UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

DISEÑO DE UNA METODOLOGIA QUE PERMITA IMPLEMENTAR EL PROTOCOLO DE INTERNET VERSION 6 EN EMPRESAS O INSTITUCIONES CON APLICACIONES BASADAS EN EL PROTOCOLO TCP/IP VERSION 4.

PRESENTADO POR:

MARVIN RONALDI ARDON QUEZADA

JHONY MIKEL ESCOBAR GALDÁMEZ

RAMÓN REYES LEIVA DÍAZ

PARA OPTAR AL TITULO DE

INGENIERO DE SISTEMAS INFORMATICOS

CIUDAD UNIVERSITARIA, JUNIO DE 2007.

UNIVERSIDAD DE EL SALVADOR

RECTORA :

DRA. MARIA ISABEL RODRIGUEZ

SECRETARIA GENERAL :

LICDA. ALCIA MARGARITA RIVAS DE RECINOS

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO :

ING. MARIO ROBERTO NIETO LOVO

SECRETARIO :

ING. OSCAR EDUARDO MARROQUIN HERNANDEZ

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

DIRECTOR :

ING. JULIO ALBERTO PORTILLO

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

TRABAJO DE GRADUACION PREVIO A LA OPCION AL GRADO DE:

INGENIERO DE SISTEMAS INFORMATICOS

TITULO :

DISEÑO DE UNA METODOLOGIA QUE PERMITA IMPLEMENTAR EL PROTOCOLO DE INTERNET VERSION 6 EN EMPRESAS O INSTITUCIONES CON APLICACIONES BASADAS EN EL PROTOCOLO TCP/IP VERSION 4.

PRESENTADO POR :

MARVIN RONALDI ARDON QUEZADA

JHONY MIKEL ESCOBAR GALDÁMEZ

RAMÓN REYES LEIVA DÍAZ

TRABAJO DE GRADUACION APROBADO POR :

DOCENTE DIRECTOR :

ING. PEDRO ELISEO PEÑATE

SAN SALVADOR, JUNIO DE 2007.

TRABAJO DE GRADUACION APROBADO POR:

DOCENTE DIRECTOR :

ING. PEDRO ELISEO PEÑATE

AGRADECIMIENTOS

Agradecemos de manera muy especial la constante y desinteresada colaboración de nuestro asesor Ing. Pedro Eliseo Peñate en la realización de este trabajo de graduación.

MARVIN
MIKEL
RAMÓN

DEDICATORIA

A Dios todopoderoso.

A mi madre por su valioso apoyo incondicional.

A la memoria de mi abuela materna.

A mi hermano y tios por su constante apoyo e interés.

Y a todos aquellos con los he compartido grandes momentos, especialmente a mis compañeros de trabajo de graduación.

Gracias a todos.

Marvin Ronaldi

DEDICATORIA

A Dios todopoderoso por darme la oportunidad de culminar esta etapa de mi vida, por todas las bendiciones y el amor que siempre me han dado fuerzas para seguir adelante a pesar de las dificultades.

A mi padre Miguel Escobar, a mi madre Antonia Galdámez y a mi hermano Roger Escobar, por la confianza, el apoyo y el amor que siempre me han tenido. Con estas líneas agradezco especialmente, todo el esfuerzo y sacrificio incondicional con el que mis padres me han ayudado a culminar mis estudios.

A toda mi familia y amigos que con su ayuda y consejos han orientado mi vida.

A mis compañeros de tesis Marvin y Ramón.

Mis agradecimientos.

Jhony Mikel

DEDICATORIA

A mi Dios bueno y perfecto: Padre, Hijo y Espíritu Santo, y a la Santísima Madre Celestial que me heredó, por las innumerables bendiciones que siempre me ha prodigado.

A la memoria de mi querido padre.

A mi fabulosa madre por su incondicional amor y comprensión.

A mis hermanos y sus familias, especialmente a mis sobrinos por la oportunidad de poder volver a jugar.

A todos aquellos que me han brindado su amistad a lo largo de los años, particularmente aquellos provistos de un gran corazón y un alma de niño.

A mis compañeros de trabajo de graduación por las interminables noches de risas y tormentos, entre aciertos y desaciertos, pero al fin de muchas satisfacciones.

Mi eterna gratitud.

Ramón.

CONTENIDO

INTRODUCCIÓN.

El protocolo de Internet versión 6 (IPv6) es el futuro de Internet pudiendo vislumbrarse no muy lejano su introducción en nuestro país. IPv6 fue lanzado como estándar por IETF el 6 de junio de 2006 y con este acontecimiento se abre al mundo las posibilidades de mejorar las técnicas existentes de comunicación de datos. IPv6 presenta muchas mejoras y beneficios frente a su antecesor IPv4, aún vigente, entre las que se pueden mencionar: el aumento del espacio de direccionamiento, mejora en la seguridad y calidad de servicios, así como el fortalecimiento del mecanismo de movilidad, principalmente para telefonía móvil.

Todo lo anterior señala la importancia que puede tener todo esfuerzo encaminado a preparar el camino para una transición al nuevo protocolo. Esto comienza con preparar un acopio de conocimiento que provea la base teórica para una posterior puesta en práctica de los mecanismos que puedan hacer posible que un conjunto de computadoras que basen su comunicación en IPv4, puedan luego hacerlo también en IPv6 sin entrar en mayores complicaciones.

Por esa razón se ha desarrollado un *Manual de Referencia del Protocolo de Internet versión 6*, llevando a cabo una investigación de los fundamentos teóricos básicos que permiten describir las características principales del Protocolo de Internet versión 6, tales como: las *especificaciones básicas* del protocolo IPv6, además se describe el manejo del nuevo *direccionamiento* y cómo se definen todos los tipos de direcciones con las que trabaja IPv6. También se detallan las características, los formatos y el proceso necesario para la creación de subredes. De igual manera, se puntualiza sobre el funcionamiento de otros protocolos que conforman la pila TCP/IP versión 6, entre los que se mencionan: *ICMPv6, DHCPv6, ND, IND, UDP, TCP y SCTP*. Conjuntamente se describen las técnicas de *ruteo* en IPv6 tomando como caso de estudio el protocolo de información de ruteo *RIPng*. Asimismo, se explica el uso del *Sistema de Nombres de Dominio (DNS,)* más específicamente, el proceso de resolución de nombres de dominio con direcciones IPv6. Por otra parte, se detalla la implementación del protocolo IPv6 en redes móviles e inalámbricas, así como una introducción al tema de seguridad en las comunicaciones en IPv6 con el protocolo de seguridad IPsec. Se continua haciendo una referencia al comportamiento de IPv6 sobre algunas tecnologías de enlace, como *Ethernet, PPP, ATM y Frame Relay* Adicionalmente, se describen las técnicas existentes que posibilitan la comunicación entre redes heterogeneas, es decir, mezcla de IPv4 e IPv6, y a establecer una *metodología de general para implementar la transición de IPv4 a IPv6.* Como un producto derivado del estudio, se incluye en el manual un ejemplo práctico de configuración de un sitio desarrollado sólo en IPv6.

También hay que tomar en consideración una de la inquietudes más desafiantes sobre la situación actual de las redes basadas en IPv4; y es la idea de qué pasaría con las aplicaciones que una empresa u organización tenga en operación, al iniciar un proceso de transición de IPv4 a IPv6. Con ese fin, se ha agregado como un estudio aparte del manual mencionado, una introducción al concepto de *interfaz socket* y a su manejo, para luego levantar una prueba que permite hacer una inferencia sobre la operación transparente de pasar de una ejecución en IPv4 a una ejecución en IPv6 de una aplicación corriente, sin experimientar mayores requerimientos.

Además, se practican una serie de encuestas, previamente diseñadas, en empresas de diversa índole de nuestro medio, con el objeto de evaluar el estado de actualización de los componentes humano, software y hardware respecto a IPv6 y que permita sugerir adecuaciones y/o sustituciones con vista a llevar a cabo el punto culminante de toda esta investigación, la implementación de una *Metodología de transición a IPv6*. Todo esto conlleva a una definición pormenorizada de ésta y a plasmarla en un ejemplo aplicado a una empresa típica, generada hipotéticamente a partir de las características presentadas por las empresas encuestadas.

OBJETIVOS

A. Generales.

Realizar una investigación para formar una base teórica que permita desarrollar una manual de referencia que sirva como consulta general sobre el uso del Protocolo de Internet versión 6, IPv6, y de las especificaciones básicas necesarias para migrar a esta nueva tecnología.

Verificar el uso que hacen las empresas o instituciones en nuestro medio de aplicaciones operando en redes basadas en el Protocolo de Internet versión 4, con la idea de desarrollar pautas que sirvan para definir una metodología general para la migración de estas redes y sus aplicaciones en operación, al nuevo Protocolo de Internet IPv6.

B. Específicos.

Realizar una investigación documental acerca del protocolo IPv6 con el objeto de obtener el conocimiento pertinente sobre el funcionamiento y aplicación del nuevo protocolo de Internet.

Recopilar la documentación de normativas del protocolo de Internet IPv6 conocidas como RFC´s, con el objeto de conocer todo las recomendaciones que se deben seguir al momento que se requiera migrar al uso de este nuevo protocolo de Internet

Redactar un manual de referencia sobre el Protocolo de Internet versión 6 en base a la investigación documental, recopilación de normativas y cualquier otra información recabada de fuentes versadas en el tema.

Obtener información y plantear pruebas que sirvan para medir el comportamiento de los programas de aplicación existentes en una red empresarial en el caso de ocurrir una transición de IPv4 a IPv6.

Llevar a cabo una investigación de campo para recolectar la información necesaria sobre todos los tipos de recursos de red empleados en empresas de nuestro medio, con el fin de inferir los cambios o sustituciones imprescindibles que sirvan de guía para una transición ordenada a IPv6.

Establecer una metodología para la migración del Protocolo de Internet versión 4 al Protocolo de Internet versión 6, de modo que pueda ser seguida por empresas o instituciones interesadas en que sus redes y aplicaciones basadas en Internet o intranets, funcionen correctamente al hacer uso del nuevo protocolo de Internet.

ALCANCES.

La investigación de campo se realizará solo en empresas nacionales, contando con una muestra representativa de la población total de usuarios del protocolo de Internet.

Cualquier empresa o institución que utilice aplicaciones basadas en los protocolos TCP/IP versión 4 puede hacer uso de este trabajo para realizar el proceso de migración de sus redes y aplicaciones en operación, a la pila de protocolos TCP/IP versión 6.

LIMITACIONES.

No existe hasta la fecha, una experiencia previa en la implementación del protocolo IPv6 en nuestro país, que pudiera servir de punto de inicio para enriqueser esta investigación.

La información a la que se tiene acceso sobre esta nueva tecnología esta destinada más que todo a personas, involucradas en el medio informático, muy informadas y específicamente aquellas versadas en el área de las comunicaciones entre dispositivos que utilizan IP.

IMPORTANCIA.

No cabe duda que Internet es un recurso que ha revolucionado las comunicaciones modernas, hoy en día se habla de la expansión que dicho recurso esta experimentando en todo el mundo. Cada vez más se unen a ella grandes cantidades de usuarios nuevos, conduciendo esto a un crecimiento a ritmo acelerado, demandando de esta forma aplicaciones sencillas, portables y transparentes por parte de sus usuarios. Unido a ello, el constante proceso de innovación tecnológica desarrollado a nivel mundial, ha propiciado la aceleración de la tendencia de las comunicaciones en formato multimedia (incluyendo la telefonía móvil) hacia un formato basado en tecnología IP.

Por tal razón es importante el asegurar que dicho recurso éste disponible siempre y que su utilización nunca se detenga. Bajo este contexto la situación actual brinda el panorama siguiente: en algunas regiones del mundo, en las que figuran algunos de los países más desarrollados, existe propensión hacia el agotamiento de direcciones IP versión 4, estimulando la cuenta de nuevos procesos de migración del protocolo actual a IP versión 6 ya ejecutados.

Como se puede verificar de algunas fuentes de nuestro medio, se observa que el crecimiento de Internet en nuestro país es significativo, manteniendo un aumento de nuevos usuarios que demandan cada vez una mayor calidad en los medios técnicos y velocidad de conectividad de los principales enlaces de comunicación de Internet (ISP). Esto ha traído como consecuencia la ocupación de una parte importante del bloque direcciones IP asignado a nuestro país,

involucrando la introducción del uso de servidores NAT por parte de proveedores de servicios de Internet. Eso no quiere decir que en un futuro, el mismo desarrollo de la implementación del nuevo protocolo en países desarrollados, con la importancia que tienen sus redes por el nivel de tráfico y por la tecnología que esto implica, nos lleve a que finalmente por esa inercia nuestro país tenga que migrar a IPv6 sin haber agotado sus direcciones IP versión 4. Esto fundamenta el requerimiento de desarrollar una metodología que permita implementar el protocolo de Internet versión 6 como un preparativo oportuno en el caso de presentarse la necesidad de realizar dicha migración en empresas o instituciones de nuestro medio, con antelación a lo previsible.

RESULTADOS ESPERADOS DEL PROYECTO.

Llevar a un buen término este proyecto propiciará los siguientes beneficios:

1. Las empresas o instituciones en nuestro país contarán con un manual de referencia que las personas interesadas podrán consultar, con el fin de conocer los detalles de una situación que puede no tardar mucho en presentarse, la transición de IPv4 a IPv6, cuestión que no es del dominio del usuario común de redes y que requerirá de fuentes de información como está.
2. Las empresas o instituciones en nuestro país tendrán a la mano los procedimientos aplicables a las situaciones más frecuentes en que se pueden encontrar sus aplicaciones y así poder tomar las decisiones adecuadas.
3. El país contaría con un esfuerzo inicial que podría desencadenar una serie de otros esfuerzos orientados a la preparación de los interesados potenciales para la migración a IPv6, todo esto a partir de un estudio como el que se plantea.
4. Haría asequible a los estudiantes de las carreras en Tecnología de Información y Comunicaciones (TIC), un material adecuado y actualizado para su proceso de aprendizaje.
5. Involucraría la Universidad de El Salvador en la tarea de estar a la vanguardia en las TIC y como una institución precursora de investigaciones en esta área, como miembro de SVNet y de otros proyectos similares.

JUSTIFICACIÓN DEL ESTUDIO.

Tomando en cuenta los argumentos expuestos en la importancia de la situación propia de nuestro país, se debe anticipar una transición del protocolo TCP/IP versión 4 al protocolo TCP/IP versión 6 como un aspecto clave en el desarrollo futuro de la interconexión de redes locales a la red mundial debido a las siguientes condiciones que se vienen presentando con el uso de protocolo actual de Internet:

- Una futura escasez de direcciones IP.
- Incremento desordenado de sistemas interconectados.
- Saturación de las redes, presentando un tiempo de respuesta largos.

- Dificultad en la incorporación de nuevas funcionalidades.
- Poca transparencia en la identidad de los usuarios conectados a Internet, que propicia fraudes y fallos de la seguridad de las redes.

Los aspectos antes mencionados se verán notablemente mejorados con la implementación del protocolo IPv6, de la siguiente manera:

- Mayor espacio de direccionamiento.
- Seguridad intrínseca de IP.
- Autoconfiguración.
- Movilidad.
- Incremento progresivo del tiempo de búsqueda DNS (Servidor de nombres de dominio).
- Evitar la solución temporal del NAT (Traductor de direcciones de red)
- Incremento en los QoS (Calidad de servicios).
- Disminución de los cuellos de botella en los Routers (tablas de enrutamiento más pequeñas).

Por tanto se hace esencialmente necesario que en países como el nuestro se generen los estudios basados en las características propias de nuestro entorno para que empresas u organizaciones puedan seleccionar un mecanismo que sea adecuado para una futura implementación del nuevo protocolo de Internet, y que estas puedan tener las herramientas para colocarse a la vanguardia en el uso de tecnologías de información y comunicaciones.

MANUAL DE REFERENCIA DEL PROTOCOLO DE INTERNET VERSIÓN 6.

1. GENERALIDADES.

A. INTRODUCCIÓN.

Un protocolo es un conjunto de reglas expresadas a través de un software que permite gestionar y establecer la comunicación entre computadoras conectadas en red. Estos mecanismos permiten que un programa de aplicación que utilice una red para intercambiar mensajes, no interactúe directamente con el hardware de la red sino que lo haga indirectamente por medio del software de los protocolos de comunicación que se encargarán de ir llevando los mensajes por etapas o capas funcionales que componen el ejercicio de la comunicación entre computadoras. Estas capas conforman una concepción que permite comprender de forma metódica la interacción entre los componentes que intervienen directamente en la comunicación entre computadoras y que se conoce como el modelo de capas. Un protocolo específico está ideado para operar en determinada capa del modelo. Donde el denominado modelo OSI constituido por 7 capas diferenciadas, ha sido el patrón para explicar cuanto esfuerzo se ha hecho por establecer reglas en la comunicación de computadoras, un marco de referencia para el desarrollo de protocolos estándares. La más exitosa concreción de un modelo de clasificación de las funciones de comunicación es el conjunto de protocolos que conforman la suite TCP/IP, la cual ha hecho posible la comunicación entre dispositivos distantes unos de otros por medio de Internet. El éxito del modelo TCP/IP no se ha debido a que se concibiera siguiendo el entorno del modelo OSI, pues éste es posterior al primero, sino a su probada eficacia al haberse convertido en la estructura en que se basa la red de redes, la Internet global.

B. EL MODELO OSI.

El modelo de referencia OSI o de Interconexión de Sistemas Abiertos también es llamado modelo ISO por su desarrollador, la Organización Internacional para la Normalización. Fue inicialmente propuesto en 1977 pero se convirtió en estándar final hasta 1984. Es un modelo teórico de arquitectura de red, pues no especifica los servicios que una capa provee a la capa superior, ni los protocolos usados en cada una de ellas, sólo dice lo que debe hacer cada capa.
El modelo OSI está constituido por siete capas:

1) Aplicación
2) Presentación
3) Sesión
4) Transporte
5) Red
6) Enlace de datos
7) Física.

Cada capa de este modelo maneja una serie de funciones que debe ejecutar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. Las cuatro capas inferiores (Física, de Enlace de Datos, de Red y de Transporte) son las encargadas de la transmisión de los datos (segmentación, empaquetamiento, encaminamiento, verificación y transmisión por los medios físicos), sin importarles el tipo de datos que se transmiten ni la aplicación que los envía o recibe. En cambio, las tres capas superiores (de Sesión, de Presentación y de Aplicación) son las encargadas de establecer las sesiones de comunicación entre aplicaciones, del formateo, cifrado y compresión de datos y además de proporcionar los mismos a las aplicaciones de usuario adecuadamente.

En la figura 1.B.1 se muestra un esquema de dos equipos comunicándose según el detalle de las capas de este modelo.

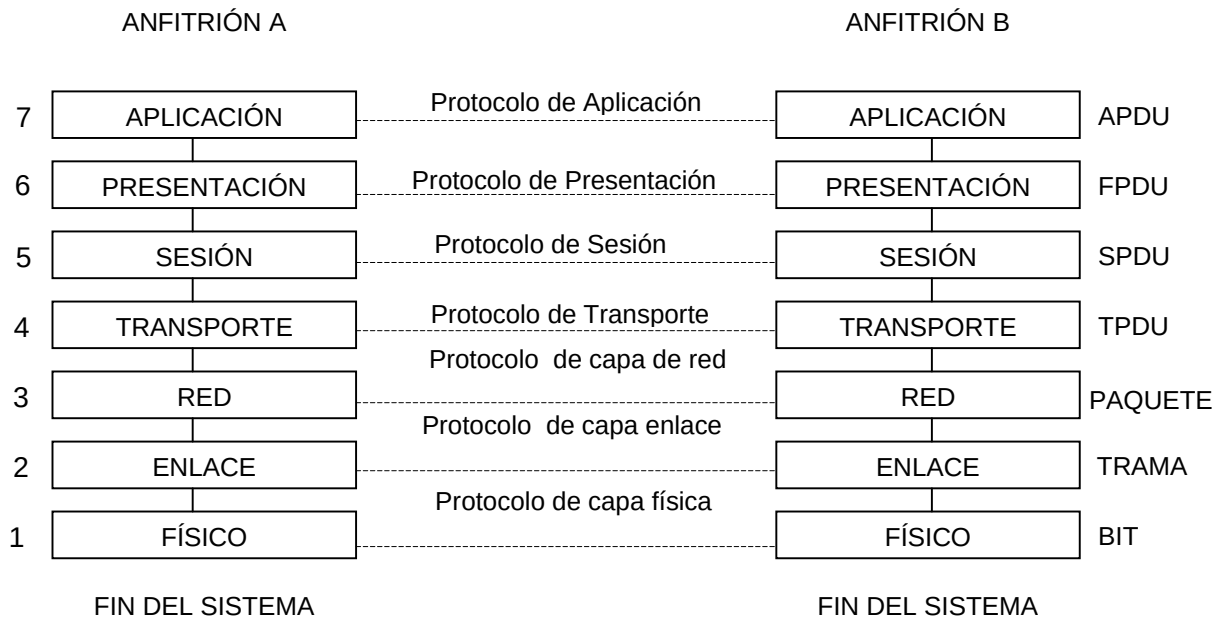


Figura 1.B.1: *Esquema OSI de dos equipos en comunicación*

Donde:
PDU: unidad de datos de protocolo

C. LOS PROTOCOLOS TCP/IP.

El Conjunto de protocolos TCP/IP fue desarrollado gracias a la imperiosa necesidad que el Ejército de los EUA tenía de conectar sus múltiples redes físicas distantes entre sí. Aunque el gobierno de EUA participaba del esfuerzo de estandarización de ISO y consecuentemente de la creación del modelo OSI, los militares financiaron la investigación a través de su agencia ARPA (Agencia de Proyectos de Investigación Avanzada), que en unión de algunas universidades de EUA daría como resultado la consecución de lo que, luego de su completo desarrollo, se convertiría en la suite TCP/IP. El camino fue largo pero se desarrolló antes que el modelo OSI pudiera generar frutos similares. El camino inicio con un precursor, el NCP, que conectó a cuatro universidades, hasta llegar a la versión 4 del que recibiría el nombre oficial de TCP/IP de dos de sus protocolos más importantes, en 1979, hasta la declaración del estándar en 1981 (RFC 791).
Aunque no existe pila oficial de capas para representar el modelo TCP/IP, se podría tomar como referencia una pila conformada por cinco capas:

1) *Aplicación:* Provee comunicación entre procesos y aplicaciones entre equipos distantes
2) *Transporte o origen-destino:* Provee servicio de transferencia de datos, sin importar su naturaleza, de extremo a extremo
3) *Internet:* Gestiona el acceso y encaminamiento de los datos a través de la red
4) *Acceso a la red o interfaz de red:* Gestiona el intercambio de datos entre el sistema final y la red a la que se está conectado.
5) *Física:* Define la interfaz física entre el dispositivo de transmisión de datos y el medio de transmisión

En este esquema de capas detallado en la tabla 1.C.1 no se requiere pasar por todas las capas intermedias para llegar a otra, así se tienen protocolos de aplicación que actúan directamente sobre IP. Asimismo, se presenta un detalle de algunos de los protocolos de TCP/IP ubicados según su función dentro del modelo de cinco capas.

Capa TCP/IP	Protocolo asociado
Aplicación	BGP: Protocolo de pasarela de frontera FTP: Protocolo de transferencia de archivos HTTP: Protocolo de transferencia de hipertextos SMTP: Protocolo sencillo de transferencia de correo electrónico TELNET: Protocolo de Red Teletipo SNMP: Protocolo sencillo de gestión de redes RIP: Protocolo de información de encaminamiento DNS: Sistema de nombres de dominio MIME: Extensiones multipropósito de correo electrónico en Internet
Transporte	TCP: Protocolo de control de transmisión UDP: Protocolo de datagrama de usuario
Internet	IP: Protocolo de Internet ICMP: Protocolo de control mensajes en Internet IGMP: Protocolo de gestión de grupos de Internet OSPF: Protocolo abierto del primer camino más corto RSVP: Protocolo de reserva de recursos ARP: Protocolo de resolución de direcciones RARP: Protocolo de resolución de direcciones invertido
Enlace	Ethernet, Token ring, FDDI, ATM, Frame relay
Físico	Medio físico, técnicas de codificación

Tabla 1.C.1: *Esquema en capas de la suite TCP/IP*

Dentro de esta pila de protocolos, el más utilizado es el denominado Protocolo de Internet, o simplemente IP, del cual la versión más utilizada es la versión 4. Este protocolo ha probado ser muy eficaz y operable, especificando que a cada equipo o anfitrión se le asigne un único número de 32 bits conocido como su dirección IP.
Hoy en día, debido a la explosión en la utilización de Internet y a las cada vez más complicadas aplicaciones que se generan, se han evidenciado las limitaciones que este esquema de direccionamiento IPv4 tiene que sobrellevar.

D. EL SURGIMIENTO DE IPV6.

Debido a la tendencia que mostraba el crecimiento de usuarios en Internet y a la demanda de nuevas direcciones IP versión 4 a esta fecha, el IETF (Grupo de esfuerzo de Ingeniería de Internet), organismo promotor de la normalización y la arquitectura de Internet, comenzó en 1990 a evaluar este contexto y procedió a la recomendación de gestar un nuevo estándar que inicialmente se denominó IPng (Protocolo de Internet de próxima generación) y que luego se convertiría en IPv6 (Protocolo de Internet versión 6). En su conjunto se presentaba toda una problemática subyacente con el uso de IPv4, pero una de las más importantes sería el limitado espacio de direccionamiento, que debido a su ineficiente utilización se preveía que no podría hacer frente a la creciente demanda de conexión de toda clase de dispositivos, con la calidad de servicio requerida. Es así, que en 1995 se publica el RFC 1752 con las especificaciones del protocolo, pasando esta

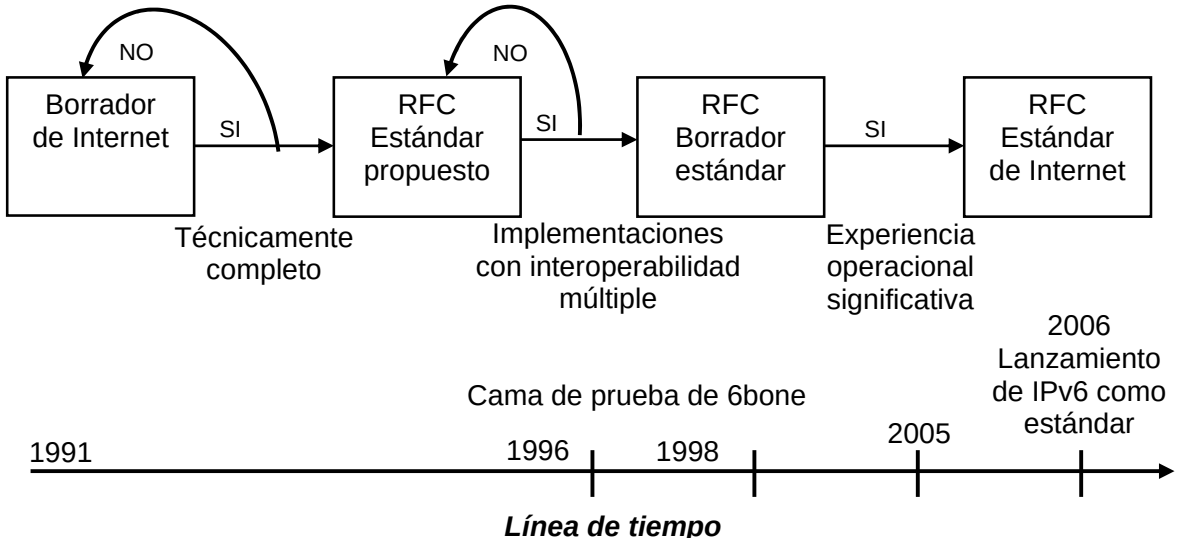
recomendación a borrador de estándar en1998. Asimismo, el IETF auspició grupos de tarea para definir todos los estándares requeridos y los mecanismos necesarios para propiciar una coexistencia o una transición ordenada de IPv4 a IPv6. Una lista detallada de RFCs y de borradores (drafts) que comprende toda la temática de IPv6 que se tratará, se incluye en el Anexo A. Hay que agregar que el camino para llegar a IPv6 fue recorrido por varias propuestas de candidatos para suceder a IPv4, que fueron siendo descartados o absorbidos paulatinamente hasta llegar al resultado final que ahora se conoce. Un listado de estos candidatos se puede ver en la tabla 1.D.1

Nombre de protocolo	Nombre completo	Referencia
IP encaps	Encapsulamiento de Protocolo de Internet	RFC1955
SIP	Protocolo Simple de Internet	
PIP	Protocolo de Internet P	RFC1621, RFC1622
CLNP simple	Protocolo Simple de Capa de Enlace de Modo sin Conexión	
Nimrod	Nueva Arquitectura de Direccionamiento y Ruteo IP	RFC1753, RFC1992
TP/IX	TP/IX: próximo Internet	RFC1475
IPAE	Encapsulamiento de Dirección IP	
TUBA	TCP y UDP con Direcciones más grandes, TCP/UDP sobre redes direccionadas con CLNP	RFC1347, RFC1561
CATNIP	Arquitectura Común para IP de nueva generación	RFC1707
SIPP	Protocolo Simple de Internet Plus	RFC1710
SIPP versión 128 bits	Protocolo Simple de Internet Plus, versión de 128 bits	
IPng	Protocolo de Internet de nueva generación	RFC1883
IPv6	Protocolo de Internet versión 6	RFC1883

Tabla 1.D.1: *Candidatos a protocolo IPng*

E. LA RUTA DE ESTANDAR PARA IPV6.

Los RFC (Request for Comments) son documentos hechos llegar al IETF, por personas vinculadas a esta organización, con el objeto de que sean comentadas y se presenten sugerencias que las mejoren. Cuando una recomendación de éstas está orientada a convertirse en un estándar tiene que seguir un proceso antes de su aprobación como tal.
El camino que ha seguido IPv6 para llegar a ser estándar puede visualizarse en la figura 1.E.1



Modificado a partir de la siguiente fuente: Yanick, Pouffary, Compaq

Figura 1.E.1: *Camino hacia el estándar de IPv6*

Es así, como el día 6 de junio de 2006, fue lanzado oficialmente IPv6 como un estándar, terminando un periodo de prueba de más de 10 años en su paso por la "Standards Track" (Huella de estándares)

En principio parece que los problemas para implementar IPv6 no llegarán a ser demasiados, bastaría que los proveedores de servicios de Internet (ISP´s) inviertan un poco para su puesta en marcha. Muchos obstáculos ha sido allanados, pero también es de tomar en cuenta el poco interés que puedan mostrar la gente encargada de Tecnologías de Información en las empresas, cuando se puede afirmar que IPv4 todavía trabaja bien, y no se vislumbra un crisis potencial como la ocurrida con el cambio de milenio (Y2K).

F. BENEFICIOS DE IPV6.

Las limitaciones e inconvenientes que IPv4 presenta en estos momentos pueden ser superadas por las mejoras que IPv6 trae consigo, entre las que se tienen:

1) *Espacio de direccionamiento ampliado:* De un espacio de direcciones de 32 bits de más de 4 mil millones que ofrece IPV4 se pasa a un espacio de direcciones de 128 bits de más de 340 sextillones.
2) *Mecanismo de opciones mejorado:* Las opciones de IPv6 se manejan en cabeceras separadas, las cuales no se examinan ni son procesadas por dispositivos de encaminamiento alguno, simplificando y acelerando su enrutamiento.
3) *Formato de cabecera simplificado:* La simplificación del formato de cabecera favorece un encaminamiento más rápido.
4) *Autoconfiguración:* Funcionamiento como *plug & play (conecte y juegue)*, que permite que un nodo que se conecta a la red reciba los datos necesarios por parte del router, para iniciar inmediatamente a comunicarse.
5) *Mejores mecanismos de movilidad:* Permite dejar una red y conectarse a otra sin apenas percibir los cambios efectuados, tal como lo requiere la telefonía móvil.
6) *Etiquetado del flujo:* Secuencia de paquetes enviados desde un origen para el cual solicita un tratamiento especial de parte de los routers.
7) *Autentificación y privacidad mejorada:* las medidas de seguridad son mejoradas. Así, IPsec es un parte del núcleo de IPv6, mientras que para IPv4 no es un requisito. Hay gran facilidad de autenticar y de encriptar datos de forma transparente.

8) *Ruteo jerárquico:* Se sigue el patrón de IPv4 utilizando el mecanismo de CIDR (Ruteo entre Dominios sin Clases), permitiendo que las tablas de encaminamiento no sean grandes, acelerando el paso de los mensajes.
9) *Multi-Homing (Multiasentamiento):* que facilita estar conectado a más de un proveedor de servicios sin mayores complicaciones.
10) *Multicast y Anycast:* Envío de un mismo paquete a un grupo de receptores, o bien, de un paquete a un solo receptor dentro de un grupo, todo esto de forma transparente.
11) *Manejo de paquetes de gran tamaño:* Es posible el manejo de paquetes con carga útil hasta de 65,575 octetos, 524600 bits.

G. LA TRANSICIÓN DE IPV4 HACIA IPV6

Los entendidos han venido manejando la idea de que la transición de IPv4 a IPv6 llevaría un relativamente largo periodo, pero ahora que ya ha sido liberado IPv6 como estándar, la situación tomará otro impulso y dependerá de las condiciones en que se encuentren las redes propensas a la migración para acelerar el proceso. Hay que visualizar que ya hay una cantidad de nodos IPv6 funcionando y que se empieza un proceso por ahora de coexistencia ante una mayoría de nodos IPv4, obligando a nodos IPv6 a encapsular su mensajes en IPv4, pero esta es una realidad que no será eterna. De tal manera, que los escenarios y los mecanismos necesarios para la migración de una red de IPv4 a IPv6 serán al inicio muy diversos y necesitarán de buenos criterios en el manejo de las herramientas que se recomiendan en documentación como *RFCs* o *drafts* para lograrlo. En unos cinco años los cerca de un millar sitios que corren a la fecha en IPv6 se multiplicarán y las dificultades para una migración se irán soslayando.

H. TENDENCIAS ORIGINADAS POR IPV6

El crecimiento de la red global seguirá incontenible, más ahora que ya existe una salida oficial a las limitaciones que sostiene IPv4. El uso de dispositivos cada vez más complejos conectados a la red requiriendo una dirección IP individual, agregado al consenso de varios fabricantes de software y de hardware de redes por incorporar IPv6 a sus productos, sumado al esfuerzo de una cantidad de instituciones y organismos que han participado en redes de prueba que ya funcionan en IPv6, y complementado finalmente con la definitiva incorporación de IPv6 como un estándar de Internet hace vislumbrar que no está muy lejano el día en que las comunicaciones en la educación, la investigación científica, la industria, el comercio y demás rubros económicos, en todas las latitudes, se enfocarán sobre el uso de la nueva versión del protocolo de Internet, IPv6.

2. ESPECIFICACIONES DEL PROTOCOLO DE INTERNET IP VERSIÓN 6 (IPv6)

A. INTRODUCCIÓN.

La cabecera del nuevo protocolo de Internet IPv6 ha pasado de tener 12 campos utilizados en el protocolo IPv4 a solo 8 campos. Esto debido a que han sido eliminados los campos que nos son necesarios por que provocan redundancia en el tratamiento de la información de la cabecera IPv4. A la cabecera del protocolo IPv6 se le llama también *Cabecera IPv6 básica.*

El protocolo de Internet IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables y una autoconfiguración más simple de direcciones.

Dentro de la cabecera del protocolo de Internet IPv6 existe un campo llamado *Siguiente Cabecera (Next Header)* que permite utilizar ciertas características avanzadas que posee la cabecera IP y que ayudan a incorporar opciones que mejoran la calidad del paquete que se envía. Estas opciones avanzadas reciben el nombre de *Cabecera IPv6 extendida.*

B. FORMATO DE LA CABECERA BÁSICA DEL PROTOCOLO IPv6.

El formato de la cabecera del protocolo de Internet IP versión 6, se encuentra detallado en el figura 2.B.1.

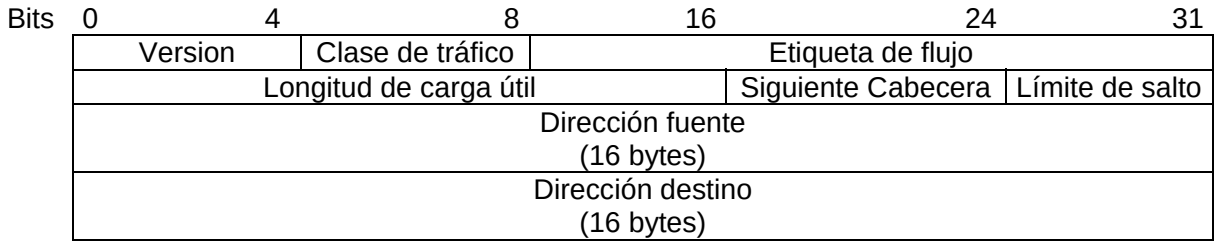


Figura 2.B.1: *Formato de la cabecera IPv6.*

Los campos que posee la cabecera IPv6 se definen a continuación:

1) *Versión* (4 bits).
Especifica el número de la versión del protocolo de Internet (Número = 6 para el caso del nuevo protocolo de Internet IPv6).

2) *Clase de Tráfico (Traffic Class*) (4 bits).
Indica la prioridad de transmisión y de entrega de cada paquete frente a otros paquetes del mismo remitente.

Los paquetes son clasificados como pertenecientes a un mismo tráfico, para que el nodo que envía el paquete proporcione un control de congestión o tráfico.

3) *Etiqueta de Flujo (Flow Label)* (24 bits).
Es el valor que identifica a todos los paquetes que forman parte del mismo flujo.

Ninguna etiqueta de flujo tiene un significado especial; en consecuencia, el tratamiento especial que se da al flujo de paquetes se debe declarar mediante información insertada en alguna cabecera adicional.

El uso y la semántica del campo *Etiqueta de Flujo* es la siguiente:

a) Un flujo es una secuencia de paquetes enviada desde un origen determinado hacia un destino (unienvío o multienvío) determinado para el cual el origen desea un tratamiento especial por los routers intermedios, por ejemplo, en una opción de salto a salto.
b) Una etiqueta de flujo se asigna a un flujo en el nodo origen del flujo. Deben escogerse nuevas etiquetas de flujo aleatoriamente y uniformemente del rango 1 al FFFF en hexadecimal. El propósito de la asignación al azar de las etiquetas de flujo es para hacer cualquier conjunto de combinaciones de bits dentro de este campo para que los routers lo usen como una clave para buscar el estado asociado con el flujo.
c) Deben enviarse todos los paquetes que pertenecen al mismo flujo con la misma dirección origen, dirección destino, y etiqueta de flujo. Si alguno de los paquetes incluye una cabecera extendida (*las cabeceras extendidas se presentan en el apartado B de este capitulo*) todos los paquetes deben originarse con los mismos datos de la cabecera extendida. Se permite a los routers verificar que estas condiciones se cumplen. Si una violación se detecta, debe reportarse al nodo origen en un mensaje ICMP de *Problema de Parámetro* (Código 0, apuntando al octeto de mayor orden del campo Etiqueta de Flujo).
d) En el nodo que envía el paquete se especifica el tiempo de vida máximo de cualquier flujo en estado de tratamiento.
e) Cuando un nodo se detiene ó reinicia (por ejemplo, como resultado de una “caída"), debe tener el cuidado de no utilizar una etiqueta de flujo que podría haber utilizado para un flujo anterior cuyo tiempo de vida pueda no haber expirado aún. Esto puede lograrse registrando el uso de las etiquetas de flujo sobre un almacenamiento estable para que esto pueda tenerse presente durante las caídas, o absteniéndose de usar cualquier etiqueta de flujo hasta que el tiempo de vida máximo de cualquier posible flujo previamente establecido haya expirado.

4) *Longitud de Carga Útil (Payload Length)* (16 bits).
Longitud del resto del paquete IPv6 excluida la cabecera.

5) *Siguiente Cabecera (Next Header)* (8 bits).
Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6

Este campo es presente en todas las cabeceras extendidas.

6) Límite de Salto (Hop Limit) (8 bits).
Entero sin signo de 8 bits, que es decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es decrementado hasta cero.

7) Dirección (Address) (128 bits cada una).
La dirección del nodo que envía el paquete es la *Dirección Fuente* (Source Address) y la dirección del nodo donde pretende llegar el paquete, posiblemente no el último si está presente una cabecera de Ruteo, es la *Dirección Destino (Destination Address)*

C. Cabecera IPv6 Extendida.

En el protocolo IPv6 se puede incorporar información opcional para mejorar la calidad del paquete que se envía, dicha información se codifica en cabeceras separadas que se colocan entre la cabecera básica IPv6 y la cabecera de capa superior (ej. Protocolo de transporte como el TCP y el UDP, protocolos de control como el ICMP, protocolos de enrutamiento) dentro de un paquete. Como hemos dicho anteriormente cada una de estas cabeceras de extensión es identificada por un valor en el campo *Siguiente Cabecera*. Como se ilustra en la figura 2.C.1. Según lo descrito en

estos ejemplos un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el campo *Siguiente Cabecera* de la cabecera precedente. Cada cabecera de extensión es un entero múltiplo de 8 octetos de largo.

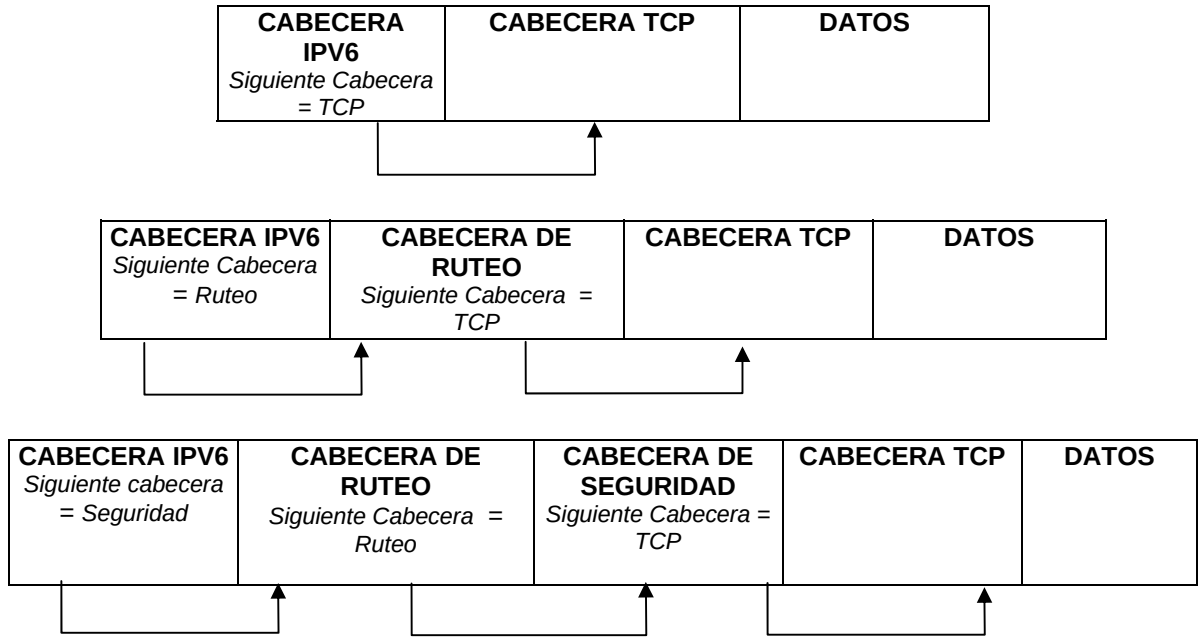


Figura 2.C.1: *Ejemplos de cabecera de extensión.*

Los valores asignados que definen las cabeceras de extensión para el campo *Siguiente Cabecera* se muestran en la tabla 2.C.1.

VALOR	CABECERA	REFERENCIA
0	Opciones de Salto a Salto	RFC2460
1	ICMPv4	RFC2460
4	IP en IP (encapsulamiento)	RFC2460
6	TCP	RFC2460
17	UDP	RFC2460
41	IPv6 (para tunelear IPv6)	RFC2460
43	Ruteo	RFC2460
44	Fragmentación	RFC2460
50	Encapsulamiento de la carga útil de seguridad	RFC2460
51	Autenticación	RFC2460
58	ICMPv6	RFC2460
59	No hay siguiente	RFC2460
60	Opciones de destino	RFC2460
135	Movilidad	RFC3775

Tabla 2.C.1: *Valores que definen las cabeceras de extensión en el campo siguiente cabecera.*

Con una excepción, las cabeceras de extensión no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega de un paquete, hasta que el paquete alcanza el nodo identificado en el campo *Dirección Destino* de la cabecera IPv6. Allí, el nodo destino toma el paquete y luego procesa todos los campos de la cabecera IPv6 básica y en el campo *Siguiente Cabecera* de la cabecera IPv6 se invoca el módulo para procesar la primera cabecera de extensión, o la cabecera de capa superior si no hay ninguna cabecera de extensión presente. Otro aspecto muy importante de resaltar es que las cabeceras de extensión se deben procesar estrictamente en el orden que aparecen en el paquete.

La excepción mencionada en el párrafo anterior es el orden para procesar la cabecera Opciones de Salto a Salto, la cual lleva información que debe ser examinada y procesada por cada nodo a lo largo de la ruta de entrega de un paquete, incluyendo los nodos de origen y de destino. La cabecera Opciones de Salto a Salto, cuando está presente, debe seguir inmediatamente a la cabecera IPv6. Su presencia es indicada por el valor de cero en el campo *Siguiente Cabecera* de la cabecera IPv6.

