4.5.3 Limitaciones

Los mecanismos de traducción descritos deben ser usados solo si no es posible usar otra técnica de transición. Este mecanismo tiene ciertas desventajas. Por ejemplo, no usa todas las capacidades de IPv6. Sin embargo, es una alternativa cuando en ciertos casos se requiere acceso a redes con hosts que tienen únicamente al protocolo IPv4 en su sistema.

En cuanto a la seguridad, dos nodos finales que requieren de IPSEC deben tener ambos el protocolo IPv4 ó IPv6 en forma nativa. Esta limitación siempre ha existido en NAT.

Hay otras aplicaciones que usan la dirección IP que esta en la parte de datos de un paquete IP. NAT no toma en cuenta a la capa de aplicación, por lo que no busca dentro de la parte de datos para encontrar direcciones IP. En este caso NAT debe usar un mecanismo adicional para soportar tales aplicaciones en este tipo de ambiente[4.12].

Estas son unas limitaciones importantes en NAT, por lo que al implementar IPv6 se prefiere que sea en forma nativa.

4.5.4 Traducción IP

En caso de que hosts que solo tienen IPv4 y se quieren comunicar con hosts que solo tienen IPv6, o viceversa, se tiene que traducir la cabecera IP en ambas partes para que sean compatibles[4.13]. Si se tiene un nuevo segmento de red y se quiere utilizar hosts IPv6, con la traducción es posible configurar una red que solo tiene IPv6, para acceder a Internet IPv4 ó algún otro nodo que solo tiene IPv4. Con este propósito se ha sido introducido la "Dirección traducible IPv4". El formato de la dirección es **0::FFFF:0:0:0 /96**. El identificador de host es una dirección IPv4 que ha sido tomada de un rango especial y asignado al nodo IPv6 que quiere comunicarse con los nodos IPv4.

Las cabeceras TCP y UDP generalmente no necesitan ser modificadas por el traductor.

[4.12] El RFC 2766 describe como un "DNS ALG" o un "FTP ALG" tiene que traducir para soportar estas aplicaciones sobre NAT.
[4.13] El RFC 2765 define la traducción de dirección y de protocolo.

4.5.4.1 Traducción de IPv4 a IPv6

Un traductor de IPv4 a IPv6 recibe un paquete IPv4, y como reconoce el rango de direcciones IPv4 que representan los nodos IPv6 internos, sabe que los paquetes deben ser traducidos. Entonces remueve la cabecera IPv4 y la reemplaza con una cabecera IPv6, traduciendo toda la información de la cabecera IPv4 en la cabecera IPv6.

El descubrimiento de la unidad de transferencia máxima MTU de una ruta es opcional en IPv4, pero obligatorio en IPv6. Si el bit de no fragmentación no esta en el paquete IPV4, un traductor IPv6 tiene que asegurarse que el paquete puede viajar seguro a través de la red IPv6. Esto lo realiza al fragmentar el paquete IPv4, si es necesario, usando el mínimo tamaño del paquete para IPv6, el cual es de 1280 bytes. IPv6 garantiza que los paquetes de 1280 bytes serán entregados sin fragmentar. En este caso, el traductor siempre incluye una cabecera de fragmentación para indicar que el emisor permite esta característica.

Campo de la cabecera	Información
Versión	6.
Clase de Tráfico	Son copiados los 8 bits del campo Tipo de Servicio y Precedencia.
Etiqueta de Flujo	Cero.
Longitud de Carga Útil	La longitud total del campo de la cabecera IPv4 menos el tamaño de la cabecera IPv4 (incluyendo las opciones si están presentes).
Siguiente Cabecera	Campo del Protocolo copiado de la cabecera IPv4.
Límite de Saltos	Valor TTL copiado de la cabecera IPv4. Si el traductor es un router, el valor tiene que ser disminuido en uno (antes o después de la traducción).
Dirección origen	Combinación del prefijo de la dirección IPv4 mapeada y la dirección IPv4 en los 32 bits de menor orden, por ejemplo: ::FFFF:0:0:192.168.0.1
Dirección destino	Combinación del prefijo de la dirección IPv4 traducible y la dirección IPv4 destino, por ejemplo: 0::FFFF:0:0:0:192.168.0.99
Opciones IPv4	Si algunas opciones IPv4 están presentes, son ignoradas.

Tabla 4.1: Campos de la cabecera IPv6 traducida

Si es necesario agregar una cabecera de fragmentación, la información de la tabla 4.2 es introducida dentro del paquete IPv6.