Una implementación completa de IPv6 comprende la aplicación de las siguientes cabeceras de extensión:

a) Opciones de Salto a Salto
b) Ruteo (Tipo 0)
c) Fragmentación
d) Opciones de Destino
e) Autenticación
f) Seguridad del Encapsulado de la Carga Útil
g) Movilidad

1) Orden de las Cabeceras de Extensión

Cuando más de una cabecera de extensión se usa en un mismo paquete, se recomienda que esas cabeceras aparezcan en el siguiente orden:

a) Cabecera IPv6.
b) Cabecera Opciones de Salto a Salto.
c) Cabecera Opciones de Destino
d) Cabecera de Ruteo.
e) Cabecera de Fragmentación.
f) Cabecera Autenticación.
g) Cabecera Seguridad del Encapsulado de la Carga Útil.
h) Cabecera Opciones de Destino.(sólo opciones a procesar en el destino final del paquete)
i) Cabecera de Capa Superior.

Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la *Cabecera Opciones de Destino* la cual debe de ocurrir a lo sumo dos veces (una vez antes de una cabecera Enrutamiento y la otra vez antes de una cabecera de capa superior).

Si la cabecera de capa superior es otra cabecera IPv6 (en el caso de que el IPv6 sea tuneleado o encapsulado en el IPv4), puede ser seguida por sus propias cabeceras de extensión, las cuales están sujetas a las mismas recomendaciones que se plantean en este apartado.

Los nodos IPv6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden. No obstante, se aconseja fuertemente que los nodos emisores de paquetes IPv6 se apeguen al orden recomendado en la lista de este apartado.

2) Cabecera de Salto a Salto.
La cabecera de opciones salto a salto lleva información opcional que, si se encuentra en el paquete, debe ser examinada por cada dispositivo de enrutamiento a lo largo del camino.

El formato de la cabecera de Salto a Salto se presenta en la figura 2.C.2.

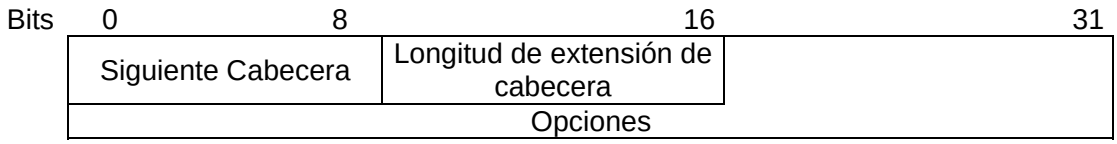


Figura 2.C.2: ***Formato de la cabecera de Salto a Salto***

Los campos de la cabecera de Salto a Salto son los siguientes:
a) *Siguiente Cabecera (8 bits):* Identifica el tipo de cabecera que sigue a esta.
b) *Longitud de extensión de cabecera (Header Extend Lengt) (8 bits):* Longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
c) *Opciones:* Campo de longitud variable que consta de una o más opciones. Cada opción esta formada por 3 subcampos:
    i. Tipo de opción (8 bits): que identifica la opción. Los 5 bits menos significativos indican la opción. Y los 3 bits más significativos indican la acción a realizar por un nodo que no reconoce el tipo de opción, de acuerdo a:
        - 00 ignorar esta opción.
        - 01 descartar el paquete.
        - 10 descartar el paquete y enviar un mensaje ICMP a la dirección de origen del paquete, indicando el tipo de opción no es reconocida.
        - 11 descartar el paquete y, solamente si la dirección destino del paquete no es una dirección multidifusión, enviar un mensaje ICMP.

      Y el tercer bit especifica si el campo de datos no puede cambiar (0) ó si puede cambiar (1) en el camino.
    ii. Longitud (8 bits): que indica la longitud en octetos del campo de datos.
    iii. Datos de la opción.

En la figura 2.C.3. Se ilustra con un ejemplo el uso de la cabecera extendida de opción Salto a Salto.

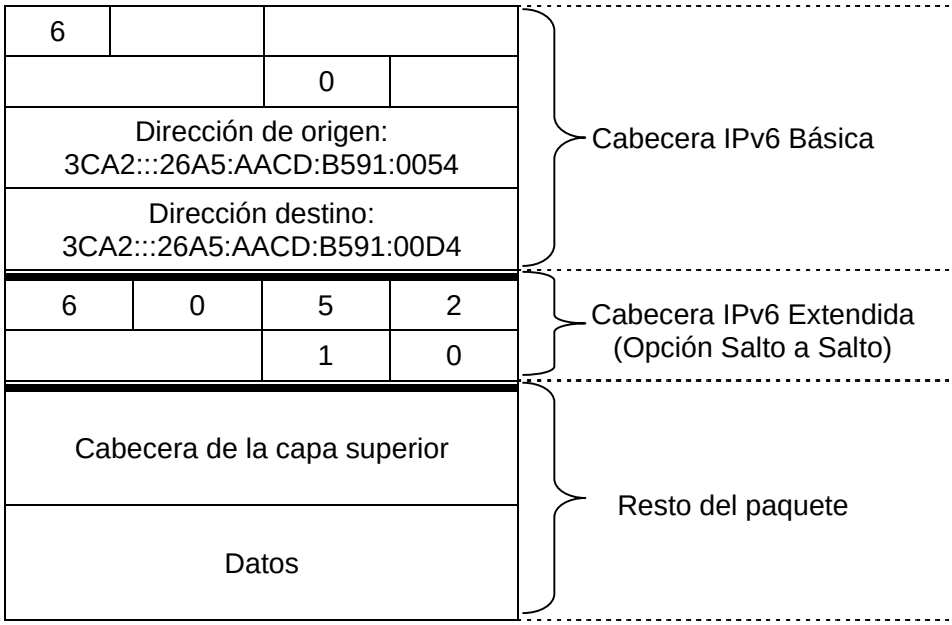


Figura 2.C.3**:** Ejemplo del uso de la cabecera extendida de opción de salto a salto.
La ilustración del paquete contiene un anuncio de router de opción salto a salto. Como se puede observar en dicho paquete los valores de los campos indican lo siguiente:

1. Cabecera IPv6 Básica:
    a. El campo de la versión tiene el valor de 6 que indica que se trabaja con el protocolo IPv6
    b. El campo de Siguiente Cabecera tiene el valor de 0 que indica que a continuación se trabajara con una cabecera extendida de opciones de salto a salto para que todos los nodos en el camino examinen y procesen el paquete.
    c. Por ultimo tenemos las direcciones origen y destino del paquete
2. Cabecera IPv6 Extendida:
    a. El campo Siguiente Cabecera tiene el valor de 6 que indica que a continuación se tiene la cabecera del protocolo de capa superior TCP
    b. El valor del campo Longitud de extensión de cabecera es de 0 lo que indica que hay una sola opción siguiente que es la Alerta de Router
3. Resto del paquete:
    a. La cabecera de la capa superior TCP
    b. Los datos

3) Cabecera de Ruteo.
La cabecera de Ruteo es utilizada por un nodo origen que envía un paquete IPv6 con el fin de listar uno o más nodos intermedios a ser "visitados" en el camino hacia el nodo destino del un paquete. La cabecera Ruteo se identifica por un valor del campo *Siguiente Cabecera* de 43 en la cabecera inmediatamente precedente.

El formato de la cabecera de ruteo se presenta en la figura 2.C.4.

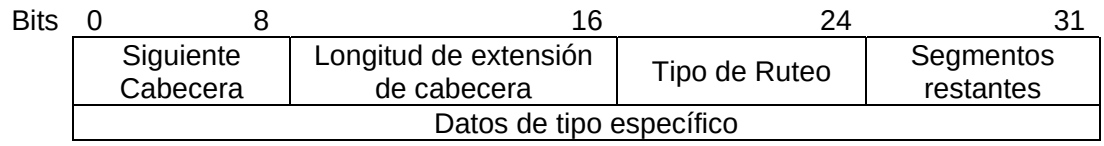


Figura 2.C.4: *Formato de la cabecera de Ruteo.*

Los campos de la cabecera de ruteo son los siguientes:

a) *Siguiente cabecera:* Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de Ruteo. Utiliza los mismos valores que el campo Protocolo.
b) *Longitud de extensión de cabecera (Header Extend Length):* Entero sin signo de 8 bits. Longitud de la cabecera de Ruteo en unidades de 8 octetos, no incluye los primeros 8 octetos.
c) *Tipo de ruteo (Routing type):* Aunque son posibles diferentes tipos de ruteo, al momento en que se realiza este estudio solamente 2 han sido reconocidos por la IANA y son los siguientes:
    d) Tipo de encaminamiento ruta de fuente (Tipo 0).
    e) Tipo definido para dar soporte a la arquitectura de red Nimrod.
f) *Segmentos restantes (Segments Left):* Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.
g) *Datos de tipo específico (Type Specific Data):* Campo de longitud variable, su formato es determinado por el campo *Tipo de Ruteo*, y de longitud tal que la cabecera de Ruteo completa es un entero múltiplo de 8 octetos de largo.

Si, después de procesar un paquete recibido, un nodo encuentra una cabecera de Ruteo con un valor en el campo *Datos de tipo específico* desconocido, el comportamiento requerido del nodo depende del valor del campo *Segmentos Restantes*, como sigue:

a) Si el valor del campo *Segmentos Restantes* es cero, el nodo debe ignorar la cabecera de Ruteo y proceder a procesar la siguiente cabecera en el paquete, cuyo tipo se identifica por el campo *Siguiente Cabecera* en la cabecera Enrutamiento.
b) Si el valor del campo *Segmentos Restantes* no es cero, el nodo debe descartar el paquete y enviar un mensaje ICMP Problema de Parámetro, Código 0, a la dirección origen del paquete, apuntando al Tipo de Ruteo desconocido.
c) Si, después de procesar una cabecera de Ruteo de un paquete recibido, un nodo intermedio determina que el paquete será remitido hacia un enlace cuya MTU de enlace es menor que el tamaño del paquete, el nodo debe descartar el paquete y enviar un mensaje ICMP Paquete Demasiado Grande a la Dirección Origen del paquete.

Para el caso particular de la cabecera de ruteo tipo cero el formato de la cabecera se presenta en la figura 2.C.5.

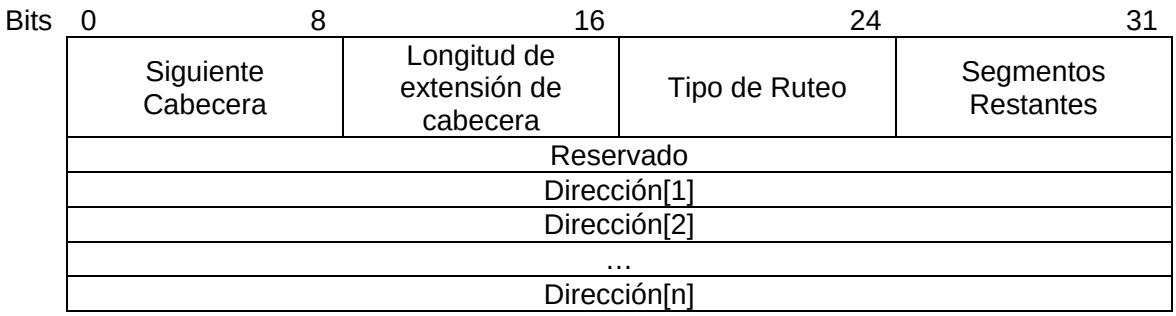


Figura 2.C.5: *Formato de la cabecera de ruteo tipo 0.*

Los campos de la cabecera de ruteo tipo 0 son los siguientes:

a) *Siguiente Cabecera (Next Header):* Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de Ruteo.
b) *Longitud de extensión de cabecera (Header Extend Length):* Entero sin signo de 8 bits. Para la cabecera de Ruteo de Tipo 0, la longitud de la cabecera extendida es igual a dos veces el número de direcciones en la cabecera.
c) *Tipo de Ruteo (Routing Type):* 0.
d) *Segmentos restantes (Segments Left:* Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.
e) *Reservado (Reserved):* Campo reservado de 32 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
f) *Dirección [1…n]:* Vector de direcciones de 128 bits, numerados desde 1 hasta n.

En la cabecera de Ruteo tipo 0 no deben aparecer direcciones multienvío, ni en el campo Dirección Destino IPv6.

Una cabecera de Ruteo no se examina o procesa hasta que alcance el nodo identificado en el campo Dirección Destino de la cabecera IPv6. En dicho nodo, al procesar el campo *Siguiente Cabecera* de la cabecera inmediatamente precedente ocasiona que el módulo cabecera de Ruteo sea invocado.
En la figura 2.C.6. y 2.C.7. Se ilustra con un ejemplo el uso de la cabecera extendida de Ruteo.

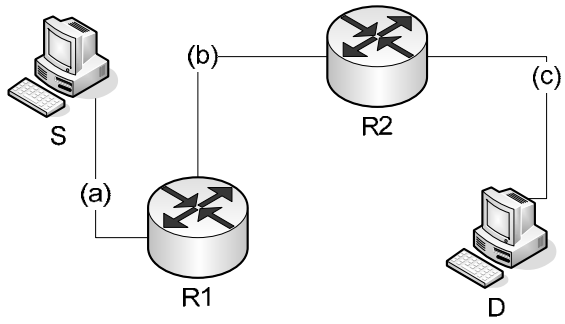
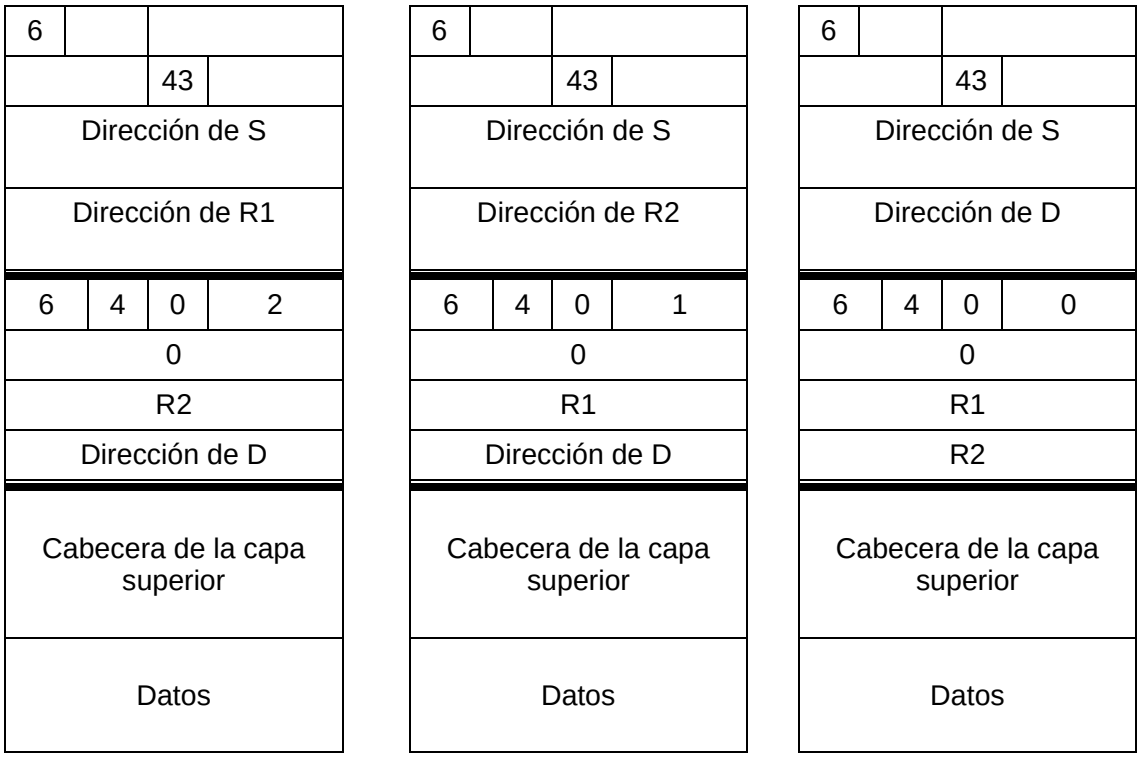


Figura 2.C.6: *Envío de un paquete entre el nodo origen S y el nodo destino D por medio de los routers R1 y R2.*



(a) Conexión entre S y R1

(b) Conexión entre R1 y R2

(c) Conexión entre R2 y D

Figura 2.C.7: En el análisis de la figura 2.C.6. El nodo origen S crea un paquete IPv6 con la cabecera de ruteo, esto se aprecia en la parte (a) de la figura, donde el campo destino del paquete es el router R1, que es el primer router en el camino, en lugar del nodo destino D. Por lo que el destino de este paquete es en primera instancia el router R1, el cual después de examinar la cabecera IPv6, y el campo *Siguiente Cabecera* determina que a continuación le sigue la cabecera extendida de ruteo, dicha cabecera será procesada por el router R1.
El campo *Longitud de extensión de cabecera* posee el valor de 4 lo que indica que la longitud de la cabecera de enrutamiento es de 4 octetos, este valor es solamente el doble del número de direcciones en la cabecera de ruteo. La primera dirección en la cabecera de ruteo es la del siguiente router en el camino, que es la del router R2, seguido de la dirección del nodo destino D.
El router R1 decrementa el valor del campo *Segmentos Restantes* y cambia la dirección destino de la cabecera IPv6 y la primera dirección en la cabecera de ruteo, después de realizar estos cambios el paquete queda como el que se aprecia en la parte (b) de la figura, luego el paquete se envía del router R1 al router R2. Similarmente, al proceso anterior el router R2 examina la cabecera IPv6 y continúa con el procesamiento de la cabecera de ruteo, después le cambia la dirección destino a la cabecera IPv6 y le coloca la dirección del router R2, de nuevo el router R2 decrementa el valor del campo *Segmentos Restantes* y cambia los valores en el campo de la dirección destino de la cabecera IPv6 y coloca la segunda dirección en la cabecera de ruteo, después de realizar estos cambios el paquete queda como el que apreciamos en la parte (c) de la figura. Luego el paquete se envía nuevamente. Este proceso se repite hasta que el campo *Segmentos Restantes* tiene el valor de 0 que es donde el nodo destino en este caso. D procesa todo el paquete.

4) Cabecera de fragmentación.
La cabecera de fragmentación es utilizada para enviar un paquete que es demasiado grande para enviarse en la MTU de la ruta hacia su destino, permitiendo que en un nodo origen pueda dividir el paquete que se necesita enviar en fragmentos, para enviar cada fragmento como un paquete separado, y luego que estos paquetes sean reensamblados en el nodo receptor.

El formato de la cabecera de fragmentación se presenta en la figura 2.C.8.

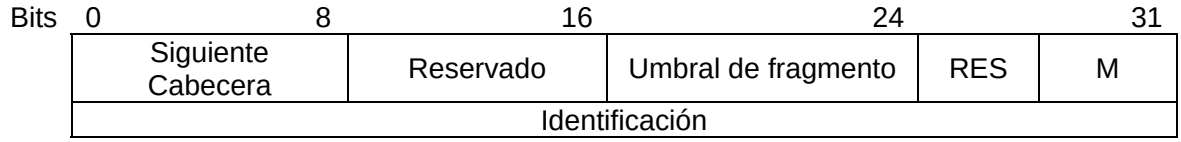


Figura 2.C.8: *Formato de la cabecera de fragmentación.*

Los campos de la cabecera de fragmentación son los siguientes:

a) *Siguiente Cabecera:* identifica el tipo de siguiente cabecera.
b) *Reservado:* para usos futuros.
c) *Umbral de fragmento:* indica donde se sitúa en el paquete original la carga útil de este fragmento (se mide en unidades de 64 bits).
d) *Indicador M:* 1 = más fragmentos; 0 = último fragmento.
e) *Identificador RES:* Utilizado para identificar de forma única el paquete original.

Por cada paquete que será fragmentado, el nodo origen genera un valor de Identificación que debe ser diferente al de cualquier otro paquete fragmentado enviado recientemente (significa dentro del máximo tiempo de vida probable de un paquete, incluyendo el tiempo que se tarda en transitar del origen hacia el destino y el tiempo gastado esperando el reensamblaje con otros fragmentos del mismo paquete) con la misma dirección origen y dirección destino. Si una Cabecera ruteo está presente, la Dirección Destino de interés es la del destino final.

Al paquete inicial que aun no esta fragmentado se le conoce como "paquete original", y se considera que consiste en dos partes, tal como se ilustra en la figura 2.C.9:

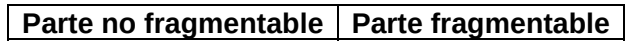


Figura 2.C.9: *Paquete original*

La *Parte no fragmentable* consiste en la cabecera IPv6 más cualquiera de las cabeceras de extensión que debe procesarse por nodos en camino hacia el destino, es decir, la cabecera de Opciones de Salto a Salto e incluso la cabecera de ruteo si está presente.

La *Parte fragmentable* consiste en el resto del paquete, es decir, cualquiera de las cabeceras de extensión que necesita que sólo se procese por el nodo destino final, más la cabecera de capa superior y los datos. Esta parte fragmentable es dividida en pequeños fragmentos del paquete original, cada uno, excepto posiblemente el último ("el de la extrema derecha"). Los fragmentos se transmiten en "paquetes fragmento" separados tal como se ilustra en la figura 2.C.10:

Paquete original:

Parte No fragmentable	Primer fragmento	Segundo fragmento	Último fragmento

Paquetes fragmento:

Parte No fragmentable	Cabecera primer fragmento

Parte No fragmentable	Cabecera segundo fragmento

Parte No fragmentable	Cabecera último fragmento

Figura 2.C.10: *Transmisión de los paquetes fragmento*

Cada paquete fragmento está compuesto de:

a) La parte no fragmentable del paquete original, con la Longitud de la Carga Útil de la cabecera IPv6 original cambiada para contener la longitud de este fragmento del paquete (excluyendo la longitud de la propia cabecera IPv6), y el campo *Siguiente Cabecera (Next Header)* de la última cabecera de la parte no fragmentable.
b) Una fragmento cabecera, que contiene el valor *Siguiente Cabecera (Next Header)* que identifica la primera cabecera de la parte fragmentable del paquete original.
c) Un desplazamiento del fragmento, que contiene el desplazamiento del fragmento, en unidades de 8 octetos, relativo al comienzo de la parte fragmentable del paquete original.
d) El propio fragmento, donde deben escogerse las longitudes de los fragmentos tal que los paquetes fragmento resultantes quepan dentro de la MTU de la ruta hacia el(los) destino(s) del paquete.

En el destino, se reensamblan los paquetes fragmento en su forma original, no fragmentada.

Las siguientes reglas gobiernan el reensamblaje:

a) Un paquete original sólo se reensambla a partir de paquetes fragmento que tienen la misma Dirección Origen, Dirección Destino, e Identificación del Fragmento.
b) La parte no fragmentable del paquete reensamblado consiste en todas las cabeceras, pero sin incluir, la cabecera Fragmento del primer paquete fragmento (es decir, el paquete cuyo Desplazamiento del Fragmento es cero), con los siguiente dos cambios:
    i. El campo *Siguiente Cabecera* de la última cabecera de la parte no fragmentable se obtiene del campo *Siguiente Cabecera* de la cabecera Fragmento del primer fragmento.
    ii. Se calcula la Longitud de la carga útil del paquete reensamblado a partir de la longitud de la Parte No Fragmentable y de la longitud y desplazamiento del último fragmento. En la figura 2.C.11 se analiza el ejemplo de una fórmula para calcular la Longitud de la carga útil del paquete original reensamblado.

LCU.orig = LCU.inicial - LF.inicial - 8 + (8*DF.final) + LF.final

Donde:

LCU.orig = campo Longitud de la Carga Útil del paquete reensamblado.

LCU.inicial = campo Longitud de la Carga Útil del primer paquete fragmento.

LF.inicial = longitud del fragmento siguiente a la cabecera Fragmento del primer paquete fragmento.

DF.final = campo Desplazamiento del Fragmento de la cabecera Fragmento del último paquete fragmento.

LF.final = longitud del fragmento siguiente a la cabecera Fragmento del último paquete fragmento.

Figura 2.C.11: *Ejemplo para calcular la longitud de la carga útil de un paquete original reensamblado.*

c) La parte fragmentable del paquete reensamblado se construye a partir de los fragmentos siguientes a las cabeceras Fragmento dentro de cada uno de los paquetes fragmento. La longitud de cada fragmento es calculada substrayendo de la Longitud de la Carga Útil del paquete, la longitud de las cabeceras entre la cabecera IPv6 y el propio fragmento, su posición relativa en la parte fragmentable se calcula a partir del valor de *desplazamiento del fragmento.*

d) La cabecera Fragmento no está presente en el paquete reensamblado final.

Las siguientes condiciones de error pueden originarse al reensamblar paquetes fragmentados:

a) Si se reciben fragmentos insuficientes para completar el reensamblaje de un paquete dentro de los 60 segundos a partir de la recepción del primer fragmento en llegar de ese paquete, el reensamblaje de ese paquete debe abandonarse y deben descartarse todos los fragmentos que se han recibido para ese paquete. Si el primer fragmento (es decir, el único con un Desplazamiento del Fragmento de cero) se ha recibido, un mensaje ICMP Tiempo Excedido para el Reensamblaje del Fragmento, debe enviarse al origen de ese fragmento.

b) Si la longitud de un fragmento, tal como se dedujo a partir de la Longitud de la Carga Útil del paquete fragmento, no es un múltiplo de 8 octetos y la bandera M de ese fragmento es 1, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Longitud de la Carga Útil del paquete fragmento.

c) Si la longitud y el desplazamiento de un fragmento son tales que la Longitud de la Carga Útil del paquete reensamblado de ese fragmento excedería los 65,535 octetos, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Desplazamiento del Fragmento del paquete fragmento.

En la figura 2.C.12. Se ilustra con un ejemplo el uso de la cabecera extendida de Fragmentación.

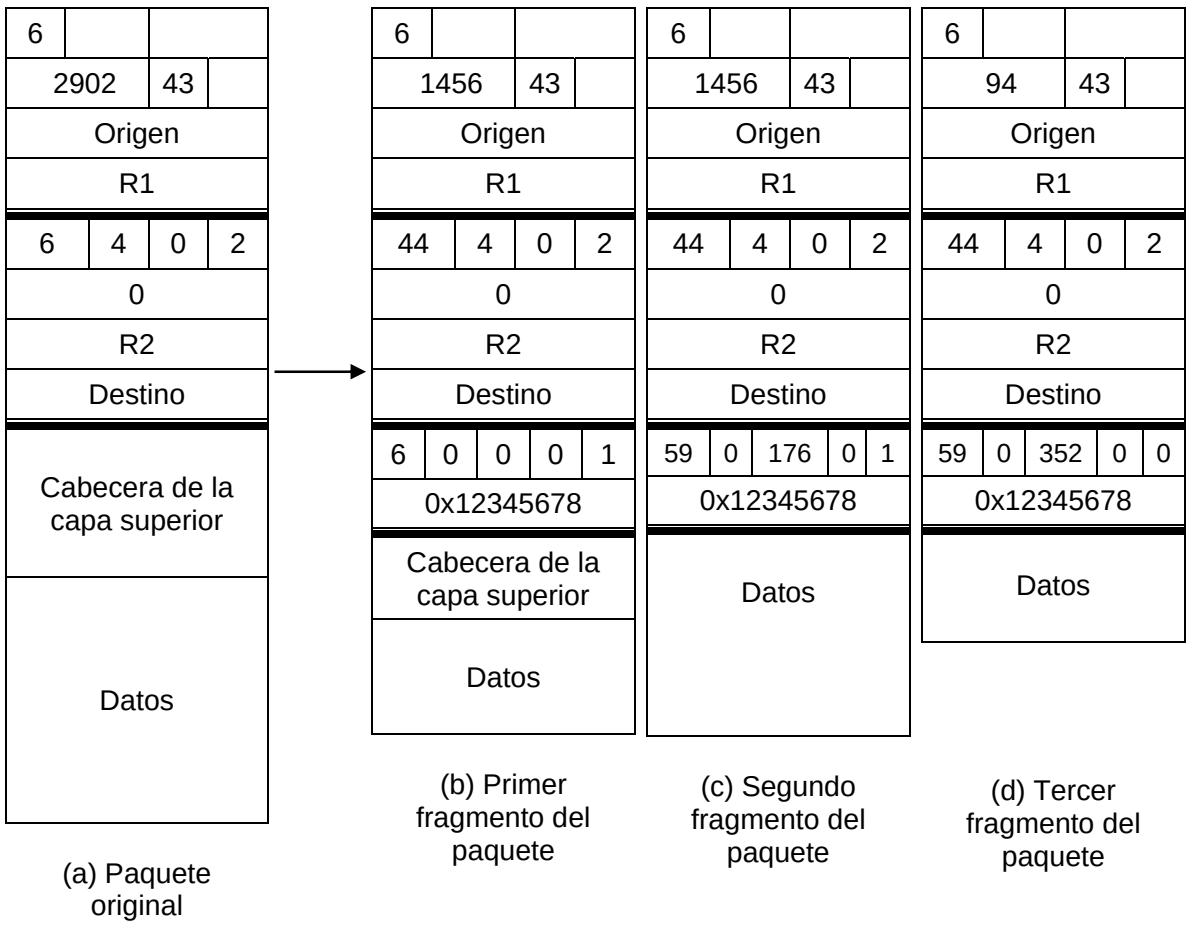


Figura 2.C.12: Considerese el paquete que se muestra en la parte (a) de esta figura. Este paquete necesita ser fragmentado por el nodo origen porque para este caso el camino MTU es de 1514 bytes. La parte no fragmentable del paquete original en este ejemplo incluye la cabecera IPv6 y la cabecera de Ruteo (Valor del campo *Siguiente Cabecera* = 43). El paquete original es dividido en tres partes y en cada parte se deben incluir estas dos cabeceras. Dichos paquetes no pueden ser más grandes que 1500 bytes. Luego se le agrega a los paquetes la cabecera de fragmentación, teniendo 1412 bytes para uso de los datos. Sin embargo el campo *Umbral de Fragmento* en la cabecera de fragmentación se mide en unidades de 64 bits. Por consiguiente el tamaño máximo de la parte fragmentable del paquete original tiene un limite de 1408 bits. En este ejemplo el campo *Longitud de Carga Útil* de la cabecera IPv6 tiene un valor de 1456 como se puede observar en la parte (b) de esta figura.
El campo *Siguiente Cabecera* en la cabecera de enrutamiento en los tres fragmentos tiene el valor de 44, indicando que a continuación le sigue la cabecera de fragmentación, en el primer fragmento el campo *Siguiente Cabecera* tiene el valor de 6 indicando que a continuación le sigue la cabecera de la capa superior, los otros dos fragmentos tienen el valor de 59 en este campo indicando que a continuación no hay más cabeceras. En este ejemplo en la cabecera de fragmentación es usado el valor hexadecimal de 0x12345678 que indica que el mismo identificador debe ser usado en todos los fragmentos. El campo *Umbral de Fragmento* indica el desplazamiento en unidades de 8 octetos de los datos que siguen la cabecera de fragmentación. La bandera *M* indica si existen o ya no existen más fragmentos del paquete original.

5) Cabecera de autentificación.
La cabecera de autentificación proporciona integridad y autenticidad de la información enviada por Internet.

El formato de la cabecera de autentificación se presenta en la figura 2.C.13.

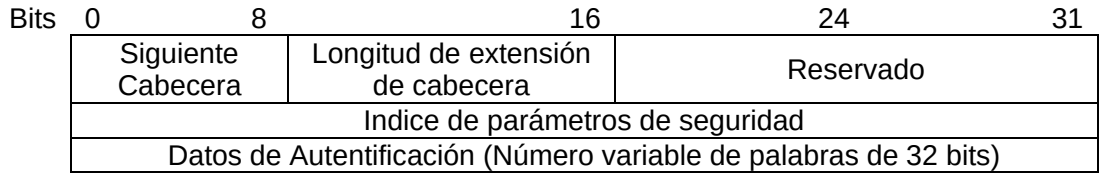


Figura 2.C.13: *Formato de la cabecera de Autentificación.*

Los campos de la cabecera de autenticación son los siguientes:
a) *Siguiente Cabecera (Next Header):* identifica la cabecera que viene a continuación.
b) *Longitud de extensión de cabecera (Header Extend Length):* longitud del campo de datos de autentificación en palabras de 32 bits.
c) *Reservado (Reserved):* para usos futuros.
d) *Indice de parámetros de seguridad (Index of parameters of security):* identifica a una asociación de seguridad.
e) *Datos de Autentificación (Authentification data):* número entero de palabras de 32 bits.

Los datos de autentificación se calcularán utilizando el paquete IP entero, excluyendo los campos que puedan cambiar en el transito (el campo *Límite de Salto* de la cabecera IPv6).

Los campos que puedan cambiar se pondrán a cero para hacer el cálculo. En caso de fragmentación los cálculos se llevarán a cabo antes de la fragmentación en el origen y después del reensamblado en el destino.

6) Cabecera de encapsulamiento de la carga útil de seguridad (ESP).
La cabecera de encapsulamiento proporciona privacidad e integridad de la información enviada por Internet. El mecanismo se puede utilizar para encriptar el segmento de la capa de transporte (TCP, UDP) o bien el paquete IP completo. El formato de la cabecera de encapsulamiento se presenta en la figura 2.C.14.

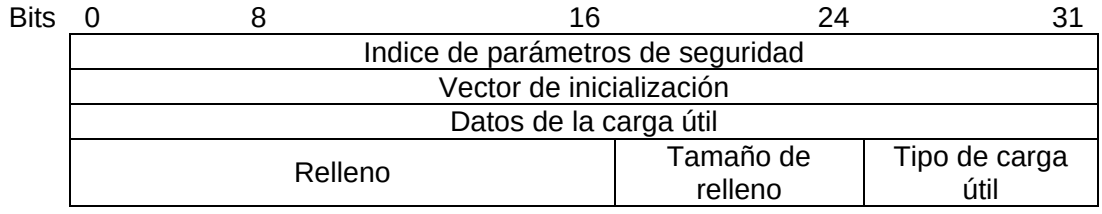


Figura 2.C.14: *Formato de la cabecera de encapsulamiento de la carga útil de seguridad.*

Los campos de la cabecera de encapsulamiento de la carga de seguridad son:
a) *Indice de parámetros de seguridad (Index of parameters of security):* identifica una asociación de seguridad.

b) *Vector de inicialización (Initialization vector):* entrada al algoritmo CBC, y es un múltiplo de 32.
c) *Datos de la carga útil (Data of the useful load):* antes del encriptado, este campo contiene el bloque de datos que se va a encriptar.
d) *Relleno (Filler):* antes del encriptado, se rellena con datos no especificados para alinear los campos longitud de relleno y tipo de carga a un límite de 64 bits.
e) *Tamaño de relleno (Filler length):* tamaño del campo de relleno no encriptado.
f) *Tipo de carga útil (Type of useful load):* indica el tipo de protocolo de los datos de carga.

Los tipos de encapsulamiento de la carga de seguridad que existen son:
a) Modo de transporte para la cabecera de encapsulamiento de carga útil de seguridad.
b) Modo túnel para la cabecera de encapsulamiento de la carga útil de seguridad.

a) Modo de transporte ESP.

En este tipo de encapsulamiento de la carga útil de seguridad el nodo origen se encarga de encriptar la parte trasera de esta cabecera más el segmento de entero de la capa de transporte. Por otra parte en el nodo destino es el encargado de desencriptar el paquete enviado.

Este tipo de cabecera de encapsulamiento proporciona privacidad, pero a la vez permite hacer un análisis del tráfico con los paquetes transmitidos. También es un método útil para proteger las conexiones entre computadores. Este modo se ilustra en la figura 2.C.15.

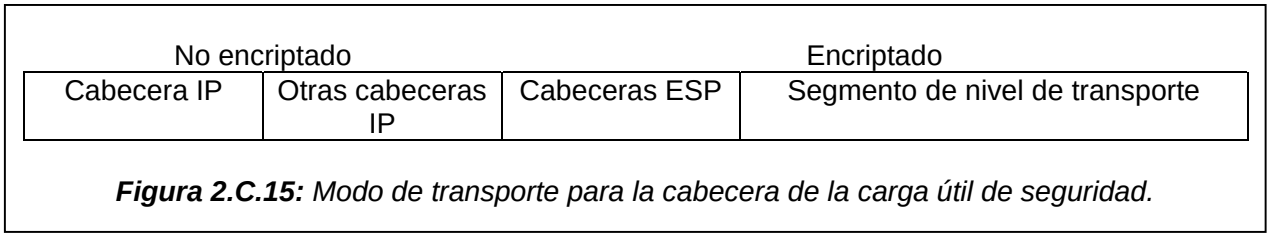


Figura 2.C.15: *Modo de transporte para la cabecera de la carga útil de seguridad.*

b) Modo de túnel ESP.

Este tipo de cabecera de encapsulamiento para la carga útil de seguridad ayuda a realizar una configuración que incluya cortafuegos u otro tipo de pasarela de seguridad, de tal forma que el paquete encriptado se lleve a cabo entre un computador externo y la pasarela de seguridad. Este método se ilustra en la figura 2.C.16

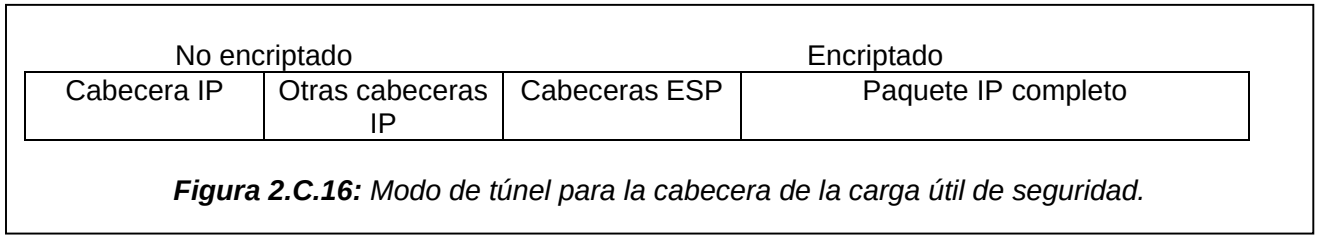


Figura 2.C.16: *Modo de túnel para la cabecera de la carga útil de seguridad.*

7) Cabecera de opciones de destino.

La cabecera *Opciones de Destino* es usada para llevar información opcional que necesita ser examinada solamente por el nodo destino del paquete. Esta cabecera es identificada por un valor del campo *Siguiente Cabecera* de 60 en la cabecera inmediatamente precedente, y su formato se puede apreciar en la figura 2.C.17:

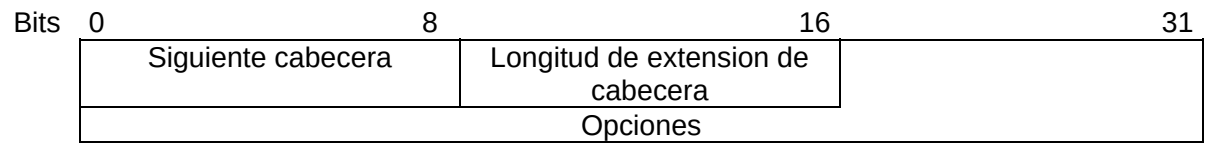


Figura 2.C.17: *Formato de la cabecera de opciones de destino.*

Los campos de la cabecera de opciones de destino son los siguientes:

a) *Siguiente cabecera (Next Header):* Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Destino.
b) *Longitud de extensión de cabecera (Header Extend Length):* Entero sin signo de 8 bits. Longitud de la cabecera de Opciones de Destino en unidades de 8 octetos, no incluye los primeros 8 octetos.
c) *Opciones (Options):* Campo de longitud variable, de longitud tal que la cabecera Opciones de Destino completa es un entero múltiplo de 8 octetos de largo.

Las cabeceras de extensión Opciones de Salto a Salto y la cabecera Opciones de Destino llevan un número variable de "opciones" codificadas de con el formato tipo-longitud-valor (TLV).
Es importante recalcar que la secuencia de opciones dentro de una cabecera se debe procesar estrictamente en el orden con el que aparecen en la cabecera. La codificación de opciones en esta cabecera de extensión presenta un formato estándar, donde el tipo, la longitud y el valor son definidos para cada opción como se ilustra en la figura 2.C.18.

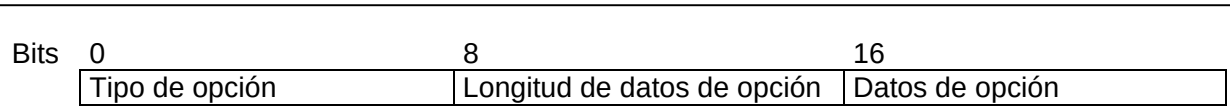


Figura 2.C.18: *Formato de las opciones de la cabecera de opciones de destino.*

El primer octeto identifica el valor del tipo de opción de 8 bits. Estos valores son mantenidos por IANA, valores identificados que se muestran en la tabla 2.C.2:

HEX	**BINARIO**			
	Act.	**Cambio**	**resto**	
0	00	0	00000	Pad1
1	00	0	00001	PadN
C2	11	0	00010	Carga útil Jumbo
C3	11	0	00011	Dirección NSAP
4	00	0	00100	Límite de encapsulamiento de túnel
5	00	0	00101	Alerta de router
C6	11	0	00110	Actualización vinculante
7	00	0	00111	Conocimiento de vinculación
8	00	0	01000	Petición vinculante
C9	11	0	01001	Dirección de casa
8A	10	0	01010	Identificación de punto final

Fuente: IANA

Tabla 2.C.2: *Valores de Tipo de Opción.*

El segundo octeto, longitud de datos de opción, es un entero sin signo de 8 bits que define la longitud del campo de datos de opción en octetos. El campo de datos de opción es un campo de longitud variable en el cual los datos opcionales son llevados para ese tipo de opción.

El octeto del tipo de opción es adicionalmente subdividido para permitir el uso de los tres bits de mayor orden para especificar como los nodos podrían manejar el paquete adjuntado en ciertas circunstancias. Los dos bits más significativos indican que debería hacer un nodo con el paquete si el nodo no reconoce el tipo de opción, estas opciones son las siguientes:

a) 00 - no tomar en cuenta esta opción y continuar procesando la cabecera.
b) 01 - descartar el paquete.
c) 10 - descartar el paquete y, sin tener en cuenta si o no la Dirección Destino del paquete fue una dirección multienvío, enviar un mensaje ICMP Problema de Parámetro, Código 2, a la Dirección Origen del paquete señalando el Tipo de Opción desconocido.
d) 11 - descartar el paquete y, solo si la Dirección Destino del paquete no fue una dirección multienvío, enviar un mensaje ICMP Problema de Parámetro, Código 2, a la Dirección Origen del paquete señalando el Tipo de Opción desconocido.

El tercer bit de mayor orden del Tipo de Opción especifica si los Datos de la Opción pueden modificar el ruteo hacia el destino final del paquete. Cuando una cabecera de Autenticación está presente en el paquete, para cualquier opción cuyos datos pueden modificar el ruteo, su campo entero Datos de la Opción se debe tratar como octetos de valor cero cuando se calcula o verifica el valor de autenticidad del paquete, el tercer bit de mayor alto orden puede tener los siguientes datos.

a) 0 - los Datos de la Opción no modifican el ruteo.
b) 1 - los Datos de la Opción pueden modificar el ruteo.

Los tres bits de mayor orden descritos arriba están para ser tratados como parte del Tipo de Opción, no independientemente del Tipo de Opción. Es decir, una opción en particular se identifica por un Tipo de Opción de 8 bits completo, no sólo por los 5 bits de manor orden de un Tipo de Opción.

8.) Cabecera no hay siguiente.

El valor 59 en el campo *Siguiente Cabecera* de una cabecera IPv6 o de cualquier cabecera de extensión indica que no se ejecutara nada siguiendo esa cabecera. Si el campo *Longitud de la Carga Útil* de la cabecera IPv6 indica la presencia de octetos más allá del final de una cabecera cuyo campo *Siguiente Cabecera* contiene 59, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

3. DIRECCIONAMIENTO IPv6

A. INTRODUCCIÓN

En el proceso de identificación de un host IPv6 como miembro de una red x, en lugar de utilizar el proceso de máscara de red (IPv4), se ha utilizado el de *Identificadores,* como lo considera el RFC1884. El formato es el siguiente:

[Prefijo suscrito] [Identificador de subred] [Identificador de interfaz]

En resumen, el direccionamiento en IPv6 posee las siguientes características:

1. No existen direcciones de multidifusión (broadcast).
2. El espacio disponible de 128 bits se divide entre la representación de la interfaz y el prefijo.
3. El prefijo permite conocer donde esta conectada la interfaz, es decir, donde conocer la ruta.
4. Los campos pertenecientes a una dirección pueden estar formados por solo ceros o solo unos.
5. Una única interfaz puede tener varias direcciones IPv6 que la representan a través de la red.
6. El direccionamiento es organizado en forma jerárquica.

IPv6 soporta tres tipos de direccionamiento los cuales serán analizados detenidamente en esta sección, como sigue:

1. *Direcciones Unicast:* La dirección de destino especifica una sola computadora (host o router). Estas son las equivalentes a las direcciones IPv4. La figura 3.A.1 muestra gráficamente el proceso de dirección de una dirección unicast.