Campo de la cabecera	Información
Campos de Cabecera	
Longitud de carga útil	La longitud total del campo de la cabecera IPv4 menos el tamaño de la cabecera IPv4 (incluyendo opciones si están presentes) más 8 bits del tamaño de la cabecera de fragmentación.
Siguiente cabecera	44 (cabecera de fragmentación).

Campos de la cabecera de Fragmentación	
Siguiente cabecera	Campo del protocolo copiado de la cabecera IPv4.
Offset de fragmentación	Campo de offset de fragmentación copiado de la cabecera IPv4.
M-Flag	Más fragmentos copiados de la cabecera IPv4.
Identificación	Los 16 bits de mayor orden son puestos a cero; los 16 de menor orden son copiados del campo de identificación en la cabecera IPv4.

Tabla 4.2: Cabecera IPv4 traducida

4.5.4.2 Traducción de IPv6 a IPv4

Este proceso no tiene mucha diferencia del proceso descrito anteriormente. En este caso el traductor sabe que tiene que traducir de IPv6 a IPv4 basándose en la dirección destino IPv4 mapeada. Quita la cabecera IPv6 y la reemplaza con la cabecera IPv4. El tamaño mínimo de la MTU para IPv4 es 68 bytes, y para IPv6 es 1280 bytes. Si un traductor recibe un paquete para una red IPv4 con una MTU más pequeña, crea paquetes de 1280 bytes y los fragmenta después la traducción. La tabla 4-3 muestra la traducción para una cabecera IPv4.

Campo de cabecera	**Información**
Versión	4.
Longitud de la cabecera de Internet	5(no opciones).
TOS y precedencia	Los 8 bits de la Clase de Tráfico son copiados.
Longitud total	Longitud de la carga útil de la cabecera IPv6 más la longitud de la cabecera IPv4.
Identificación	Cero.
Banderas	Más banderas de Fragmentación son puestas en cero; las de fragmentación son puestas en uno.
Offset de fragmentación	Cero.
Tiempo de vida	Valor del límite de saltos copiado de la cabecera IPv6. Si el traductor es un router, el valor tiene que ser disminuido en uno (antes y después de la traducción).
Protocolo	El campo de la siguiente cabecera es copiado de la cabecera IPv6.
Suma de comprobación de la cabecera	Procesado después de la generación de la cabecera IPv4.
Dirección origen	Si la dirección IPv6 es una dirección IPv4 traducida, los 32 bits de menor orden de esta última son copiados al campo de dirección IPv4 origen. De otra manera, NAT asignará una dirección IPv4 diferente a las que ya tiene configuradas, y la copiará dentro del campo de "Dirección origen IPv4"
Dirección destino	Los 32 de menor orden de la dirección destino IPv4

	mapeada son copiados al campo de la dirección destino IPv4.
Opciones	Si una cabecera de opciones salto a salto IPv6, cabecera de opciones de destino, o una cabecera de enrutamiento con los segmentos dejados en el campo igual a cero están presentes, no son traducidos. En este caso el campo de longitud total y el campo de protocolo tienen que ser ajustados adecuadamente.

Tabla 4.3: Cabecera IPv4 traducida

Si el paquete IPv6 contiene una cabecera de fragmentación, los campos respectivos son traducidos como se muestra en la tabla 4.4.

Campo de la cabecera	Información
Longitud total	Longitud de la carga útil de la cabecera IPv6, menos 8 por la cabecera de fragmentación, más el tamaño de la cabecera IPv4.
Identificación	Copiado de los 16 bits de menor orden en el campo de identificación de la cabecera de fragmentación.
Banderas	Más banderas de fragmentación copiadas de la bandera M en la cabecera de fragmentación. La bandera de fragmentación es puesta a cero, por lo que los routers IPv4 pueden fragmentar el paquete.
Offset de fragmentación	El campo de offset de fragmentación copiado de la cabecera IPv6.
Protocolo	Valor de la siguiente cabecera copiado de la cabecera de fragmentación.

Tabla 4.4: Traducción de la cabecera de fragmentación

4.6 Comparación

Ahora que hemos revisado las técnicas, hagamos una comparación de las técnicas vistas anteriormente.

4.6.1 Pila Dual

Esta es una técnica fácil de usar y flexible. Los hosts pueden comunicarse con hosts IPv4 usando IPv4 o comunicarse con hosts IPv6 usando IPv6. Tan pronto como se migre a IPv6, la pila IPv4 puede ser deshabilitada o removida. Las desventajas de esta técnica son: se tienen dos protocolos funcionando al mismo tiempo, por lo que se requiere procesamiento y memoria adicional; se tiene una tabla para cada protocolo. Además se requiere el uso de diferentes comandos para cada protocolo. Algunos protocolos de capa superior necesitan interpretar adecuadamente los dos protocolos.