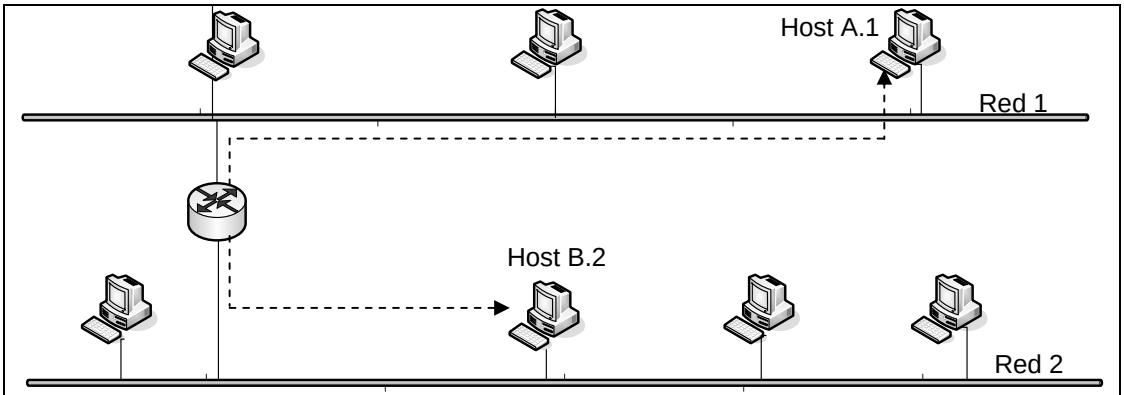


Figura 3.A.1: *Direccionamiento Unicast en IPv6.*

2. *Direcciones Anycast:* El destino es un conjunto de anfitriones en donde todas comparten un solo prefijo de dirección. La figura 3.A.2 muestra gráficamente el proceso de direccionamiento de una dirección anycast.

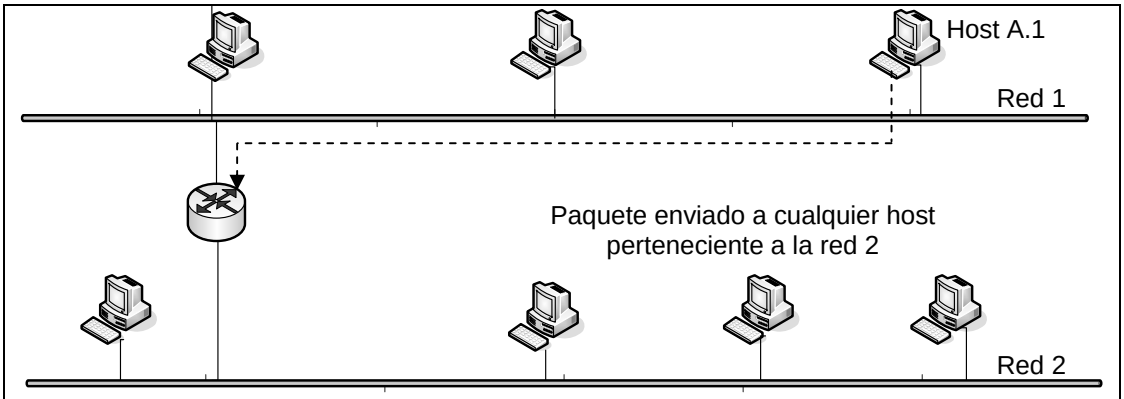


Figura 3.A.2: *Direccionamiento anycast en IPv6.*

3. *Direcciones Multicast:* El destino es un conjunto de anfitriones, posiblemente en múltiples localidades. La figura 3.A.3 muestra gráficamente el proceso de direccionamiento de una dirección multicast.

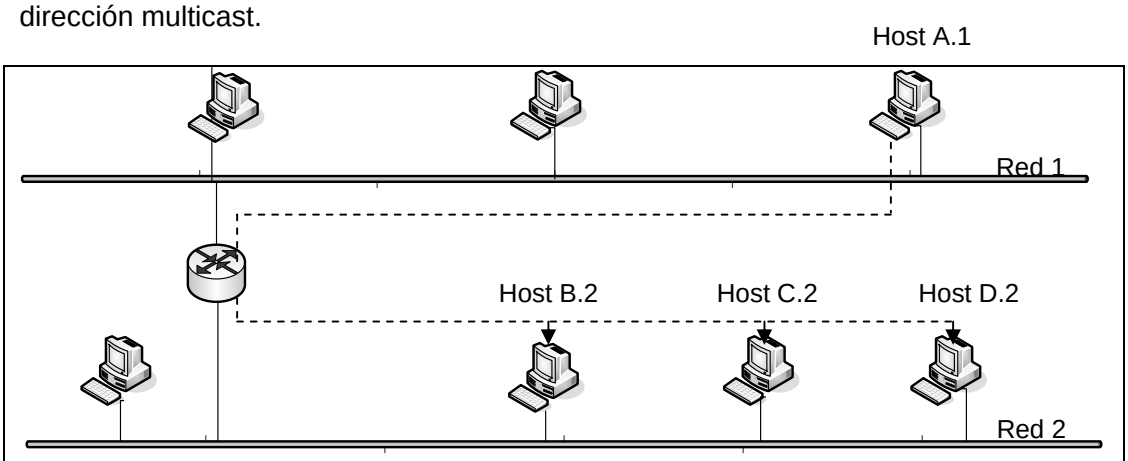


Figura 3.A.3: *Direccionamiento multicast en IPv6.*

B. ESPACIO DE DIRECCIONAMIENTO

A diferencia de su antecesor, IPv6 presenta direcciones mas grandes, siendo este el cambio más significativo con que deben lidiar los protocolos, cuadruplicando el tamaño de 32 bits (IPv4) a 128 bits (IPv6). El espacio de direcciones de IPv6 es bastante amplio, lo que descarta su caducidad por un buen espacio de tiempo. Dicho espacio de direccionamiento permite crear niveles adicionales de direccionamiento (jerarquía de direccionamiento extendida) así como también mejora el desempeño del ruteo. El espacio de direccionamiento esta dividido en diferentes categorías basadas en los valores de sus bits de mayor orden. Como se muestra en la tabla 3.B.1, el espacio de direccionamiento reservado para cada prefijo representado en formato binario, es como sigue:

Estado	Prefijo (en formato binario)	Fracción del espacio
Reservado (Compatible con IPv4)	0000 0000	1/256
No asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No asignado	0000 011	1/128

Estado	Prefijo (en formato binario)	Fracción del espacio
No asignado	0000 1	1/32
No asignado	0001	1/16
Direcciones Unicast globales Agregables	001	1/8
No asignado	010	1/8
No asignado	011	1/8
No asignado	100	1/8
No asignado	101	1/8
No asignado	110	1/8
No asignado	1110	1/16
No asignado	1111 0	1/32
No asignado	1111 10	1/64
No asignado	1111 110	1/128
No asignado	1111 1110 0	1/512
Direcciones Unicast locales de enlace	1111 1110 10	1/1024
Direcciones Unicast locales de sitio	1111 1110 11	1/1024
Direcciones Multicast	1111 1111	1/256

Tabla 3.B.1: *Reserva de prefijos.*

Es importante aclarar que en IPv4 las direcciones se dividen en diferentes clases (A,B,C,D,E) basadas en los valores de sus bits de mayor orden. En IPv6 también se dividen en diferentes categorías basadas en sus bits de mayor orden de acuerdo a la utilización de prefijos.

La representación de los prefijos en IPv6 es de la siguiente manera:

[Dirección IPv6] / [Longitud del prefijo]

C. FORMATO DE DIRECCIONAMIENTO

Una dirección de tipo IPv6, está compuesta por ocho campos de 16 bits[1] cada uno expresados en forma hexadecimal separados por dos puntos (:), formando una dirección de 128 bits. En la figura 3.C.1 se muestra un ejemplo de una dirección en formato IPv6.

3CA2:0000:0000:0000:26A5:AACD:B591:0025

Figura 3.B.1: *Dirección IPv6.*

En la representación de la dirección en IPv6, es permitido simplificar aquellos campos cuyos elementos sean ceros, sustituyéndolos por un par de dos puntos, aunque es importante señalar que no es permitido simplificar dos campos que no se encuentren contiguos, por lo que la dirección que se muestra en la figura 3.B.1, estaría representada de la siguiente manera:

3CA2::26A5:AACD:B591:0025

[1] Un octeto lo forman 8 dígitos binarios. Un nibble lo forman 4 dígitos hexadecimales.

Otro aspecto importante a tomar en cuenta es que a diferencia de las direcciones en formato IPv4, en IPv6 las direcciones identifican a un host o a un conjunto de interfaces, no así a un host específico como se hace actualmente con el protocolo TCP/IP versión 4.
En la tabla 3.B.1 se detallan el formato de una dirección IPv6 como una dirección *URL* (RFC2732).

Dirección Ipv6	Representación como URL
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210	http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
1080:0:0:0:8:800:200C:4171	http://[1080:0:0:0:8:800:200C:417A]/index.html
3ffe:200:100:7031::1	http://[3ffe:2a00:100:7031::1]
1080::8:800:200C:417	http://[1080::8:800:200C:417A]/foo
::192.9.5.5	http://[::192.9.5.5]/ipng
::FFFF:129.144.52.38	http://[::FFFF:129.144.52.38]:80/index.html

Tabla 3.B.1: *Representaciones de direcciones IPv6 como URL´s.*

D. DIRECCIONES UNICAST

Como se señaló previamente las direcciones unicast especifican un solo destino (direcciones uno a uno), son agregables con máscaras de bits contiguos, similares a las utilizadas en IPv4 con el CIDR (protocolo de encaminamiento sin clases).

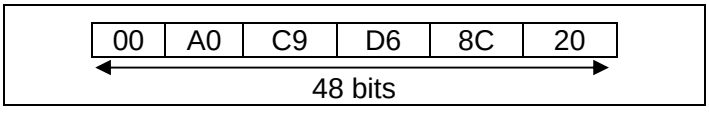
Existen varias formas de asignación de direcciones unicast en IPv6, entre la que se tienen: las direcciones unicast globales, que son utilizadas para comunicaciones entre hosts en el Internet, agregable globalmente, la dirección NSAP (Punto de acceso de servicio de red), la dirección jerárquica IPX, la dirección de sitio local, la dirección de enlace local, y la dirección de host compatible con IPv4. Otros tipos de direcciones podrán ser definidas en el futuro.

Se parte del hecho de que un host debe asumir que una dirección unicast, incluyendo la suya, no posee una estructura interna definida.

1) Identificador de interfaces
Los identificadores de interfaz en direcciones unicast IPv6 son utilizados para identificar interfaces en un enlace[2]. Dicha dirección será única en cada enlace, además pueden también ser únicas en un ámbito[3] más amplio. Además la misma interfaz puede ser usada para identificar múltiples interfaces o a un host.

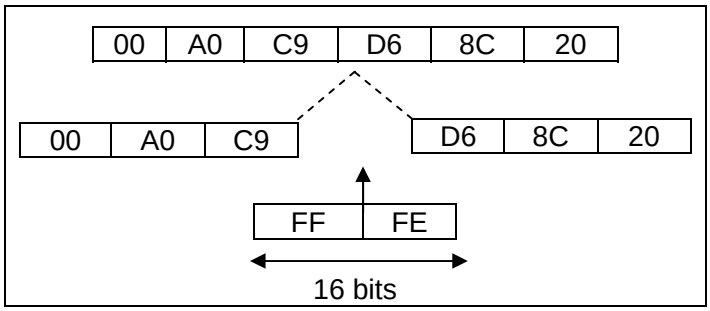
El proceso de composición de un identificador de interfaz para formar una dirección MAC IPv6[4] es como sigue:

a. Dirección MAC de 48 bits.
La dirección que se muestra a continuación representa una dirección Ethernet de 48 bits.

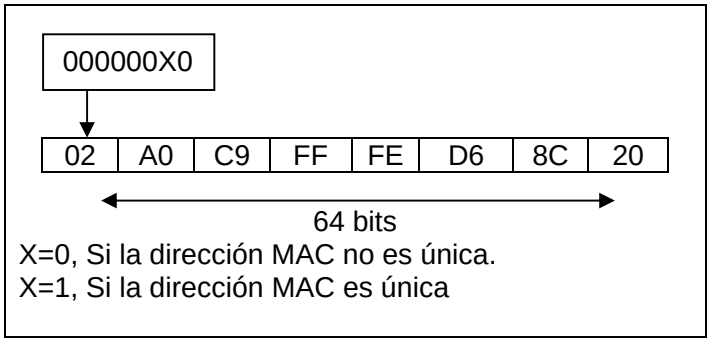


b. Conversión de una dirección MAC de 48 bits a una dirección de 64 bits.
En medio de la dirección de 48 bits se insertan los 16 bits (FFFE) que da una dirección de 64 bits.

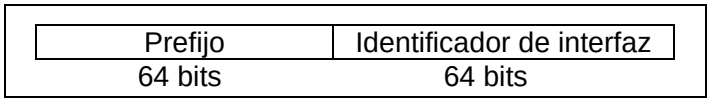
[2] RFC 2373 “Arquitectura de Direccionamiento en IPv6”
[3] Representa un área dentro de la cual la dirección puede ser utilizada como identificador único de una o varias interfaces
[4] Este procedimiento esta desarrollado en el estándar IEEE EUI-64.



c. Unicidad de bit.
El segundo bits del octeto más significativo a la izquierda sirve para declarar que la dirección MAC es única.



d. Dirección IPv6 establecida.
Terminado el proceso e incorporado el identificador de interfaz, se obtiene la dirección completa.



Es importante señalar que el empleo del mismo identificador de interfaz en un host, no afecta el identificador único de la interfaz o cada dirección única global IPv6.

Otro aspecto importante a tomar en cuenta es el hecho de que los números del formato del prefijo de los identificadores de las interfaces deben tener una longitud de 64 bits y además estas deben ser creadas siguiendo el formato del estándar de IEEE EUI-64. Para ello se hace uso de un bit que se denominará "u" (terminología de bit universal/local en IEEE-EUI-64), dicho bit es fijado en (1) para indicar un ámbito global y en (0) para indicar un ámbito local. Los detalles se muestran en la figura 3.D.1:

cccc	ccug	cccc	cccc	cccc	cccc

Dicho formato esta escrito en el orden de bit del estándar de Internet, donde:
“u” es el bit universal/ local
“g” es el bit individual/grupo, y
“c” son los bits de la identificación de la compañía fabricante.

Figura 3.D.1: *Dirección de identificación de interfaz según EUI-64.*

El motivo de hacer uso del bit “u” al momento de construir el identificador de interfaz es facilitar a los sistemas administradores manejar la configuración de identificadores de ámbito local. Y el uso del bit universal local en el identificador basado en IEEE EUI-64, es para permitir el desarrollo de una futura tecnología que pueda tener identificadores de interfaces avanzados con ámbito global.

2) Dirección no especificada
La dirección 0:0:0:0:0:0:0:0 es llamado una dirección no especificada, dicha dirección no debe de ser asignada a un host, su uso esta limitado para indicar la ausencia de dirección, un ejemplo de ello seria cuando un host esta en estado de iniciación y esta actualmente conociendo su propia dirección. Dicha dirección no puede ser usada para direcciones de paquetes de destino y mucho menos para cabeceras de encaminamiento en IPv6.

3) Dirección de autoretorno o de bucle de retorno (Loopback Address)
La dirección unicast 0:0:0:0:0:0:0:1 es llamada dirección de autoretorno (equivalente a 127.0.0.1 en IPv4). Dicha dirección podría ser utilizada por un host para enviarse paquetes a si mismo. Nunca debe ser asignada a un host, está permite hacer pruebas de iniciación del protocolo TCP/IP en un host especifico.

4) Direcciones IPv6 con direcciones IPv4 embebidas
Entre los mecanismos de transición entre IPv6 e IPv4, se establece una técnica aplicable a hosts y routers, llamada *paquetes IPv6 encaminados sobre una estructura IPv4 a través de túneles dinámicos.* Los anfitriones que utilizan dicha técnica, asignan direcciones unicast IPv6 especiales que llevan intrínseca la dirección con formato IPv4. Este tipo de direccionamiento es denominado direcciones IPv4 compatible con direcciones IPv6. Su formato se muestra en la figura 3.D.2.

0000……0000	0000	Dirección IPv4
80 bits formato IPv6	16 bits	32 bits

Figura 3.D.2: *Formato de direcciones IPv6 con direcciones IPv4 embebidas.*

Otra forma de representar direcciones IPv6 conteniendo direcciones IPv4 embebidas es la utilizada en la representación de hosts que manejan solo direcciones con el formato IPv4 (este tipo no es soportado por IPv6), a este tipo de direccionamiento se le denomina direcciones IPv6 mapeadas en IPv4 y su formato se muestra en la figura 3.D.3.

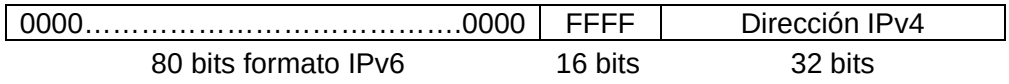


Figura 3.D.3: *Formato de direcciones IPv6 mapeadas en IPv4.*

5) Direcciones IPv6 globales agregables

Dado que IPv6 resuelve de mejor forma el problema de organización de jerarquización de routers en redes públicas, es evidente que el concepto de direccionamiento agregable es importante para entender dicha mejora al presente protocolo (IPv4). En principio se tiene que el direccionamiento agregable se organiza dentro de tres niveles de jerarquía[5], las cuales son:

1. Topología pública
2. Topología de sitio
3. Identificador de interfaz

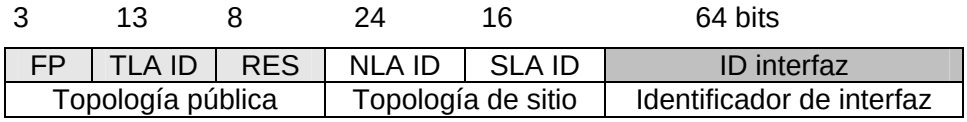
Donde:

Topología pública representa una colección de proveedores e intercambios de proveedores de servicios de Internet de tránsito público.

La topología de sitio representa sitios locales específicos u organizaciones que no proveen servicios de tránsito público para hosts que se encuentran fuera del sitio.

El identificador de interfaz caracteriza a las interfaces en los enlaces.

Este formato de direccionamiento ha sido diseñado para soportar tanto la agregación base, así como también un nuevo tipo de agregación llamada intercambios. La combinación de ésto permite un encaminamiento eficiente de agregación. El formato de una dirección IPv6 unicast globalmente agregable se muestra en la figura 3.D.4.



Donde:

FP	Prefijo de formato
TLA ID	Identificador de agregación de nivel superior
RES	Reservado para uso futuro
NLA ID	Identificador de agregación de siguiente nivel
SLA ID	Identificador de agregación de nivel de sitio
ID interfaz	Identificador de interfaz

Figura 3.D.4: *Formato de dirección IPv6 unicast globalmente agregables.*

6) Direcciones IPv6 unicast de uso local

Existen dos tipos de esta categoría para direcciones unicast de uso local, entre las que tenemos las locales de enlace y las locales de sitio[6].

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace. Esto es así para dar cabida a procesos de autoconfiguración que son una de las características principales de IPv6, donde se tiene una situación en la cual no existe un router, dicha dirección sólo se limita a

[5] RFC2374: Direccionamiento IPv6.
[6] RFC2374 Direccionamiento IPv6.

la red local, eso quiere decir que su ámbito es local. El formato de este tipo de direcciones se muestra en la figura 3.D.5.

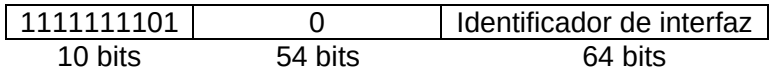


Figura 3.D.5: *Dirección unicast local de enlace.*

Las direcciones locales de sitio permiten direccionar paquetes dentro de un mismo sitio local u organización. Se configura mediante un identificador de subred de 16 bits. El ámbito de este tipo de dirección esta limitado a la red local o a la organización. El formato de la dirección se muestra en la figura 3.D.6.

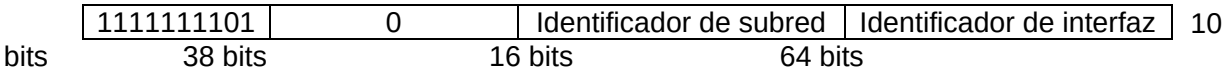


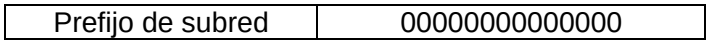
Figura 3.D.6: *Dirección unicast local de sitio.*

E. DIRECCIONES ANYCAST

Una dirección anycast es una dirección que es asignada a más de una interfaz, con la propiedad de que el paquete enviado para una dirección anycast es encaminado para la interfaz que posee dicha dirección. Las direcciones anycast permiten el envío de paquetes para un grupo de hosts pertenecientes a una misma subred, o localizados topológicamente dentro de diferentes enlaces en una red. Este tipo de direcciones es utilizado para descubrimiento de servicios dentro de una red o para proveer redundancia.

Por su sintaxis una dirección anycast no puede ser distinguida por una dirección unicast, por lo que si una interfaz tiene asignada una dirección anycast debe ser notificada previamente. Otro aspecto importante es que las direcciones anycast tienen el mismo rango de direcciones que las unicast.

El formato de una dirección anycast encaminada en una subred[7] se muestra en la figura 3.E.1.



Donde:

El prefijo de subred en una dirección anycast que identifica un enlace específico.

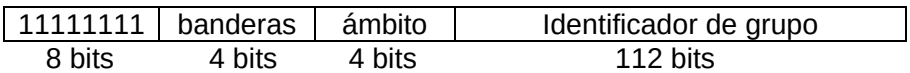
Figura 3.E.1: *Dirección anycast dentro de una subred.*

F. DIRECCIONES MULTICAST

Las direcciones multicast son identificadores para un grupo de hosts, donde cada host puede formar parte de varios grupos multicast. Este tipo de direcciones habilitan la eficiencia de redes de banda ancha por el envío del mínimo numero de paquetes para el máximo numero de host en un mismo enlace local. Un paquete de tipo multicast es enviado posiblemente a un numero ilimitado

[7] RFC3513 Arquitectura de direccionamiento.

de hosts. Un prefijo de dirección especial identifica un paquete multicast[8] y una dirección específica dentro de este prefijo identifica cada grupo de nodos. El formato de la dirección se muestra en la figura 3.F.1.



11111111	banderas	ámbito	Identificador de grupo
8 bits	4 bits	4 bits	112 bits

Donde:

11111111	Identificador de las direcciones multicast
Banderas	Es un conjunto de cuatro bits que representan banderas, siendo los tres primeros bits reservados e inicializados a cero. Si el último valor es cero indica que la dirección ha sido asignada por la autoridad de numeración de Internet, en caso contrario significa una dirección temporal, es decir, no asignada temporalmente. Identifica el tiempo de vida de un grupo multicast.
Ámbito	Indica el ámbito del grupo multicast. (ver tabla 3.F.1)
ID grupo	Identifica el grupo multicast dentro de un ámbito determinado.

Figura 3.F.1: *Dirección multicast IPv6.*

Un ámbito son valores de 4 bits utilizados para limitar el alcance de un grupo de direcciones multicast. En la tabla 3.F.1 se muestran los valores de ámbitos respectivos utilizados en direcciones multicast.

Valores de ámbitos (4 bits binarios)	Valores de ámbitos (4 dígitos hexadecimales)	Descripción del ámbito
0000	0	Reservado
0001	1	Interfaz local
0010	2	Enlace local
0100	4	Administrador local
0101	5	Sitio local
0110	6	No asignado
0111	7	No asignado
1000	8	Organización local
1001	9	No asignado
1010	A	No asignado
1011	B	No asignado
1100	C	No asignado
1101	D	No asignado
1110	E	Global
1111	F	Reservada

Tabla 3.F.1: *Bits de ámbito en direcciones multicast.*

[8] En IPv4, el prefijo multicast es 224.0.0.0/8.

Definiciones de ámbitos multicast:

1. Interfaz local: Es el que abarca solamente interfaces simples en un nodo, para transmitir paquetes multicast sobre direcciones de *autoretorno* o de *bucle de retorno* (loopback).
2. Enlace y sitio local: Abarcan las mismas regiones topológicas como las correspondientes a los ámbitos unicast.
3. Administrador local: Es el ámbito más pequeño que puede ser configurado administrativamente y no derivado de la conectividad física.
4. Organización local: Esta orientado a cubrir múltiples sitios dentro de una organización sencilla.
5. Los ámbitos denominados como no asignados son para que los administradores los asignen en sus regiones.

En la tabla 3.F.2 se muestran las direcciones reservadas multicast válidas sobre un valor de ámbito específico.

Dirección	Ámbito	Descripción
FF01:0:0:0:0:0:0:1	Interfaz	Todas las interfaces dentro del nodo
FF01:0:0:0:0:0:0:2	Interfaz	Todos los routers dentro del nodo
FF02:0:0:0:0:0:0:1	Enlace	Todos los nodos en el enlace
FF02:0:0:0:0:0:0:2	Enlace	Todos los router en el enlace
FF02:0:0:0:0:0:0:4	Enlace	Routers DVMRP
FF02:0:0:0:0:0:0:5	Enlace	Routers OSPF
FF02:0:0:0:0:0:0:6	Enlace	OSFP designado a routers
FF02:0:0:0:0:0:0:9	Enlace	Routers RIP
FF02:0:0:0:0:0:0:B	Enlace	Dispositivos IP Móviles
FF02:0:0:0:0:0:0:D	Enlace	Routers PIM
FF02:0:0:0:0:0:0:2	Enlace	Dispositivos DHCP
FF02::0:1:FFXX:XXXX	Enlace	Solicitud de nodo
FF05:0:0:0:0:0:0:2	Sitio	Routers en el sitio
FF05:0:0:0:0:0:0:3	Sitio	Servidores DHCP en el sitio
FF05:0:0:0:0:0:0:4	Sitio	Dispositivos DHCP en el sitio
FF05::1:1000-13FF	Sitio	Localización de servicios
FF0X:0:0:0:0:0:0:0:101	Cualquiera	Protocolo de tiempo de red

Tabla 3.F.2: *Direcciones multicast reservadas.*

En la tabla 3.F.3 se muestran los tipos de identificación de direcciones que soporta IPv6. En IPv6 el tipo de dirección es definido por el bit de mayor orden.

Tipo de dirección	Prefijo binario	Notación IPv6
No especificada	000…0 (128 bits)	:: /128
Loopback	000…1 (128 bits)	::1 /128
Multicast	11111111	FF00:: /8
Unicast de enlace local	1111111010	FE80:: /10
Unicast de sitio local	1111111011	FEC0:: /10
Unicast global	Todo lo demás	

Tabla 3.F.3: *Identificadores de tipos de direcciones IPv6*

G. DIRECCIÓN IP VERSIÓN 6

En la tabla 3.G.1 se muestran las recomendaciones para la delegación de direcciones IPv6 según los organismos IAB e IESG[9]. Para el alojamiento de entre la frontera de topologías públicas y privadas.

Tamaño asignado al prefijo	Utilidad
/48	En el caso general para sitios finales. Estos pueden ser redes caseras, pequeñas o grandes empresas.
/64	Cuando es conocido que una y solamente una subred necesita ser designada. Para una subred simple. Principalmente redes móviles tales como redes de área personal. Podría ser una red casera si esta no hacen uso de subredes múltiples en el futuro de esta red casera.
/128	Cuando es absolutamente conocido que uno y solamente un dispositivo es conectado. Para un host simple con interfaz punto a punto, tal como PPP (Point to Point Protocol).

Tabla 3.G.1: *Recomendaciones para el alojamiento de direcciones IPv6 por la IAB e IESG*

En la figura 3.G.1 se muestra la estructura general de una dirección IP versión 6.

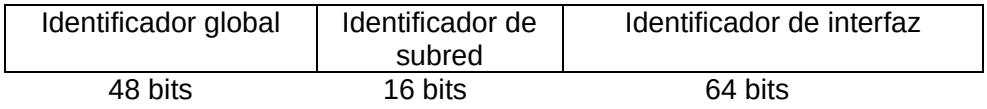


Figura 3.G.1: *Formato general de una dirección IPv6.*

H. RESUMEN DE ARQUITECTURA DE DIRECCIONAMIENTO EN IPv6

Hay que tomar en cuenta que en IPv6 el 13% del actual espacio de direccionamiento es asignado para el uso de direcciones unicast globales. Esto no significa que esto ha sido asignado actualmente. Simplemente quiere decir que este espacio de direccionamiento es reservado para que sea usado por Internet. En la figura 3.H.1 se muestra la arquitectura de direccionamiento del protocolo de Internet versión 6. (RFC3513)

[9] Según RFC3177: IAB/IESG Recommendations on IPv6 Addresses September 2001

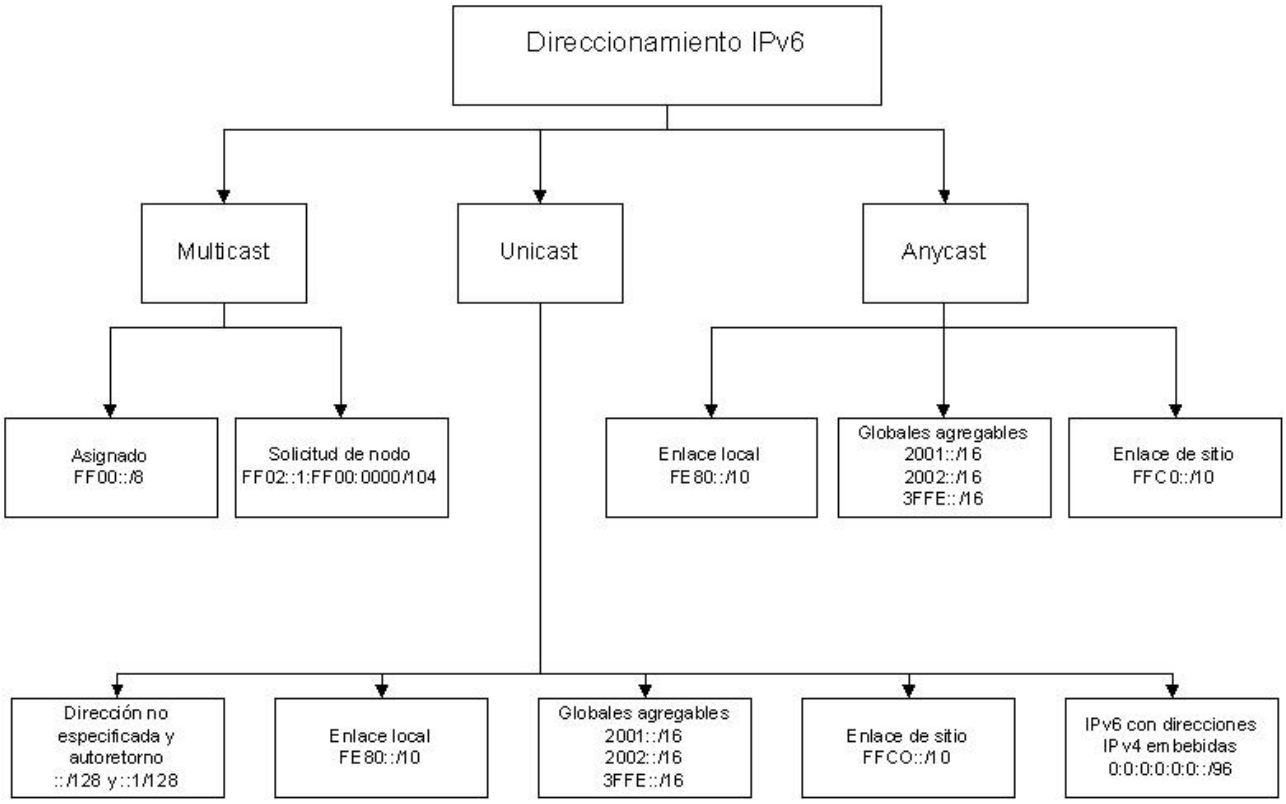


Figura 3.H.1: *Arquitectura de direccionamiento IPv6.*

I. SUBREDES EN IPV6

En el contexto de separar la parte de red de la parte de host de una dirección IPv6, la longitud del prefijo representa el equivalente de la máscara de subred en IPv4.
En el caso del espacio de direccionamiento de sitios, como por ejemplo 3ffe:0b00:c18::/48, el prefijo representa el rango de direcciones disponibles para enumeración de redes y hosts.

Para las subredes el espacio de direcciones IPv6 se deben usar técnicas de subneteo para dividir el campo de identificación de subred de 16 bits para un prefijo de dirección global de 48 bits de manera que permita la sumarización de la ruta y delegación del espacio de dirección remanente para diferentes porciones de una dirección IPv6.
Tal como IPv4, se puede subnetear prefijos de dirección IPv6 recursivamente, hasta los 64 bits que definen el prefijo de la dirección para una subred individual, de forma que provea sumarización de ruteo en varios niveles de una intranet organizacional. A diferencia de IPv4 no se puede utilizar subneteo de longitud variable para crear subredes de diferentes tamaños debido a que todas las subredes en IPv6 utilizan un prefijo de subred de 64 bits y un identificador de interfaz de 64 bits.

1) Subneteo de prefijos de direcciones globales.
Para las direcciones globales la Autoridad de Asignación de Números de Internet (IANA) o los proveedores de servicios de Internet (ISP) asignan un prefijo de dirección IPv6 en los primeros 48 bits fijados en el la dirección. El subneteo del campo de identificador de subred para un prefijo de de dirección global de 48 bits requiere seguir los siguientes dos procedimientos:

1. *Determinar el número de bits a utilizar en el subneteo.*
2. *Enumerar el nuevo prefijo de dirección de subred.*

Determinar el número de bits a utilizar en el subneteo:

El número de bits que se pueden usar en el subneteo, determina el número posible de prefijos de direcciones de subredes que se pueden asignar a los miembros de una red basada en un área geográfica o divisiones de departamentos. En una infraestructura jerárquica de ruteo es necesario determinar cuantos prefijos de direcciones y por consiguiente cuantos bits se demandarán en cada nivel de la jerarquía.

En cualquier nivel dado en una jerarquía, un número de bits son fijados por el nivel previo en la jerarquía (f); un número de bits son utilizados para subnetear el nivel en cuestión en la jerarquía (s), y un número de bits remanente para el próximo nivel hacia abajo en la jerarquía denominado (r). De tal modo, que todo el tiempo $f + s + r = 16$, ya que dentro del formato básico de la estructura de una dirección IPv6 este es el tamaño reservado para la identificación de subred (ver figura 3.G.1). En la figura 3.I.1 se muestra gráficamente lo anterior.

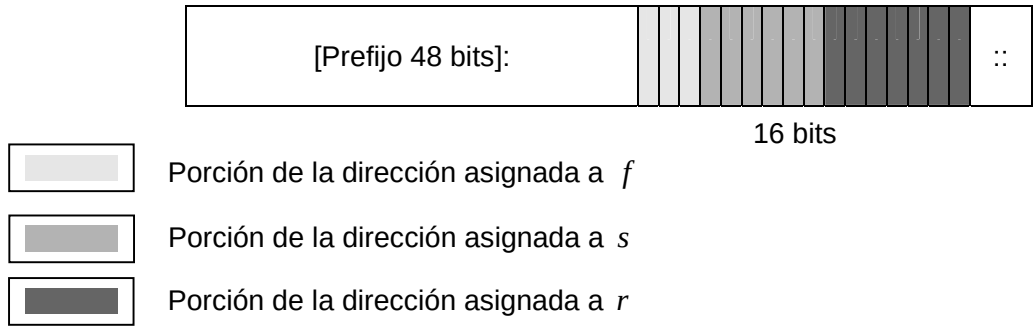


Figura 3.I.1: *Subneteando el campo de identificación de subred de una dirección global IPv6.*

Enumeración de prefijos de dirección subneteada.

En base al número de bits usados en el subneteo, se deben enumerar los nuevos prefijos de la dirección subneteada, utilizando la representación hexadecimal del identificador de subred y un incremento acumulado, siguiendo los pasos a continuación:

1. En base a s, el número de bists seleccionado para subnetear, y m, la longitud del prefijo de la dirección siendo subneteada, calcular lo siguiente:
   $f = m - 48$
   Donde: f es el número de bits dentro del identificador de subred que ya ha sido fijado.
   $n = 2^s$
   Donde: n es el número de prefijos de dirección que se obtendrán.
   $i = 2^{16-(f+s)}$

Donde: i es el valor del incremento entre cada identificador de subred sucesivo expresado en hexadecimal.

$$p = m + s$$

Donde: p es la longitud del prefijo de los nuevos prefijos de la dirección subneteada.

2. Crear una tabla de dos columnas con n filas. La primera columna contiene los número de prefijos de dirección (comenzando con 1), y la segunda columna contiene los nuevos prefijos de la dirección subneteada.

3. En la primera fila, colocar el prefijo de la dirección original con la nueva longitud del prefijo en la segunda columna. Por ejemplo, basado en f, el valor hexadecimal de identificador de subred subneteada, el prefijo de la dirección subneteada es [prefijo de 48 bits]:F::/p. (*F* es el valor hexadecimal del identificador de subred)

4. En la siguiente fila, incrementar el valor dentro de la porción del identificador de subred de la dirección global o de sitio local por el valor de i, y colocar el resultado en la segunda columna. Por ejemplo, en la segunda fila, el prefijo subneteado es [prefijo de 48 bits]:F+i::/p.

5. Repetir el paso 4 hasta completar la tabla.

Definir la longitud de un nuevo prefijo depende de cuantas subredes se necesiten. La tabla 3.I.1 muestra cuantas subredes pueden crearse utilizando un número de bits variable (hasta 16) para especificar cada subred.

Número de bits utilizados para subnetear (s)	Número de subredes (n) requeridas
1	1-2
2	3-4
3	5-8
4	9-16
5	17-32
6	33-64
7	65-128
8	129-256
9	257-512
10	513-1024
11	1025-2048
12	2049-4096
13	4097-8192
14	8193-16384
15	16385-32768
16	32769-65536

Tabla 3.I.1: *Identificadores del número de bits utilizados para subnetear sugun el número de redes requeridas.*

Finalmente, hay que agregar que dado que el tamaño del prefijo de la dirección es de 64 bits, lo cual viene siendo la máscara de subred en IPv6, queda definido el número fijo de 264 hosts en cada subred obtenida al subnetear.

3) Ejemplo de subneteo en IPv6.

En una organización se requiere dividir el espacio de direccionamiento asignado en una dirección unicast global 3FFE:FFFF:0:E100::/54, para un máximo de 8 subredes. Desarrollar el procedimiento para subnetear el prefijo de la dirección indicada.

Paso1:

$m = 54$, entonces, $f = m - 48 = 54 - 48 = 6$

Para un máximo de 8 subredes de tabla 3.I.1, se tiene que $s = 3$

O bien, $n = 2^s = 2^3 = 8$

$i = 2^{16-(f+s)} = 2^{16-(6+3)} = 2^7 = 128_{10} = 80_{16}$

$p = m + s = 54 + 3 = 57$

F = 0xE100

Paso 2 y sucesivos:

Número de subred	Prefijo de dirección subneteado	Rango de direcciones de hosts (2^{64})
1	3FFE:FFFF:0:***E100***::/57	3FFE:FFFF:0:E100::1 - 3FFE:FFFF:0:E100:FFFF:FFFF:FFFF:FFFF
2	3FFE:FFFF:0:***E180***::/57	3FFE:FFFF:0:E180::1 - 3FFE:FFFF:0:E180:FFFF:FFFF:FFFF:FFFF
3	3FFE:FFFF:0:***E200***::/57	3FFE:FFFF:0:E200::1 - 3FFE:FFFF:0:E200:FFFF:FFFF:FFFF:FFFF
4	3FFE:FFFF:0:***E280***::/57	3FFE:FFFF:0:E280::1 - 3FFE:FFFF:0:E280:FFFF:FFFF:FFFF:FFFF
5	3FFE:FFFF:0:***E300***::/57	3FFE:FFFF:0:E300::1 - 3FFE:FFFF:0:E300:FFFF:FFFF:FFFF:FFFF
6	3FFE:FFFF:0:***E380***::/57	3FFE:FFFF:0:E380::1 - 3FFE:FFFF:0:E380:FFFF:FFFF:FFFF:FFFF
7	3FFE:FFFF:0:***E400***::/57	3FFE:FFFF:0:E400::1 - 3FFE:FFFF:0:E400:FFFF:FFFF:FFFF:FFFF
8	3FFE:FFFF:0:***E480***::/57	3FFE:FFFF:0:E480::1 - 3FFE:FFFF:0:E480:FFFF:FFFF:FFFF:FFFF

J. ASIGNACIÓN DE DIRECCIONES IPv6

En la figura 3.J.1 se muestra gráficamente el proceso de asignación de direcciones IPv6, considerando a una compañía de servicios de Internet como un ISP.

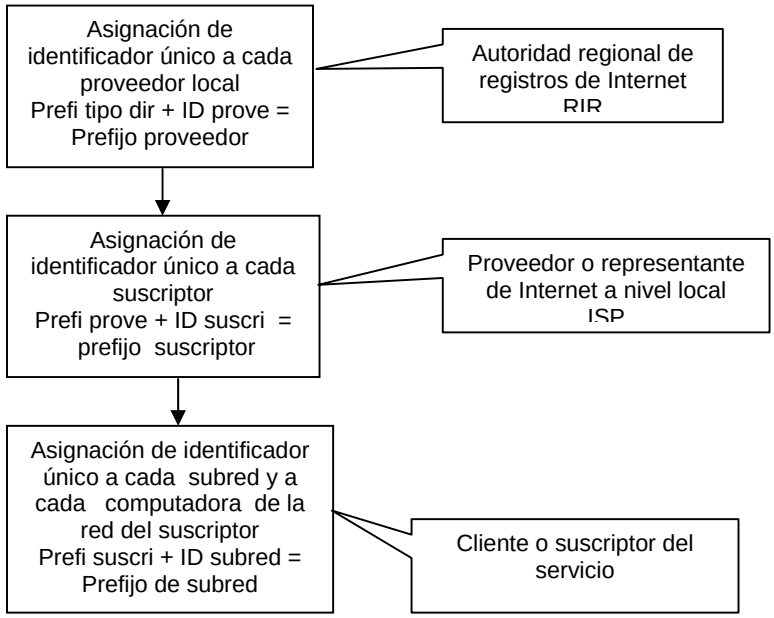


Figura 3.J.1: *Proceso de asignación de direcciones IPv6.*

En la figura 3.J.2 se muestra un esquema de jerarquía de direcciones IPv6 para una dirección asignada por un proveedor de servicios de Internet.

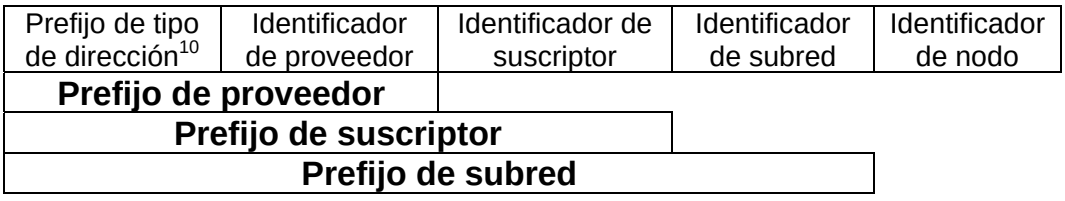


Figura 3.J.2: *Jerarquía de direcciones IPv6 para dirección asignada.*

Para que un proveedor local o ISP le sea asignado un bloque de direcciones IPv6 por parte de un RIR como LACNIC, tiene que hacerlo a través de una solicitud cuya versión LACNIC IPv6 Template 20060503-2-SP se adjunta en Anexos B.

[10] Ver tabla 3.B.1

4. PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET VERSIÓN 6 (ICMPv6)

A. INTRODUCCIÓN

El *Protocolo de Mensajes de Control de Internet* (ICMP) ha sido definido desde IPv4 en el RFC792 y modificado para IPv6 en el RFC1885 de 1995; luego fue actualizado por el RFC2463 de 1998, para que en el 2006 sea sustituido por el RFC4443 incorporando algunos cambios o mejoras.
Los mensajes ICMPv6 son utilizados por nodos intermedios (routers) o destino (host) para enviar información o notificación de errores producidos por la transmisión de datagramas desde un nodo origen.
ICMPv6 no sólo es la base para que operen funciones de diagnóstico de red tales como *ping* y *traceroute*, sino de mecanismos como el *Descubrimiento de la MTU de la ruta*. Trabaja también como protocolo de transporte de los protocolos *Descubrimiento de Vecindario* y *Descubrimiento de Escuchas Multicast*.

B. MENSAJES DE CONTROL DE INTERNET

1) Formato general del mensaje ICMPv6
ICMPv6 es fundamental para IPv6, sus mensajes son encapsulados dentro de paquetes IP, tomando el valor de 58 en el campo *siguiente cabecera* para su anexión. El formato de los mensajes ICMPv6 se muestra en la figura 4.B.1 tal como se vería ligado a la cabecera IPv6 básica.

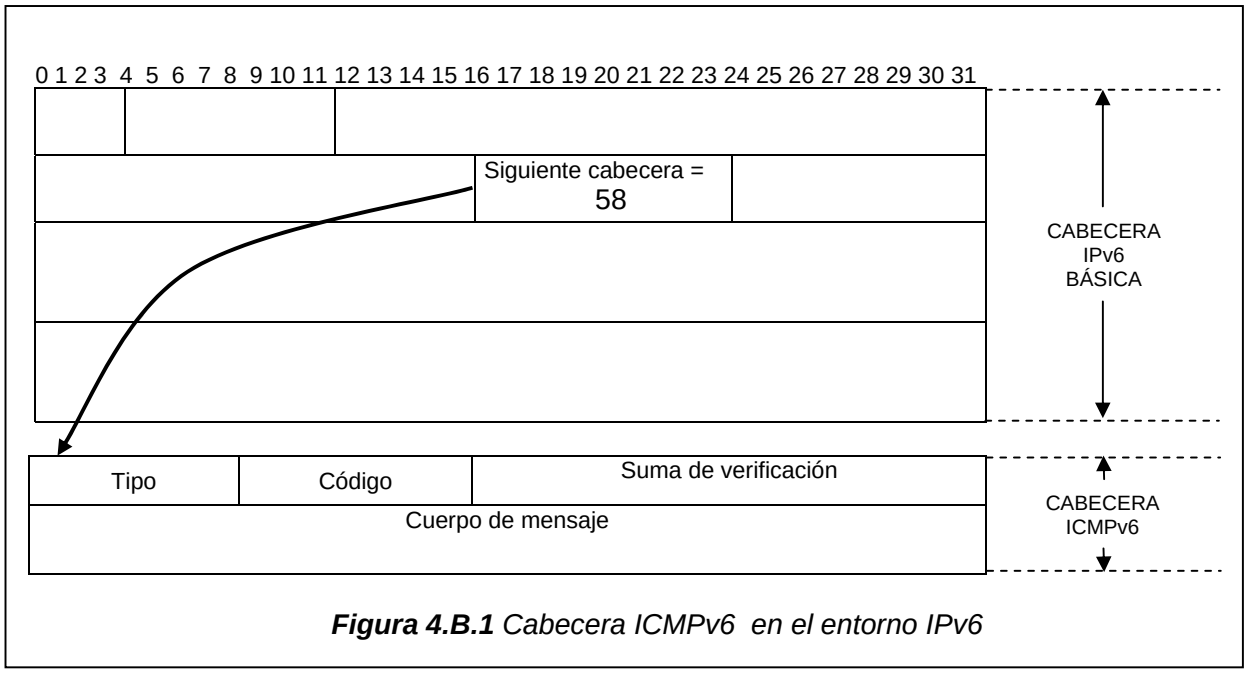


Figura 4.B.1 *Cabecera ICMPv6 en el entorno IPv6*

Los campos que componen un mensaje ICMPv6 son:

a. *Tipo*: valor representado en ocho bits que señala el tipo de mensaje que está siendo transmitido y que puede caer en dos categorías identificadas por el valor del bit de mayor orden, donde un 0 indica un mensaje de error y un 1 un mensaje de información. De tal manera que los valores del tipo de mensajes de error van desde 0 a 127, mientras que los de mensajes de información desde 128 a 255. En la tabla 4.B.1 se muestra el detalle de los mensajes ICMPv6 válidos a la fecha registrado por IANA (Autoridad de Números de Internet Asignados) y descritos en varios RFC.

b. *Código*: este valor de 8 bits se utiliza para refinar el detalle del tipo de mensaje.
c. *Suma de Verificación*: este campo de 16 bits se utiliza para detectar corrupción en los datos del mensaje ICMPv6 y de las partes de la cabecera IPv6.
d. Cuerpo de mensaje.

Tipo	Nombre	Referencia
1	Destino inalcanzable	RFC 4443
2	Paquete demasiado grande	RFC 4443
3	Tiempo excedido	RFC 4443
4	Problema de parámetros	RFC 4443
100	Experimentación privada	RFC 4443
101	Experimentación privada	RFC 4443
127	Reservado para expansión de mensajes de error	RFC 4443
128	Petición de eco	RFC 4443
129	Respuesta de eco	RFC 4443
130	Consulta de escucha multicast versión 1/versión 2	RFC 2710/3810
131	Reporte de escucha multicast versión 1	RFC 2710
132	Escucha multicast realizada versión 1	RFC 2710
133	Solicitud de router [a]	RFC 2461
134	Anuncio de router [a]	RFC 2461
135	Solicitud de vecino [a]	RFC 2461
136	Anuncio de vecino [a]	RFC 2461
137	Redirección de mensaje [a]	RFC 2461
138	Renumeración de router	RFC 2894
139	Consulta de información de nodo ICMP	RFC 2894
140	Respuesta de información de nodo ICMP	RFC 2894
141	Mensaje de solicitud de descubrimiento inverso de vecino [a]	RFC 3122
142	Mensaje de anuncio de descubrimiento inverso de vecino [a]	RFC 3122
143	Reporte de escucha multicast versión 2	RFC 3810
144	Petición de descubrimiento de la dirección de agente en casa [b]	RFC3775
145	Respuesta de descubrimiento de la dirección de agente en casa [b]	RFC3775
146	Solicitud de prefijo móvil [b]	RFC3775
147	Anuncio de prefijo móvil [b]	RFC3775
200	Experimentación privada	RFC 4443
148	Solicitud de ruta de certificación	RFC3971
149	Anuncio de ruta de certificación	RFC3971
150	Movilidad experimental	RFC4065
151	Anuncio de router multicast	RFC4286
152	Solicitud de router multicast	RFC4286
153	Terminación de router multicast	RFC4286
201	Experimentación privada	RFC 4443
255	Reservado para expansión de mensajes de información	RFC 4443

Tabla 4.B.1: *Valores válidos para tipos de Mensaje ICMPv6*

[a] Se desarrollan en el capítulo 5: Protocolo de Descubrimiento de Vecindario.
[b] Se desarrollan en el capítulo 9: Movilidad e IP inalámbrico.

2) Algunos tópicos sobre mensajes ICMPv6

a. *MTU* de IPv6: es la *Unidad de Transmisión Máxima* que IPv6 requiere que cada enlace maneje. Está definida en el RFC2460 que la especifica en un mínimo de1280 octetos y un valor óptimo de 1500 octetos.

b. MTU de la ruta (Path MTU): es el tamaño del paquete más grande que puede ser llevado sobre cualquier red a lo largo de la ruta entre la fuente y el destino sin tener que fragmentarlo. Existe un método basado en este concepto, denominado *Descubrimiento de la MTU de la ruta*, que utiliza mensajes ICMP para determinarla.

c. Cálculo de *Suma de Verificación (Checksum)*: la suma de verificación es el complemento a uno de 16 bits de la suma de complemento a uno del mensaje ICMPv6 completo, comenzando con el campo ICMPv6 *tipo de mensaje*, más los campos que comprende la *Pseudo-Cabecera* (Figura 4.B.2), que se utiliza sólo para este cálculo en todos los protocolos de transporte. Para este caso, se utiliza el valor 58 en el campo *siguiente cabecera* de la *Pseudo-Cabecera*.

Dirección origen	
Dirección destino	
Longitud de carga útil de transporte	
0	Siguiente cabecera

Figura 4.B.2: *Pseudo-Cabecera para Suma de Verificación*

d. *Descubrimiento de Escuchas Multicast (MLD) v1/ v2*: protocolo que permite que cada router IPv6 descubra la presencia de escuchas multicast en los enlaces a los que están conectados directamente, utilizando mensajes ICMPv6. Se considera un sub-protocolo de ICMPv6 y equivale a IGMP (Protocolo de gestión de grupos de Internet) para IPv4. MLDv2 añade a un nodo la habilidad para mostrar interés en escuchar a los paquetes con una dirección multicast particular.

e. *Renumeración de Routers (RR)*: mecanismo que permite configurar y reconfigurar prefijos de direccionamiento de routers tan fácilmente como lo que la combinación de *Descubrimiento de vecindario* y *Autoconfiguración de direcciones* hace para hosts.

C. ESPECIFICACIONES DE VARIOS MENSAJES ICMPv6

1) Especificaciones de mensajes de error ICMPv6

a. *Destino inalcanzable* (Figura 4.C.1): es enviado por un nodo intermedio (router), o bien, por la capa de IPv6 en el nodo que lo origina, como respuesta cuando no se puede alcanzar el destino de un datagrama o paquete por razones distintas a la de congestión de la red, de lo contrario no es generado.

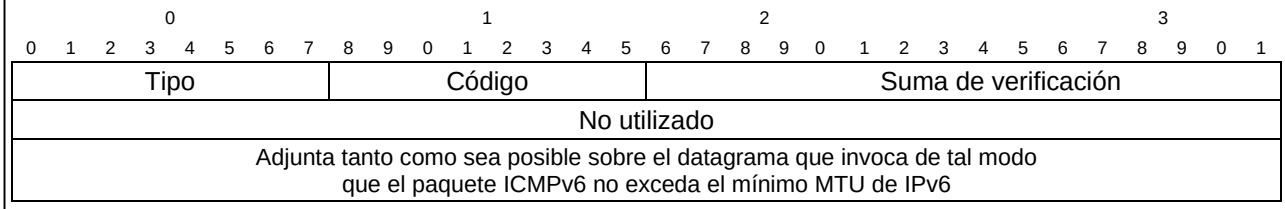


Figura 4.C.1: *Formato de Mensaje de Destino Inalcanzable*

Valores para los campos:

i. Campos IPv6:

- *Dirección destino*: se obtiene del campo *dirección destino* del datagrama que invoca la acción.

ii. Campos ICMPv6:

- *Tipo*: 1
- *Código*:
  - 0- No hay ruta hacia destino
    Cuando no hay una ruta por defecto en la tabla de ruteo
  - 1- Comunicación con destino prohibida administrativamente
    Falla en envío por prohibición administrativa. Ej. Filtro Firewall
  - 2- Fuera del ámbito de dirección fuente
    Destino está fuera del ámbito de la dirección fuente
  - 3- Dirección inalcanzable
    Inhabilidad de convertir la dirección IPv6 de destino en una dirección de enlace correspondiente, o bien, cualquier otra razón que no se adapte a los otros códigos.
  - 4- Puerto inalcanzable
    Cuando el protocolo de transporte no tiene medios para informar al emisor sobre un paquete, el nodo destino origina un mensaje
  - 5- Dirección origen no cumple políticas de ingreso / egreso
    Falla en el envío debido a que el paquete no cumple con las políticas de ingreso / egreso.
  - 6- Ruta de destino rechazada
    Fallo en el envío debido a que la ruta de destino es rechazada
- *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c*
- *No utilizado*: este campo no es utilizado por todos los valores de código. Debe ser inicializado a cero por el emisor e ignorado por el receptor

b. *Paquete demasiado grande* (Figura 4.C.2): es enviado como respuesta por un router que no puede hacer seguir adelante un paquete debido a que es más grande que la MTU del nodo siguiente. El procedimiento de *Descubrimiento del MTU de la ruta* utiliza este tipo de mensaje.

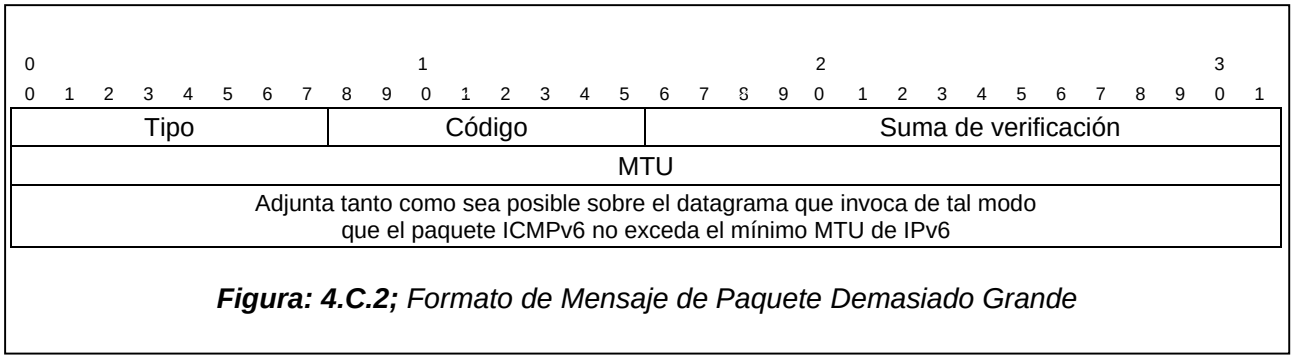


Figura: 4.C.2; *Formato de Mensaje de Paquete Demasiado Grande*

Valores para los campos:

i. Campos IPv6:

- *Dirección destino*: se obtiene del campo *dirección destino* del datagrama que invoca la acción.

ii. Campos ICMPv6:

- *Tipo*: 2
- *Código*: puesto a 0 por el emisor e ignorado por receptor
- *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c*
- *MTU*: la unidad de transmisión máxima del enlace del próximo salto.

c. Tiempo excedido (Figura 4.C.3): es enviado cuando un nodo intermedio recibe un paquete con un límite de salto de cero o si lo disminuye a cero, también se envía este mensaje si el reensamblado de fragmentos está fuera de tiempo. En el primero de los casos es descartado el paquete. Este mensaje es sumamente útil para construir la función *traceroute*, que permite a un nodo identificar todas las rutas que un paquete toma a lo largo de su camino entre el origen y el destino.

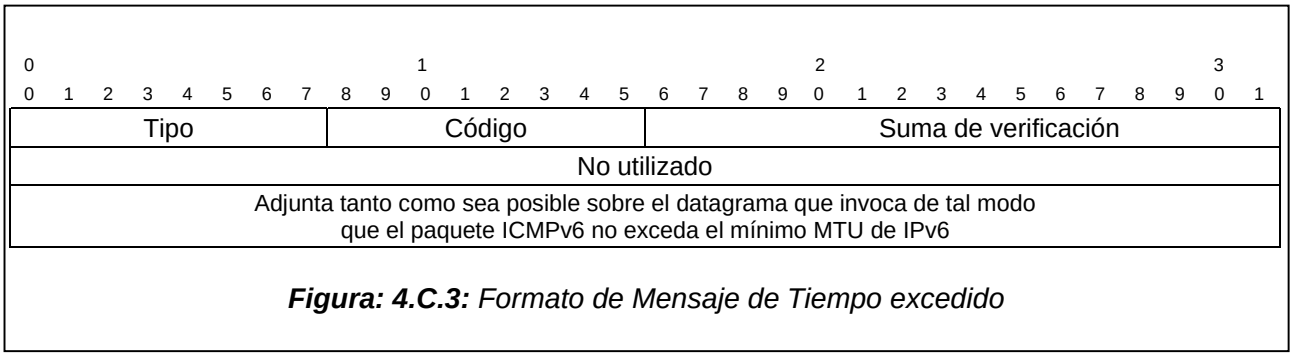


Figura: 4.C.3: *Formato de Mensaje de Tiempo excedido*

Valores para los campos:

i. Campos IPv6:

- *Dirección destino*: se obtiene del campo *dirección destino* del datagrama que invoca la acción.

ii. Campos ICMPv6:

- *Tipo*: 3
- *Código*:

  0- Límite de salto excedido en tránsito
  Encaminamiento cíclico o valor inicial de límite de salto muy bajo

  1- Tiempo de reensamble de fragmentos excedido

Reporte por tiempo de reensamble de fragmentos expirado

- *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c*
- *No utilizado*: este campo no es utilizado por todos los valores de código. Debe ser inicializado a cero por el emisor e ignorado por el receptor

d. *Problema de parámetro* (Figura 4.C.4): se envía si un nodo encuentra un problema con algún campo de la cabecera IPv6 o de alguna cabecera de extensión, indicando el tipo y la localización del problema, y descartando el paquete que origina el problema.

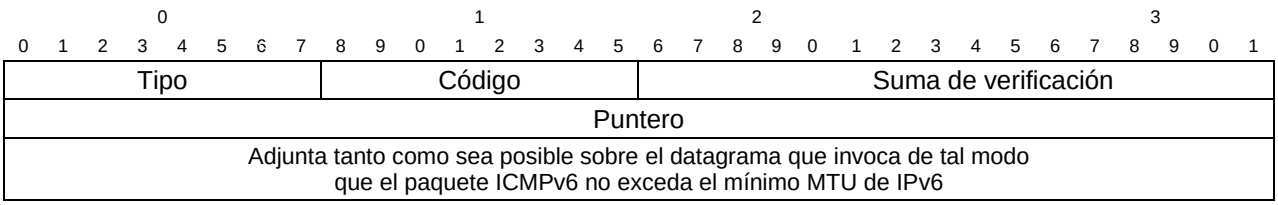


Figura 4.C.4: *Formato de Mensaje de Problema de Parámetro*

Valores para los campos:

i. Campos IPv6:

- *Dirección destino*: se obtiene del campo *dirección destino* del datagrama que invoca la acción.

Campos ICMPv6:

- *Tipo*: 4
- *Código*:
  0- Encontrado campo de cabecera erróneo
  1- Encontrado tipo de *siguiente cabecera* irreconocible
  2- Encontrada opción IPv6 irreconocible
- *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c*
- *Puntero*: identifica el umbral del octeto, dentro del paquete que invoca, donde el error fue detectado, aún si el campo en error está más allá del tamaño máximo en que se ajusta el mensaje ICMPv6.

2) Especificaciones de mensajes de información ICMPv6

a. *Petición de Eco* (Figura 4.C.5): en un nodo IPv6 se debe implementar una función interlocutora, que trabaje también con propósitos de diagnóstico, emitiendo y recibiendo peticiones de eco. No hay limitación en la cantidad de datos que se puede poner en un mensaje de *petición de eco* y puede ser enviado a cualquier dirección IPv6 válida. Este tipo de mensaje forma parte del fundamento de la función *ping*, valiosa herramienta de diagnóstico utilizada para determinar si un host particular está conectado a la misma red que cualquier otro host.

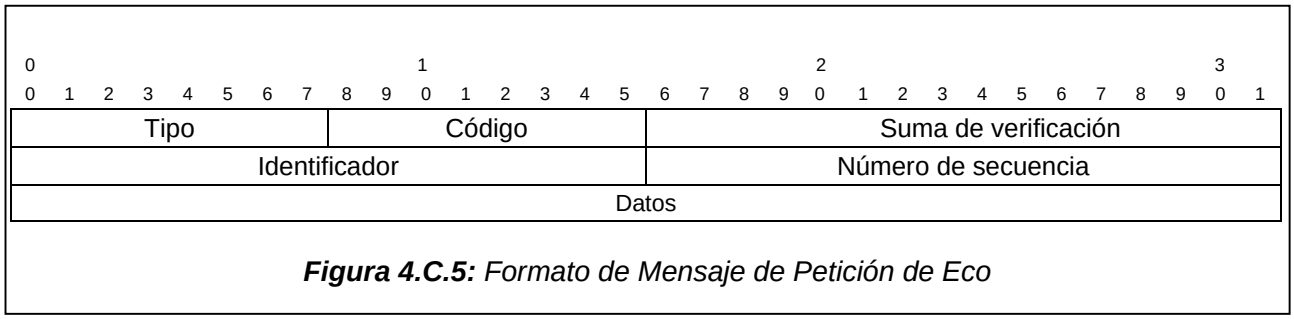


Figura 4.C.5: *Formato de Mensaje de Petición de Eco*

Valores para los campos:

i. Campos IPv6:
   - *Dirección destino*: cualquier dirección IPv6 legal.

ii. Campos ICMPv6:
   - *Tipo*: 128
   - *Código*: 0
   - *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c*
   - *Identificador*: ayuda ajustar las *respuestas de eco* a esta *petición de eco*. Puede tener el valor de cero. Es opcional.
   - *Número de secuencia*: ayuda en ajustar *respuestas de eco* a esta *petición de eco*. Puede tener el valor de cero. Es opcional.
   - *Datos*: cero o más octetos de datos arbitrarios. Es opcional.

b. *Respuesta de eco* (Figura 4.B.6): en un nodo IPv6 se debe implementar una función interlocutora, que trabaje también con propósitos de diagnóstico, recibiendo peticiones de eco y emitiendo respuestas de eco. No hay limitación en la cantidad de datos que se puede poner en un mensaje de respuesta de eco. La dirección de origen que deben incluir los mensajes respuesta de eco será, en el caso de un mensaje de petición de eco a una dirección unicast, la misma dirección destino de este mensaje. En el caso de un mensaje de petición de eco a una dirección multicast o anycast, la dirección destino del mensaje de respuesta de eco a enviar será una dirección unicast perteneciente a la interfaz en la cual dicho mensaje de petición de eco fue recibido. Estos tipos de mensaje son fundamento de la función ping, valiosa herramienta de diagnóstico utilizada para determinar si un host particular está conectado a la misma red que cualquier otro host.

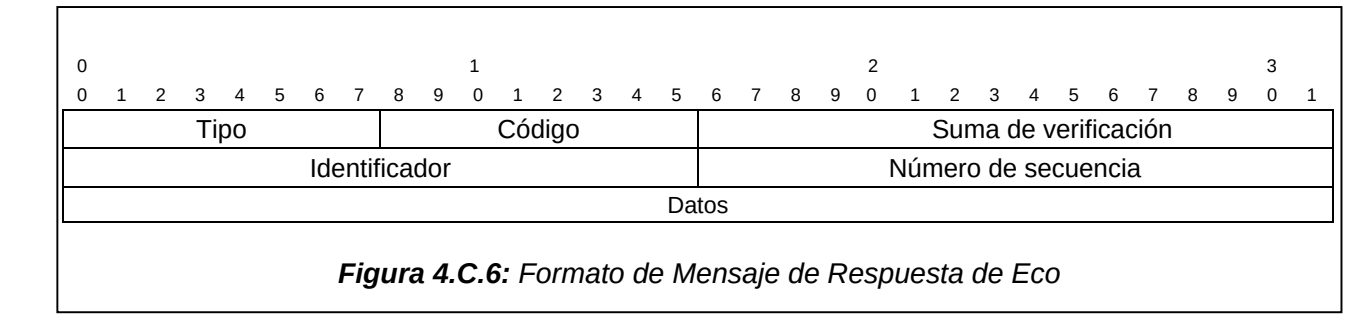


Figura 4.C.6: *Formato de Mensaje de Respuesta de Eco*

Valores para los campos:

i. Campos IPv6:
   - *Dirección destino*: cualquier dirección IPv6 legal.

ii. Campos ICMPv6:
   - *Tipo*: 129

- *Código*: 0
- *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c*
- *Identificador*: El identificador del mensaje de petición de eco invocado.
- *Número de secuencia*: Número de secuencia del mensaje de petición de eco invocado.
- *Datos*: Los datos del mensaje de petición de eco invocado.

c. *Consulta de Escucha Multicast (*Figura 4.C.7): mensaje MLD utilizado por un router para conocer cuáles direcciones multicast (consulta general), o bien, si una dirección de éstas en particular (consulta específica), tienen escuchas en un enlace conectado.
Versión 1: longitud de mensaje= 24 octetos (RFC 2710)

Figura 4.C.7: *Formato de Mensaje de Consulta de Escucha Multicast versión 1*

Valores para los campos:

i. Campos IPv6
- *Dirección origen IPv6 de enlace local*
- *Límite de salto IPv6 : 1*
- *Opción de Alerta de Encaminador IPv6 en una cabecera de Opciones salto por salto.*

ii. Campos ICMPv6
- *Tipo:* 130
- *Código:* Puesto a cero por el emisor, ignorado por los receptores
- *Suma de verificación:* Se procede como se indica en el apartado 4.B.2.c
- *Retraso máximo de respuesta:* Máximo retraso permitido antes de enviar un reporte de respuesta, expresado en milisegundos.
- *Reservado:* Puesto a cero por el emisor, ignorado por los receptores
- *Dirección multicast:*
  0 - Consulta general
- *Dirección multicast IPv6 específica - Consulta específica de dirección multicast*

Versión 2: longitud de mensaje>= 28 octetos (RFC 3810)

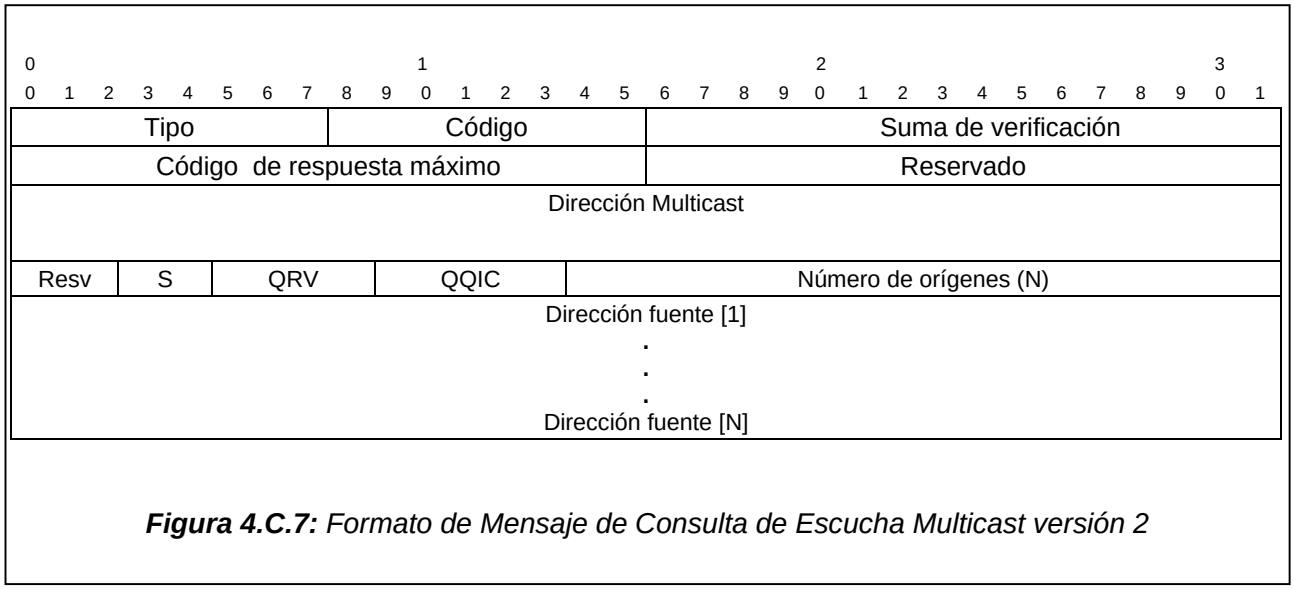


Figura 4.C.7: *Formato de Mensaje de Consulta de Escucha Multicast versión 2*

Valores para los campos:

i. Campos IPv6

- *Dirección origen IPv6 de enlace local*
- *Límite de salto IPv6 : 1*
- *Opción de Alerta de Router IPv6 en una cabecera de Opciones salto por salto.*

ii. Campos ICMPv6

- *Tipo*: 130
- *Código*: Puesto a cero por el emisor, ignorado por los receptores
- *Suma de verificación*: Se procede como se indica en el apartado *4.B.2.c*
- *Código máximo de respuesta*:
  Especifica el tiempo máximo permitido antes de que se envíe un reporte de respuesta. El Retraso máximo de respuesta, que es el tiempo real permitido en milisegundos, se deriva de éste como sigue:
  -Retraso máximo de respuesta = Código máximo de respuesta,
  si Código máximo de respuesta < 32768
  -Retraso máximo de respuesta = (mant | 0x1000) << (exp+3),
  si Código máximo de respuesta >= 32768, donde éste representa un valor de punto flotante como sigue:

  0 1 2 3 4 5 6 7 8 9 A B C D E F

1	exp	mant.

- *Reservado*: Puesto a cero por el emisor, ignorado por los receptores

- *Dirección multicast:*
  0 - Consulta general
  Dirección multicast IPv6 - Consulta específica de dirección multicast específica
  Dirección multicast IPv6 - Consulta específica de dirección multicast y específica de dirección fuente
- *Reservado (Resv):* Puesta a cero por el emisor. Ignorado por los receptores

- *Bandera S (Router supresor):* 1, indica a cualquier router receptor que tiene que suprimir las actualizaciones normales de cronómetro que ejecuta al escuchar una consulta. (Esto no elimina la elección propia del consultante)
- *QRV (Variable de robustez del consultante):* 1-7, valores normales que puede utilizar el consultante. Se le asigna el valor de 0, si excede a 7.
- *QQIC (código de intervalo de consulta del consultante):* Especifica el intervalo de consulta utilizado por el consultante. El intervalo real (QQI) en segundos se deriva de este código de la siguiente manera:
  QQI = QQIC, si QQIC < 128
  QQI = (mant | 0x10) << (exp + 3), si QQIC >= 128, donde éste representa un valor de punto flotante como sigue:

0	1	2 3 4	5 6 7
1	exp	mant	

d. *Reporte de Escucha Multicast versión 1 (*Figura 4.C.8*):* mensaje MLD generado en repuesta a un mensaje de consulta enviado por un router. Es también un mensaje no solicitado enviado por cualquier nodo cuando comienza a escuchar a una dirección multicast.

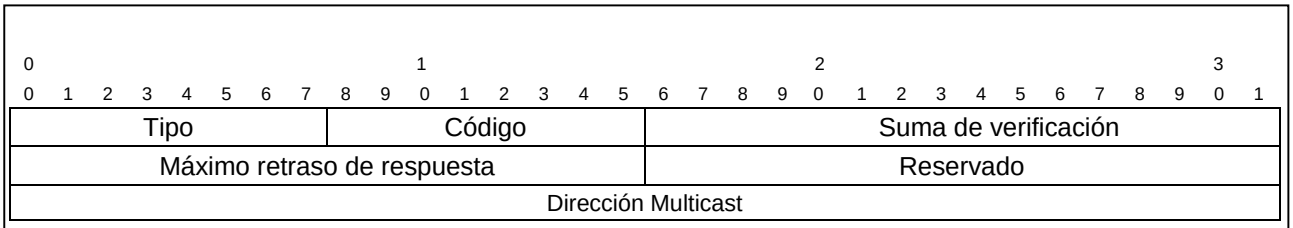


Figura 4.C.8: *Formato de Mensaje de Reporte de Escucha Multicast versión 1*

Valores para los campos:

i. Campos IPv6

- *Dirección origen IPv6 de enlace local*
- *Límite de salto IPv6 : 1*
- *Opción de Alerta de Router IPv6 en una cabecera de Opciones salto por salto.*

ii. Campos ICMPv6

- *Tipo: 131*
- *Código:* Puesto a cero por el emisor, ignorado por los receptores
- *Suma de verificación:* Se procede como se indica en el apartado 4.B.2.c
- *Máximo de retraso de respuesta:* Puesto a cero por el emisor, ignorado por los receptores
- *Reservado:* Puesto a cero por el emisor, ignorado por los receptores
- *Dirección multicast:* Especifica la dirección multicast a la cual el emisor de mensaje está escuchando

e. *Escucha Multicast realizada versión 1 (t*Figura 4.C.9*):* mensaje MLD enviado por un nodo al parar de escuchar a una dirección multicast.

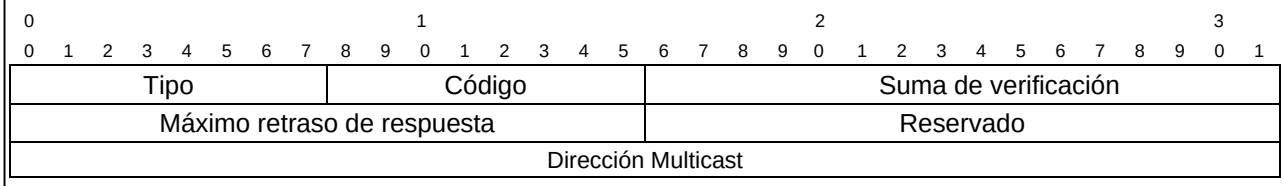


Figura 4.C.9: *Formato de Mensaje de Escucha Multicast realizada versión 1*

Valores para los campos:

i. Campos IPv6

- *Dirección origen IPv6 de enlace local*
- *Límite de salto IPv6 : 1*
- *Opción de Alerta de Router IPv6 en una cabecera de Opciones salto por salto.*

ii. Campos ICMPv6

- *Tipo: 132*
- *Código:* Puesto a cero por el emisor, ignorado por los receptores
- *Suma de verificación:* Se procede como se indica en el apartado 4.B.2.c
- *Máximo de retraso de respuesta:* Puesto a cero por el emisor, ignorado por los receptores
- *Reservado:* Puesto a cero por el emisor, ignorado por los receptores
- *Dirección multicast:* Especifica la dirección multicast a la cual el emisor de mensaje está cesando de escuchar

f. *Renumeración de router* (Figura 4.C.10): mensaje utilizado como medio para informar a un conjunto de routers de las operaciones de renumeración que han de desarrollar, incluyendo un modo de operación en ambientes en los cuales el número de routers es desconocido.

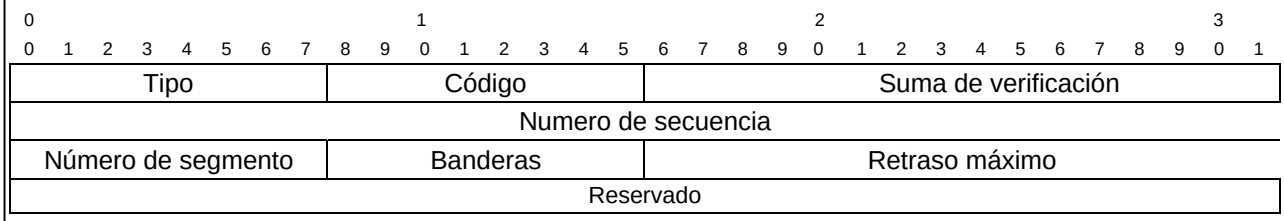


Figura 4.C.10: *Formato de Mensaje de Renumeración de router*

Valores para los campos:

i. Campos ICMPv6

- *Tipo:* 138
  1. *Código*:
     - 0 - Comando de renumeración de router
     - 1 - Resultado de renumeración de router
     - 255 - Reinicio de número de secuencia
- *Suma de verificación:* Se procede como se indica en el apartado 4.B.2.c
- *Número de secuencia:* un número de secuencia de 32 bits sin signo

- *Número de segmento:* un campo de 8 bits sin signo el cual enumera diferentes mensajes RR que tienen el mismo *Número de secuencia*
- *Banderas:* combinación de banderas de un bit, cinco de los cuales son definidos y tres bits son reservados

T	R	A	S	P	reserv

T Comando de prueba
0 - configuración de router va a modificarse
1 - mensaje de prueba
R Resultado pedido
0 - mensaje de resultado no debe ser enviado
1 - router debe enviar mensaje de resultado hasta completar proceso
A Todas las interfaces
0 - comando no debe aplicarse a interfaces fuera de servicio
1 - comando debe aplicarse aunque interfaces estén fuera de servicio
S Sitio - específico
0 - se aplica a interfaces sin importar al sitio que pertenecen
1 - comando se aplica a interfaces del mismo sitio
P Procesado previamente
0 - mensaje de resultado contiene reporte completo del proceso
1 - mensaje de comando fue previamente procesado

- *Retraso máximo:* campo de 16 bits sin signo que especifica el tiempo máximo en milisegundos que un router puede retardarse para enviar cualquier respuesta a ese comando
- *Cuerpo del mensaje:* secuencia de ceros o más operaciones de control de prefijo

g. *Reporte de escucha multicast versión 2* (Figura 4.C.11): es enviado por nodos IP para informar a routers del vecindario sobre el estado al corriente de las escuchas multicast, o sobre los cambios en el estado de las escuchas multicast de sus interfaces.

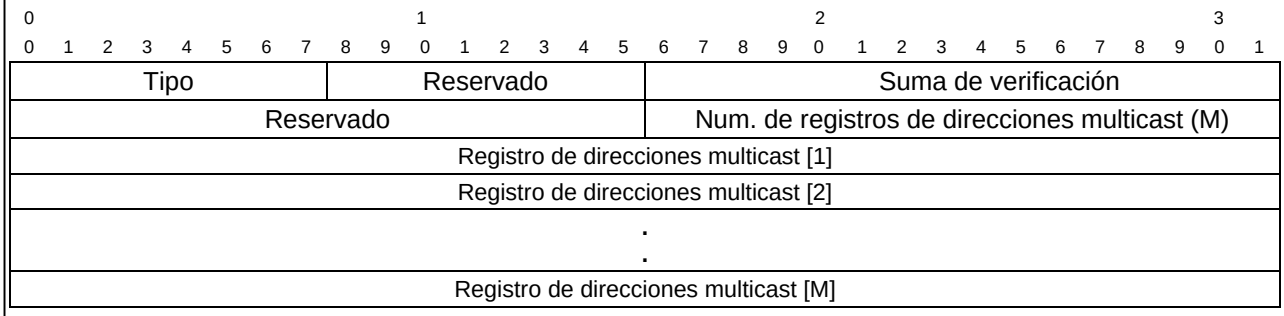


Figura 4.C.11: *Formato de Mensaje de Reporte de Escucha Multicast versión 2*

Valores para los campos:

i. Campos IPv6

- Dirección origen IPv6 de enlace local
- *Límite de salto IPv6* : 1
- *Opción de Alerta de Router IPv6* en una cabecera de *Opciones salto por salto.*

ii. Campos ICMPv6

- *Tipo*: 143
- *Reservado*: Puesto a cero en la transmisión, ignorado en la recepción
- *Suma de verificación*: Se procede como se indica en el apartado *4.B.2.c*
- *Máximo de retraso de respuesta*: Puesto a cero por el emisor, ignorado por los receptores
- *Reservado*: Puestos a cero por el emisor, ignorado por los receptores
- *Número de registros de direcciones multitast (M)*: Número de estos registros presentes en este reporte
- *Registro de dirección multicast*: bloque de campos que contiene información del emisor que escucha una dirección multicast simple en la interfaz de la cual se envía el reporte. Su formato es el siguiente:

Tipo de registro	Longitud de datos aux.	Número de fuentes (N)
Dirección multicast		
Dirección fuente [1] . . Dirección fuente [N]		
Datos auxiliares		

Valores de campos:

- *Tipo de registro*
  1 MODE_IS_INCLUDE
  2 MODE_IS_EXCLUDE
  3 CHANGE_TO_INCLUDE_MODE
  4 CHANGE_TO_EXCLUDE_MODE
  5 ALLOW_NEW_SOURCES
  6 BLOCK_OLD_SOURCES
- *Longitud de datos auxiliares*: longitud en unidades de palabras de 32 bits, que puede contener un cero para indicar ausencia de datos.
- *Número de Fuentes*: número de fuentes presente en el registro
- *Dirección multicast*: dirección multicast a la que pertenece este registro .
- *Dirección fuente [i]* : vector de N direcciones unicast
- *Datos auxiliares*: si el campo de *Longitud de carga útil* en la cabecera IPv6 del reporte recibido indica presencia de octetos adicionales, se incluirán en el cálculo de la *Suma de verificación*.

5. PROTOCOLO DE DESCUBRIMIENTO DE VECINDARIO (ND)

A. INTRODUCCIÓN.

En este apartado se estudian las características principales que posee el protocolo de descubrimiento de vecindario para IPv6 y se compara con su protocolo antecesor en IPv4. Además se describen los mensajes de los que se vale este protocolo para realizar diferentes tareas y se definen las funciones principales que tiene este protocolo en la comunicación entre los nodos de una red que usan IPv6. El estudio completo del tema que trata este apartado se encuentra publicado en el estándar de Internet RFC 2461 y algunas actualizaciones de éste.

Para iniciar el estudio de este apartado es esencial comprender que el funcionamiento básico del protocolo ND se focaliza en que todos los nodos (host o routers) que utilicen el nuevo protocolo de Internet IPv6 utilicen el descubrimiento de vecindario para determinar las direcciones de la capa de enlace de todos los otros nodos que se encuentran en la interfaz de red y verifiquen si estos nodos continúan siendo alcanzables. Asimismo, este protocolo tiene el objetivo de almacenar cualquier actualización que se realice en dichos nodos. La ilustración de esta idea se presenta en la figura 5.A.1.

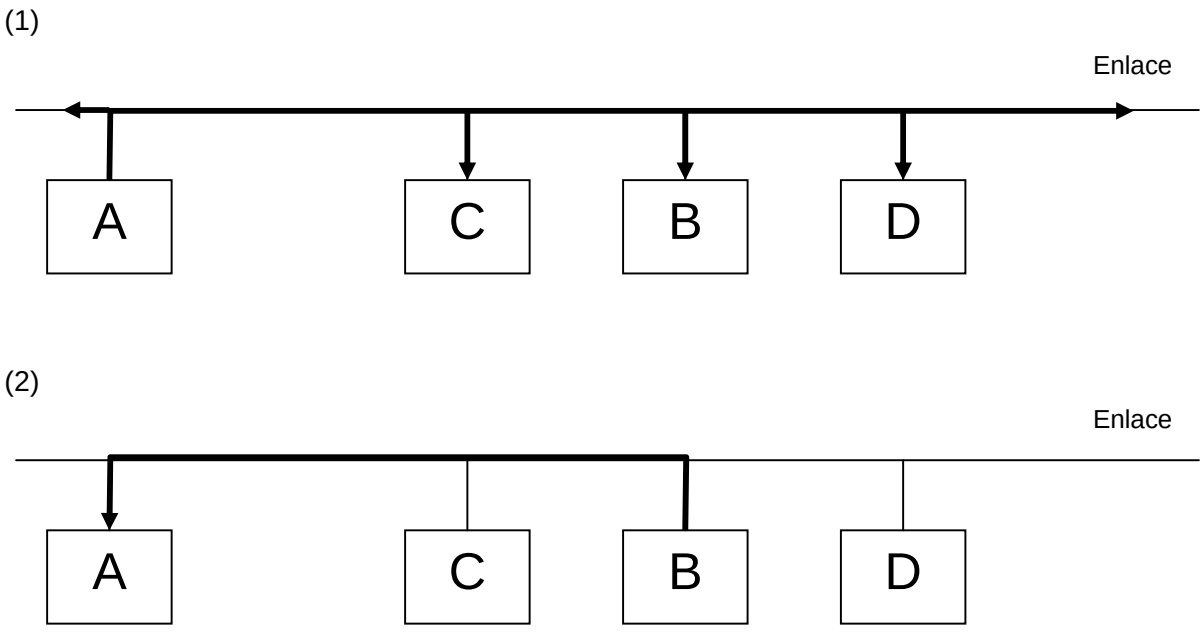


Figura 5.A.1: *Ilustración del funcionamiento básico del Protocolo ND. (1) El nodo A transmite una solicitud de multidifusión para descubrir la presencia del nodo B y determinar su dirección de la capa de enlace o cualquier cambio que pueda haber sufrido. (2) El nodo B le anuncia su presencia al nodo A y le envía los parámetros que necesita conocer.*

También se incluye en este apartado el estudio de los mensajes del protocolo de descubrimiento inverso de vecindario (IND). El estudio completo del protocolo IND se encuentra publicado en el estándar de Internet RFC 3122.

B. EL PROTOCOLO ND DE IPv6 COMPARADO CON ARP DE IPv4.

El protocolo de descubrimiento de vecindario frente a los mecanismos existentes en IPv4, reporta numerosas ventajas entre las que tenemos las siguientes:

a) El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de encaminamiento.
b) El anuncio de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
c) El anuncio de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
d) El anuncio de router permite la autoconfiguración de direcciones.
e) Los routers pueden anunciar a los host que se encuentran en el mismo enlace la capacidad de la MTU.
f) Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
g) Se pueden asignar múltiples prefijos al mismo enlace y por defecto los hosts aprenden todos los prefijos por los anuncios del router. Sin embargo, los routers pueden ser configurados para omitir parte o todos los prefijos en el anuncio, de forma que los host consideren que los destinos están fuera del alcance; de esta forma, enviarán el trafico a los routers, quien a su vez los redirigirá según corresponda.
h) A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto esta en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible de que los nodos conozcan todos los prefijos de los destinos en el mismo enlace.
i) La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
j) A diferencia de ARP en este protocolo no son precisos campos de preferencia (para definir la “estabilidad” de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.
k) El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una renumeraciónde router para usar nuevos prefijos globales.
l) El límite de saltos siempre es igual a 255, lo que evita que haya envíos accidentales o intencionados desde nodos fuera del alcance, dado que los routers decrementan automáticamente este campo en cada salto.
m) Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

C. MENSAJES ICMPv6 CON LOS QUE TRABAJA EL PROTOCOLO ND.

Para operar con el protocolo de descubrimiento de vecindario se emplean 5 tipos de mensajes ICMPv6. Es importante recalcar que para definir las funciones del protocolo de descubrimiento de vecindario en términos de mensajes ICMPv6 no son necesarios protocolos adicionales (como es el caso del protocolo ARP).

Los mensajes ICMPv6 y particularmente las peticiones son usualmente mensajes de multidifusión, mientras que las respuestas que se hacen al nodo que realiza la petición son mensajes unicast ó mensajes de multidifusión que son enviados a todos los nodos del grupo de direcciones multicast, equivalente funcional del concepto de broadcast (difusión) en IPv4.

Los mensajes ICMPv6 que se definen en el RFC 2461 para el descubrimiento de vecindario son los mostrados en la tabla 5.C.1

Tipo de mensaje	Valor del tipo de paquete del mensaje ICMPv6
Solicitud de Router	133
Anuncio de Router	134
Solicitud de vecino	135
Anuncio de vecino	136
Redirección	137
Solicitud de descubrimiento inverso de vecino	141
Anuncio de descubrimiento inverso de vecino	142

Tabla 5.C.1: *Tipos de mensaje ICMPv6 usados en el protocolo de descubrimiento de vecindario.*

Los mensajes ICMP expuestos en la tabla 5.C.1 se encapsulan dentro de paquetes IP y afectan los siguientes campos de la cabecera IPv6 básica:

a) *Dirección Fuente (Source Address):* Se asigna la dirección IP de la interfaz que envía el mensaje.
b) *Dirección Destino (Destination Address):* Típicamente se asigna una dirección multicast para todos los routers.
c) *Límite de Salto (Hop Limit):* Debe poseer un valor máximo de 255
d) *Cabecera de Autentificación (Authentication Header):* Si existe un certificado de autenticación entre el nodo remitente y el nodo destino. Entonces el remitente debe incluir esta cabecera.

1) Solicitud de Router.
Este mensaje se genera cuando una interfaz de red es activada permitiendo al host enviar un anuncio fuera del router para solicitar a los routers que se anuncien inmediatamente. El formato del mensaje de solicitud de router se encuentra ilustrado en la figura 5.C.1.