4.6.2 Túneles

Los túneles permiten migrar a IPv6 solo las rutas que uno desee. No hay un orden de actualización específico que deba ser seguido. Se pueden actualizar simples hosts o redes dentro de la red corporativa y conectar nubes IPv6 separadas por medio de los túneles. No se requiere que el ISP soporte IPv6 para acceder a redes IPv6, ya que se pueden hacer túneles a través de una infraestructura IPv4.

Las desventajas ya son conocidas por otras técnicas de túneles usadas en el pasado. Hay carga adicional en los routers. Los extremos del túnel requieren de tiempo y poder de procesamiento para encapsular y desencapsular paquetes. Además estos extremos son puntos de fallas. Además, pueden aparecer otros problemas con respecto a la cuenta de saltos, el tamaño correcto de la MTU, así como la fragmentación.

4.6.3 NAT

Este mecanismo debe ser usado solo si no es posible usar otro. Además se debe ver como una solución temporal. Las desventajas de esta técnica son que no hay soporte para características avanzadas de IPv6. Plantea limitaciones en el diseño de la topología porque la respuesta es a través del mismo router NAT desde el que fueron enviados los paquetes. El router NAT representa un punto de falla. Todas las aplicaciones que llevan una dirección IP en la carga útil de los paquetes difícilmente funcionarán bien. La ventaja de este método es que permite la comunicación directa entre hosts IPv4 e IPv6.

4.7 Migración a IPv6

Cuando se empieza a usar IPv6, diferentes aproximaciones son posibles. Es importante el saber que empezar a trabajar con IPv6 no significa que se pierda toda la infraestructura de IPv4, o que se cambie toda al mismo tiempo. Existen mecanismos para la coexistencia de IPv4 e IPv6, tales como túneles y traducción de protocolo.

La forma más simple de empezar a usar IPv6 es el habilitar con este protocolo algunos hosts dentro de una red IPv4. Estos se auto-configurarán con una dirección IPv6 local y estarán habilitados para comunicarse con otros mediante IPv6. Si estos también tienen una pila IPv4, se podrán comunicar con el mundo de IPv4. Si uno de los nodos es configurado como gateway 6to4 y es conectado a Internet, otros sitios IPv6 en Internet pueden ser alcanzados a través del uso de un 6to4 relay router.

El siguiente paso para la expansión es agregar un router al escenario. Descubrimiento del router y mensajes de anuncio del router pueden ser usados para la configuración de hosts IPv6 en una subred. Por ejemplo, un router puede ser configurado para anunciar el prefijo de una red y el límite de saltos, de esta manera, todos lo hosts IPv6 de la subred pueden ser configurados con su dirección IPv6, sin necesidad de una configuración estática o de un servidor DHCP. Todo esto esta dado por los mecanismos de auto-configuración, incluyendo el anuncio de prefijo de la subred del router. Dentro de una red corporativa múltiples opciones son posibles, pueden existir segmentos mixtos de hosts IPv4 e IPv6 y hots con pila dual. Puede haber segmentos que solo tienen hosts IPv6; estos segmentos pueden comunicarse con los hosts IPv6 de segmentos mixtos por

medio de un router que tenga una interfaz IPv6 al segmento que solamente tiene hosts IPv6 y una interfaz de pila dual al segmento mixto.

Tan pronto como dos routers IPv6 sean agregados a la red, debe ser usado un protocolo de enrutamiento, RIPv6 por ejemplo. El router también puede ser configurado como gateway 6to4, conectando la red interna IPv6 a otros sitios IPv6 en Internet. En este punto pueden ser agregados al escenario servidores DNS y DHCP.

Hasta el momento se plantea una implementación simple del protocolo IPv6, de donde se va de menos a más. Lo primero es comunicación entre dos hosts dentro de la misma LAN, después un elemento que permita la comunicación entre hosts en distintas LAN's, con ayuda de un protocolo de enrutamiento interno, después la comunicación entre dos hosts de distintos AS's, esto con ayuda de un protocolo de enrutamiento externo y un DNS.

En el capitulo 3 se describió el modelo jerárquico de la Red UNAM que se encuentra en la siguiente situación:

- En el nivel de core se tienen dos modelos de equipos de la marca Foundry, uno es el NetIron 800 y el otro es el BigIron 8000.
- En el nivel de distribución se tienen más equipos de la marca Foundry, de los mencionados anteriormente; y otros tres modelos de equipos de la marca 3Com: uno es el Lanplex 2500, otro el CoreBuilder 2500 y el CoreBuilder 3500.
- Ninguno de los equipos tanto de core como de distribución cuenta con soporte para IPv6. En 3Com no hay soporte para estos modelos. Mientras que en Foundry por el momento tampoco cuenta con soporte para IPv6 en esos equipos, pero si lo hay para otros modelos.

Ante esta situación, es necesario el cambio de equipos del nivel de Distribución, por otros que soporten el protocolo y esperar a que Foundry libere una versión de IOS que soporte IPv6 para los modelos que se tienen en el Core[4.14].

En los niveles de acceso y distribución es posible utilizar los mecanismos de transición para utilizar IPv6, mientras la dependencia en turno consigue equipo que soporte el protocolo. Hay que recordar que no es recomendable usar estas técnicas indefinidamente ya que implica mayor consumo de recursos en los equipos, lo cual disminuye su rendimiento.

[4.14] En el apendice se pueden encontrar los URL's para equipos sugeridos

CONCLUSIONES

CONCLUSIONES

El crecimiento de Internet no fue contemplado inicialmente y ahora se debe eliminar la barrera de una versión de protocolo que ya comienza a ser obsoleta. Con IPv6 se aprovechan características importantes de IPv4, pero se contempla que sus funciones sean útiles desde ahora y en el futuro.

La Red UNAM, que forma parte de la comunidad de Internet, es un recurso muy importante en México, ya que además de proporcionar servicio, en ella se trabaja para adoptar nuevas tecnologías. Por esta razón se debe continuar con el desarrollo de IPv6, un protocolo que ya es una realidad.

Cada vez es más difícil asignar direcciones públicas en IPv4, por lo que muchos administradores y diseñadores de redes se ven en la necesidad de utilizar mecanismos alternos como la traducción de muchas direcciones privadas en pocas direcciones públicas. Pero este tipo de medidas es complicado implementarlas, y además restan potencial a las aplicaciones y servicios de los usuarios finales de la red.

IPv6 supera los problemas que tiene IPv4 y se adapta a las nuevas necesidades de los usuarios de redes en Internet. Al crear IPv6 se contempló no afectar drásticamente la continuidad del servicio de red. En realidad la transición al nuevo protocolo es muy flexible, aunque ello no significa que sea sencilla. El caso concreto se encuentra en el backbone de la Red UNAM, donde los equipos de "Core" que transportan la mayor cantidad de información no cuentan en su sistema operativo con soporte para IPv6. Este soporte en algunos casos esta en desarrollo. Los equipos de distribución tampoco pueden utilizar IPv6. Es difícil instalar IPv6 en estos equipos porque su memoria y procesamiento son limitados. La pila del nuevo protocolo de inicio requiere de ciertos recursos para funcionar, recursos que los fabricantes de dispositivos de red implementan en los equipos más recientes. Por esta razón en la mayoría de los casos se tendrá que cambiar de equipos para poder trabajar con IPV6.

Con lo anterior podemos sugerir que el cambio a la nueva versión de IP se de cuando ya sea deficiente el servicio bajo IPv4. Cuando los servicios de red requieran de características que IPv4 no pueda ofrecer será el momento oportuno de cambiar la versión en los equipos que sea necesario.

Aunque no se debe dejar todo al último momento, IPv6 proporciona una transición gradual para comenzar a cambiar en cuanto sea posible. Se puede empezar a probar las nuevas funciones que se están creando e implementando sobre la base del nuevo protocolo, y así evaluar su potencial. Muchas de estas funciones se originaron desde IPv4, pero en IPv6 se han incrementado sus posibilidades de desarrollo, algo que vale la pena estudiar.

Este trabajo es una exposición detallada del Protocolo Internet versión 6. Muestra la parte que el protocolo aprovecha de la versión 4 e introduce las características que solo son posibles en la nueva estructura. Es un estudio que ayudará en la implementación de IPv6 en la Red UNAM. Actualmente ya se trabaja con este protocolo en algunos equipos, pero se espera que pronto se de un progreso importante en muchos otros.

APÉNDICE A

GLOSARIO DE TÉRMINOS

Area

Conjunto lógico de segmentos de red y sus dispositivos conectados. Las áreas habitualmente se conectan entre si mediante routers, formando un sistema autónomo único.

Backbone

Parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de, y se destina a, otras redes.