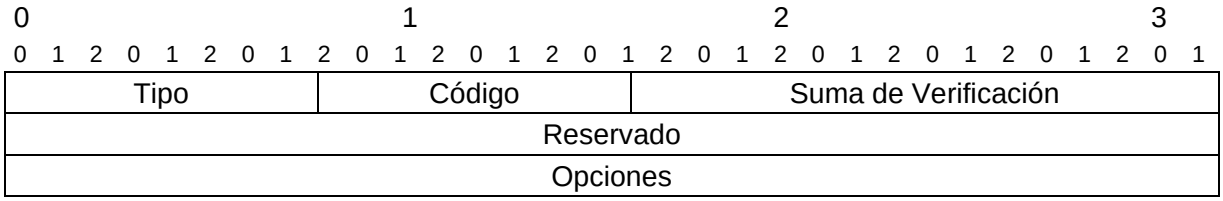


Figura 5.C.1: *Formato del mensaje de solicitud de router*

Los campos que posee el mensaje ICMP de solicitud de router se definen a continuación:

a) *Tipo (Type):* Posee el valor de 133
b) *Código (Code):* Posee el valor de 0
c) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
d) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.

e) *Opciones (Options):* Se incluye la dirección de la capa de enlace del nodo origen si la dirección de origen se encuentra especificada en la capa de enlace, de lo contrario no se debe incluir. La única opción valida para este mensaje es:
Dirección de la capa de enlace de origen.

2) Anuncio de Router.

Los routers anuncian su presencia junto con varios enlaces y parámetros de Internet periódicamente (el anuncio se da entre 4 y 1800 seg.) en respuesta a la solicitud de mensaje de un router. El anuncio del router contiene.

i. un prefijo que es usado para enlaces determinados.
ii. una configuración de dirección.
iii. un tiempo de vida.
iv. sugieren un valor límite de saltos.

El formato del mensaje de anuncio de router se encuentra ilustrado en la figura 5.C.2.

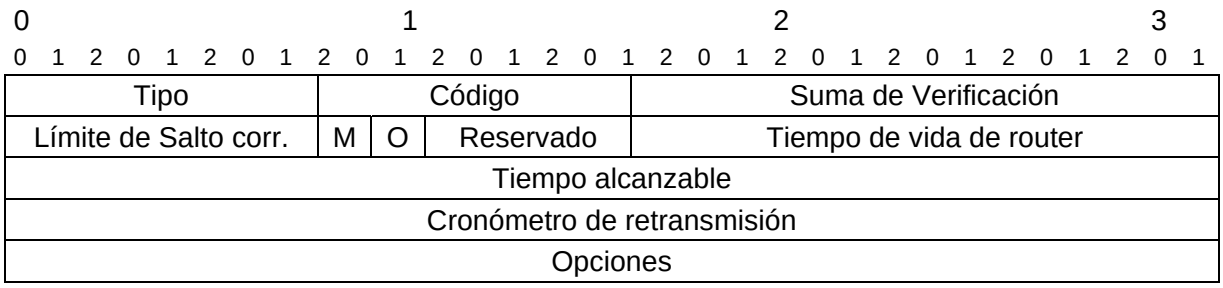


Figura 5.C.2: *Formato del mensaje de anuncio de router*

Los campos que posee el mensaje ICMP de solicitud de router se definen a continuación:

a) *Tipo (Type):* Posee el valor de 134
b) *Código (Code):* Posee el valor de 0
c) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
d) *Límite de Salto corriente (Cur Hop Limit):* Entero sin signo de 8 bits. El valor predefinido que debe ponerse en este campo es el de la cuenta del salto de la cabecera IP para los paquetes IP salientes.
e) *M:* Bandera de 1 bit que indica que un host puede utilizar la autoconfiguración sin estado (*stateless autoconfiguration*) para obtener su propia dirección.
f) *O:* Bandera de 1 bit que indica si el host puede hacer uso de la autoconfiguración con estado (stateful *autoconfiguration*) y asi obtener información adicional de configuración.
g) *Reservado (Reserved):* Campo sin usar de 6 bits. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.
h) *Tiempo de vida del router (Router Lifetime):* Entero sin signo de 16 bits. El *tiempo de vida* se asocia con el router predefinido y su medida se da en las unidades de segundos. El valor máximo corresponde a 18.2 horas. Un tiempo de vida con valor de 0 indica que el router no es un router predefinido y no debe aparecer en la lista de routers predefinidos.
i) *Tiempo alcanzable (Reachable Time):* Entero sin signo de 32 bits. Indica el tiempo medido en milisegundos en que un nodo asume que un vecino es alcanzable después de haber recibido una confirmación de conectividad.
j) *Cronómetro de retransmisión (Retrans Timer):* Entero sin signo de 32 bits. indica el tiempo medido en milisegundos entre los que se retransmiten mensajes de solicitudes de vecino.

Usado en la resolución de direcciones empleado por el algoritmo de Descubrimiento de Vecino Inalcanzable.

k) *Opciones (Options):* Las posibles opciones empleadas en este mensaje son las siguientes:
   i. Dirección de la capa de enlace de origen
   ii. MTU
   iii. Información del prefijo*:*

3) Solicitud de vecino.

Es un mensaje generado por un router para determinar la dirección de la capa de enlace de sus vecinos, o verificar que su nodo vecino sigue activo, también se usa para detectar direcciones duplicadas. El formato del mensaje de solicitud de vecino se encuentra ilustrado en la figura 5.C.3.

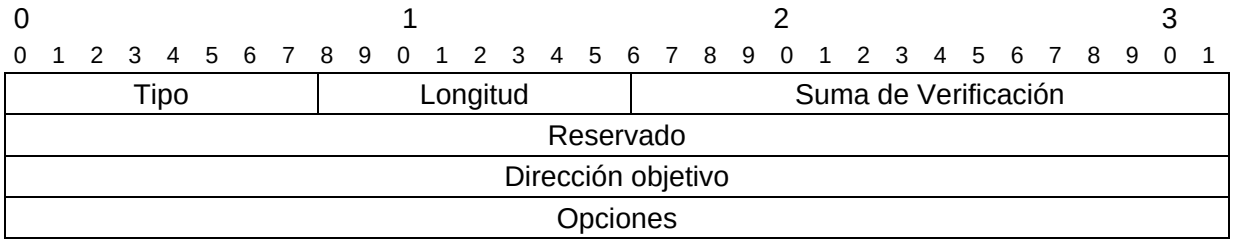


Figura 5.C.3: *Formato del mensaje de solicitud de vecino.*

Los campos que posee el mensaje ICMP de Solicitud de vecino son:

a) *Tipo (Type):* Posee el valor de 135
b) *Código (Code):* Posee el valor de 0
c) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
d) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.
e) Dirección objetivo (Target Address): La dirección IP del destino de la solicitud, no debe ser una dirección multicast.
f) *Opciones (Options):* La única opción valida para este mensaje es:
   Dirección de la capa de enlace de origen.

4) Anuncio de vecino.

Es un mensaje generado por los nodos como una respuesta al mensaje de solicitud de vecino. Un nodo también solicita a sus vecinos le envíen un anuncio de cambios en la capa de enlace. El formato del mensaje de anuncio de vecino se encuentra ilustrado en la figura 5.C.4.

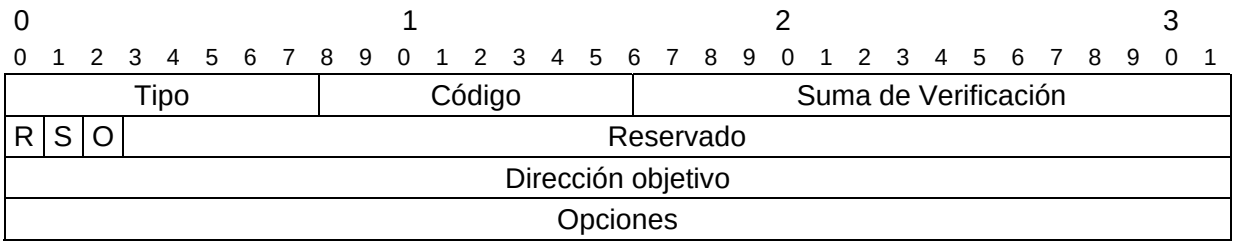


Figura 5.C.4: *Formato del mensaje de anuncio de vecino.*

Los campos que posee el mensaje ICMP de anuncio de vecino se definen a continuación:

a) *Tipo (Type):* Posee el valor de 136
b) *Código (Code):* Posee el valor de 0
c) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
d) *R (bandera de Router):* Cuando se usa, el bit R indica que el remitente es un router. El bit R se usa tambien en el Descubrimiento de vecino inalcanzable para detectar un router que cambia a un host.
e) *S (bandera solicitada):* Cuando se usa, el bit S indica que el anuncio se envió como respuesta a la Solicitud de un Vecino de la dirección Destino. El bit S se usa como una confirmación de conectividad para el Descubrimiento de Vecino Inalcanzable. No debe ponerse en los anuncios multicast.
f) *O (Anular bandera):* Anular la bandera. Cuando se usa, el bit O indica que el anuncio debe anular una entrada de la Cache existente y debe actualizar la Cache de direcciones de la capa de enlace.
g) *Reservado (Reserved):* Campo sin usar de 29 bits. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.
h) *Dirección objetivo (Target Address):* Dirección del vecino que dio lugar a este anuncio.
g) *Opciones (Options):* La única opción valida para este mensaje es:
Dirección de la capa de enlace destino.

5) Redirección.

Generado por los routers para informar a los hosts que existe un mejor salto para llegar a un determinado destino. El formato del mensaje de Redirección se encuentra ilustrado en la figura 5.C.5.

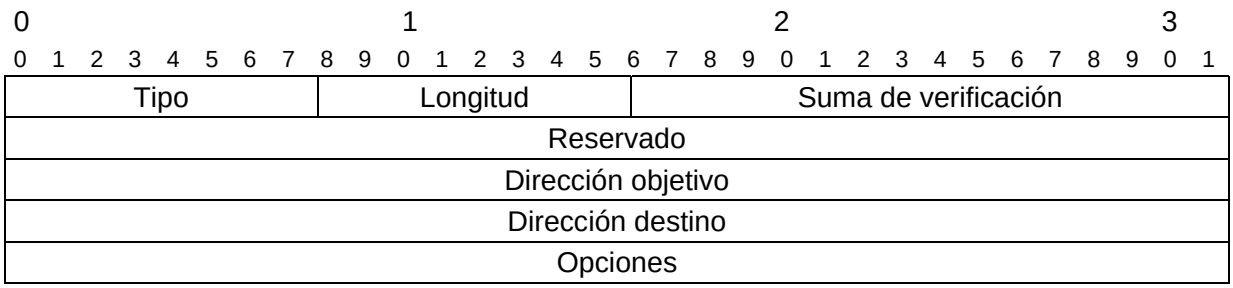


Figura 5.C.5: *Formato del mensaje de Redirección.*

Los campos que posee el mensaje ICMP de redirección son:

a) *Tipo (Type):* Posee el valor de 137
b) *Código (Code):* Posee el valor de 0
c) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
d) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.
e) *Dirección objetivo (Target Address):* Una dirección IP que es el mejor primer salto a una dirección destino que debe usar el Mensaje ICMP. Cuando el nodo destino es un vecino, el campo de *Dirección Objetivo* debe contener el mismo valor que el campo *Dirección destino*. Por otra parte si el nodo destino es un router el mejor primer salto a una dirección destino debe ser la dirección del enlace local del router para que los host puedan identificar los routers singularmente.
f) *Dirección destino (Destination Address):* La dirección IP de el destino al cual es redirigido un paquete.

l) *Opciones (Options):* Las posibles opciones empleadas en este mensaje son las siguientes:
   i. Dirección de la capa de enlace destino
   ii. Cabecera de redirección

6) Solicitud de descubrimiento inverso de vecino.
Un nodo envía a un vecino un mensaje de solicitud de descubrimiento Inverso de vecino para pedir una dirección IPv6 que corresponde a una dirección de la capa de enlace del nodo destino mientras que además proporciona su propia dirección de la capa de enlace. El Descubrimiento Inverso de Vecino (IND) envía las Solicitudes a todos los nodos por medio de multidifusión. Sin embargo, al nivel de capa de enlace, una Solicitud de IND se envía directamente al nodo destino, identificado por la dirección de la capa de enlace conocida. El formato del mensaje de solicitud de descubrimiento de vecino inverso se detalla en la figura 5.C.6.

Figura 5.C.6: *Formato del mensaje de solicitud redescubrimiento inverso de vecino.*

Los campos que posee el mensaje ICMP del solicitud de router se definen a continuación:

f) *Tipo (Type):* Posee el valor de 141
g) *Código (Code):* Posee el valor de 0
h) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
i) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.
j) *Opciones (Options):* Las opciones requeridas en este mensaje son:
   i. La Dirección de la capa de enlace de origen.
   ii. La Dirección de la capa de enlace destino.

   El nodo del remitente puede escoger agregar las opciones siguientes en el mensaje de la Solicitud:
   i. Listado de Direcciones de origen
   ii. MTU

7) Anuncio de descubrimiento inverso de vecino.
Un nodo envía un anuncio de descubrimiento de vecino inverso como respuesta a una solicitud de descubrimiento de vecino inverso. El formato del mensaje de anuncio de descubrimiento de vecino inverso se detalla en la figura 5.C.7.

Figura 5.C.7: ***Formato del mensaje de anuncio de descubrimiento inverso de vecino.***

Los campos que posee el mensaje ICMP de solicitud de router se definen a continuación:

a) *Tipo (Type):* Posee el valor de 142
b) *Código (Code):* Posee el valor de 0
c) *Suma de Verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*
d) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse con el valor de cero por el nodo remitente y debe ignorarse por el nodo receptor.
e) *Opciones (Options):* Las opciones requeridas en este mensaje son:
   i. La Dirección de la capa de enlace destino.
   ii. Listado de direcciones destino.

   El nodo del remitente puede escoger agregar las opciones siguientes en el mensaje de la Solicitud:

   MTU.

D. FORMATO DE OPCIÓN EN MENSAJE ICMPv6 PARA ND.

Los mensajes ICMPv6 con los que trabaja el protocolo de descubrimiento de vecindario incluyen cero o más tipos de opciones, algunas de estas opciones pueden aparecer al mismo tiempo en un mensaje. El formato de las opciones de los mensajes ICMPv6 con los que trabaja el protocolo ND se ilustran en la figura 5.D.1.

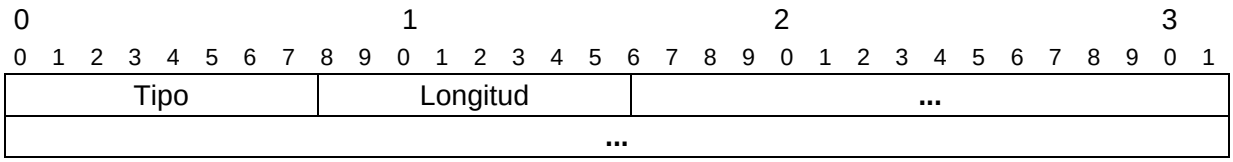


Figura 5.D.1: *Formato de las opciones de los mensajes ICMPv6 con los que trabaja el protocolo ICMP*

Los campos de las opciones del mensaje ND son:

a) *Tipo (Type):* El tipo de opción es un campo que posee 8 bits. Las opciones definidas en este campo se muestran en la tabla 5.D.1.

Tipo	Opciones definidas	Referencia
1	Dirección de la capa de enlace de origen	RFC2461
2	Dirección de la capa de enlace de destino	RFC2461
3	Información del prefijo	RFC2461
4	Cabecera redirigida	RFC2461
5	MTU	RFC2461

Tipo	Opciones definidas	Referencia
6	Opción de límite de atajo *NBMA*	RFC2491
7	Intervalo de anuncio	RFC3775
8	Información de agente de casa	RFC3775
9	Listado de direcciones de origen	RFC3122
10	Listado de direcciones de destino	RFC3122

Tabla 5.D.1: *Valores del campo Tipo del mensaje ND*

b) *Longitud (Length):* Entero sin signo de 8 bits. Es un campo para indicar la longitud de la opción.

E. OPCIONES DE LOS MENSAJES ICMPV6 CON LOS QUE TRABAJA EL PROTOCOLO ND.

1) Dirección de la capa de enlace Origen/Destino.
La dirección de la capa de enlace de origen contiene la dirección de la capa de enlace del nodo remitente del paquete. Se usa en los siguientes anuncios ICMPv6:

i. Solicitud del Vecino
ii. Solicitud de router
iii. Paquetes de Anuncio de router.

La dirección de la capa de enlace de destino contiene la dirección de la capa de enlace del nodo donde pretende llegar el paquete. Se usa en los siguientes anuncios ICMPv6:

i. Anuncio de Vecino
ii. Envío de los paquetes.

El formato de la opción de la dirección de la capa de enlace Origen/Destino se encuentra ilustrado en la figura 5.E.1.

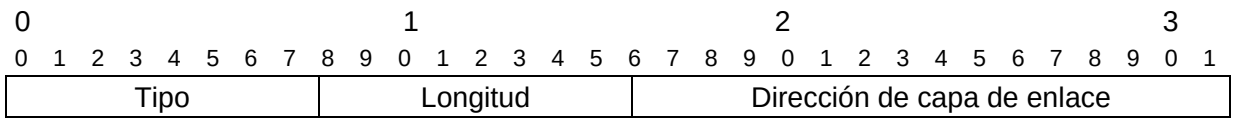


Figura 5.E.1: ***Formato de la opción de la dirección de la capa de enlace para el Origen/Destino***

Los campos de las opciones de dirección de la capa de enlace Origen/Destino son:

a) *Tipo (Type):* Posee los siguientes valores
   i. 1 para la dirección de la capa de enlace de origen
   ii. 2 para la dirección de la capa de enlace destino
b) *Longitud (Length):* Ver la especificación del apartado E
c) *Dirección de capa de enlace (Link-Layer Address):* La dirección de la capa de enlace de longitud variable. El volumen y formato de este campo (incluso el *tipo* y el bit de ordenamiento) se espera que sea especificado en documentos específicos que describen cómo opera IPv6 sobre las capas de enlace diferentes.

2) Información del prefijo.
Esta opción les proporciona a los hosts información sobre los prefijos del enlace y prefijos para direcciones de autoconfiguración, esta opción aparece en los paquetes de anuncio de router. El formato de la opción de la información del prefijo se encuentra detallado en la figura 5.E.2.

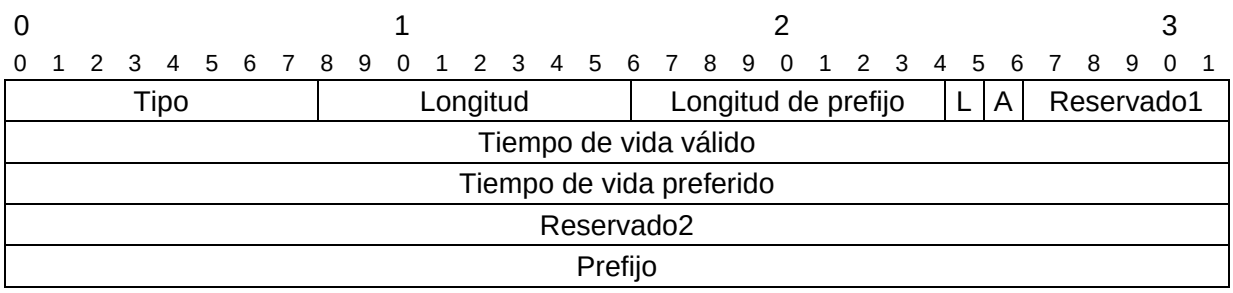


Figura 5.E.2: *Formato de la opción de la información del prefijo.*

Los campos de la opción de la información del prefijo son:

a) *Tipo (Type):* Posee el valor de 3
b) *Longitud (Length):* Posee el valor de 4
c) *Longitud de prefijo (Prefix Length):* Entero sin signo de 8 bits. El número de bits principales en el Prefijo que es válido. El valor tiene un rango de 0 a 128.
d) *L (Bandera del enlace)*. Cuando se usa, el bit L indica que este prefijo puede usarse para la determinación del enlace. Cuando no se usa el anuncio no hace ninguna declaración dentro del enlace o fuera del enlace de las propiedades del prefijo. Por ejemplo, el prefijo podría usarse para la configuración de una dirección con alguna información pertinente de direcciones del prefijo que se encuentran dentro o fuera del enlace.
e) *A (Bandera de dirección y configuración autónoma):* Cuando se usa, el bit A se puede configurar una dirección autónoma.
f) *Reservado1 (Reserved1):* Campo sin usar de 6 bits. Debe inicializarse para ponerse a cero en el remitente y debe ignorarse por el receptor.
g) *Tiempo de vida válido (Valid Lifetime):* Entero sin signo de 32 bits. Indica la longitud de tiempo en segundos (relativo al tiempo del paquete que se envía) en el cual el prefijo se valida con el propósito de la determinación del enlace.
h) *Tiempo de vida preferido (Preferred Lifetime):* Entero sin signo de 32 bits. Indica la longitud de tiempo en segundos (relativo al tiempo del paquete que se envía) en el cual las direcciones generan el prefijo por medio de la autoconfiguración de dirección sin estado (Stateless).
i) *Reservado2 (Reserved2):* Este campo no se usa. Debe inicializarse para ponerse a cero en el remitente y debe ignorarse por el receptor.
j) *Prefijo (Prefix):* Una dirección IP o un prefijo de una dirección IP. El campo de Longitud de Prefijo contiene el número de bits principales válidos en el prefijo. Este campo debe inicializarse para poner a cero en el remitente y debe ignorarse por el receptor. Una router no debe enviar una opción de prefijo para el prefijo del enlace local y un host debe ignorar una opción del prefijo.

3) Cabecera redirigida.
La opción de cabecera redirigida se usa en el reenvío de mensajes y contiene todo o parte del paquete que se está reenviando. El formato de la opción de la cabecera redirigida se muestra en la figura 5.E.3.

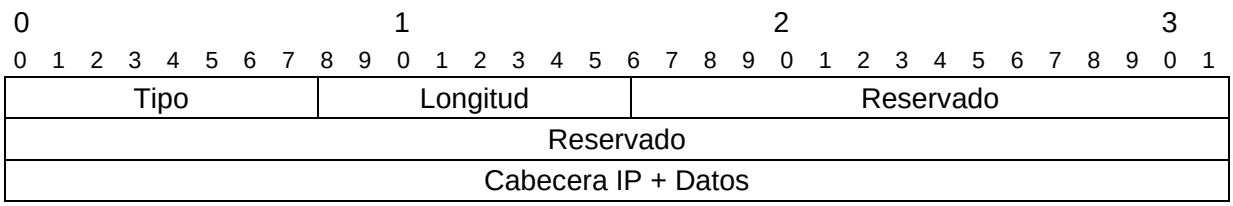


Figura 5.E.3: ***Formato de la opción cabecera redirigida***

Los campos de opciones de la cabecera redirigida son:

a) *Tipo (Type):* Posee el valor de 4
b) *Longitud (Length):* Ver la especificación del apartado E
c) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse para ponerse a cero en el remitente y debe ignorarse por el receptor.
d) *Cabecera IP + Datos (IP header + data):* El paquete original se trunca para asegurar que el tamaño del mensaje de redirección no exceda los 1280 octetos.

4) MTU.
La opción de MTU se usa en los mensajes ICMPv6 de Anuncio de router para asegurar que todos los nodos en un enlace usan el mismo valor de la MTU.
En los casos en que las configuraciones de red poseen tecnologías heterogéneas conectadas, la MTU soportado máximo puede diferir de un segmento a otro. Por lo que se debe generar un mensaje ICMP que especifique que los paquetes enviados son demasiado grandes, los routers usan esta opción para especificar el valor de la MTU máximo que es soportado por todos los segmentos de la red. El formato de la opción MTU se encuentra detallado en la figura 5.E.4.

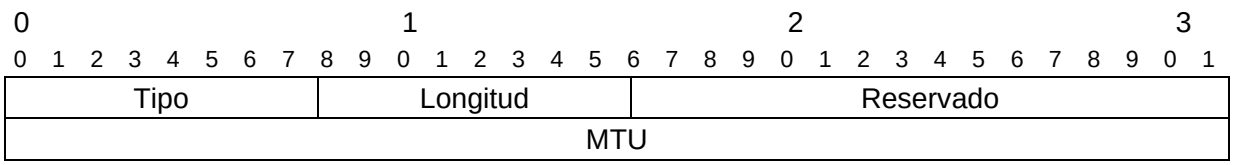


Figura 5.E.4: ***Formato de la opción MTU.***

Los campos de la opción MTU son:

a) *Tipo (Type):* Posee el valor de 5
b) *Longitud (Length):* Posee el valor de 1
c) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse para ponerse a cero en el remitente y debe ignorarse por el receptor.
d) *MTU:* Entero sin signo de 32 bits. La MTU recomendado para el enlace.

5) Listado de direcciones Origen/Destino.
El Listado de Dirección de Origen contiene una lista de direcciones IPv6 de la interfaz identificada por las direcciones de origen de la capa de enlace.

El listado de Dirección Designado contiene una lista de direcciones IPv6 de la interfaz identificada por las direcciones destino de la capa de enlace.

El número de direcciones "n" que posee la lista es calculado basado en la longitud de la opción:

n = (la Longitud - 1)/2 (la Longitud es el número de grupos de 8 octetos)

La Lista de Dirección de Origen debe caber en un mensaje de solicitud IND.

La Lista de Dirección Destino debe ser la lista completa de direcciones de la interfaz identificada por la Direcciones Destino de la capa de enlace. Si la lista de direcciones IPv6 de una interfaz no cabe en un mensaje de anuncio IND, se deben enviar uno o más mensajes de anuncios IND, con los mismos campos que posee el primer mensaje, y que contengan el resto de direcciones destino de la capa de enlace que no pudieron ser enviados en el primer mensaje. El formato de la opción de listado de direcciones Origen/Destino para los mensajes IND se encuentra detallado en la figura 5.E.5.

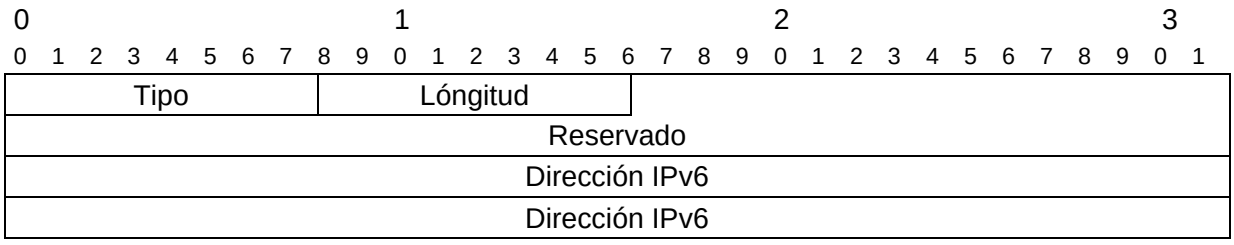


Figura 5.E.5: ***Formato de la opción cabecera de redirección***

Los campos de opciones de la cabecera de redirección son:

a) *Tipo (Type):* Posee los siguientes valores
   i. 9 para el listado de las direcciones de origen
   ii. 10 para el listado de las direcciones destino
b) *Longitud (Length):* Ver la especificación del apartado E
c) *Reservado (Reserved):* Este campo no se usa. Debe inicializarse para ponerse a cero en el remitente y debe ignorarse por el receptor.
d) *Dirección IPv6 (IPv6 Address):* Una o más direcciones IP de la interfaz.

F. MODELO CONCEPTUAL DE UN HOST.

En este apartado se describe un modelo conceptual de una posible estructura de datos de un host (y algunos routers) y la forma en la que este actúa recíprocamente con los nodos vecinos. La información descrita en este apartado se proporciona para facilitar la explicación de cómo el protocolo de Descubrimiento de Vecindario debe comportarse.

1) Estructuras de datos conceptuales.
Los host de una red necesitarán mantener información para las siguientes interfaces:

a) Caché de vecino:

En esta estructura de datos se conserva información sobre las entradas individuales del tráfico de los vecinos que han enviado algún paquete recientemente. Se codifican las entradas de los vecinos en el enlace de direcciones IP unicast conteniendo la siguiente información:

i. Su dirección de la capa de enlace
ii. Una bandera que indica si el vecino es un router o un host
iii. Un puntero a cualquier cola de paquetes que esperan por la resolución de dirección para completar su envío
iv. Contiene información usada por el algoritmo de descubrimiento de vecinos alcanzables e inalcanzables
v. El número de mensajes sin contestar
vi. El tiempo de detección del siguiente vecino inalcanzable.

b) Caché de destino:

Se conserva información sobre el tráfico hacia los destinos donde se han enviado paquetes recientemente. La Caché de Destino incluye la siguiente información:

i. Los nodos que se encuentran dentro del enlace y los que se encuentran fuera del enlace
ii. Los mapas de las direcciones IP destino a la dirección IP del vecino próximo.

Esta Caché se actualiza con información aprendida de los mensajes de reenvío. Es importante hacer notar que las aplicaciones pueden encontrar conveniente no guardar información adicional que esta directamente relacionada al Descubrimiento del Vecino en la Caché de Destino, como la MTU de la ruta (PMTU) y los tiempos del viaje con retorno mantenidos por los protocolos de transporte.

c) Lista de prefijos:

Se conserva una lista de los prefijos que se definen en el enlace. Además se crea una lista de prefijos con todas las entradas de la información recibida en los anuncios de router. Cada entrada tiene asociado un valor de tiempo de invalidación de prefijos.
En esta lista de prefijos se considera que el prefijo del enlace local tiene un tiempo de invalidación de infinito, incluso sin tener en cuenta si los routers están anunciando un prefijo para él.

d) Lista de routers predefinidos:

Se conserva información de la lista de los routers donde pueden enviarse los paquetes; esta lista se obtiene del algoritmo para seleccionar un router alcanzable. Cada entrada también tiene un valor de cronómetro de invalidación asociado (extraído de los Anuncios de router) utilizado para anular entradas que ya no se anuncian.

2) Algoritmo conceptual de envío.
Al enviar un paquete a un destino, un nodo usa una combinación de los siguientes elementos:

a) Caché de destino
b) Lista del Prefijo
c) Lista de router predefinida para determinar la dirección IP del próximo salto apropiado, un procedimiento conocido como la *"Determinación del próximo salto"*.

Una vez la dirección IP del próximo salto es conocida, la Caché del Vecino se consulta para ver la información de la capa de enlace sobre ese vecino.

El algoritmo para determinar el próximo salto para un destino con una dirección unicast dada, se detalla en los siguientes pasos:

a) El remitente realiza una comparación del prefijo que posee de la dirección destino contra la Lista de Prefijos que posee para determinar si el destino del paquete se encuentra dentro o fuera del enlace.
b) Si el destino se encuentra en el enlace, la dirección del próximo salto está igual que la dirección del destino del paquete.
c) El remitente debe seleccionar un router de la Lista de Routers Predefinidos.
d) Si la Lista de Routers predefinidos está vacía, el remitente asume que el destino se encuentra en el enlace.

Por las razones de eficacia, la determinación del próximo salto no se realiza en cada paquete que se envía. En cambio, los resultados de las operaciones para la determinación de próximo salto son guardados en la Caché de Destino (qué también contiene actualizaciones aprendidas de los mensajes reenviados). Cuando un nodo tiene un paquete para enviar, examina la Caché de Destino primero. Si ninguna entrada existe para el destino, la determinación del próximo salto se invoca para crear una entrada en la Caché de Destino.

Una vez que la dirección IP del nodo a donde se realizara el próximo salto es conocida, el remitente examina la Caché de Vecino para conocer la información de la capa de enlace sobre ese vecino. Si ninguna entrada existe, el remitente crea una.

Para los paquetes de multidifusión el próximo salto es siempre la dirección del destino y se considera que se encuentra dentro del enlace.

Cada cierto tiempo una entrada de la Caché de Vecino se accede mientras se esta transmitiendo un paquete unicast, para que el remitente verifique si el vecino es inalcanzable, relacionando la información del destino con la información que posee del algoritmo de Descubrimiento de Vecino Inalcanzable.

La determinación del próximo salto, al principio de un tráfico que se envía a un destino, se realiza para que la comunicación subsiguiente que se envía a ese destino proceda con éxito. La entrada de la Caché de Destino continúa siendo usada en este proceso.

Si a algún punto de comunicación deja de proceder, la determinación del próximo salto puede necesitar ser realizada de nuevo. Por ejemplo, un tráfico que se realiza a través de un router que falla debe cambiarse a un router que se encuentra activo.

El detalle esquemático de este proceso se encuentra ilustrado en la figura 5.F.1.

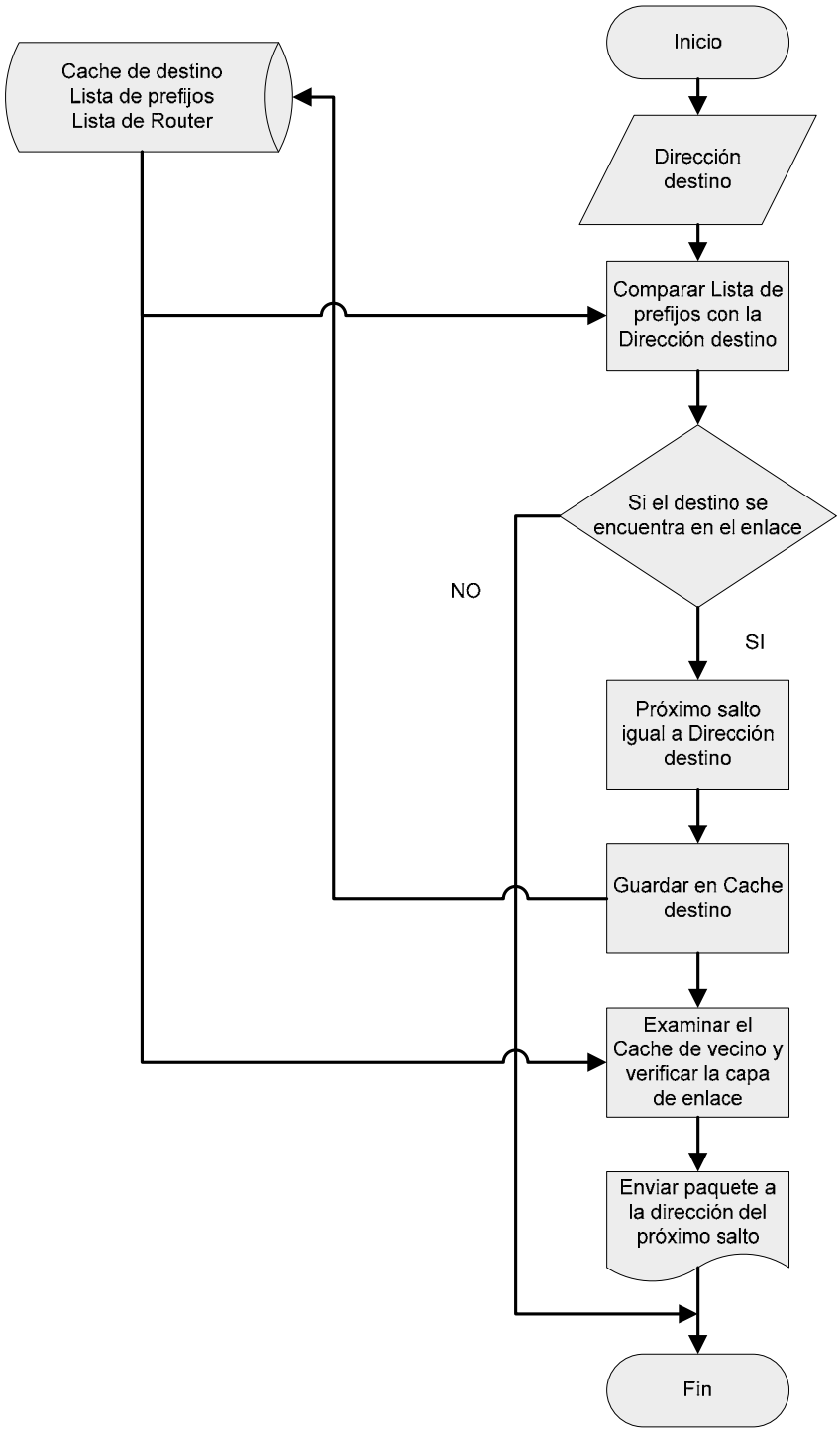


Figura 5.F.1: *Algoritmo para determinar la dirección del próximo salto para enviar un paquete a un destino.*

G. DESCUBRIMIENTO DE ROUTERS Y DE PREFIJOS.

En este apartado se describe la conducta del router y del host relacionado con el Descubrimiento de Router y del Descubrimiento del Vecindario.

El *Descubrimiento del Router* se usa para localizar los routers vecinos así como para aprender los prefijos.

El Descubrimiento del prefijo es el proceso a través del cual los host aprenden los rangos de direcciones IP que residen en el enlace y pueden alcanzarse directamente sin pasar por un router.

Los routers envían Anuncios de Router que indican si el remitente desea ser un router predefinido.

1) Validación de mensajes.

a) Aprobación de mensajes de solicitud de router

Las siguientes especificaciones se deben cumplir para aprobar un mensaje de Solicitud de Router:

i. Los hosts deben desechar cualquiera mensaje de Solicitud de Router.
ii. Un Router debe desechar cualquier Solicitud de Router que no satisfacen las siguientes especificaciones:
    - El campo *Límite de Salto* del paquete IP tiene un valor menor de 255.
    - Si el mensaje incluye un Título de Autenticación de IP, el mensaje se autentica como correcto.
    - El campo *Suma de Verificación* del mensaje ICMP debe ser válido.
    - El Código del mensaje ICMP es 0.
    - La longitud del mensaje ICMP es 8 o más octetos.
    - Todas las opciones incluidas tienen una longitud que es mayor que cero.
    - Si la dirección IP de origen es una dirección no especificada se debe descartar el mensaje.

b) Aprobación de mensajes de anuncio de router

Un nodo debe desechar cualquier mensaje de Anuncio de Router que no satisfacen todas las especificaciones de validez siguientes:

- La Dirección IP de Origen es una dirección del enlace local. Los Routers deben usar su dirección de enlace local como el origen para el Anuncio de Router y reenviar los mensajes para que los host puedan identificar los routers individualmente.
- El campo *Límite de Salto* del paquete IP tiene un valor menor de 255
- Si el mensaje incluye un Título de Autenticación de IP, el mensaje autentica correctamente.
- El campo *Suma de Verificación* del mensaje ICMP es válido.
- El Código del mensaje ICMP es 0.
- La longitud de mensaje ICMP es 16 o más octetos.
- Todas las opciones incluidas tienen una longitud que es mayor que cero.

H. RESOLUCIÓN DE DIRECCIONES Y DESCUBRIMIENTO DE VECINOS INALCANZABLES.

En este apartado se describen las funciones relacionadas con la Solicitud de Vecino y los mensajes de Anuncio de Vecino además se incluyen descripciones de resolución de direcciones y el algoritmo de descubrimiento de vecino inalcanzable.

1) Validación de mensajes.

a) Validación de solicitud de vecino

Un nodo debe desechar cualquier mensajes de Solicitud de Vecino que no satisfacen todos las especificaciones de validez siguientes:

- El campo *Límite de salto* del paquete IP debe tener un valor menor que 255.
- Si el mensaje incluye un Título de Autenticación de IP, el mensaje autentica correctamente.
- El campo *Suma de Verificación* del mensaje ICMP es válido.
- El Código del mensaje ICMP es 0.
- La longitud del mensaje ICMP es 24 o más octetos.
- La Dirección designada no es una dirección multicast.
- Todas las opciones incluidas tienen una longitud que es mayor que cero.
- Si la dirección IP de origen es una dirección no especificada, la dirección de destino de IP es una dirección de multidifusión de solicitud del nodo.

b) Validación de anuncio de vecino

Un nodo debe desechar cualquier mensaje de Anuncio de Vecino que no satisfacen las especificaciones de validez siguientes:

- El campo *Límite de Salto* del paquete IP tiene un valor menor que 255.
- Si el mensaje incluye un Título de Autenticación de IP, el mensaje se autentica correctamente.
- El campo *Suma de Verificación* del mensaje ICMP es válido.
- El Código de ICMP es 0.
- La longitud de ICMP es 24 o más octetos.
- La Dirección designada no es una dirección de la multidifusión.
- Si la Dirección de Destino de IP es una dirección de la multidifusión la solicitud de bandera es el cero.
- Todas las opciones incluidas tienen una longitud que es mayor que cero.

2) Resolución de direcciones.

La resolución de direcciones es el proceso a través del cual un nodo determina la dirección de la capa de enlace de un vecino dada sólo su dirección IP. La resolución de dirección nunca se realiza en las direcciones de multidifusión.

a) Envío de solicitud de vecino

Cuando un nodo tiene un paquete unicast para enviarle a un nodo vecino, pero no sabe la dirección de la capa de enlace del vecino debe realizar una resolución de dirección. En este proceso el nodo crea una entrada en la Caché de Vecino y le asigna el estado de INCOMPLETO, luego transmite un mensaje de Solicitud de Vecino al nodo destino. Si la dirección de origen del paquete por el cual se inicia la solicitud es igual que alguna de las direcciones asignadas a las direcciones de la interfaz de la red, esa dirección debe ponerse en el campo *Dirección objetivo* de la solicitud que se envía. Usando la dirección del origen del paquete se asegura que el destinatario de la Solicitud de Vecino instale en su Caché esta dirección IP porque es muy probable que sea usada en el tráfico del retorno del paquete.

Mientras el nodo espera que se complete la resolución de dirección, el remitente DEBE, retener para cada vecino una cola pequeña de paquetes que esperan que se complete la resolución de la dirección. La cola debe tener por lo menos un paquete. Sin embargo, el número de paquetes que

se encuentran en la cola debe limitarse a algún valor pequeño. Cuando una cola se satura, la nueva entrada debe reemplazar la entrada más vieja. Una vez la resolución de dirección se completa, el nodo transmite los paquetes.

Mientras se espera una respuesta, el remitente DEBE de retransmitir el mensaje de solicitud de vecino por lo menos una vez.

Si ningún Anuncio del Vecino se recibe después de las solicitudes enviadas, la resolución de dirección ha fallado. El remitente debe devolver las indicaciones de destino inalcanzable por medio de un mensaje ICMP con código 3 (la Dirección Inalcanzable) para cada paquete que hizo cola esperando la resolución de dirección.

b) Envío de solicitud de anuncios de vecino

Un nodo envía un Anuncio de Vecino como respuesta a una Solicitud de Vecino enviada por un nodo. La Dirección destino del nodo que debe recibir el anuncio se copia de la Dirección del nodo que envía la solicitud. Si la dirección IP Destino de la solicitud no es una dirección multidifusión, el campo del mensaje ND que define la dirección de la capa de enlace puede omitirse. Si la dirección IP Destino de la solicitud de vecino es una dirección de multidifusión, el nodo destino debe incluir en el campo del mensaje ND donde se define la dirección de la capa la dirección respectiva de la capa de enlace.

Es posible que un nodo que envía un Anuncio del Vecino como respuesta a una solicitud no tenga una dirección de la capa de enlace correspondiente para su vecino en su Caché de Vecino. En esta situación, un nodo tendrá que usar el Descubrimiento del Vecino para determinar la dirección de la capa de enlace de su vecino próximo.

c) Descubrimiento de vecinos inalcanzables

La comunicación a través de un vecino puede fallar por numerosas razones como por ejemplo el error de hardware, error de una tarjeta de la interfaz de red, etc. Si el nodo destino ha fallado, ninguna recuperación es posible. Por otro lado, si es el camino el que ha fallado, la recuperación puede ser posible. Así, un nodo debe rastrear a los demás vecinos por donde se esta enviando un paquete y declararlos "Alcanzables".

El Descubrimiento de Vecino Inalcanzable se usa para todos los caminos entre un host y otro host, ó entre un host y un router y viceversa.

Cuando un camino a un vecino parece estar fallando, el procedimiento de la recuperación específico depende de cómo el vecino está usándose. Si el vecino es el último destino, por ejemplo, la resolución de dirección debe realizarse de nuevo. Si el vecino es un router, lo apropiado es cambiar el camino a otro router. La recuperación específica de una falla se realiza determinando otro próximo salto y anulando una entrada de la Caché de Vecino.

El Descubrimiento de Vecino Inalcanzable solo se realiza en los vecinos que se envían paquetes Unicast, no se usa para enviar a las direcciones de multidifusión.

a) Confirmación de vecino alcanzable

Un vecino es considerado alcanzable si el nodo que ha recibido la confirmación de que los paquetes enviados recientemente al vecino se recibieron a través de su capa IP. La confirmación positiva de un nodo alcanzable puede recibirse de dos formas:

- una forma indirecta que indica que los protocolos de la capa superior están haciendo una conexión en progreso

- Recibir un mensaje de Anuncio de Vecino que es una respuesta a un mensaje de Solicitud de Vecino.

b) Estado de las entradas de Caché de Vecino

Una entrada del Cache de Vecino puede estar en uno de estos cinco estados:

- INCOMPLETE (Incompleto): La resolución de dirección está realizándose en la entrada. Específicamente, una Solicitud de Vecino se ha enviado a la dirección de multidifusión para solicitar a un nodo destino que se anuncie, pero el Anuncio del Vecino correspondiente no se ha recibido todavía.

- REACHABLE (Alcanzable): Se ha recibido una confirmación positiva y se determina que el camino hacia el vecino estaba funcionando apropiadamente.

- STALE (Caducado): Ha pasado cierto tiempo (orden de milisegundos) desde que la última confirmación positiva fue recibida y que se definió que el camino estaba funcionando apropiadamente. Mientras tanto, ninguna acción tiene lugar hasta que un paquete se envíe.

- DELAY (Retraso): Ha pasado cierto tiempo desde que la última confirmación positiva fue recibida y que se definió que el camino hacia un vecino estaba funcionando, y además un paquete se envió dentro de los últimos segundos. Si ninguna confirmación de vecino alcanzable se recibe dentro de los próximos segundos la entrada pasa al estado de RETRASO, y se envía una Solicitud de Vecino y cambia el estado para INVESTIGAR. El estado de RETRASO es una optimización que da el tiempo adicional a los protocolos de la capa superior para proporcionar la confirmación de vecino alcanzable.

- PROBE (Prueba): Búsqueda activa de confirmación de vecino alcanzable por las Solicitudes de Vecino para retransmitir cada cierto tiempo, en el orden de los milisegundos, hasta que una confirmación de vecino alcanzable se reciba.

6. PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST VERSIÓN 6 (DHCPv6)

A. INTRODUCCIÓN.

Antes de entrar en detalles respecto a la configuración de un host mediante el uso del Protocolo de Configuración Dinámica de Hosts versión 6, se revisarán algunos conceptos necesarios para la comprensión de dicho mecanismo que aporta como una de sus características principales IPv6.

Configuración de direcciones estática:

Para configurar un host se hace uso de la información de asignación de los medios de configuración, ya sea proporcionada en un archivo estático o en una línea de comando. Dicha información incluye además de la dirección IP, la longitud del prefijo (o mascara de subred) y el servidor DNS. El proceso de configuración de un host IPv6 puede ser realizado de la misma manera que se configura un host IPv4.

Autoconfiguración de direcciones (Autoconfiguración de direcciones sin estado en IPV6[11]):

Este modelo permite a los hosts obtener su propia dirección de interfaz u otra información adicional necesaria para autoconfigurarse dentro de un enlace desde un servidor. Estos servidores poseen una base de datos donde son almacenados todos los registros de direcciones que pueden ser asignados a los diferentes nodos que se agreguen al enlace de dicho servidor. La autoconfiguración sin estado y con estado son complementarias. Por ejemplo un host podría hacer uso de la autoconfiguración sin estado (*Stateless)* para la asignarse a si mismo una dirección IPv6 que es válida en la red de ámbito local y mientras tanto podría hacer uso del la autoconfiguración con estado (*Statefull*) para determinar su propia dirección global IPv6, el prefijo de red y el router por defecto.

Anuncio y solicitudes del router:

La autoconfiguración de un host es realizada mediante el prefijo asociado a la red de destino. Este prefijo de red es enviado por los routers a través de avisos de routers (RA). Son enviados en forma de mensajes, los cuales forman parte del Protocolo *Descubrimiento de Vecindario,* que da soporte a la mayoría de interacciones dentro de un enlace local entre hosts y routers, y sólo entre hosts.

Los mensajes de *anuncio de router* (RA) son enviados por los routers o hosts para notificar a ambos acerca de la información de enlace, de manera que cada host IPv6 sea capaz de autoconfigurarse. La información clave para ello es el prefijo o los prefijos del enlace o enlaces y el router o routers por defecto que lo interconectan. Un *anuncio de router* contiene dos banderas indicando que tipo de autoconfiguración sin intervención debe realizarse. Una de las banderas indica si el host puede usar la autoconfiguración sin estado (stateless autoconfiguration) para obtener su propia dirección y la otra indica si el host puede hacer uso de la autoconfiguración con estado (stateful autoconfiguration) para obtener información adicional de configuración.

Es importante señalar que todos los hosts configurados para hacer uso del proceso de autoconfiguración, siempre deben de listar los anuncios de los routers en sus procesos inmediatamente éstos son recibidos.

Tan pronto los *anuncios de routers* son enviados, los hosts pertenecientes al enlace destino procesan la información contenida en los avisos y son configurados de acuerdo a dicha información. Estos anuncios son enviados cada 5 minutos. Cuando un host es inicializado y éste no ha podido recibir el *anuncio del router* enviado justo unos segundos antes, éste podría esperar

[11] RFC 2462: IPv6 Stateless Address Autoconfiguration.

por el próximo anuncio, enviado en 5 minutos, para autoconfigurase el mismo. La orden de recepción de *anuncios del router* es inmediatamente durante la secuencia de iniciación del host.
Cada host envía un mensaje de solicitud (RS) para todos los routers pertenecientes al enlace, solicitando de ellos el envío de la notificación de información del enlace (dirección IP, dirección DNS, dirección del router), para así este pueda autoconfigurarse inmediatamente.

B. PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOSTS (DHCPv6)

Es un mecanismo de autoconfiguración, descrito en el RFC3315, que crea una dirección donde la parte del identificador de la red es proporcionada por los avisos del router y la parte del identificador del host es creada por el mismo host basado en la dirección de capa de enlace (identificador de interfaz). DHCPv6 es un mecanismo de configuración de host centralizado donde el servidor DHCPv6 contiene toda la información ya sea parte del identificador de red como la del identificador del host, así como también es capaz de enviar información adicional como la dirección del DNS. El servidor DHCPv6 envía direcciones IPv6 utilizando paquetes IPv6 clásicos. También debería enviar direcciones IPv6 de los servidores DNS. Con el DHCPv4 la administración de la red se volvía una tarea difícil cuando se tienen conexiones con datos de configuración nuevos y estos cambios tienen que ser asignados a los clientes. Algunas de las diferencias entre DHCPv4 y DHCPv6 y las ventajas de éste sobre DHCPv4 se detallan en la tabla 6.B.1.

Característica	DHCPv4	DHCPv6	Beneficios
1.Manejo de configuración de banderas.	No disponible	Los routers utilizan banderas de controles de *avisos de routers* para verificar si los hosts son capaces de usar el DHCP.	La configuración de hosts puede ser manejada por políticas de redes.
2. Las peticiones iniciales de las direcciones de destino.	*Broadcast*	Multicast de sitio para todos servidores DHCP de direcciones de enlace local de los clientes DHCP.	-Señalización más especifica. -Uso más eficiente del enlace.
3. Petición inicial de la dirección de origen	0.0.0.0	Dirección de enlace local del cliente.	-Señalización más especifica. -Uso más eficiente del enlace.
4. Reenvío	Necesita una lista estática del servidor DHCP en el sitio.	Posibilidad de usar todos los servidores DHCP dentro del sitio de dirección multicast.	Facilidad para activar cualquier configuración nueva de sitios amplios.
5. Configuración de mensajes	No disponible	El servidor DHCP puede responder a los clientes DHCP para actualizar su información de configuración.	Facilidad de volver a configurar cualquier sito amplio.

Característica	DHCPv4	DHCPv6	Beneficios
6. Identidad de asociación	No disponible	Los clientes pueden manejar múltiples servidores DHCP y recibir múltiples direcciones.	Mayor estabilidad en el uso del DHCP.
7. Mecanismo de transición de pila dual (DSTM)[12]	No aplicable	Direcciones IPv4 temporales en el DSTM	Uso eficiente vigente espacio de direcciones IPv4.

Tabla 6.B.1: *Principales diferencias entre DHCPv4 y DHCPv6.*

1) Inicialización de clientes DHCP

Con el protocolo DHCPv6, clientes y servidores intercambian mensajes usando el protocolo de la capa de transporte UDP. Los clientes utilizan las direcciones de enlace local o las determinan a través de otros mecanismos como routers u otros dispositivos de red para transmitir o recibir mensajes DHCP. Mientras que los servidores DHCP reciben mensajes de los clientes a través de direcciones multicast reservadas de ámbito de enlace. Para que un cliente DHCP pueda enviar un mensaje al servidor DHCP, este hace uso de un dispositivo de reenvío, por ejemplo un router que se encuentre en el mismo enlace del cliente, para que este envíe el mensaje entre el cliente el servidor; dicha operación es transparente para el cliente. Se tienen dos escenarios para el proceso de inicialización de un cliente DHCP, los cuales son:

a) Inicialización del cliente DHCP cuando el servidor DHCP se encuentra en mismo enlace.

El primer paso que debe realizar el cliente es encontrar un router el cual le permita enviar un mensaje de solicitud para todos los routers dentro del enlace. Si un conjunto de routers responde a dicha petición, el cliente analiza el mensaje para comprobar si el manejo de configuración de banderas está fijada (tabla 6.B.1). En la tabla 6.B.2 se muestra el proceso de inicialización de un cliente DHCPv6.

Proceso	Ilustración	Descripción
1		El cliente del enlace local envía a todos los routers dentro del enlace de tipo multicast (FF02::2), una solicitud (RS) que se envía durante el tiempo de inicialización para conseguir notificar al router de su presencia.
2		El router del enlace local envía la notificación (RA) al cliente DHCP que hizo la solicitud.
3	El cliente ejecuta el proceso de recibo de la solicitud RA para poder encontrar si el manejo de configuración de banderas está fijada, si la bandera está fijada o si la notificación del router RA no ha sido recibida después de múltiples solicitudes RS entonces se continua con el siguiente paso.	

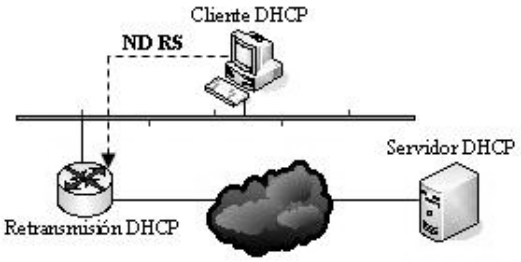
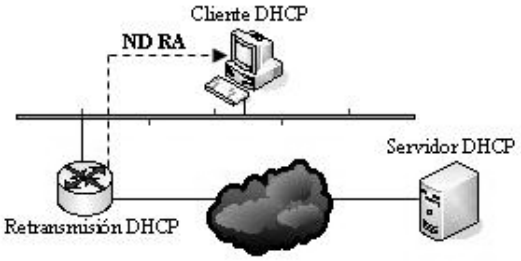
[12] DSTM se desarrolla en el cap. 13.

Proceso	Ilustración	Descripción
4		El cliente del enlace local envía una solicitud DHCP a todos los dispositivos DHCP dentro del enlace de tipo multicast (FF02::1:2), para intentar encontrar el servidor DHCP.
5		El servidor DHCP del enlace local responde al cliente del enlace local con la notificación DHCP.

Tabla 6.B.2: *Proceso de inicialización de un cliente DHCPv6 en un mismo enlace.*

b) Inicialización del cliente DHCP cuando el servidor DHCP no se encuentra en el mismo enlace.

Si se presenta una retransmisión DHCP, donde el servidor no se encuentre en el mismo enlace, entonces la comunicación entre el cliente y servidor DHCP se realiza a través de la retransmisión. Este proceso es similar al anterior excepto porque la retransmisión podría interceptar la solicitud de cualquiera de las dos partes en la comunicación (cliente/servidor) formándose así un mensaje de reenvío DHCP. Que incluyen tanto el mensaje original del cliente unido a la dirección de reenvío y la longitud del prefijo. Esta forma de retrasmisión es similar a la utilizada en IPv4, con la diferencia que para el caso de IPv6 las solicitudes son enviadas a todos los servidores DHCP dentro de un sitio. El la retransmisión del DHCPv6 no requiere una lista de sitios de servidores DHCP si se utilizan direcciones multicast. En la tabla 6.B.3 se muestra dicho proceso.

Proceso	Ilustración	Descripción
1		El cliente del enlace local envía una solicitud RS a todos los routers dentro del enlace local multicast FF02::2, dicha solicitud es enviada durante el tiempo de inicialización para obtener los anuncios de router.
2		El router del enlace local envía la notificación RA al cliente en el enlace local.
3	El cliente ejecuta el proceso de recibo de la solicitud RA para poder encontrar si el manejo de configuración de banderas está fijada, si la bandera está fijada o si la notificación del router RA no ha sido recibida después de múltiples solicitudes RS entonces se continua con el siguiente paso.	

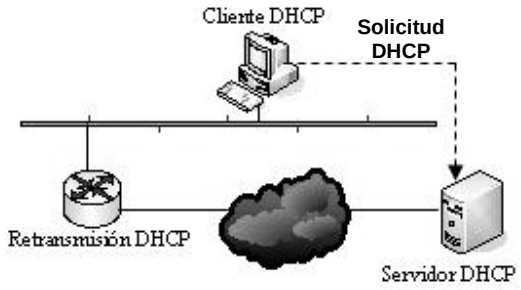
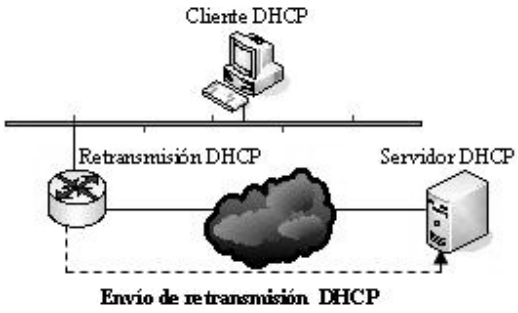
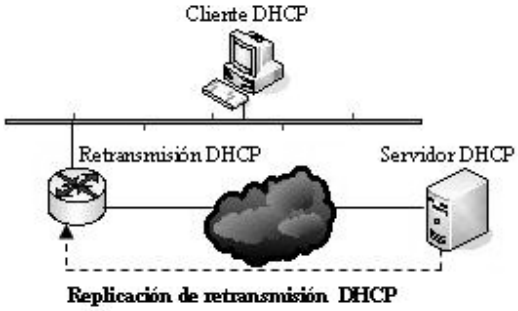
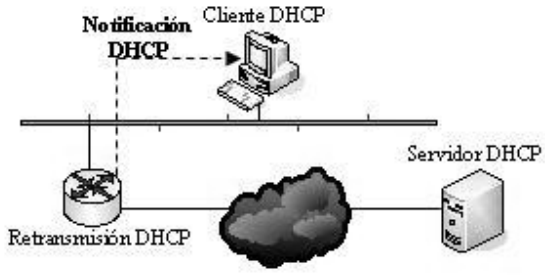
Proceso	Ilustración	Descripción
4		El cliente del enlace local envía una solicitud DHCP a todos los dispositivos DHCP dentro del enlace de tipo multicast (FF02::1:2), para intentar encontrar el servidor DHCP.
4.1		La dirección de retransmisión reenvía la solicitud incluyendo el reenvío del mensaje original del cliente a todos los servidores DHCP en el sitio multicast.
5		El servidor DHCP responde a la dirección de retransmisión, así el servidor responde a cada cliente enviando al retransmisor de DHCP quien se encarga de enviarlos a cada cliente respectivamente.
5.1		La dirección de reenvío responde desde el servidor enviando la réplica del mensaje a los clientes del enlace local.

Tabla 6.B.3: *Proceso de inicialización de un cliente DHCP en un enlace diferente.*

2) Mensaje DHCP

Como ya se mencionó anteriormente tanto clientes como servidores DHCP intercambian mensajes haciendo uso del protocolo de datagrama de usuario (UDP), Un cliente puede enviar mensajes usando UDP sin hacer uso de una dirección de tipo IPv6. Sin embargo éste debería especificar alguna dirección de la capa de enlace desde donde se envían los mensajes, ya que de lo contrario las respuestas desde el servidor no podrán ser entregadas al cliente. El comportamiento por defecto de un cliente DHCP es enviar todos los mensajes DHCP para todas las direcciones de tipo multicast reservadas para servicios DHCP, en lugar de enviarlos a una dirección unicast de un servidor DHCP específico. La razón de ésto es permitir el uso de dispositivos de reenvío que

permiten intercambiar mensajes entre servidores y clientes remotos. En la figura 6.B.3 se muestra el formato de un mensaje entre clientes y servidores DHCPv6.

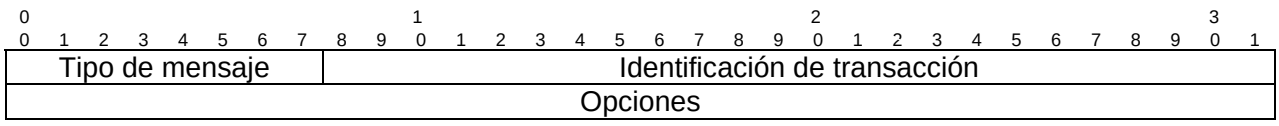


Figura 6.B.3: *Formato de mensaje DHCPv6.*

Donde:
Tipo de mensaje (msg-type): Campo que especifica el tipo de mensaje DHCP a intercambiar.
Identificación de transacción (transaction-Id): Campo utilizado para el intercambio de mensajes.
Opciones (Options): Campo utilizado para transportar el mensaje DHCP.

En la tabla 6.B.4 se detallan los tipos de mensajes que define el DHCPv6. Entre corchetes se muestra el valor codificado para cada tipo de mensaje.

Tipo de mensaje	Valor	Desde	Para	Descripción
Solicitud [Solicit]	1	Clientes	Todo dispositivo DHCP	Envío de una solicitud por parte de un cliente para localizar a un servidor.
Anuncio [Advertise]	2	Servidor	Cliente	Auncio enviado por parte de un servidor para indicar que esta disponible el servicio DHCP. Esto en respuesta de una solicitud del servicio realizada desde un cliente.
Petición [Request]	3	Cliente	Servidor	Un cliente envía una *petición* solicitando los parámetros de configuración como la dirección IP, desde un servidor específico.
Confirmación [Confirm]	4	Cliente	Servidor	Un cliente envía un mensaje de *confirmación* a cualquier servidor disponible para indicar que las direcciones que han sido asignadas todavía son apropiadas para los enlaces en cada cliente que es conectado.
Reanudar [Renew]	5	Cliente	Servidor	Un cliente envía un mensaje de *reanudar* para el servidor que originalmente provee la dirección IP del cliente y los parámetros de configuración, para extender el tiempo de vida en las direcciones asignadas para el cliente y actualizar otros parámetros de configuración.

Tipo de mensaje	Valor	Desde	Para	Descripción
Reenlace [Rebind]	6	Cliente	Servidor	Un cliente envía un mensaje *reenlace* para cualquier servidor disponible solicitando extender el tiempo de vida de las direcciones asignadas para los clientes y actualizar otros parámetros de configuración. Este mensaje es enviado después que un cliente no ha recibido respuesta a un mensaje de reanudar.
Respuesta [Reply]	7	Servidor	Cliente	Un servidor envía este tipo de mensaje conteniendo la dirección asignadas y los parámetros de configuración, en respuesta a una solicitud, una petición, reanudar o un mensaje de *reenlace* recibido desde un cliente. El servidor envía este tipo de mensaje para confirmar recibo de mensajes, confirmar o denegar que las direcciones asignadas a los clientes son apropiadas para los enlaces en donde son conectados los clientes. Un servidor envía un mensaje de *respuesta* para reconocer si un mensaje fue aceptado o declinado por parte de un cliente.
Liberar [Release]	8	Cliente	Servidor	Un cliente envía este tipo de mensaje indicandole al servidor que ya no utilizará más la dirección que le fue asignada, permitiéndole así al servidor liberar dicha dirección y reasignarla posteriormente.
Rehusar [Decline]	9	Cliente	Servidor	Un cliente envía este tipo de mensaje para un servidor indicando que un cliente ha determinado que una o mas direcciones asignadas por el servidor hasta el momento dentro del enlace están siendo utilizadas.
Reconfigurar [Reconfigure]	10	Servidor	Cliente	Un servidor envía este tipo de mensaje para informar a un cliente de cambios realizados como un nuevo servidor o parámetros de configuración adicionales.
Petición de información [Information-Request]	11	Dispositivo de retransmisión	Servidor	Un cliente envía este mensaje a un servidor para solicitar los parámetros de configuración sin la asignación de cualquier dirección IP para el cliente.

Tipo de mensaje	Valor	Desde	Para	Descripción
Retransmisión [Relay-Forw]	12	Dispositivo de retransmisión	Clientes	Un dispositivo de reenvío envía este mensaje para hacer llegar el mensaje directamente desde los servidores o desde otro dispositivo de reenvío a los clientes. Un mensaje para un cliente enviado desde otro dispositivo de reenvío es encapsulado en una opción de *retransmisión* (*relay-forward*).
Réplica [Relay-Repl]	13	Servidor	Dispositivo de retransmisión	Un servidor envía este tipo de mensaje para un dispositivo de reenvío conteniendo el mensaje que el dispositivo de reenvío entregará al cliente. Este tipo de mensaje podría ser retransmitido por otros dispositivos de reenvío. El servidor encapsula el mensaje al cliente como una opción de *réplica* (*relay-Reply*). Cada dispositivo de reenvío extrae dicho mensaje y lo retransmite a cada cliente.

Tabla 6.B.4: *Tipos de mensajes DHCP soportados bajo IPv6.*

Un cliente DHCP utiliza peticiones de tipo: *renew, rebind, release* y *decline* durante el ciclo normal de una dirección. Estos son utilizados para confirmar la validez de una dirección, cuando se dé el caso que el cliente ha sido ubicado en otro enlace. Éste hace uso de mensajes de petición de información cuando necesita información de configuración en lugar de direcciones.

a) Direcciones IPv6 válidas para enviar consultas DHCPv6.

i. Para todos los dispositivos de reenvío y servidores es: [FF02::1:2]: Dirección multicast de ámbito de enlace usada por un cliente para comunicarse con su vecindario (por ejemplo dentro de un enlace). Todos los dispositivos de reenvío y los servidores son nombrados por este grupo multicast.

ii. Todos los servidores DHCP es: [FF05::1:3]: Una dirección multicast de ámbito de sitio usada por los dispositivos de reenvío para comunicarse con los servidores, cuando necesitan enviar mensajes a todos los servidores o cuando no conocen la dirección unicast del servidor. Todos los servidores dentro de este sitio son nombrados por este grupo multicast.

b) En DHCPv6 la comunicación cliente/servidor involucra dos tipos de intercambios:

i. Intercambio cliente/servidor involucrando dos mensajes:

Un procedimiento de configuración mediante DHCP puede ser completado por el intercambio de dos mensajes. Una solicitud desde un cliente y una respuesta desde un servidor.

Petición de información de configuración: Esta interacción cliente/servidor ocurre cuando un cliente no necesita una dirección IPv6 proveniente del servidor. Más bien necesita de alguna

otra configuración, por ejemplo una lista de servidores DNS. El cliente envía el mensaje de petición con toda la información solicitada a todos los dispositivos de reenvío y todos los servidores con direcciones multicast.

Petición para extender el tiempo de vida de la dirección: El cliente envía un mensaje de *Reanudar* y los servidores envían un mensaje de respuesta especificando el nuevo tiempo de vida con el que el cliente podrá seguir usando la dirección.

ii. Intercambio cliente/servidor involucrando cuatro mensajes:

Cuando un nodo necesita una dirección IPv6 válida para realizar las peticiones y además de eso, información de configuración desde el servidor, normalmente en este escenario cliente/servidor se dá un intercambio involucrando 4 mensajes desde el cliente para el servidor.

c) Proceso de la búsqueda de autoconfiguración dentro de un enlace de un cliente DHCP

Solicitud (RS): El cliente envía un mensaje de solicitud para todos los dispositivos DHCP de reenvío y direcciones multicast de los servidores con el objeto de localizar un servidor DHCP disponible.

Anuncio: Cualquier servidor que esté en la disposición de responder la solicitud del cliente lo hará. Enviando el mensaje de notificación a los clientes.

Petición: El cliente envía un mensaje de petición para el servidor seleccionado. Más de un servidor podría responder a la solicitud original del cliente, pero es el cliente quien seleccionará a uno en particular para responderle. Haciéndole saber a través de un solicitud que parámetros de configuración necesita.

Respuesta: El servidor responde a la solicitud del cliente con un mensaje de respuesta conteniendo los parámetros de configuración requeridos por el cliente.

3) Identificador único DHCP (DUID)

Cada cliente y servidor DHCP debe poseer exactamente un *DUID* (Identificador único DHCP), Un servidor DHCP lo utiliza para identificar clientes para la selección de parámetros de configuración y para identificar la *identidad de asociación* (IA) donde pertenece el cliente[13]. Un cliente DHCP utiliza un *DUID* para identificar a un servidor dentro de un mensaje cuando un servidor requiere ser identificado. El *DUID* ha sido diseñado para ser único tanto para clientes como para servidores DHCP, no permitiendo su cambio por ningún motivo. Además, un cliente que es normalmente configurado por ambos mecanismos (DHCPv4 y DHCPv6), podría automáticamente usar el mismo *DUID* sin hacer uso de ningún operador de intervención[14].

4) Transmisión y retransmisión de parámetros (RFC3315)

En la tabla 6.B.5 se detalla los valores usados para describir los mensajes de transmisión entre cliente/servidor.

[13] Un cliente podría tener varias IA asignadas para cada una de las interfaces que posee.
[14] RFC 4361: Node-specific Identifiers for DHCPv4.

Parámetro	Tiempo por defecto	Descripción
SOL_MAX_DELAY	1 segundo	Retardo máximo de la primera solicitud
SOL_TIMEOUT	1 segundo	Solicitud inicial fuera de tiempo
SOL_MAX_RT	120 segundos	Valor máximo de Solicitud fuera de tiempo
REQ_TIMEOUT	1 segundo	Petición inicial fuera de tiempo
REQ_MAX_RT	30 segundos	Valor máximo de petición fuera de tiempo
REQ_MAX_RC	10 segundos	Esfuerzos de reintento máximos de petición
CNF_MAX_DELAY	1 segundo	Máximo retardo de la primera confirmación
CNF_TIMEOUT	1 segundo	Tiempo fuera inicial confirmado
CNF_MAX_RT	4 segundo	Tiempo fuera máximo confirmado
CNF_MAX_RD	10 segundos	Duración máxima confirmada
REN_TIMEOUT	10 segundos	Iniciando reanudar en tiempo fuera
REN_MAX_RT	600 segundos	Valor de tiempo fuera máximo de reanudar
REB_TIMEOUT	10 segundos	Valor de tiempo fuera inicial de *Reenlace*
REB_MAX_RT	600 segundos	Valor de tiempo fuera máximo de *Reenlace*
INF_MAX_DELAY	1 segundo	Máximo retardo de la primera *Petición de información*
INF_TIMEOUT	1 segundo	Tiempo fuera inicial de *Petición de información*
INF_MAX_RT	120 segundos	Valor máximo de tiempo fuera de *Petición de información*
REL_TIMEOUT	1 segundo	Tiempo fuera inicial de *Liberar*
REL_MAX_RC	5 segundos	Esfuerzo máximo de *Liberar*
DEC_TIMEOUT	1 segundo	Tiempo fuera inicial de *Rehusar*
DEC_MAX_RC	5 segundos	Esfuerzo máximo de *Rehusar*
REC_TIMEOUT	2 segundos	Tiempo fuera inicial de *Reconfigurar*
REC_MAX_RC	8 segundos	Esfuerzo máximo de *Reconfigurar*
HOP_COUNT_LIMIT	32 segundos	Máxima numero de saltos dentro de un mensaje de *Retransmisión*.

Tabla 6.B.5: *Parámetros de transmisión y retransmisión.*

5) Anuncios de router

En la tabla 6.B.6 y 6.B.7 se muestran los campos pertenecientes a un paquete de anuncios del router.

Campos de la cabecera IP	Longitud (bits)	Valor	Descripción
Dirección de origen	128	Dirección de enlace local del router	La dirección de enlace local de la interfaz del router envía los avisos del router.
Dirección de destino	128	FF02::1	Direcciones multicast para todos los nodos dentro del enlace.

Campos de la cabecera IP	Longitud (bits)	Valor	Descripción
Limite de saltos	8	255	Es el máximo valor de límites de saltos y permite que el paquete sea enviado a 254 router antes de ser descartado, mientras éste no deje r el enlace.
Campos de cabecera ICMP	**Longitud (bits)**	**Valor**	**Descripción**
Tipo	8	134	134 es el tipo ICMP para un mensaje de *aviso del router* ND.
Código	8	0	
Campos de anuncios de router	**Longitud (bits)**	**Valor**	**Descripción**
Bandera de configuración de dirección manejada	1		Asignada si se permite usar DHCP dentro del enlace.
Otra Bandera de configuración sin estado	1		Asignada si otra información tal como servidores DNS pueden obtenerse del servidor DHCP.
Tiempo de vida del router	16		Si no es cero identifica al router como un router por defecto para el periodo especificado.
Tiempo de acceso	32		Tiempo que es usado por los nodos para determinar si es alcanzable otro nodo dentro del enlace.
Campos de anuncios de router	**Longitud (bits)**	**Valor**	**Descripción**
Tiempo de retransmisión	32		Retardo en segundos entre las *peticiones de solicitud de vecindario*.
Prefijo		Ver tabla 6.B.2	Prefijo usado por los nodos para el proceso de autoconfiguración.
Dirección de capa de enlace del destino (router)	128		Es la dirección de capa de enlace del router destino.
Campos de anuncios de router	**Longitud (bits)**	**Valor**	**Descripción**
MTU (Máxima unidad de transmisión)	32		Es el MTU del enlace.

Tabla 6.B.6: *Parámetros de transmisión y retransmisión.*

Nombre	Longitud (bits)	Valor	Descripción
Tipo	8	3	Identifica el tipo de opción; Información del prefijo asignado en este caso.
Longitud	8	4	Longitud total de los campos de opciones.
Longitud del prefijo	8	0-128, usualmente 64	Longitud del prefijo de abajo, indicando el numero de bits más útil en el prefijo para la autoconfiguración de nodos.
L	1	0,1, usualmente 1	Asigando cuando cuando el prefijo es usado en el enlace. Usualmente es asignado.
A	1	0,1, usualmente 1	Asignado para indicar que el nodo usará el prefijo para autoconfiguración. Usualmente asignado.
Tiempo de vida válido	32		Duración en segundos de la validez del prefijo. Valor de 0xFFFFFFFF define infinidad.
Tiempo de vida preferido	32		Duración en segundos del estado preferido de las direcciones, lo que significa que cada cliente podría usar esta dirección como una dirección de origen cuando es preferido que sea diferente de cero.
Prefijo	128		Prefijo disponible para cada nodo para la dirección de autoconfiguración.

Tabla 6.B.7: *Campos de prefijos en los anuncios de router.*

6. Variables DHCP, direcciones, puertos y tipos de errores

DHCP utiliza los números de puertos UDP de destino. Mientras el puerto de origen podría ser arbitrario. La implementación del cliente podría permitir su especificación a través de los parámetros de configuración local, esto para facilitar el uso del DHCP a través de cortafuegos. La tabla 6.B.8 muestra el número de puerto usado por el protocolo DHCP y la tabla 6.B.9 detalla los tipos de direcciones IPv6 utilizadas en DHCP.

Nombre	Número	Transporte	Descripción
dhcpv6-client	546	UDP	Puerto de destino usado por servidores y dispositivos de retransmisión como router para enviar mensajes a los clientes.
dhcpv6-server	547	UDP	Puerto de destino usado por los clientes para enviar mensajes a los servidores DHCP.

Tabla 6.B.8: *Números de puertos DHCP.*

Nombre	Direcciones	Descripción
Todo dispositivo DHCP	FF02::1:2 (Multicast)	Dirección de destino usada por los clientes para encontrar servidores DHCP dentro del enlace.
Todo servidor DHCP	FF05::1:3 (Multicast)	Dirección de destino usada por los clientes o dispositivos de retransmisión para encontrar servidores dentro del sitio.

Tabla 6.B.9: *Direcciones DHCP*

En toda comunicación cliente/servidor existen errores al momento del envío de mensajes, estos son identificados tanto por clientes, como por cualquier dispositivo DHCP y servidores. En la tabla 6.B.10 se detallan los nombres simbólicos usados entre clientes y servidores para obtener las condiciones del error que ha ocurrido en la comunicación. Debe notarse que los valores numéricos no comienzan en 1 ni tampoco son números consecutivos, estos más bien son organizados en grupos lógicos. Además de eso también los nombre simbólicos usados por los servidores para obtener las condiciones del error ocurrido para clientes. La tabla 6.B.11 muestra el detalle dichos valores.

Nombre del error	Identificador del error	Descripción
Success	00	Éxito
UnspecFail	16	Motivo de fallo no especificado
AuthFailed	17	Fallo de autenticación o inexistencia
PoorlyFormed	18	Mensaje vagamente formado
Unavail	19	Direcciones no disponible

Tabla 6.B.10: *Valores de errores genéricos para cliente y servidores.*

Nombre del error	Identificador del error	Descripción
NoBinding	20	Cliente almacenado no disponible
InvalidSource	21	Dirección del cliente invalida
NoServer	23	Dispositivo de reenvío no encuentra dirección de servidor.
ICMPError	64	Servidor DHCP inalcanzable

Tabla 6.B.11: *Valores de errores genéricos para servidores.*

7. RUTEO IPV6

A. INTRODUCCIÓN

El *ruteo IP* es el proceso de envío de datagramas basados en la dirección IP de destino. El ruteo es realizado por medio de envíos de un host TCP/IP o de un router IP. Cualquiera que sea el caso, la capa de red en el envío del host o del router, debe decidir hacia donde enviar el datagrama, o sea, la ruta hacia el destino final.

Una red IPv6 esta compuesta por un conjunto de subredes IPv6 interconectadas por routers IPv6. Todo nodo en una red IPv6 debe conocer algunas rutas hacia ubicaciones en el mismo enlace al que pertenece, dentro de la misma subred. Algunos de éstos inclusive llegan a conocer rutas hacia ubicaciones fuera del enlace, en otras subredes o fuera de la misma red, mediante un proceso de acumulación.

Un host utiliza directamente rutas asociadas a la subred que pertenece para descubrir nodos en el vecindario y rutas por defecto para llegar a otras ubicaciones. En cambio, un router utiliza rutas para alcanzar todos los nodos dentro del sitio al que pertenece y acumula rutas hacia otros sitios o hacia Internet. Un host conoce rutas automáticamente, mediante mensajes de a*nuncios de router,* al mismo enlace, hacia subredes remotas y a través de rutas por defecto. Por el contrario, configurar las rutas para un router es mas complejo, pudiéndose hacer manualmente con rutas estáticas o utilizando los mecanismos complejos de los protocolos de ruteo para obtención de rutas dinámicas.

Los nodos IPv6 utilizan las tablas de ruteo para determinar como remitir paquetes. Las entradas de la tabla de ruteo IPv6 son creadas por defecto al momento que es inicializado IPv6 y estas son aumentadas tanto a través de configuración manual como por la recepción de mensajes de *anuncios de router* conteniendo rutas y prefijos en el enlace.

1) Entrega directa e indirecta de paquetes

La remisión de paquetes IPv6 utiliza al menos de dos tipos de entrega basados, uno en que el paquete IP sea remitido directamente al destino final, o bien, si es remitido a un router IPv6. Estos dos tipos de entrega son conocidos como entrega directa e indirecta de paquetes.

La entrega directa ocurre cuando el nodo IPv6 remite un paquete a un destino final en una subred a la cual esta directamente conectada.

La entrega indirecta ocurre cuando el nodo IPv6 remite un paquete a un nodo intermedio (router IPv6) debido a que el destino final no esta conectado directamente a la subred.

En la figura 7.A.1 se muestra gráficamente la entrega directa e indirecta de paquetes.

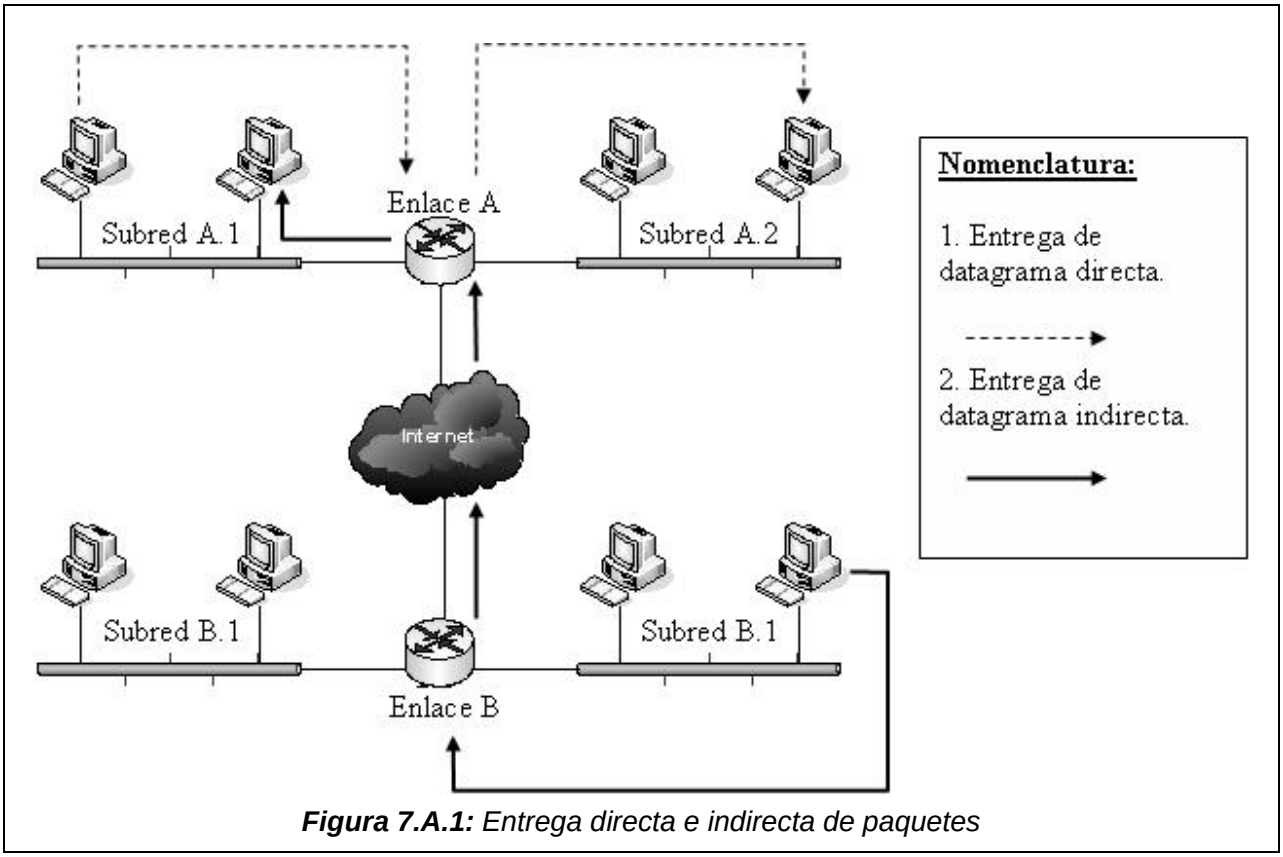


Figura 7.A.1: *Entrega directa e indirecta de paquetes*

2) Tablas de ruteo IPv6

Una tabla de ruteo esta presente tanto en el router como en el host que ejecutan la familia de protocolos TCP/IP, Esta tabla almacena información referente a prefijos de direcciones IPv6 y la manera de acceder a ellos, ya sea directa o indirectamente. El funcionamiento de esta herramienta de ruteo es el siguiente: Antes de revisar la tabla de ruteo IPv6, se verifica la caché de destino comparando las entradas con la dirección de destino en el paquete IPv6 recién enviado. En el caso que la caché de destino no contenga una entrada para la dirección de destino, IPv6 usa la tabla de ruteo para determinar lo siguiente:

a) interfaz utilizada para el envío (o sea, el campo de interfaz del próximo salto): El identificador de interfaz es la interfaz lógica o física que es usada para remitir el paquete para cada destino o para el próximo router.

b) La dirección IPv6 del próximo salto: Para una entrega directa o indirecta, en donde el destino esta dentro del enlace local, la dirección del próximo salto es la dirección IPv6 de destino en el paquete. Para una entrega indirecta, en donde el destino no esta dentro del enlace local, la dirección IPv6 del próximo salto es la dirección de un router.

Una vez determinada la interfaz del próximo salto y la dirección, IPv6 actualiza la caché de destino.

3) Tipos de Entradas de la tabla de ruteo IPv6

Las entradas de la tabla de ruteo pueden almacenar los siguientes tipos de rutas:

a) Rutas directamente conectadas a la subred:
Estas rutas son prefijos de subred para las subredes que están directamente conectadas y generalmente tienen una longitud de prefijo de 64 bits.

b) Rutas de subredes remotas:
Las rutas de subredes remotas pueden ser prefijos de subred, generalmente con una longitud de prefijo de 64 bits, o prefijos de direcciones que totalizan un espacio de dirección, habitualmente con una longitud de prefijo menor de 64 bits.

c) Rutas de hosts:
Para las rutas de hosts IPv6, el prefijo de ruta es una dirección IPv6 específica con una longitud de prefijo de 128 bits. Por el contrario, para los dos tipos de rutas de subred se tiene que la longitud del prefijo de 64 bits o menos.

d) Rutas por defecto:
El prefijo de las rutas por defecto en IPv6 es: [::/0]

4) Proceso de determinación de la ruta

Para determinar que entrada usar dentro de la tabla de ruteo para la decisión de envío de paquetes, IPv6 utiliza los procesos siguientes:

a) Para cada entrada en la tabla de ruteo, se compara los bits dentro del prefijo de dirección con los mismos bits en la dirección de destino por el número de bits indicado en la longitud del prefijo de la ruta. Si todos los bits en el prefijo de la dirección coinciden con todos los bits en la dirección de destino IPv6, la ruta coincide para el destino.

b) Revisando la lista de rutas iguales y seleccionando la ruta que tiene la longitud de prefijo más grande, o sea la ruta que iguala el mayor número de bits en la dirección de destino, La ruta mas larga es generalmente especifica para el destino. En el caso de encontrarse múltiples entradas con longitudes iguales, o sea múltiples rutas para el mismo prefijo de dirección, el router utiliza la *métrica*[15] mas baja para seleccionar la mejor ruta. En el caso de la existencia de múltiples entradas que sean iguales en longitud y tamaño de la métrica, entonces IPv6 puede seleccionar las entradas de la tabla de ruteo en uso.

Para cualquier destino que se tenga. El procedimiento para encontrar la ruta que mejor se adapte se especifica a continuación:

a) Una ruta de host que coincida con las entradas de direcciones de destino.
b) Una subred o conjunto de rutas con el prefijo de longitud que sean iguales al destino.
c) La ruta por defecto [::/0].

Cuando el proceso de determinación de la ruta ha sido completado, IPv6 selecciona una ruta simple contenida en la tabla de ruteo.

[15] Métrica: Número que indica la distancia que existe hacia el destino final (número de saltos).

5) Tecnologías de protocolos y algoritmos de ruteo.

Típicamente los protocolos de ruteo IP esta basados en las siguientes tecnologías:

a) Vector distancia: El protocolo de ruteo de vector distancia propaga la información de ruteo en un formato de prefijo de dirección, esto significa "distancia", Los routers utilizan periódicamente este protocolo para realizar *anuncios de router* dentro de sus propias tablas de ruteo. La utilización de este tipo de tecnología utiliza un mayor ancho de banda, y no es escalable para redes grandes.

b) Estado del enlace: Los routers utilizan los protocolos de ruteo basados en el estado del enlace para intercambian anuncios de estado del enlace (LSA) a través de la red y así poder actualizar las tablas de ruteo. Los LSA consiste de un prefijo de dirección para la red y para cada router que es conectado y el costo asignado a estas redes. El protocolo de ruteo basado en el estado del enlace demanda poco ancho de banda, y es escalable para redes grandes, sin embargo este puede ser más complejo de configurar. En la figura 7.A.2 se muestra routers usando un protocolo de ruteo de enlace de estado para deducir la estructura de su *sistema autónomo*.

Red A conecta a redes B y C
Red B conecta a redes A y D
Red C conecta a redes A y D
Red D conecta a redes B y C

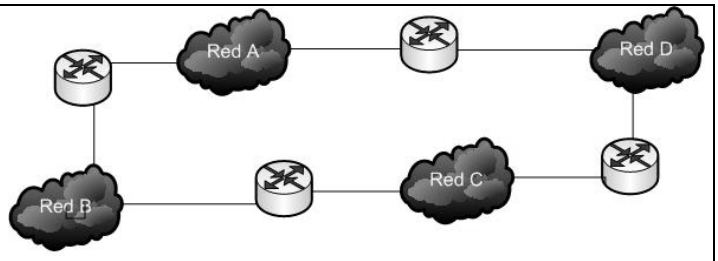


Figura 7.A.2: *Mapa de red creado utilizando enlace de estado.*

c) Vector de ruta: Los router utilizan los protocolos de ruteo basado en el vector de ruta para intercambiar números de sistemas autónomos que indican el camino hacia una ruta, El protocolo de ruteo basado en el vector de ruta demanda poco ancho de banda, y es escalable para redes de tamaño de Internet. Sin embargo estos pueden ser difíciles de configurar.

6) Protocolos de ruteo interior y exterior.

Para describir los conceptos de protocolos de ruteo interior y exterior es necesario definir el concepto de *sistema autónomo (AS)* en término de sus características:

a) Está constituido por sistemas de ruteo que intercambian información por medio de un protocolo de ruteo común.

b) Comprende un conjunto de redes y de routers bajo la gestión de un mismo administrador.

c) Está siempre conectado, con excepción de una situación de fallo, o sea, que siempre existe una ruta entre dos nodos cualesquiera.

Un *protocolo de ruteo interior* es aquel que intercambia información de ruteo entre routers dentro de un sistema autónomo. No obstante, los routers en un sistema autónomo necesitan al menos de una base mínima de información acerca de las redes con las que se puede comunicar fuera del *sistema autónomo*. Es entonces que se necesita un *protocolo de ruteo exterior* para intercambiar información de ruteo entre sistemas autónomos diferentes.

Utilizando estos protocolos y estrategias simples como la designación del router por defecto y *anuncios de ruta* ICMP será suficiente para mover el tráfico de red dentro y fuera de sistemas autónomos (intranets). Sin embargo, los simples protocolos no definen el proceso de ruteo, sólo definen el proceso por el cual los routers intercambian información acerca de la red.

7) Entrega punto a punto

Cuando un host fuente IPv6 envía un paquete IPv6, primero verifica su caché de destino, ejecutando una determinación de rutas si es necesario, y luego verifica su caché de vecindario, ejecutando una resolución de dirección si es necesario. Una vez que el host fuente ha determinado la dirección MAC que corresponde a la dirección del *próximo salto* para el paquete IPv6, éste es enviado al destino o a un router intermedio.

Cuando un router intermedio IPv6 reenvía un paquete IPv6, primero decrementa el limite de saltos, luego verifica su caché de destino, ejecutando una determinación de ruta si es necesario y posteriormente verificando su caché de vecindario, ejecutando una resolución de dirección si es necesario. Una vez que el router ha determinado la dirección MAC que corresponde a la dirección del *próximo salto* para el paquete IPv6, éste es reenviado hacia el destino o hacia otro router.