Dirección

Identificador de un interfaz o conjunto de ellos en la capa IP.

Enlace

Medio o facilidad de comunicación sobre el que los nodos pueden comunicarse en la capa de enlace, es decir, la capa inmediatamente encima de IP. Sirvan como ejemplo Ethernet (simple o puenteada), enlaces PPP, X.25, Frame Relay ,redes ATM, "túneles" de capa internet (o superior) como túneles sobre IPv4 o IPv6 mismo.

Enrutamiento

Envio de paquetes de acuerdo a un conjunto de reglas que pueden ser determinadas por un protocolo o por un administrador. Esta función se da en la capa 3 del modelo OSI. En redes también se utiliza el término "Ruteo".

Host

Nodo terminal. Generalmente es el punto de acceso a la red por parte de los usuarios.

IAB

Comité de Arquitectura de Internet. Comité de investigadores de Internet que discute temas relativos a la arquitectura de Internet. Responsables por designar una serie de grupos relacionados con Internet, como IANA, IESG e IRSG. El IAB es nombrado por integrantes de la ISOC.

IANA

Agencia de Asignación de Números Internet. Organización que funciona bajo el auspicio de la ISOC como parte del IAB. La IANA delega la autoridad de asignar

espacios de direcciones IP y nombres de dominio al InterNIC y otras organizaciones. La IANA mantiene también una base de datos de identificadores de protocolo asignados que se utilizan en la pila TCP/IP, incluyendo los números de sistemas autónomos.

Interfaz

Punto de conexión de un nodo con un enlace.

ISOC

Sociedad Internet. Organización internacional sin fines de lucro fundada en 1992, que coordina la evolución y el uso de la Internet. Además la ISOC delega facultades a otros grupos relacionados con la Internet, por ejemplo el IAB.

NLA ID (Next Level Aggregation Identifier)

Identificador usado por organizaciones a las que se les asignó un TLA para crear una estructura jerárquica de direccionamiento de acuerdo a su propia red y a las organizaciones que dependen de ella.

Nodo

Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales, pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

Paquete

Una cabecera IP mas su carga.

Router

Dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Envía paquetes desde una red a otra basándose en la información de la capa de red. De vez en cuando denominado *gateway* (aunque esta definición de gateway se está tornando obsoleta).

SLA ID (Site Level Aggregation Identifier)

Identificador usado por organizaciones locales para crear su propia jerarquía de direccionamiento.

TLA ID(Top Level Aggregation Identifier)

Identificador de nivel superior en la jerarquía de enrutamiento. Los routers situados en este nivel tienen en la tabla de enrutamiento una entrada para cada TLA activa, aunque pueden tener más dependiendo de la topología. El objetivo será minimizar el número de entradas en las tablas de enrutamiento.

Sistema Autónomo (AS)

Colección de redes bajo una administración común que comparten una estrategia de enrutamiento común. Los sistemas autónomos se subdividen en áreas. Un sistema autónomo puede ser asignado un número de 16 bits exclusivo por la IANA. A veces se abrevia *AS*.

APÉNDICE B

RFC's DEL PROTOCOLO INTERNET VERSIÓN 6

- **Especificaciones de la nueva versión de IP**

1809 Using the Flow Label Field in IPv6. C. Partridge. June 1995. (Format: TXT=13591 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc1809.txt

1883 Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1995. (Format: TXT=82089 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1883.txt
Obsoleted by RFC2460 http://www.ietf.org/rfc/rfc2460.txt

1888 OSI NSAPs and IPv6. J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd. August 1996. (Format: TXT=36469 bytes) (Status: EXPERIMENTAL)
http://www.ietf.org/rfc/rfc1887.txt

1970 Neighbor Discovery for IP Version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson. August 1996. (Format: TXT=197632 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1970.txt
Obsoleted by RFC2461 http://www.ietf.org/rfc/rfc2461.txt

2452 IP Version 6 Management Information Base for the Transmission Control Protocol. M. Daniele. December 1998. (Format: TXT=19066 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2452.txt

2454 IP Version 6 Management Information Base for the User Datagram Protocol. M. Daniele. December 1998. (Format: TXT=15862 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2454.txt

2460 Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. (Format: TXT=85490 bytes) (***Obsoletes RFC1883***) (Status: DRAFT STANDARD)
http://www.ietf.org/rfc/rfc2460.txt

2465 Management Information Base for IP Version 6: Textual Conventions and General Group. D. Haskin, S. Onishi. December 1998. (Format: TXT=77339 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2465.txt