Cuando un host destino IPv6 recibe un paquete IPv6, primero verifica que el paquete sea encaminado a una dirección IPv6 asignada al host y luego pasa la carga útil IPv6 al protocolo de capa superior apropiado. Para tráfico TCP y UDP, el host transfiere los datos a la aplicación que esté escuchando.

B. PROTOCOLOS DE RUTEO IPV6

1) RIP para IPv6 (RIPng).

En una red tan grande como lo es Internet se hace imposible que un solo protocolo de ruteo se aplique a toda la red, esto debido al continuo desarrollo que posee Internet y al incremento de sus usuarios, aplicaciones y servicios. Por lo que la red entera se organiza como una colección de sistemas autónomos, que son administrados por una sola entidad y que poseen su propia tecnología de asignación de rutas, es por esto que se definen dos protocolos de ruteo para estos sistemas autónomos y son los siguientes:

i. *Protocolo de Pasarela Interior (IGP):* Que es usado dentro de un mismo sistema autónomo.
ii. *Protocolo de Pasarela Exterior (EGP):* Que es usado para transferir información de ruteo entre diferentes Sistemas Autónomos.

En este apartado se describe la estructura y el funcionamiento del protocolo para ruteo *RIP para IPv6* que es basado en el algoritmo del *Vector Distancia* y que trabaja como un *Protocolo de Pasarela Interior* para sistemas autónomos de tamaño moderado. El estudio completo del tema que trata este apartado se encuentra publicado en el estándar de Internet RFC2080.

a) Limitaciones del protocolo RIP para IPv6

i. El protocolo RIP para IPv6 esta limitado a redes con un diámetro máximo de 15 saltos. Esta es la razón por la cual el diseño básico de este protocolo es inapropiado para redes grandes.

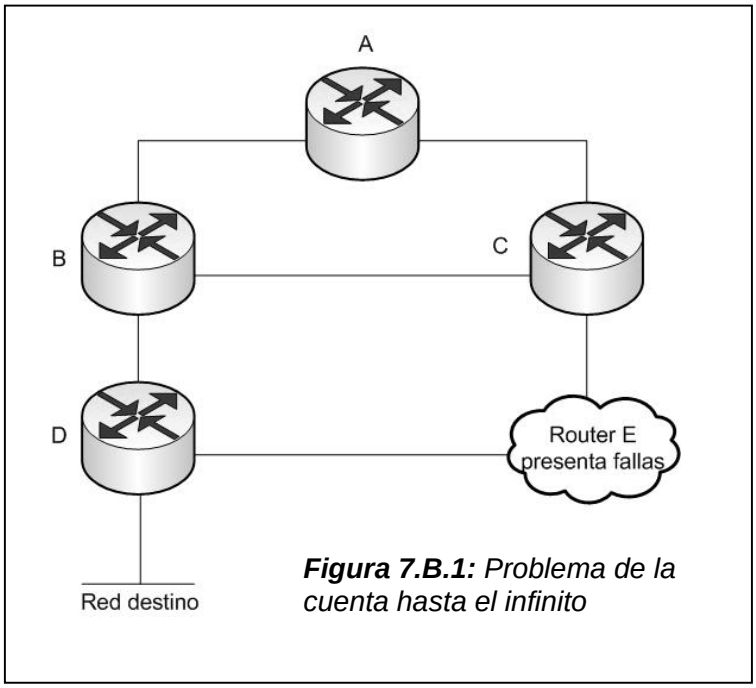


Figura 7.B.1: *Problema de la cuenta hasta el infinito*

ii. El protocolo RIP para IPv6 depende de *"contar hasta el infinito"* para resolver ciertas situaciones que no son normales. Por ejemplo cuando las rutas cambian rápidamente, como en el caso de producirse fallas o caídas de enlaces como se muestra en la figura 7.B.1, la topología de red puede no estabilizar las rutas que han cambiado debido a que la información se propague lentamente y mientras se esté propagando, algunos routers tendrán información incorrecta.

iii. En este tipo de algoritmos, la tarea más difícil es prevenir la inestabilidad.

iv. Este protocolo usa métricas fijas para comparar rutas alternativas. Esto no es apropiado para situaciones donde las rutas necesitan ser seleccionadas, basadas en parámetros tales como una medida de retardo, confiabilidad o carga. Las extensiones obvias permiten métricas de este tipo que son parecidas a introducir las características de una clase que los protocolos no están diseñados para manejar.

b) Especificaciones para el protocolo RIP para IPv6

El protocolo de ruteo RIP es implementado únicamente en routers que tengan una interfaz para una o más redes conectadas directamente, este protocolo extrae información sobre cada una de estas redes siendo la información más importante de estas redes su métrica (que es un entero entre 1 y 15), las implementaciones deben permitir al administrador de la red establecer las métricas especificas de cada red. En adición a la métrica de cada red también es necesario que el administrador de la red establezca también un prefijo de dirección destino y la longitud de este prefijo.

En cada router donde se implementa RIP se tiene una tabla de ruteo donde existe una entrada para cada destino que es accesible en todo el sistema operando RIPng.

Cada entrada debe contener al menos la siguiente información:

i. El prefijo del destino.
ii. Una métrica que represente el costo total de obtener un paquete desde el router hacia un destino (la métrica representa la suma de los costos asociados del recorrido que se debe hacer por las redes para alcanzar un destino).
iii. La dirección IP del próximo router que se encuentra en el camino hacia el destino (si el destino esta conectado directamente a una de las redes, este punto no es necesario).
iv. Una bandera que indique si la información sobre una ruta ha cambiado recientemente.
v. Los Timers asociados con la ruta.

c) Formato del mensaje.

El protocolo RIPng se basa en el protocolo de transporte UDP, pues cada mensaje ue se envía o se recibe, lo hacen los routers a través de puerto UDP 521, el puerto RIPng. Estos mensajes pueden ser de dos tipos:

i. Mensajes que brindan la información sobre el ruteo
ii. Mensajes utilizados para solicitar la información del ruteo

Es importante aclarar que ambos mensajes ocupan el mismo formato que consiste en una cabecera RIP que es fija y una lista de entrada de tablas de ruteo (RTE).

El formato del paquete UDP que utiliza RIPng se ilustra en la figura 7.B.2.

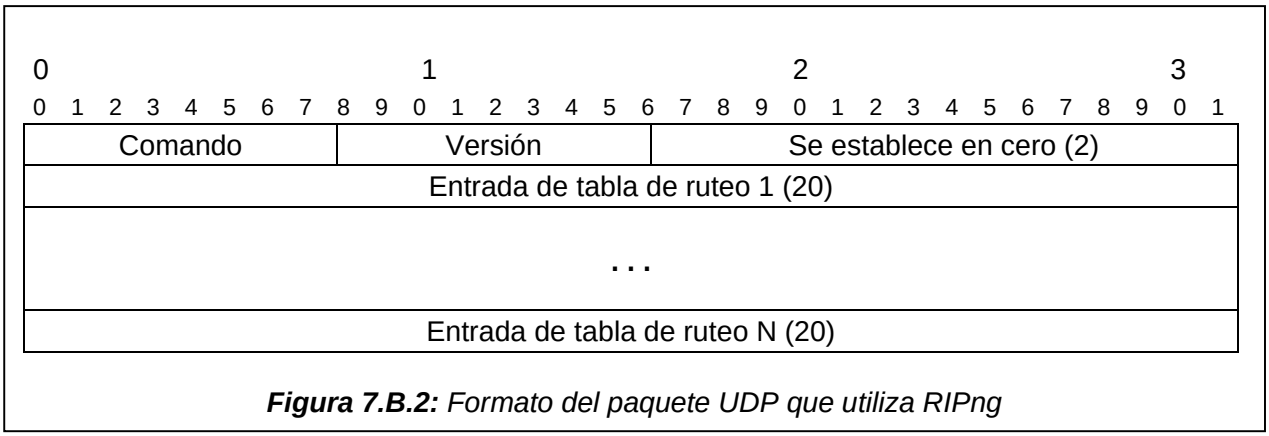


Figura 7.B.2: *Formato del paquete UDP que utiliza RIPng*

Los campos del mensaje UDP para RIPng se detallan a continuación:

i. Comando: Este campo es usado para especificar el propósito del mensaje. Los comandos que son implementados en este protocolo son:
   - *Petición (request):* Se envía un mensaje para solicitar información al sistema, que responde enviando toda su tabla de ruteo o parte de ella.
   - *Respuesta (response):* Es un mensaje que contiene toda la tabla de ruteo o parte de ella y se envia en respuesta a un mensaje *de Petición* o puede ser una actualización de ruteo generada y no solicitada.
ii. Versión: Para el caso del protocolo RIPng la versión es la 1

Como se explicó al inicio de esta sección estos mensajes también contienen una lista de entrada de tablas de ruteo (RTE) en el resto del paquete, donde cada entrada de tabla de ruteo que aparecen en el paquete UDP que utiliza RIPng tiene el formato que se aprecia en la figura 7.B.3.

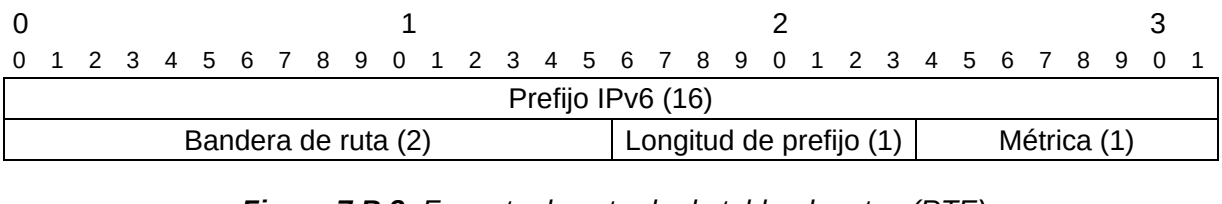


Figura 7.B.3: *Formato de entrada de tabla de ruteo (RTE)*

Los campos de cada entrada de tabla de ruteo se detallan a continuación:

i. *Prefijo IPv6*: Este campo contiene el prefijo destino, que es usualmente de 128 bits (16 octetos).
ii. *Bandera de ruta*: Este campo es un atributo asignado a una ruta la cual debe ser preservada y reanunciada. Los routers soportan otros protocolos que en RIP deben ser configurables para que esta etiqueta sea configurada para trabajar con rutas importadas desde diferentes fuentes.
iii. *Longitud de prefijo*: Este campo contiene el número de bits significativos en el prefijo que es un valor que se encuentra entre 0 y 128 comenzando desde la izquierda del prefijo.
iv. *Métrica*: Este campo contiene el costo de alcanzar ese destino también llamado métrica. Este campo posee un valor entre 1 y 15, o el valor de 16 (infinito), para indicar que el destino no es alcanzable.

El tamaño máximo del paquete UDP para el protocolo RIPng esta limitado por la MTU del medio sobre el cual el protocolo esta siendo usado. La determinación del número de tablas de entrada de router se determina por los siguientes aspectos:

i. La MTU del medio.
ii. El número de octetos de información de la cabecera que preceden al mensaje RIP
iii. El tamaño de la cabecera RIPng
iv. El tamaño de una entrada de tabla de ruteo

La formula que determina el número de tablas de entrada de ruteo es:

$$\#\,\mathrm{RTES} = \mathrm{INT}\left[\frac{\mathrm{MTU} - \mathrm{TamañoCabeceraIPv6} - \mathrm{LongitudCabeceraUDP} - \mathrm{LongitudCabeceraRIPng}}{\text{Tamaño de entrada de tabla de ruteo}}\right]$$

d) Próximo salto del mensaje RIPng

El próximo salto es especificado por una entrada de tabla de ruteo especial y se aplica a todas las direcciones que son almacenadas en la tabla de ruteo que posee el mensaje RIP.

Un próximo salto es identificado por los siguientes valores en la entrada de tabla de ruteo:

i. Un valor de 0xFF en el campo *Métrica*
ii. El campo *Prefijo IPv6* especifica la dirección IP del próximo salto.
iii. Los campos *Bandera de ruta* y *Longitud de prefijo* deben ser establecidos a cero en el nodo remitente y deben ser ignorados en el nodo destinatario del paquete.

Cuando se especifica en el campo *IPv6 Prefijo* con valor de 0:0:0:0:0:0:0:0 indica que la próxima dirección del salto debe ser la del nodo remitente del anuncio RIP. Una consideración importante es que la dirección especificada como un próximo salto debe tener una dirección local de enlace.

El propósito del próximo salto es eliminar los paquetes que están siendo ruteados a través de saltos extras en el sistema. Esto es muy útil cuando el protocolo RIPng no esta corriendo sobre todos los routers de una red.

e) Consideraciones de direccionamiento.

i. No existe una distinción entre rutas de red, subred y host para RIPng porque el prefijo de dirección IP no especifica de que se trata.
ii. Cualquier prefijo con una longitud de prefijo de cero es usado para diseñar una ruta por defecto.

iii. Se sugiere que el prefijo 0:0:0:0:0:0:0:0 sea usado cuando se especifica la ruta por defecto, pero sin embargo el prefijo es esencialmente ignorado.
iv. Una ruta por defecto es usada cuando no es conveniente listar todas las posibles redes en la actualización RIPng, y cuando uno o más routers en el sistema están preparados para manejar trafico en las redes que no están explícitamente listadas. Estos “Routers por Defecto” usan la ruta por defecto como un camino para todos los paquetes para los cuales ellos no tienen ruta explícita.
v. La decisión de cómo un router llega a ser un *router por defecto* es dejada al implementador.
vi. En general, el sistema administrador estará provisto con una forma de especificar cual router debe crear y anunciar las entradas de las rutas por defecto. Si este mecanismo es usado, la implementación debe permitir al sistema administrador seleccionar la métrica asociada con el anuncio de las rutas por defecto. Esto hará posible establecer una precedencia entre múltiples routers por defecto.
vii. Las entradas de rutas por defecto son manejadas por RIPng exactamente de la misma manera de cómo fuese para otro prefijo destino. Los administradores del sistema deben tener cuidado de asegurarse que las rutas por defecto no se propaguen mas allá de lo necesario.

f) Cronómetro del mensaje RIPng

Cada 30 segundos, el proceso de RIPng se activa para enviar un mensaje de *Respuesta* que contiene las tablas de ruteo completas, a cada router vecino. Cuando hay muchos routers en una sola red, hay una tendencia de ellos a sincronizarse para actualizarse al mismo tiempo. Es indispensable que los mensajes de actualización se sincronicen, ya que esto puede evitar colisiones innecesarias en la transmisión de paquetes entre las redes. Por consiguiente, se exige a las aplicaciones tomar las siguientes precauciones:

i. Las actualizaciones que se dan cada 30 segundos y se activan por un reloj cuya tasa no debe ser afectado por la carga del sistema o el tiempo necesario para atender el cronómetro de actualización anterior.
ii. Estos 30 segundos se compensan por un tiempo aleatorio pequeño (+ / - 0 a 15 segundos). El desplazamiento se deriva de: [0.5 * el período de actualización] (es decir, 30).

Hay dos cronómetros asociados con cada ruta y son los siguientes:

i. Cronómetro de interrupción: En este proceso se retiene la información sobre una entrada cuya ruta ha dejado de estar activa en la tabla de asignación de ruta durante un tiempo corto, para que puedan notificarse los vecinos que la ruta ya no es accesible.
ii. Cronómetro de desecho de información: Este proceso se activa 180 segundos después que la última interrupción fue inicializada para quitar la ruta de la tabla de asignación de ruta.

g) Ejemplo de ruteo utilizando RIPng

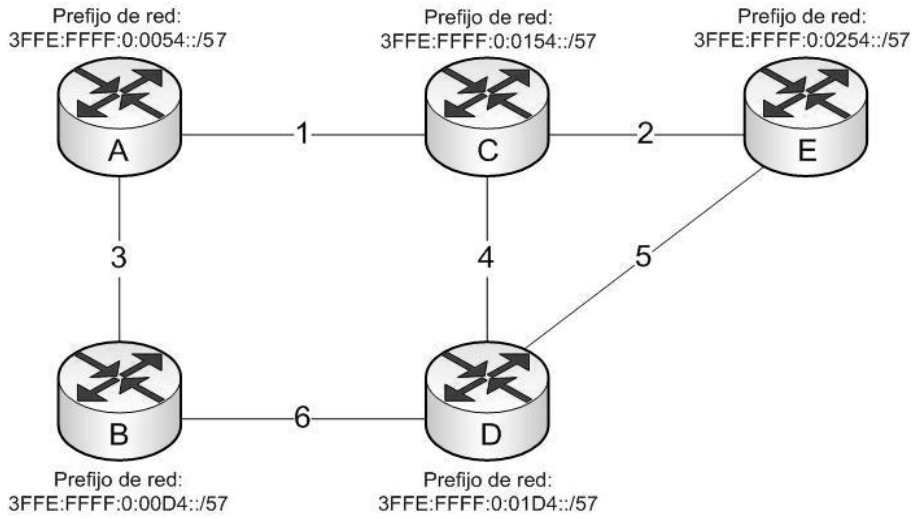


Figura 7.B.4: *Nodos A, B, C, D, E y sus enlaces correspondientes*

Si tenemos los routers A, B, C, D, E y los enlaces 1, 2, 3, 4, 5, 6 que se encuentran en la figura 7.B.4.

Los valores del paquete UDP que utilizará el protocolo RIPng para cada actualización de las tablas de ruteo son:

Response	1	0
Tabla de Entrada de Ruteo: A		
Tabla de Entrada de Ruteo: B		
Tabla de Entrada de Ruteo: C		
Tabla de Entrada de Ruteo: D		
Tabla de Entrada de Ruteo: E		

Para este ejemplo se asume que todos los enlaces tienen una métrica de distancia que posee un costo de 1.

El valor del *Cronómetro* es de 30 segundos

Los prefijos de cada red se observan en la figura 7.B.4.

Tenemos los siguientes procesos en la actualización de las tablas de asignación de rutas del protocolo RIPng

i. Estado de las tablas de entrada de ruteo sin que haya ningún intercambio de información entre los nodos.

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0

ii. *Primer intercambio:* Todos los routers envían sus tablas de entrada de ruteo a sus routers adyacentes

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	1	1
D	3	1

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	1	1
C	2	1
E	4	1

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1

En A: Recibe de B: B=0 Calcula distancia a B = Distancia que pasó B (0) + distancia de A a B (1)

iii. *Segundo intercambio:* Cada router recibe la tabla completa de cada uno de sus routers adyacentes para cada destino, calcula su métrica o costo (costo al router que pasó el destino más el costo a ese router destino). Si el destino no esta en la tabla, lo agrega y si el destino ya esta en la tabla, coloca la entrada de menor costo, si el destino es alcanzado a través del enlace por el que se recibió la actualización el costo es modificado aunque sea mayor que el de la tabla.

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	1	1
D	3	1

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	1	1
C	2	1
E	4	1

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1

iv. *Tercer intercambio.*

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	1	1
D	3	1
C	1	2
E	1	2

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	1	1
C	2	1
E	4	1
D	1	2

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1
A	2	2
D	5	2

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1
C	6	2
B	3	2

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1
A	4	2

Luego de los intercambios anteriores los routers se sincronizan.

Si en este ejemplo se diera el problema de la caída del enlace 1 como se muestra en la figura 7.B.5. Se realizaría el siguiente proceso para actualizar las tablas de ruteo del sistema:

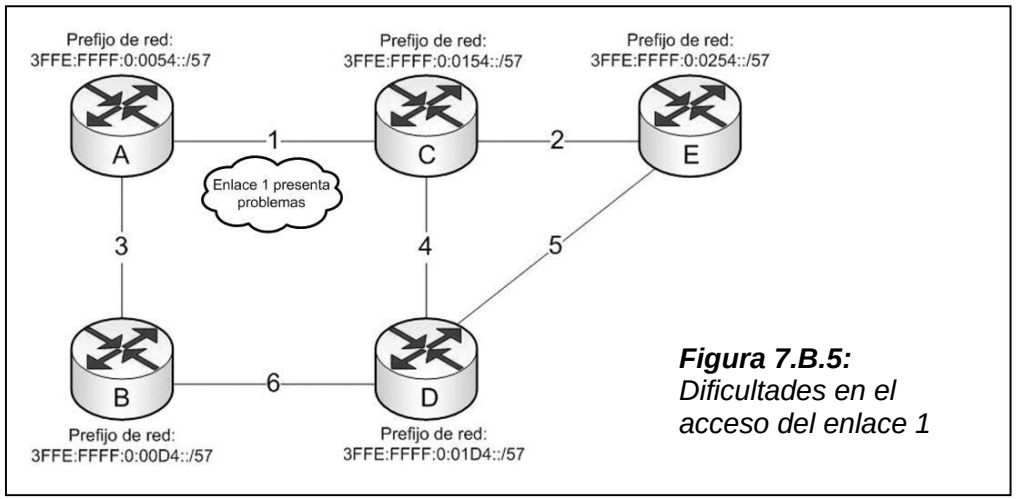


Figura 7.B.5: *Dificultades en el acceso del enlace 1*

i. Los routers A y B detectarían inmediatamente el problema y asignarían una métrica o un costo de infinito (inf) a las rutas que utilizan el enlace 1.

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	1	inf
D	3	1
C	1	inf
E	1	inf

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	1	inf
C	2	1
E	4	1
D	1	inf

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1
A	2	2
D	5	2

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1
C	6	2
B	3	2

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1
A	4	2

ii. El router D actualiza su costo al router B ya que utiliza el enlace 3 para comunicarse con el, lo mismo ocurre con los router C y E.

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	1	inf
D	3	1
C	1	inf
E	1	inf

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	1	inf
C	2	1
E	4	1
D	1	inf

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1
A	2	inf
D	5	2

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1
C	6	2
B	3	inf

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1
A	4	inf

iii. Los routers C, D y E envían sus nuevas tablas

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	1	inf
D	3	1
C	3	3
E	3	2

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	1	inf
C	2	1
E	4	1
D	4	2

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1
A	2	inf
D	5	2

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1
C	6	2
B	6	2

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1
A	6	2

iv. Luego, el intercambio de los routers A,B,D y E produce un estado en el cual todos los routers se sincronizan y se vuelve a tener conectividad.

RTE A		
Prefijo de red: 3FFE:FFFF:0:***0054***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
A	Local	0
B	3	3
D	3	1
C	3	3
E	3	2

RTE B		
Prefijo de red: 3FFE:FFFF:0:***00D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
B	Local	0
A	4	3
C	2	1
E	4	1
D	4	2

RTE C		
Prefijo de red: 3FFE:FFFF:0:***0154***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
C	Local	0
B	2	1
E	5	1
A	5	3
D	5	2

RTE D		
Prefijo de red: 3FFE:FFFF:0:***01D4***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
D	Local	0
A	3	1
E	6	1
C	6	2
B	6	2

RTE E		
Prefijo de red: 3FFE:FFFF:0:***0254***::		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
E	Local	0
B	4	1
C	5	1
D	6	1
A	6	2

Si en el sistema de red mostrado en la figura 7.B.6 el host S requiere enviar un paquete al host T, necesitaría conocer la ruta óptima al destino como sigue:

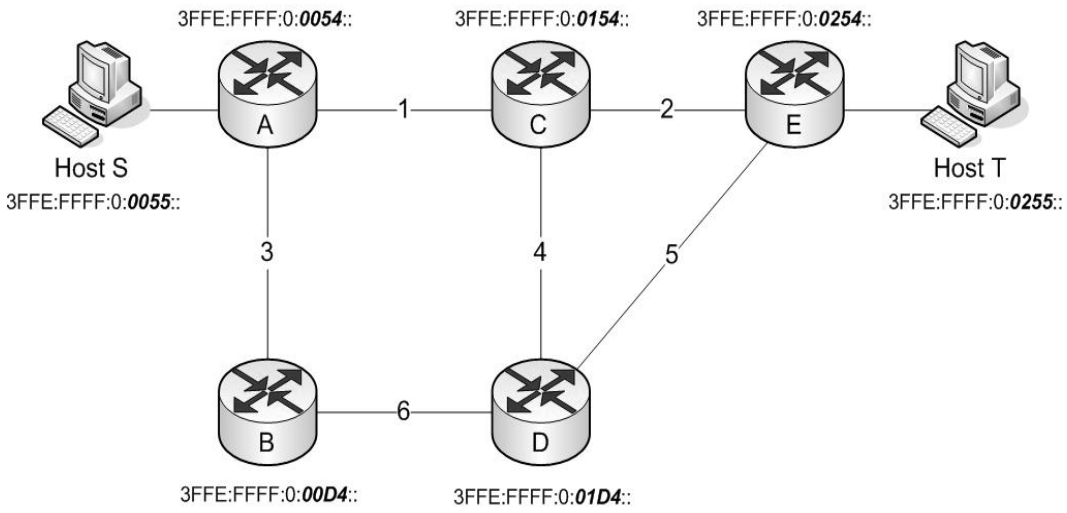


Figura 7.B.6: *Host S requiere enviar un paquete al Host T*

El Host S revisa el identificador de red y comprueba que el host T al que desea enviar el paquete no se encuentra en su mismo enlace. Entonces, aquél construye un paquete IP con la cabecera IP básica y la cabecera de ruteo. En la cabecera IP básica asigna su dirección IP en el campo de la dirección de origen, y la dirección IP del router más próximo en su enlace en el campo de la dirección destino, para este caso el router A. En la cabecera de ruteo se asignan las direcciones de los routers en la ruta y continuación la dirección IP del destino del paquete, para este caso la dirección de T. Ver figura 7.B.6.a.

Paquete IPv6

Cabecera IP	Origen	3FFE:FFFF:0:***0055***::
	Destino	3FFE:FFFF:0:***0054***::
Cabecera de Ruteo	DirRouter C	3FFE:FFFF:0:***0154***::
	DirRouter E	3FFE:FFFF:0:***0254***::
	DirDestino	3FFE:FFFF:0:***0255***::
	Datos	

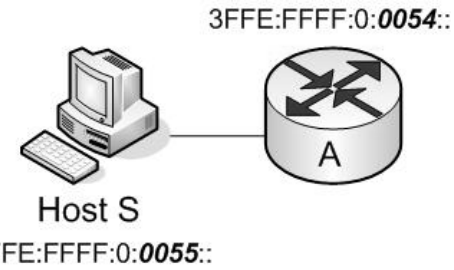


Figura 7.B.6.a.: *Asignación inicial de direcciones en la ruta al destino en cabecera de ruteo*

Cuando el router A recibe el paquete lo examina, procesando primero la cabecera IP y a continuación la cabecera de ruteo. En esta cabecera extendida el router cambia la primera dirección que es la del siguiente router en el camino por la dirección destino de la cabecera IP tal como se muestra en la figura 7.B.6.b. A continuación el router A envía el paquete al router C.

Paquete IPv6

Cabecera IP	Origen	3FFE:FFFF:0:***0055***::
	Destino	3FFE:FFFF:0:***0154***::
Cabecera de Ruteo	DirRouter C	3FFE:FFFF:0:***0054***::
	DirRouter E	3FFE:FFFF:0:***0254***::
	DirDestino	3FFE:FFFF:0:***0255***::
	Datos	

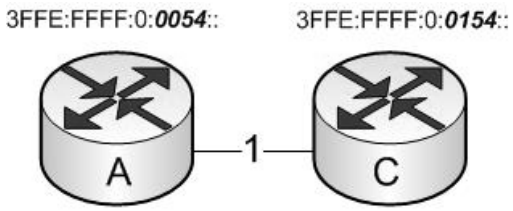


Figura 7.B.6.b.: *Segunda asignación de direcciones en la ruta al destino en cabecera de ruteo*

Cuando el router C recibe el paquete realiza el mismo procedimiento que en el router anterior, examinando y procesando dicho paquete, primero la cabecera IP y a continuación la cabecera de ruteo. Nuevamente en esta cabecera extendida el router cambia la segunda dirección, que es la del siguiente router en el camino, por la dirección destino de la cabecera IP tal como se muestra en la figura 7.B.6.c. A continuación el router C envía el paquete al router E.

Paquete IPv6

Cabecera IP	Origen	3FFE:FFFF:0:***0055***::
	Destino	3FFE:FFFF:0:***0254***::
Cabecera de Ruteo	DirRouter C	3FFE:FFFF:0:***0054***::
	DirRouter E	3FFE:FFFF:0:***0154***::
	DirDestino	3FFE:FFFF:0:***0255***::
	Datos	

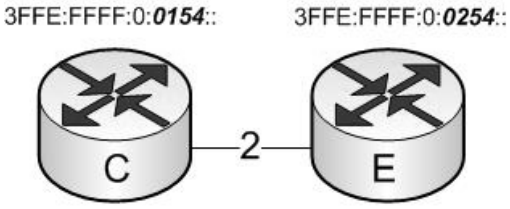


Figura 7.B.6.c.: *Tercera asignación de direcciones en la ruta al destino en cabecera de ruteo*

Finalmente el router E recibe el paquete y después de examinar la cabecera IP y la cabecera extendida las procesa, y luego intercambia la ultima dirección de la cabecera de ruteo por la dirección destino de la cabecera IP, y como el destino se encuentra en su mismo enlace envía directamente el paquete a host T.

Paquete IPv6

Cabecera IP	Origen	3FFE:FFFF:0:***0055***::
	Destino	3FFE:FFFF:0:***0255***::
Cabecera de Ruteo	DirRouter C	3FFE:FFFF:0:***0054***::
	DirRouter E	3FFE:FFFF:0:***0154***::
	DirDestino	3FFE:FFFF:0:***0254***::
	Datos	

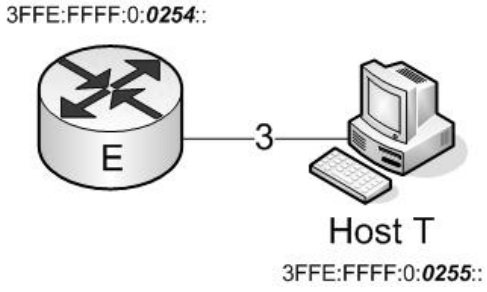


Figura 7.B.6.d.: *Asignación final de direcciones en la ruta al destino en cabecera de ruteo*

2). OSPF para IPv6:

OSPF es el protocolo de estado del enlace definido en el RFC2740 y designado para mantenimiento de la tabla de ruteo dentro de un sistema autónomo simple. OSPF para IPv6 es una adaptación del protocolo de ruteo OSPF versión 2 para IPv4 definido en el RFC2328.

Principales diferencias entre OSPF versión 4 y OSPF versión 6:
En la tabla 7.B.1, se detallan los principales cambios del protocolo de ruteo OSPF ha tenido en la implementación del Pbrotocolo de Internet versión 6.

Característica	Descripción
Procesamiento del protocolo por enlace y no por subred	IPv6 utiliza el término enlace para indicar la facilidad de comunicación sobre un medio, o sea, cuales nodos pueden comunicarse en la capa de enlace. Subredes de múltiples IP pueden ser asignadas para enlaces simples. Dos nodos pueden comunicarse directamente en un enlace simple, aunque no compartan una subred en común.
Remoción de semántica de direccionamiento	En OSPF para IPv6, la semántica de direccionamiento puede ser removida, desde los paquetes de OSPF y desde los tipos principales de LSA.
Adición de ámbito de inundación	La inundación de ámbitos por LSA puede ser generalizado y ahora es un código explícito en el LSA, con el tipo de campo LS. Actualmente se tienen 3 tipos de inundación de ámbitos para LSA: 1. Ámbitos de enlace local. 2. Ámbitos de área. 3. Como enlace.
Soporte explícito para instancias múltiples por en enlace.	Puede correr múltiples instancias del protocolo OSPF en un enlace simple.

Característica	Descripción
Uso de direcciones de enlace local	A todo router asociado a un segmento físico en OSPF para IPv6 le es asignado una dirección unicast de enlace local, Estas direcciones son utilizadas para el envío de paquetes.
Cambios de autenticación	OSPF ha descartada todo campo referente a autenticación de su cabecera, dejándole todo el problema a la suma de verificación que ejecuta el protocolo asociado UDP.
Cambio de formato de paquete	El formato de paquetes OSPF es independiente del protocolo de red, dejando la información de direccionamiento para los diversos tipos de LSA.
Cambio del formato de LSA	En algunos formatos de LSA la información de direccionamiento ha sido removida. Pero se han introducido nuevos tipos de LSA que se utilizan para distribuir dicha información y los datos requeridos para la resolución del próximo salto.
Manejo de tipos de LSA desconocidos	Este manejo ha sido hecho mas flexible de tal manera que estos LSA se tratan como si tuvieran un ámbito de inundación de enlace local.
Soporte de área base	Las áreas base se diseñan para minimizar la base de datos de estado de enlace y los tamaños de las tablas de ruteo para los routers internos de estas áreas.
Identificación de vecinos para identificador del router	Los routers del vecindario en un enlace dado son siempre identificado por su identificador de routers OSPF.

Tabla 7.B.1: *Principales cambios del protocolo OSPF en IPv6.*

3). Sistema intermedio integrado para sistema intermedio para IPV6 (IS-IS):

El protocolo integrado IS-IS, también conocido como el IS dual, es un protocolo de ruteo de estado de enlace que es muy similar al OSPF y que ha sido definido por la Organización Internacional para la Estandarización en el documento ISO 10589. Este protocolo de ruteo fue diseñado independiente del protocolo de la red. IS-IS fue adaptado fácilmente para IPv6 añadiendo unos cuantos valores de tipo y longitud. No necesita direcciones IPv6 en paquetes, puesto que utiliza encapsulamiento en la capa 2. El uso de bases de datos integradas de estado de enlace obliga a una topología idéntica de todos los protocolos de red que maneja, para ambientes donde IPv6 es desplegado incrementalmente o diferentemente a la topología de red IPv4, este protocolo no trabaja integrando IPv4 e IPv6.

4.) El protocolo de pasarela de frontera BGP versión 4 (BGP-4):

El protocolo de pasarela de frontera BGP, conforma un conjunto de protocolos de ruteo para la interconexión de *sistemas autónomos* (AS). La función principal de este protocolo es la escucha de otros sistemas con el fin de intercambiar información de redes disponibles con otros sistemas BGP[16]. Éste es utilizado fundamentalmente para intercambiar rutas entre diferentes dominios administrativos. Cuando es usado entre routers para intercambiar rutas se le conoce con el nombre de eBGP (BGP externo) y cuando es usado dentro de un dominio administrativo es llamado iBGP (BGP interno).
Este protocolo de ruteo tiene soporte en IPv4, utiliza el protocolo de transporte TCP utilizando el puerto 179, y ha experimentado algunos cambios para poder ser implementado en IPv6. En la tabla 7.B.2 se muestra los cambios que ha sufrido BGP para IPv6.

[16] RFC4271: A Border Gateway Protocol 4 (BGP-4).

Característica	Descripción
Próximo salto siguiente (Next hop)	La dirección apropiada del próximo salto asociado con el router BGP para cada NLRI que recientemente sea adjuntada.
Información de disponibilidad de capa de red. (NLRI)	El anuncio de rutas. Esto es expresado como un prefijo IPv6 además la longitud de prefijo.
Información de familia de direcciones	Indica cuáles direcciones del protocolo de capa de red están siendo indicadas. Se utiliza una familia de direcciones específica para identificar rutas IPv6.

Tabla 7.B.2: *Lista de cambios para BGP en IPv6.*

En IPv4 el BGP-4 maneja tres tipos de información, que son especificadas en la dirección IPv4, entre las cuales se tiene:
a) El atributo de próximo salto (NEXT HOP attribute), este es expresado en la dirección IPv4.
b) Agregación (Aggegation), también contenido en una dirección IPv6.
c) Información de disponibilidad de capa de red (NLR), expresado como un prefijo de dirección IPv4.

Entonces para hacer que el BGP-4 soporte a IPv6, o sea soporte el ruteo para protocolos de múltiples capas de red. Se tienen que agregar dos elementos los cuales son:
a) La habilidad de asociar un protocolo de capa de red particular con la información del próximo salto.
b) La habilidad para asociar un protocolo de capa de red particular con información de disponibilidad de la capa de red (NLRI), para identificar protocolos de capa de red individuales.

IPv6 define tres ámbitos de direcciones unicast. La de tipo global, la de local de sitio y la de local de enlace. Las direcciones locales de sitio no son direcciones de enlace local, cada una de ellas es validada dentro del “ámbito” de un sitio y no puede ser exportada fuera de él. Las direcciones de enlace local pueden usarse cuando son generados mensajes de redirección ICMP o como la dirección del próximo salto en algunos protocolos de ruteo, por ejemplo RIPng.

5). Protocolo de ruteo de interdominio versión 2 (IDRPv2):

Es un protocolo de basado en el vector de ruta definido en el ISO 10747. Al igual que BGP-4, el IDRP es utilizado entre sistemas autónomos, conocido como dominio de ruteo IDRP. La versión de IDRP que soporta IPv6 es la IDRP versión 2. IDRPv2 es un protocolo de enrutamiento mejorado ya que permite el uso adicional de identificadores de *sistemas autónomos*. El ruteo de dominios IDRP es identificado en IPv6 por medio de prefijos.

C. CONSECUENCIAS DEL RUTEO EN IPV6.

Aunque los protocolos de ruteo interior y exterior han sido completamente adaptados para utilizarse en redes IPv6 y a pesar del tiempo y la experiencia que se ha acumulado sobre el uso de estos protocolos en el entorno IPv4, se han anticipado algunos posibles problemas que se tienen que resolver para el ruteo IPv6. Es posible que surjan algunos otros adicionales en la medida que más redes IPv6 se unan a la red global. Entre estos problemas se pueden mencionar los siguientes:.

1) Subneteo

Los administradores de red deben tener presente que la asignación más pequeña de prefijo de red que corrientemente es asignado por un RIR es un bloque de 48 bits. Esto significa que las redes IPv6 tendrían 16 bits o más de espacio de subred para jugar alrededor de él. Tradicionalmente, en redes IPv4, el mayor espacio está disponible sólo para redes con el equivalente del bloque de direcciones de red clase A. Pero con un potencial de alrededor de 65,000 subredes en IPv6, los diseñadores de redes deben tener cuidado de construir y operar sus redes y subredes de tal manera que mantengan el tamaño de las tablas de ruteo manejablemente pequeñas. Si la asignación de subredes se deja al azar, puede generar estructuras de ruteo inmanejables para el protocolo de ruteo interior existente.

2) Hardware

Muchos router departamentales o de nivel de sucursal en una red institucional son muy capaces de manejar las necesidades de ruteo típicas de IPv4, pero la posibilidad de tener tablas de ruteo muy grandes podría colapsar a los mismos routers tanto como a los protocolos de ruteo interior.

3) Multihoming (Multiasentamiento)

Cuando una organización recibe dos o más asignaciones de prefijo de direccionamiento IPv6 de diferentes ISP, se dice que éstas son multiasentadas (multihomed). La clave es hacer que la red se comporte como si fuera un solo sistema, tanto cuando interactúe con nodos dentro de la red como cuando interactúe con nodos externos a la red. Una complicación adicional es querer minimizar el número de entradas de la tabla de ruteo para cada red; las soluciones propuestas hasta ahora se enfocan en el uso de túneles entre las diferentes redes asignadas e incorporando rutas alternas dentro de cada entrada de la tabla de ruteo.

8. SISTEMA DE NOMBRE DE DOMINIO (DNS).

A. INTRODUCCIÓN.

Un *nombre de dominio* no es más que una forma fácil de recordar una dirección IP y que está unívocamente asociada a ésta, bajo una autoridad correspondiente. Al igual que las direcciones IP los nombres de dominio nos permiten identificar a los nodos de una red. El *Sistema de Nombre de Dominio*, más conocido por su siglas DNS, es usado tanto en redes privadas como en Internet para proveer un medio de asociar nombres de dominio con direcciones IP, tanto direcciones IPv4 como direcciones IPv6, como sería el caso de coexistencia de redes con preeminencia de uno u otro protocolo. El DNS está basado en una base de datos ligera, escalable y distribuida constituida por tuplas formadas de nombre de dominio, dirección IP y de otra información relacionada, lo que permite la formalización de un espacio de nombres jerárquico bajo delegación y distribución de su administración.
Al protocolo *DNS* se le relaciona con un conjunto de mensajes que pueden enviarse por medio del puerto 53 de los protocolos de transporte *UDP* y *TCP*. En este punto, hay que mencionar que un asunto medular del *DNS* es la *resolución de nombres de dominio,* o su proceso inverso, que es simplemente un mecanismo por el cual un nodo averigua cuál es la dirección IP asociada a un nombre de dominio o al revés. Estos nodos, conocidos aquí como *clientes DNS*, envían consultas sobre resolución de nombres sobre *UDP* primero por ser más rápido, recurriendo a *TCP* cuando se truncan los datos enviados. Los nodos que almacenan porciones de la base de datos *DNS*, conocidos como *servidores DNS*, utilizan *TCP* cuando replican información sobre la base de datos.
Una base de datos *DNS* contiene datos tanto para direcciones IPv4 como para direcciones IPv6. El mecanismo de transporte para el envío de consulta y respuestas es independiente del tipo de datos consultado. Así por ejemplo, se podrían hacer consultas DNS de direcciones IPv6 sobre un transporte basado en IPv4.

B. COMPONENTES DNS.

En las especificaciones primarias para DNS (RFC1034) se precisan los componentes principales para su funcionamiento:

1) *Espacio de nombres de dominio y registros de recursos*.

Es una especificación para un espacio de nombres estructurado en forma de árbol y los datos asociados con los nombres, donde cada nodo y hoja del árbol del espacio de nombre de dominio denomina a un conjunto de información, y donde se procura realizar operaciones de consulta para extraer tipos específicos de información de un conjunto particular. En términos prácticos, se habla de que el *espacio de nombres de dominio* es una base de datos distribuida entre distintos medios de procesamiento y almacenamiento independientes (servidores).

Los *registros de recursos* son archivos en la en la base de datos DNS que puede utilizarse para configurar un servidor de base de datos DNS. La consulta a esta base de datos se hace a través de consulta de nombre de dominio, la cual solicita un nombre de interés y el tipo de recurso de información deseado.

2) *Servidores de nombre de dominio (Servidores DNS)*.

Son programas especiales de servidor que almacenan registros de recursos e información acerca de la estructura de árbol del dominio, y que permiten contestar a las solicitudes de los clientes DNS, consultando para ello sus bases de datos de resolución de dominios. En caso de no encontrar una semejanza a lo solicitado por el cliente pueden reenviar la solicitud a otro servidor de otra parte del árbol del dominio. Esto es así porque conocen las partes del árbol de dominio para las que tienen información completa. Un *servidor de nombre de dominio* se dice que es una *autoridad* para estas partes del espacio de nombre de dominio.

La información de la *autoridad* se organiza en unidades denominadas *zonas*, donde estas zonas pueden ser distribuidas automáticamente a los *servidores de nombre de dominio* que proveen servicio redundante para los datos en una zona.

3) Resolventes (Resolvers).

Son programas que extraen información de los servidores de nombre de dominio en respuesta a las peticiones de clientes DNS. Un cliente DNS utiliza un *resolvente* para generar una consulta de nombre DNS. Un servidor DNS utiliza un resolvente para contactar otros servidores DNS para resolver un nombre de dominio en representación de un cliente DNS. Los *resolventes* generalmente son construidos dentro de programas de utilidad o son accesibles por medio de funciones de biblioteca (sockets) [17].

C. JERARQUIA DE DOMINIOS, ZONAS Y AUTORIDAD.

Un *dominio* es una rama del árbol y puede ubicarse en cualquier punto de la estructura del árbol DNS. Los *dominios* pueden ser divididos en *subdominios* para propósitos de administración o de balance de carga. Los *dominios* y *subdominios* se agrupan dentro de *zonas* para permitir una administración distribuida del espacio de nombres DNS.
Los *dominios* definen diferentes niveles de *autoridad* en una estructura jerárquica. El espacio de nombres DNS en el Internet tiene la siguiente estructura (Figura 8.C.1):

1) Dominio raíz (Root domain)
2) Dominio de nivel superior (Top-level domain)
3) Dominio de nivel secundario (Second-level domain)

El tope de la jerarquía es llamado el *dominio raíz* y son manejados por autoridades regionales de Internet en su respectiva escala de influencia. El próximo nivel en la jerarquía está dividido en una serie de nodos denominados *dominios de nivel superior*, los cuales son asignados por tipo de organización y por región o país. Dentro de éstos caben *dominios de nivel secundario* y hosts.
Una *zona* es una porción contigua de un dominio del espacio de nombres DNS cuyos registros de base de datos existen y son manejados en un archivo particular de base de datos DNS en uno o varios servidores DNS. Se puede configurar un solo servidor DNS para manejar una o varias *zonas*. Cada *zona* está adscrita a un nodo específico de dominio, referido como *dominio raíz de la zona*. Los archivos de zona no abarcan necesariamente a todos los subdominios bajo el *dominio raíz de la zona*.
Las *zonas* están delimitadas por *cortes de zona*. Cada *corte de zona* separa una *zona hija* (debajo del corte) de la *zona matriz* (arriba del corte). El nombre de dominio que aparece en la cima de una *zona* (justo debajo del corte que separa la zona de su matriz) es llamada el origen de la zona. El nombre de la zona es el mismo que el nombre de dominio del origen de la zona. Cada zona comprende ese subconjunto del árbol DNS que está en el origen de la zona o bajo de él esto es, arriba de los cortes que separan la *zona* de sus *hijas* (si las hubiere). La existencia de un *corte de zona* está indicado en la *zona matriz* por la presencia de registros de recursos NS[18] especificando el origen de la *zona hija*. Una *zona hija* no contiene ninguna referencia a su *matriz*.