2466 Management Information Base for IP Version 6: ICMPv6 Group. D. Haskin, S. Onishi. December 1998. (Format: TXT=27547 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2466.txt

3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol. B. Haberman, R. Worzella. January 2001. (Format: TXT=28293 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3019.txt

- **Direccionamiento**

1881 IPv6 Address Allocation Management. IAB, IESG. December 1995. (Format: TXT=3215 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc1881.txt
1884 IP Version 6 Addressing Architecture. R. Hinden, S. Deering, Eds.. December 1995. (Format: TXT=37860 bytes) (Status: HISTORIC)
http://www.ietf.org/rfc/rfc1884.txt
Obsoleted by RFC2373 http://www.ietf.org/rfc/rfc2373.txt

1887 An Architecture for IPv6 Unicast Address Allocation. Y. Rekhter, T. Li, Eds.. December 1995. (Format: TXT=66066 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc1887.txt

1897 IPv6 Testing Address Allocation. R. Hinden, J. Postel. January 1996. (Format: TXT=6643 bytes) (Status: EXPERIMENTAL)
http://www.ietf.org/rfc/rfc1897.txt
Obsoleted by RFC2471 http://www.ietf.org/rfc/rfc2471.txt

1924 A Compact Representation of IPv6 Addresses. R. Elz. Apr-01-1996. (Format: TXT=10409 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc1924.txt

1971 IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten. August 1996. (Format: TXT=56890 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1971.txt
Obsoleted by RFC2462 http://www.ietf.org/rfc/rfc2462.txt

2073 An IPv6 Provider-Based Unicast Address Format. Y. Rekhter, P. Lothberg, R. Hinden, S. Deering, J. Postel. January 1997. (Format: TXT=15549 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2073.txt
Obsoleted by RFC2374 http://www.ietf.org/rfc/rfc2374.txt

2373 IP Version 6 Addressing Architecture. R. Hinden, S. Deering. July 1998. (Format: TXT=52526 bytes) (***Obsoletes RFC1884***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2373.txt

2374 An IPv6 Aggregatable Global Unicast Address Format. R. Hinden, M. O'Dell, S. Deering. July 1998. (Format: TXT=25068 bytes) (***Obsoletes RFC2073***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2374.txt

2375 IPv6 Multicast Address Assignments. R. Hinden, S. Deering. July 1998. (Format: TXT=14356 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2375.txt

2462 IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten. December 1998. (Format: TXT=61210 bytes) (***Obsoletes RFC1971***) (Status: DRAFT STANDARD)
http://www.ietf.org/rfc/rfc2462.txt

2471 IPv6 Testing Address Allocation. R. Hinden, R. Fink, J. Postel (deceased). December 1998. (Format: TXT=8031 bytes) (***Obsoletes RFC1897***) (Status: EXPERIMENTAL)
http://www.ietf.org/rfc/rfc2471.txt

2491 IPv6 over Non-Broadcast Multiple Access (NBMA) networks. G. Armitage, P. Schulter, M. Jork, G. Harter. January 1999. (Format: TXT=100782 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2491.txt

2526 Reserved IPv6 Subnet Anycast Addresses. D. Johnson, S. Deering. March 1999. (Format: TXT=14555 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2526.txt

2732 Format for Literal IPv6 Addresses in URL's. R. Hinden, B. Carpenter, L. Masinter. December 1999. (Format: TXT=7984 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2732.txt

2928 Initial IPv6 Sub-TLA ID Assignments. R. Hinden, S. Deering, R. Fink, T. Hain. September 2000. (Format: TXT=11882 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2928.txt

3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6. T. Narten, R. Draves. January 2001. (Format: TXT=44446 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3041.txt

3177 IAB/IESG Recommendations on IPv6 Address. IAB, IESG. September 2001. (Format: TXT=23178 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc3177.txt

- **Transmisión y control**

1972 A Method for the Transmission of IPv6 Packets over Ethernet Networks. M. Crawford. August 1996. (Format: TXT=6353 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1972.txt
Obsoleted by RFC2464 http://www.ietf.org/rfc/rfc2464.txt

1981 Path MTU Discovery for IP version 6. J. McCann, S. Deering, J. Mogul. August 1996. (Format: TXT=34088 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1981.txt

2019 Transmission of IPv6 Packets Over FDDI. M. Crawford. October 1996. (Format: TXT=12344 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2019.txt
Obsoleted by RFC2467 http://www.ietf.org/rfc/rfc2467.txt

2023 IP Version 6 over PPP. D. Haskin, E. Allen. October 1996. (Format: TXT=20275 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2023.txt
Obsoleted by RFC2472 http://www.ietf.org/rfc/rfc2472.txt

2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. D. Mills. October 1996. (Format: TXT=48620 bytes) (***Obsoletes RFC1769***) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2030.txt

2147 TCP and UDP over IPv6 Jumbograms. D. Borman. May 1997. (Format: TXT=1883 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2147.txt
Obsoleted by RFC2675 http://www.ietf.org/rfc/rfc2675.txt

2464 Transmission of IPv6 Packets over Ethernet Networks. M. Crawford. December 1998. (Format: TXT=12725 bytes) (***Obsoletes RFC1972***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2464.txt

2467 Transmission of IPv6 Packets over FDDI Networks. M. Crawford. December 1998. (Format: TXT=16028 bytes) (***Obsoletes RFC2019***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2467.txt

2470 Transmission of IPv6 Packets over Token Ring Networks. M. Crawford, T. Narten, S. Thomas. December 1998. (Format: TXT=21677 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2470.txt

2492 IPv6 over ATM Networks. G. Armitage, P. Schulter, M. Jork. January 1999. (Format: TXT=21199 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2492.txt

2497 Transmission of IPv6 Packets over ARCnet Networks. I. Souvatzis. January 1999. (Format: TXT=10304 bytes) (***Also RFC1201***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2497.txt

2590 Transmission of IPv6 Packets over Frame Relay Networks Specification. A. Conta, A. Malis, M. Mueller. May 1999. (Format: TXT=41817 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2590.txt

3146 Transmission of IPv6 Packets over IEEE 1394 Networks. K. Fujisawa, A. Onoe. October 2001. (Format: TXT=16569 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3146.txt

- **ICMP**

1885 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). A. Conta, S. Deering. December 1995. (Format: TXT=32214 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1885.txt
Obsoleted by RFC2463 http://www.ietf.org/rfc/rfc2463.txt

2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. A. Conta, S. Deering. December 1998. (Format: TXT=34190 bytes) (***Obsoletes RFC1885***) (Status: DRAFT STANDARD)
http://www.ietf.org/rfc/rfc2463.txt

- **Transición**

2473 Generic Packet Tunneling in IPv6 Specification. A. Conta, S. Deering. December 1998. (Format: TXT=77956 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2473.txt

2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels. B. Carpenter, C. Jung. March 1999. (Format: TXT=21049 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2529.txt

3053 IPv6 Tunnel Broker. A. Durand, P. Fasano, I. Guardini, D. Lento. January 2001. (Format: TXT=27336 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc3053.txt

3056 Connection of IPv6 Domains via IPv4 Clouds. B. Carpenter, K. Moore. February 2001. (Format: TXT=54902 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3056.txt

3142 An IPv6-to-IPv4 Transport Relay Translator. J. Hagino, K. Yamamoto. June 2001. (Format: TXT=20864 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc3142.txt

- **DNS**

1886 DNS Extensions to support IP version 6. S. Thomson, C. Huitema. December 1995. (Format: TXT=6424 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1886.txt
Updated by RFC2874 http://www.ietf.org/rfc/rfc2874.txt
RFC3152 http://www.ietf.org/rfc/rfc3152.txt

2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering. M. Crawford, C. Huitema. July 2000. (Format: TXT=44204 bytes) (***Updates RFC1886***) (Status: EXPERIMENTAL)
http://www.ietf.org/rfc/rfc2874.txt
Updated by RFC3152 http://www.ietf.org/rfc/rfc3152.txt
RFC3226 http://www.ietf.org/rfc/rfc3226.txt
RFC3363 http://www.ietf.org/rfc/rfc3363.txt
RFC3364 http://www.ietf.org/rfc/rfc3364.txt

3226 DNSSEC and IPv6 A6 aware server/resolver message size requirements. O. Gudmundsson. December 2001. (Format: TXT=12078 bytes) (***Updates RFC2535, RFC2874***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3226.txt

3363 Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS). R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain. August 2002. (Format: TXT=11055 bytes) (***Updates RFC2673, RFC2874***) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc3363.txt

3364 Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6). R. Austein. August 2002. (Format: TXT=26544 bytes) (***Updates RFC2673, RFC2874***) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc3364.txt

- Enrutamiento

1933 Transition Mechanisms for IPv6 Hosts and Routers. R. Gilligan, E. Nordmark. April 1996. (Format: TXT=47005 bytes) (Obsoleted by RFC2893) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc1933.txt

Obsoleted by RFC2893 http://www.ietf.org/rfc/rfc2893.txt

2080 RIPng for IPv6. G. Malkin, R. Minnear. January 1997. (Format: TXT=47534 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2080.txt

2185 Routing Aspects of IPv6 Transition. R. Callon, D. Haskin. September 1997. (Format: TXT=31281 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2185.txt

2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing. P. Marques, F. Dupont. March 1999. (Format: TXT=10209 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2545.txt

2711 IPv6 Router Alert Option. C. Partridge, A. Jackson. October 1999. (Format: TXT=11973 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2711.txt

2740 OSPF for IPv6. R. Coltun, D. Ferguson, J. Moy. December 1999. (Format: TXT=189810 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2740.txt

2893 Transition Mechanisms for IPv6 Hosts and Routers. R. Gilligan, E. Nordmark. August 2000. (Format: TXT=62731 bytes) (***Obsoletes RFC1933***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2893.txt

2894 Router Renumbering for IPv6. M. Crawford. August 2000. (Format: TXT=69135 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2894.txt

3178 IPv6 Multihoming Support at Site Exit Routers. J. Hagino, H. Snyder. October 2001. (Format: TXT=24453 bytes) (Status: INFORMATIONAL)

http://www.ietf.org/rfc/rfc3178.txt

- **Servicios y aplicaciones**

2133 Basic Socket Interface Extensions for IPv6. R. Gilligan, S. Thomson, J. Bound, W. Stevens. April 1997. (Format: TXT=69737 bytes) (Obsoleted by RFC2553) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2133.txt
Obsoleted by RFC2553 http://www.ietf.org/rfc/rfc2553.txt

2292 Advanced Sockets API for IPv6. W. Stevens, M. Thomas. February 1998. (Format: TXT=152077 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2292.txt

2428 FTP Extensions for IPv6 and NATs. M. Allman, S. Ostermann, C. Metz. September 1998. (Format: TXT=16028 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2428.txt

2461 Neighbor Discovery for IP Version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson. December 1998. (Format: TXT=222516 bytes) (***Obsoletes RFC1970***) (Status: DRAFT STANDARD)
http://www.ietf.org/rfc/rfc2461.txt

2472 IP Version 6 over PPP. D. Haskin, E. Allen. December 1998. (Format: TXT=29696 bytes) (***Obsoletes RFC2023***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2472.txt

2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. K. Nichols, S. Blake, F. Baker, D. Black. December 1998. (Format: TXT=50576 bytes) (***Obsoletes RFC1455, RFC1349***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2474.txt
Updated by RFC3168 http://www.ietf.org/rfc/rfc3168.txt
Updated by RFC3260 http://www.ietf.org/rfc/rfc3260.txt

2553 Basic Socket Interface Extensions for IPv6. R. Gilligan, S. Thomson, J. Bound, W. Stevens. March 1999. (Format: TXT=89215 bytes) (***Obsoletes RFC2133***) (Updated by RFC3152) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc2553.txt
Updated by RFC3152 http://www.ietf.org/rfc/rfc3152.txt

2675 IPv6 Jumbograms. D. Borman, S. Deering, R. Hinden. August 1999. (Format: TXT=17320 bytes) (***Obsoletes RFC2147***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2675.txt

2710 Multicast Listener Discovery (MLD) for IPv6. S. Deering, W. Fenner, B. Haberman. October 1999. (Format: TXT=46838 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc2710.txt

3089 A SOCKS-based IPv6/IPv4 Gateway Mechanism. H. Kitamura. April 2001. (Format: TXT=25193 bytes) (Status: INFORMATIONAL)
http://www.ietf.org/rfc/rfc3089.txt

3111 Service Location Protocol Modifications for IPv6. E. Guttman. May 2001. (Format: TXT=25543 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3111.txt

3122 Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification. A. Conta. June 2001. (Format: TXT=40416 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3122.txt

3162 RADIUS and IPv6. B. Aboba, G. Zorn, D. Mitton. August 2001. (Format: TXT=20492 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3162.txt

3175 Aggregation of RSVP for IPv4 and IPv6 Reservations. F. Baker, C. Iturralde, F. Le Faucheur, B. Davie. September 2001. (Format: TXT=88681 bytes) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3175.txt

3266 Support for IPv6 in Session Description Protocol (SDP). S. Olson, G. Camarillo, A. B. Roach. June 2002. (Format: TXT=8693 bytes) (***Updates RFC2327***) (Status: PROPOSED STANDARD)
http://www.ietf.org/rfc/rfc3266.txt