[17] Socket: interfaz entre programas de aplicación y software de protocolo, y que es particular de un sistema operativo.
[18] Los Registros de Recursos (RR) se definen en la sección 8.E

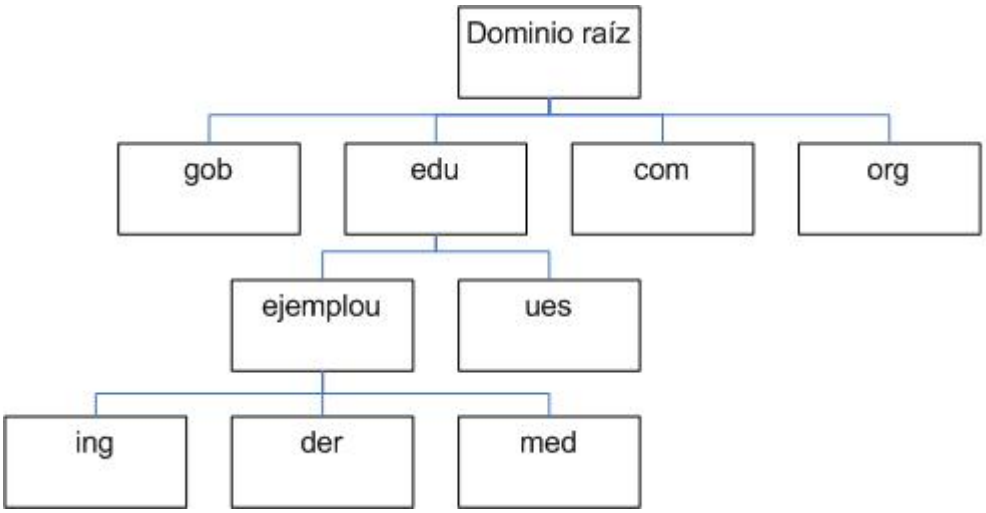


Figura 8.C.1: *Ejemplo de jerarquías de dominios.*

D. RESOLUCIÓN DE NOMBRES DE DOMINIO.

1) El proceso de Resolución de Nombres de Dominio.

La *resolución* de nombres de dominio es el proceso de traducción de un nombre de dominio en su dirección IP correspondiente. Los dos tipos de *mecanismos consultivos* que un *resolvente DNS*, ya sea un cliente DNS u otro servidor DNS, le puede hacer a un servidor DNS son las siguientes:

a) Recursivo.
El servidor de nombre de dominio consultado es requerido para responder con los datos solicitados o con un error estableciendo que los datos del tipo requerido o el nombre de dominio especificado no existen. El servidor DNS consultado no puede sólo referir a un servidor DNS diferente al resolvente DNS. Este es la clase de consulta típica que envía un cliente DNS hacia un servidor DNS.

b) Iterativo.
El servidor de nombre de dominio consultado retorna la mejor respuesta que corrientemente puede proporcionar al resolvente DNS. La mejor respuesta podría ser el nombre de dominio resuelto o una referencia a otro servidor DNS que está más cerca de satisfacer la consulta original del cliente DNS. Este es la clase de consulta típica que envían los servidores DNS hacia otros servidores DNS.

2) Ejemplo de resolución.

En la Figura 8.D.1 se muestra un típico camino de resolución para el nombre de dominio ing.ejemplou.edu entre un cliente DNS y los servidores autoritativos. El proceso se desarrolla paso a paso en la Tabla 8.D.1

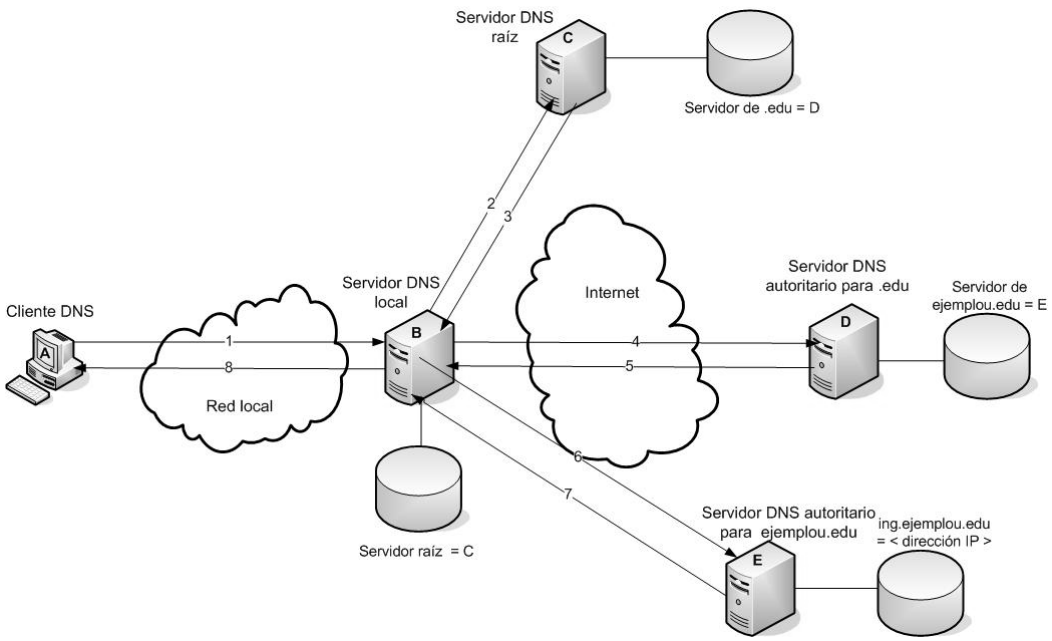


Figura 8.D.1: *Ejemplo de camino típico de resolución para el nombre de dominio en IPv6.*

Paso	De	A	Acción
1	A	B	El cliente DNS (A) envía una petición para la dirección IP de *ing.ejemplou.edu* a su servidor DNS local (B).
2	B	C	El servidor DNS local (B) luego envía la consulta al servidor raíz (C). La dirección del servidor raíz es configurada estáticamente en el servidor DNS local (B).
3	C	B	El servidor raíz retorna la información sobre el servidor autoritario para *.edu* (D).
4	B	D	El servidor DNS local (B) envía la misma consulta al servidor autoritario para *.edu* (D).
5	D	B	El servidor DNS local (B) recibe la respuesta sobre el servidor autoritario para *ejemplou.edu* (E) del servidor autoritario para *.edu* (D).
6	B	E	El servidor DNS local (B) envía la misma consulta al servidor autoritario para *ejemplou.edu* (E).
7	E	B	El servidor DNS local (B) recibe la respuesta para *ing.ejemplou.edu* de el servidor autoritario para *ejemplou.edu* (E).
8	B	A	El servidor DNS local (B) retorna la información al cliente DNS (A).

Tabla 8.D.1: *Proceso de resolución de nombre de dominio para el ejemplo de la Figura.8.D.1*

3) La Consulta DNS.

Las *consultas DNS* son mensajes que pueden enviarse a un servidor de nombres para producir una respuesta. En Internet, las consultas son acarreadas en datagramas UDP o sobre conexiones TCP. La repuesta dada por el servidor de nombres responderá la pregunta puesta en la consulta, referirá al peticionario a otro conjunto de servidores de nombres, o bien, indicará alguna condición de error.

En general, el usuario no genera directamente consultas, pero si hace peticiones a un resolvente que a cambio envía una o más consultas a servidores de nombres y trata con las condiciones de error y las referencias que resultan.

Las consultas y respuestas DNS son acarreadas en un formato estándar como en la Figura 8.D.2.

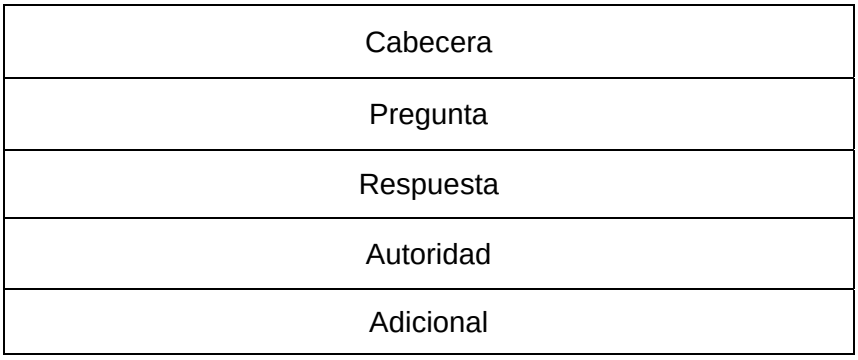


Figura 8.D.2 *Formato de mensaje DNS.*

Donde:

a) *Cabecera (Header):* Acarrea campos que especifican cual de las secciones remanentes están presentes y también si el mensaje es una consulta o una respuesta, una consulta estándar o algún otro *código de operación (opcode)*.

b) *Pregunta (Question):* Acarrea el nombre de la consulta y otros parámetros de ésta.

c) *Respuesta (Answer):* Acarrea los registros de recursos (RR) que directamente responden a la consulta.

d) *Autoridad (Authority):* Acarrea RR's que describen otros servidores autoritarios. Puede ser opcional acarrear un RR SOA para los datos autoritarios en la sección de respuesta.

e) *Adicional (Additional):* Acarrea RR's que pueden ser valiosos en el uso de RR's en las otras secciones.

Hay que denotar que el contenido, pero no el formato, de estas secciones varían con el campo *opcode* de la *cabecera* del formato de mensaje DNS, que se detalla en la Figura 8.D.3.

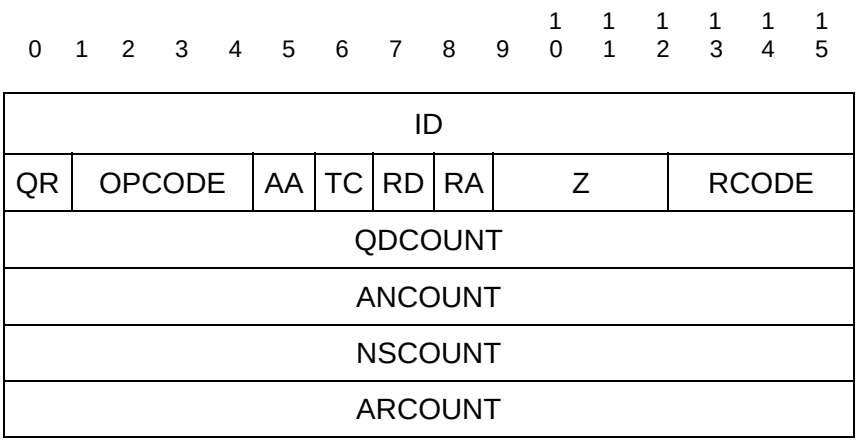


Figura 8.D.3 *Formato de la sección Cabecera de un mensaje DNS*

Donde:

a) *Identificador (ID):* Identificador de 16 bits asignado por el programa que genera cualquier clase de consulta.

b) *Consulta o Respuesta (QR):* Campo de un bit que especifica si un mensaje es una consulta (0) o una respuesta (1).

c) *Código de operación (OPCODE):* Campo de cuatro bits que especifica la clase de consulta en el mensaje, que es puesto por el que lo origina y copiado en la respuesta. Estos son algunos valores para este campo:

0 consulta estándar (QUERY)
1 consulta inversa (IQUERY) (Obsoleta por RFC 3425)
2 consulta de estado de servidor (STATUS)
4 consulta de notificación (NOTIFY)
5 consulta de actualización (UPDATE)

d) Respuesta autoritaria (AA): Este bit es válido en respuestas y específica que el servidor de nombre de dominio que responde es una autoridad para el nombre de dominio en la sección *pregunta.*

e) *Truncamiento (TC):* Especifica que el mensaje fue truncado debido a que la longitud es mayor que la permitida por el canal de transmisión.

f) *Recursividad deseada (RD):* Este bit puede fijarse en una consulta y se copia en la respuesta. Si RD es fijado, se ordena al servidor de dominio a proseguir la consulta recursivamente. El soporte a esta consulta es opcional.

g) *Recursividad disponible (RA):* Este bit es fijado o limpiado en una respuesta, y denota si está disponible el soporte a la consulta recursiva en el servidor de nombre de dominio.

h) *Z :* Reservado para uso futuro. Debe ser cero en todas las consultas y respuestas.

i) *Código de Respuesta (RCODE):* Este campo de 4 bits es ubicado como parte de las respuestas. Los valores que puede tener el código de respuesta se presentan en la tabla 8.D.2:

Nombre	Valor	Descripción
No error	0	No hay condición de error
Error de formato	1	El servidor de nombres fue incapaz de interpretar la petición
Fallo en servidor	2	El servidor de nombres estaba inhabilitado para procesar la consulta debido a problemas con el mismo.
Error de nombre	3	Específico para respuestas de un servidor autoritario de nombres, e indica que el nombre de dominio referenciado en la consulta no existe.
No implementado	4	El servidor de nombres no soporta la clase de consulta solicitada.
Rechazada	5	El servidor de nombres rechaza realizar la operación por razón de políticas.
Reservado	6-15	Reservados para uso futuro.

Tabla 8.D.2: *Valores de Código de Respuesta*

j) *QDCOUNT:* Entero sin signo de 16 bits que especifica el número de entrada en la sección *pregunta*

k) *ANCOUNT:* Entero sin signo de 16 bits que especifica el número de registros de recursos en la sección *respuesta.*

l) *NSCOUNT:* Entero sin signo de 16 bits que especifica el número de registros de recursos de Servidor de nombres en los registros de la sección *autoridad.*

m) *ARCOUNT:* Entero sin signo de 16 bits que especifica el número de registros de recursos en Los registros de la sección *adicional.*

4) La Consulta DNS Inversa.

En una *consulta inversa***,** en lugar de suministrar un nombre y solicitar una dirección IP, el cliente DNS provee la dirección IP y pide el correspondiente nombre de dominio. Las *consultas inversas* son también conocidas como *búsquedas inversas (reverse lookups)*.
Debido a no se puede derivar la dirección IP a partir de un nombre de dominio en el espacio de nombres DNS, solamente a través de búsqueda en todos los dominios podría garantizar una respuesta correcta. Para prevenir una búsqueda exhaustiva en todos los dominios para una consulta inversa, se han creado el *dominio de búsqueda inversa (reverse lookup domain)* y el registro de recurso *puntero (PTR).* Un ejemplo de aplicación de *consulta inversa* es la herramienta de diagnóstico *traceroute*, la que utiliza por defecto *consultas inversas* para mostrar los nombres de los routers en paso de la ruta.
En el caso de IPv6 las consultas inversas utilizan el dominio IP6.arpa (RFC3152). Para crear los dominios para consultas inversas, cada dígito hexadecimal de los 32 que consta una dirección IPv6 pasan en orden inverso a un nivel separado en la jerarquía del dominio inverso. Por tanto, el orden de los dígitos hexadecimales en la dirección se invierte, separando cada uno por un punto, y luego agregándole el sufijo *IP6.ARPA* al final. Así la dirección IPv6:

4321:0:1:2:3:4:567:89AB

Puede registrarse de la forma siguiente:

Nombre	***Registro***	***Valor***
B.A.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA	PTR	ing.ejemplou.edu

Aunque el dominio de búsqueda en reversa estándar actual es *IP6.ARPA*, todavía se sigue utilizando el dominio *IP6.INT* (RFC1886) para asociar direcciones IPv6 a nombres de dominio.

Tal como en las direcciones IPv4, los registros PTR en el *dominio de búsqueda inversa* hacen corresponder direcciones IPv6 con *nombres de dominio completamente calificado (FQDN).*

5) Tipos de Servidores DNS.

DNS define varios tipos de servidores de nombre de dominio, en función de si son responsables de una o más zonas y de su posición dentro de la jerarquía de dominios:

a) *Autoritario*
Un *servidor autoritario* para una zona es enumerado en los registros NS para el origen de la zona, los cuales, junto con el registro de *Inicio de Zona de Autoridad (SOA)* son los registros

mandatarios en cada zona. Un servidor así es *autoritario* para todos los registros de recursos en una zona que no existen en otra zona.

b) *Primario*
Recaban datos para sus zonas de archivos almacenados y mantenidos localmente. Para cambiar una zona, tal como añadir subdominios o registros de recursos, se tiene que cambiar el archivo de zona en el servidor primario de nombre de dominio, pues éstos son responsables de mantener actualizada la información de sus zonas.

c) *Secundario*
Recaban datos para sus zonas a través de la red desde otro servidor DNS, ya sea primario u otro secundario. El proceso de copia desde servidores primarios de esta información de zona como *transferencia de zona*. Las *transferencias de zona* se dan sobre el puerto 53 de TCP. Una de la funciones que pueden cumplir los servidores secundarios es la de respaldo, al mantener información redundante, con lo que si uno falla se puede recuperarla de otro. Adicionalmente, se logra evitar posible sobrecargas de servidores primarios.

d) *Maestro*
Transfieren la información de zona desde servidores primarios a secundarios. Puede ser a la vez primario o secundario para la zona consultada. Cuando un servidor DNS secundario inicia su servicio localiza un servidor maestro y le pide una *transferencia de zona*, la cual éste obtiene previamente del servidor primario correspondiente antes de responder. Esto evita que los servidores secundarios sobrecarguen con transferencias de zona a uno primario.

e) *Sólo almacenaje (Caching-only)*
Se limitan a desarrollar consultas, almacenar respuestas y retornar los resultados a sus clientes. No tiene autoridad sobre ningún dominio y contiene sólo la información que han capturado mientras resuelven consultas. Cuando un cliente les pide una resolución de nombre de dominio, consultan primero su caché, si ubican la dirección IP asociada se la retornan, de lo contrario la consulta prosigue con otros servidores hasta conseguirla, almacenándola para nuevas consultas.

E. REGISTROS DE RECURSOS (RR).

Ninguna base de datos puede existir sin registros, y DNS fue definido para almacenar información de nombres de dominio y direcciones como para proveer capacidad de almacenar otra información relacionada también. La información de DNS es almacenada en registros de recursos (RR). Cada nodo en un dominio posee un conjunto de información sobre recursos, el cual puede estar vacío. El conjunto de información sobre recursos asociado a un nombre particular de dominio está compuesto de registros de recursos separados.
Es posible también que coexistan grupos de registros de recursos con una misma etiqueta, clase y tipo, pero que guarden diferentes datos según su propósito. En este caso se dice que el grupo de registros es un conjunto de registros de recursos (RRSet).

1) Formato de un Registro de Recurso.

La representación gráfica de los campos que comprende el formato de un *registro de recurso* se muestra en la Figura 8.E.1 (RFC1035).

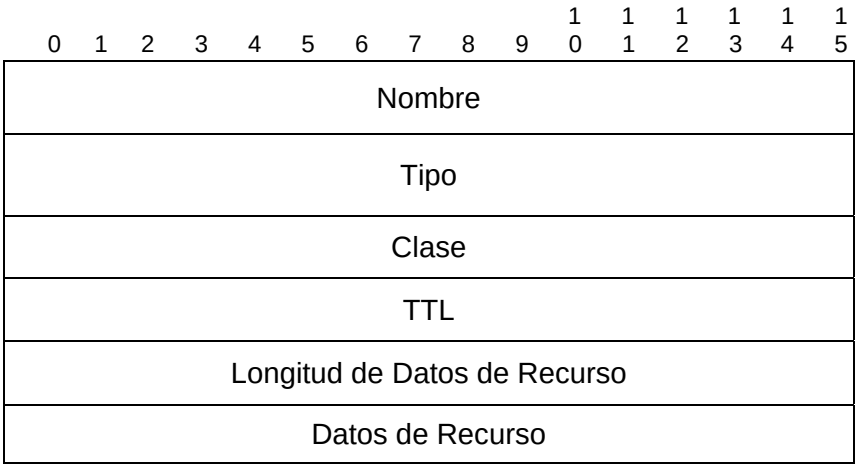


Figura 8.E.1 *Formato de un Registro de Recurso*

Los campos de un RR se describen a continuación:

a) *Nombre (Name):* el nombre de dominio adonde el RR pertenece.

b) *Tipo (Type):* valor codificado en 16 bits que especifica que clase de recurso es referido, entre los cuales están algunos definidos para IPv4 y dos especificados exclusivamente para IPv6 (RFCs 1035, 2535, 2782, 2874, 2915, 3596, 4034):

Tipo	Nombre	Número
SIG	Firma digital de seguridad	24
KEY	Llave pública de seguridad	25
NXT	Siguiente dominio	30
PTR	Puntero a otra parte del espacio de nombre de dominio	12
NAPTR	Puntero a autoridad de nombre de dominio	35
TXT	Cadena de caracteres (texto)	16
CNAME	Nombre canónico para un alias utilizado al acceder a recurso	5
HINFO	CPU y S. O. usado por el host	13
MX	Intercambio de correo para el dominio	15
NS	Servidor autoritario de nombre de dominio	2
SOA	Inicio de zona de autoridad	6
SRV	Dirección IP de servidor para un servicio específico	33
NSEC	Negación autenticada de existencia	47
DS	Firmante de delegación	43
A	Asocia un nombre de dominio a una dirección IPv4	1
AAAA	Asocia un nombre de dominio a una dirección IPv6	28
A6	Asocia un nombre de dominio a una dirección IPv6 en 1 o más registros concatenados, incluyendo otros tipos de información	38

Tabla 8.E.1: *Valores de tipos de Registros de Recursos*

c) *Clase (Class):* Valor codificado de 16 bits que especifica una familia de protocolos o instancia de un protocolo. Es un valor poco utilizado.

d) *Tiempo de Vida (TTL):* Entero de 32 bits que especifica el número de segundos antes de que el RR expirase. Es utilizado principalmente después que un resolvente ha recogido un RR para indicar cuánto tiempo el valor capturado sería almacenado y usado antes de ser descartado como fuera de tiempo.

e) *Longitud de datos de recurso (RDLENGHT):* Valor de 16 bits que indica la longitud de los datos del recurso, en bytes, limitando la cantidad de datos en cualquier RR a no más de 65,535 bytes.

f) *Datos de recurso (RDATA):* Datos asociados con el recurso. La composición y longitud de este campo puede variar dependiendo del tipo de RR.

Algunos RR como NS y MX definidos para uso con IPv4 tienen que ser modificados para que puedan replicar resultados de los tipos A y AAAA. Hacer esto permite a los servidores DNS enviar a los clientes todos los resultados relevantes para una consulta particular de nombre de dominio, incluyendo ambas direcciones IPv4 e IPv6.

2) Tipos de Registros de Recursos para IPv6.

Son dos los registros de recursos definidos para mantener direcciones IPv6 y enlazarlas a nombres de dominio con diferente complejidad. Estos son:

a) El tipo de registro de recurso AAAA.

Este registro de recurso almacena una sola dirección IPv6 de 128 bits en el campo *Datos de recurso (RDATA)*. Cuando se hace una consulta DNS AAAA por un nodo cliente, el servidor DNS responde con una lista de todos los registros de recursos AAAA asociados con el nombre de dominio. Aunque este fue el primer registro para IPv6 (RFC1886, 3596), continua siendo el registro de recurso de IPv6 por defecto en el DNS. Esto es debido a que permite una consulta y respuesta sencilla en la interacción entre clientes y servidores. El valor asignado por IANA para el tipo de este recurso es el número decimal 28 para la clase Internet (IN).
Una consulta de tipo AAAA no desencadena procesos de secciones adicionales como lo hace la consulta de tipo A6.
Un registro de tipo AAAA asocia un nombre de dominio a una dirección IPv6 de la siguiente manera:

Nombre	***Clase***	***Registro***	***Valor***
ing.ejemplou.edu	IN	AAAA	4321:0:1:2:3:4:567:89AB

b) El tipo de registro de recurso A6.

Este registro fue desarrollado en el RFC2874 y no ha podido desplazar al AAAA por su complejidad inherente, de tal manera que en el RFC3363 fue reclasificado a la categoría de experimental. Este tipo de registro es específico de la clase IN (Internet) y tiene número de tipo 38 (decimal).Este registro cuando se combina con otros registros A6, acarrea información completa sobre la dirección asociada con un nombre particular de dominio.
El formato de este registro incluye en su porción de *datos de recurso (RDATA)* una formación de dos o tres campos como se muestra en la Figura 8.E.2.

Longitud de Prefijo (1 octeto)	Sufijo de Dirección (0..16 octetos)	Nombre de Prefijo (0..255 octetos)

Figura 8.E.2 *Formato de la porción RDATA del RR A6*

Los campos en RDATA del RR A6 son:

i) Longitud de prefijo (Prefix len.): Entero sin signo codificado de 8 bits con valores entre 0 y 128, ambos inclusive.

ii) Sufijo de dirección (Address suffix): Sufijo de una dirección IPv6, codificado en el orden de red (octeto de mayor orden primero). Debe haber suficientes octetos en este campo para contener un número de bits igual a 128 menos la longitud de prefijo, con 0 a 7 bits liderando bits de relleno hacer este campo un número integral de octetos. Los bits de relleno, si están presentes, deben ser puestos a cero cuando se cargue una archivo de zona e ignorado en la recepción. (Diferente que para la verificación SIG)

iii) Nombre de prefijo (Prefix name): El nombre del prefijo, codificado como un nombre de dominio, de acuerdo a las reglas en RFC1035. Este nombre no debe ser comprimido.

c) Procedimiento de resolución de nombres con A6:

Para obtener la o las direcciones IPv6 que pertenecen a un nombre dado, un cliente DNS debe obtener una o más cadenas completas de registros A6, cada cadena comenzando con un registro perteneciente al nombre dado e incluyendo un registro perteneciente al nombre de prefijo en ese registro, y así en adelante recursivamente, terminando con un registro A6 con una longitud de prefijo de cero. Una dirección IPv6 se forma de tal cadena tomando el valor de cada posición de bit desde el primer registro A6 en la cadena que cubre válidamente esa posición, como se indica por la longitud de prefijo. El conjunto de todas las direcciones IPv6 para un nombre dado comprende las direcciones formadas de todas las cadenas de registros A6 en ese nombre, descartando registros que tengan longitudes de prefijo inválidas.

Si algunas consultas A6 fallan y otras tienen éxito, un cliente debería obtener un conjunto no vacío pero incompleto de direcciones IPv6 para un host. En muchas situaciones esto puede ser aceptable. La totalidad de un conjunto de registros A6 puede ser determinada por inspección.

Para ilustrar, considérese que pasa cuándo un cliente DNS consulta un servidor para obtener la dirección IPv6 para el nombre de dominio ing.ejemplou.edu. La primera respuesta sería un registro A6 para el nodo mismo, con un valor de prefijo de 8 (64 bits), y el nombre de dominio donde pueda ser adquirida más información, ejemplou.edu. El siguiente paso sería consultar por el nombre de dominio, en tal caso la respuesta sería un registro A6 conteniendo justo la dirección IPv6 de red.; esto es, la longitud del prefijo sería 0, y no habría nombre de dominio del todo., y la dirección misma sería puesta a cero en los 64 bits menos significativos.

El cliente que hace la consulta podría luego concatenar la parte del host de la dirección (del primer registro A6) con la parte de red de la dirección (del segundo registro A6), dando como resultado la propia dirección IPv6 del nodo denominado ing.ejemplou.edu.

3) Actualización dinámica de DNS.

En el RFC2136, con algunas modificaciones del RFC3007, se define el procedimiento de *actualización dinámica de DNS* cuando el escenario es una configuración de direcciones cambiante con cierta regularidad. El método automatizado descrito extiende el espacio de nombres de dominio con nombres y direcciones corrientes para computadoras clientes y servidores actualizando dinámicamente los datos de una zona en el servidor primario de la zona. Con la *actualización dinámica de DNS*, los registros DNS son creados, modificados y removidos automáticamente tanto por las computadoras host como por servidores DHCP en representación de ellas. Así, si un computadora cliente que soporta *actualización dinámica de DNS* envía un mensajes de *actualización* (*update*) a su servidor DNS para añadir automáticamente registros A, A6, AAAA y PTR, el servidor, que también debe soportar la *actualización dinámica de DNS*, verifica si el emisor está autorizado para hacer las actualizaciones y luego actualiza sus archivos de zona local. Todos los cambios y pruebas que se hacen al realizar una *petición de actualización DNS* están restringidas a una sola zona, y son ejecutados en el servidor primario para la zona. El servidor primario para una zona dinámica debe incrementar el número de serie de la SOA cuando ocurra una *actualización* o antes de que se recobre el SOA. Si se hacen algunos cambios, el servidor debe, si es necesario, generar un nuevo registro SOA y nuevos registros NXT, y firmar éstos con las apropiadas llaves de zona. Cambios a los registros NXT por una actualización dinámica segura están explícitamente prohibidos. El registro SOA puede ser actualizado a discreción.
El formato del mensaje de actualización (RFC2136) es el mismo descrito en la Fig. 8.D.2, pero la denominación y usos de los campos que incluyen la sección de *cabecera* son diferentes, tal como se visualizan en la Figura 8.E.3.

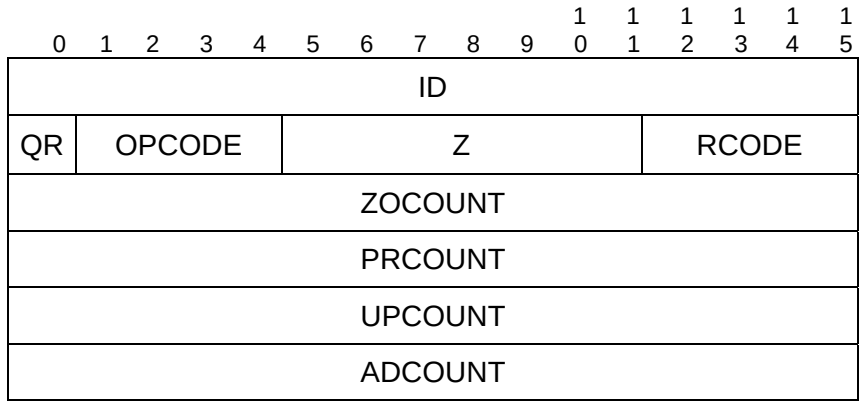


Figura 8.E.3 *Formato de la sección Cabecera del mensaje DNS de Actualización*

Donde:

a) *Identificador (ID):* Identificador de 16 bits asignado por la entidad que genera cualquier clase de petición. Este identificador es copiado en la respuesta correspondiente y puede ser usado por el peticionario para asociar respuestas a peticiones sobresalientes, o para que el servidor detecte peticiones duplicadas.

b) *Consulta o Respuesta (QR):* Campo de un bit que especifica si el mensaje es una consulta (0), o si es una respuesta (1).

c) *Código de operación (OPCODE):* Campo de cuatro bits que especifica la clase de consulta en el mensaje, que es puesto por el que lo origina y copiado en la respuesta. El valor de código que identifica una actualización (update) es cinco (5).

d) *Z:* Reservado para uso futuro. Debería ser cero (0) en todas las peticiones y respuestas. Un valor diferente de cero sería ignorado por implementaciones de esta especificación.

e) Código de Respuesta (RCODE): Campo de 4 bits no definido en peticiones y fijado en respuestas. Los valores y significados de este campo dentro de respuestas son como siguen:

Mnemónico	Valor	Descripción
NOERROR	0	No hay condición de error
FORMERR	1	El servidor de nombres fue incapaz de interpretar la petición debido a un error de formato
SERVFAIL	2	El servidor de nombres encontró un fallo interno mientras procesaba la consulta, ej. error de S.O. o tiempo de reenvío expirado
NXDOMAIN	3	Algún nombre que debiera existir, no existe
NOTIMP	4	El servidor de nombres no soporta el código especificado
REFUSED	5	El servidor de nombres rechaza ejecutar la operación especificada por razones de políticas o de seguridad
YXDOMAIN	6	Algún nombre que debiera no existir, existe
YXRRSET	7	Algún RRset que no debiera existir, existe
NXRRSET	8	Algún RRset que debiera existir, no existe
NOTAUTH	9	El servidor no es autoritario para la zona denominada en la sección *zona*
NOTZONE	10	Un nombre usado en la sección *prerrequisito* o *actualización* no está dentro de la zona denotada por la sección *zona*

Tabla 8.E.2: *Valores de código de respuesta*

f) ZOCOUNT : Número de RR en la sección *zona.*

g) PRCOUNT : Número de RR en la sección *prerrequisito.*

h) UPCOUNT : Número de RR en la sección *actualización.*

i) ADCOUNT : Número de RR en la sección *datos adicionales.*

Cuando un servidor maestro ha actualizado uno o más RR en lo cuales servidores esclavos puedan estar interesados, el servidor maestro puede enviar el nombre, clase, tipo y opcionalmente el nuevo RDATA del RR cambiado, a cada servidor esclavo conocido utilizando el mensaje DNS de notificación (NOTIFY).

9. MOVILIDAD E IP INALAMBRICO EN IPv6.

A. INTRODUCCIÓN

La movilidad en IPv6 está mejorada respecto a IPv4, pues ahora es un atributo intrínseco del nuevo protocolo de Internet, ya que en IPv4 se tiene que incorporar programación compleja para implementar algunas opciones de movilidad.
Con respecto a la movilidad en IPv6 un nodo móvil siempre será alojado en su dirección origen, ya sea si éste está adjunto a su actual enlace de origen o si está actualmente lejos del enlace.
La *dirección de casa* es una dirección IP asignada al nodo móvil dentro de su prefijo de subred en su enlace origen. Cuando un nodo móvil es conectado por algún enlace externo lejos de su origen, permite ser direccionado por una o mas *direcciones de invitado (care-of address)*, que son direcciones IP asociadas con el nodo móvil que tiene el prefijo de subred de un enlace externo en particular. El nodo móvil puede adquirir su *dirección de invitado* a través de los mecanismos convencionales IPv6, tales como autoconfiguración con estado o sin estado.
Una *dirección de casa* es una dirección unicast encaminable asignada a un nodo móvil, utilizada como la dirección permanente del nodo móvil. Esta dirección esta dentro del enlace de origen del nodo móvil
Un *nodo móvil* es aquel cambia su punto de conexión de un enlace a otro, mientras aún es alcanzable mediante su *dirección de casa*.
Un *nodo correspondiente* es un nodo puntual con el cual el nodo móvil esta comunicándose. El nodo correspondiente puede se tanto móvil como estacionario.
Un *agente en casa* es un router en el enlace al que pertenece el nodo móvil y en donde ha registrado su actual *dirección de invitado*. Mientras el nodo móvil está fuera de casa, el *agente en casa* intercepta paquetes en el enlace de casa destinados a la *dirección de casa* (Home address) del nodo móvil, los encapsula, y los tunelea a la *dirección de invitado* registrada al nodo móvil.
Todo nodo móvil puede también aceptar paquetes de varias *direcciones de invitado,* por ejemplo cuando se está moviendo a través de un enlace, pero aún es accesible en el enlace anterior.
Las asociaciones entre los nodos móviles, direcciones de origen y *direcciones de invitado* son conocidas como *aseguramiento (binding)*[19] por el nodo móvil.

En la actualidad lP es usado sobre enlaces inalámbricos, haciéndose este tipo de mecanismo cada día más popular. Algunas de las características de los enlaces inalámbricos se muestran en la tabla 9.A.1.

[19] Es la asociación de la dirección origen un nodo móvil con una *dirección de invitado* para ese nodo móvil, junto con el remanente del tiempo de vida de esa asociación.

Característica	Descripción
Limitado ancho de banda	El espectro de radio es un recurso raro y costoso, donde el ancho de banda disponible en los enlaces de radio es usualmente muy pequeño tal y como los enlaces inalámbricos. Redes 2.5G tienen de 10 a 20 kilobit por segundo (kbps) cuando están conectadas y de 1Oa 40 kbps sin conexión. Para redes 3G tiene 64 Kbps cuando se esta enlazado y 384 Kbps cuando no hay enlace.
Razón de error más alta	Debido a lo caro del espectro de radio, el diseño de redes de celulares tienden a preferir tasa de error más altas, para minimizar el uso del espectro.
Latencia y tiempo aproximado del viaje redondo de enlace largo	Típicamente de 100 a 200 ms tiempo aproximado de viaje en redes de radio, es bastante largo comparado con las redes inalámbricas.
Cambios en las características del enlace	El movimiento de un dispositivo móvil, cambia su distancia a la estación base. El protocolo inalámbrico adapta y además realiza los cambios en las características del enlace.

Tabla 9.A.1: *Características de los enlaces inalámbricos.*

B. EL PROTOCOLO DE INTERNET MÓVIL VERSIÓN 6

1) La cabecera de movilidad IPv6 Móvil (RFC3775)

IP móvil es un protocolo IP diseñado para sostener las conexiones IP mientras la dirección IP cambia. IP móvil está diseñado para trabajar con IPv4 e IPv6, aunque es optimizado con IPv6.
La cabecera de movilidad identificada por el valor de 135 de la próxima cabecera, es inmediatamente antes de la cabecera IPv6 básica. En la figura 9.B.1 se muestra gráficamente lo anterior.

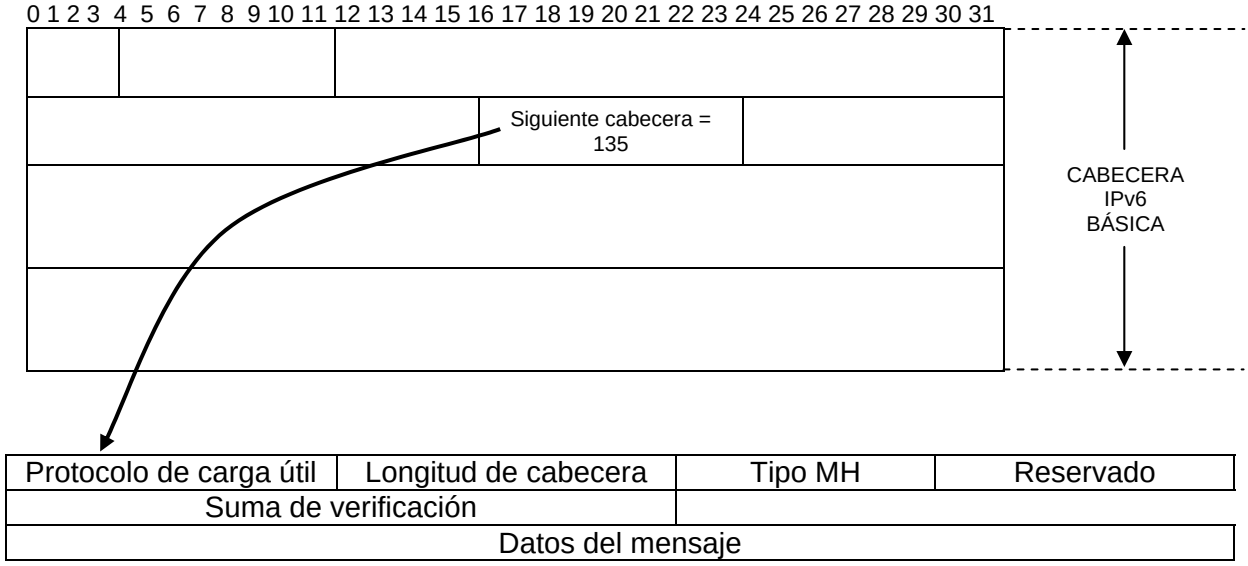


Figura 9.B.1: *Formato de la Cabecera de movilidad.*

Donde:

- *Protocolo de carga útil:* Selector de 8 bits. Identifica el tipo de cabecera inmediatamente después de la cabecera de la movilidad. Usa los mismos valores del campo próxima cabecera.
- *Longitud de la cabecera:* Entero sin signo de 8 bits, representa la longitud de la cabecera de movilidad en unidades de 8 octetos.
- *Tipo MH:* Selector de 8 bits. Identifica el mensaje particular de la movilidad en la pregunta.
- *Reservado:* Campo de 8 bits reservado para uso futuro.
- *Suma de verificación:* Entero sin signo de 16 bits. Este campo contiene la suma de verificación del campo de movilidad. La suma de verificaciones calculada desde la secuencia que consisten en la pseudo cabecera.
- *Datos del mensaje:* Un campo de la longitud variable que contiene el los datos específicos al tipo indicado de la cabecera de la movilidad.

2) Tipos de mensajes de la cabecera de movilidad

En la tabla 9.B.1se detallan los tipos de mensajes de la cabecera de movilidad en IPv6.

Nombre	Tipo de cabecera de movilidad	Descripción
Petición de actualización del aseguramiento (Binding refresh request).	0	Enviado por el correspondiente nodo para el nodo móvil para pedirle que actualice el aseguramiento.
Inicialización de la prueba de origen (Home test init)	1	Enviado por el nodo móvil para inicializar el retorno del procedimiento de ruteo. El mensaje contiene una *cookie*[20] de inicialización de origen.
Inicialización de la prueba de custodia (Care of test init).	2	Enviado por el nodo móvil para iniciar el procedimiento de ruteo de retorno. El mensaje contiene una *cookie* de inicialización de custodia.
Prueba de casa (Home test)	3	Enviado por el nodo correspondiente para el nodo móvil. El mensaje contiene una *cookie* de inicialización de casa y un *token(ficha)* de generación de llave casera.
Prueba de custodia (care-of test)	4	Enviado por el nodo correspondiente para el nodo móvil. El mensaje contiene una *cookie* de inicialización de custodia y un *token(ficha)* de generación de llave casera.
Actualización de aseguramiento (Binding update)	5	Enviado por el nodo móvil para el agente en casa y el nodo correspondiente. El mensaje contiene algunas banderas, una secuencia de números y el tiempo de vida del aseguramiento (binding).
Reconocimiento del aseguramiento (Binding acknowledgement)	6	Enviado por el agente en casa y el nodo correspondiente para reconocer la recepción de la actualización del aseguramiento (binding update).

[20] Cookie: trozo de nformación en un script que puede ser almacenado.

Nombre	Tipo de cabecera de movilidad	Descripción
Error de aseguramiento (Binding error)	7	Enviado por el nodo correspondiente para señalar un error. El mensaje contiene un estatus de números y la dirección destino de origen recibida desde el nodo móvil.

Tabla 9.B.1: *Tipos de mensajes de la cabecera de movilidad*

Los mensajes 1, 2, 3 y 4 se utilizan para desarrollar el procedimiento de ruteo de retorno, cuyo diagrama de flujo se muestra en la figura 9.B.2.

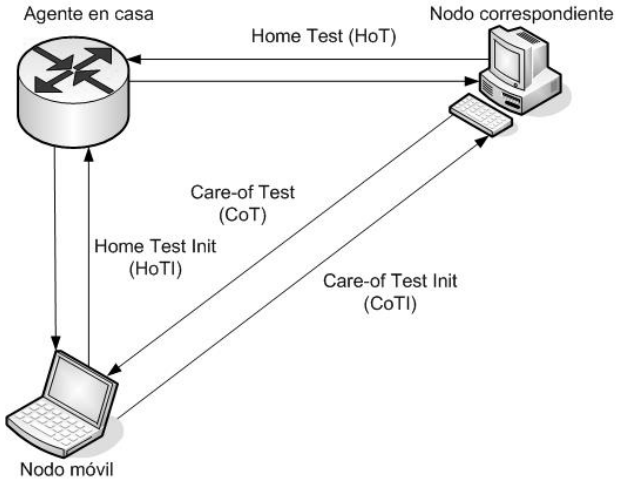


Figura 9.B.2: *Flujo de mensajes para el procedimiento de ruteo de retorno.*

3) Modos de comunicación entre nodos móviles

Existen dos posibles modos para comunicaciones entre el nodo móvil y el nodo correspondiente. El primer modo, *tuneleado bidireccional,* no requiere soporte para IPv6 móvil del nodo correspondiente y esta disponible aun si el nodo móvil no tiene registrado su *aseguramiento* actual con el nodo correspondiente.

Los paquetes del nodo correspondiente son encaminados al agente en casa y luego tuneleados al nodo móvil. Los paquetes al nodo correspondiente son tuneleados del nodo móvil al agente en casa (tuneleados en reversa) y luego encaminados normalmente de la red de casa al nodo correspondiente. En este modo, el agente en casa utiliza un proxy ND para interceptar cualquier paquete IPv6 direccionado a la dirección de casa del nodo móvil o en el enlace origen. Cada paquete interceptado es tuneleado a la dirección de invitado primaria del nodo móvil. Este tuneleado es desarrollado utilizando *encapsulamiento IPv6*.

El segundo modo, *optimización de ruta,* requiere que el nodo móvil registre su *aseguramiento* actual al nodo correspondiente. Los paquetes del nodo correspondiente pueden ser encaminados directamente a la dirección de invitado del nodo móvil cuando envía un paquete a cualquier destino IPv6, el nodo correspondiente busca en sus *aseguramientos* almacenados una entrada para la dirección de destino del paquete. Si el *aseguramiento* almacenado para esta dirección destino es encontrado, el nodo utiliza un nuevo tipo de cabecera de ruteo IPv6 para encaminar el paquete al nodo móvil por el camino de la dirección de invitado indicada en este aseguramiento.

El IP móvil utiliza tuneleado del agente en casa a la dirección de invitado del nodo móvil, pero raramente en la dirección en reversa. Usualmente, un nodo móvil envía sus paquetes a través de un router en la red foránea, y asume que ruteo es independiente de la dirección fuente.

Cuando esta asunción no es cierta, es conveniente establecer un tuneleado en reversa topológicamente correcto de la dirección de invitado al agente en casa. Esto conforma el tema central del RF3024, el cual no intenta resolver los problemas planteados por los cortafuegos localizados entre el agente en casa y la dirección de invitado del nodo móvil.

4) Diferencias entre IPv4 móvil e IPv6 móvil

El diseño de la movilidad en IPv6 mantiene algunas características del diseño hecho en IPv4, más sin embargo presenta algunas mejoras. Entre las diferencias mencionadas en el RFC3775 se tienen:

a) No hay necesidad de desplegar los routers especiales como *agentes foráneos*, como en IPv4 móvil. IPv6 móvil funciona en cualquier localización sin ninguna ayuda especial requerida desde el router local.

b) La ayuda para la optimización de la ruta es una parte fundamental del protocolo, mejor que un sistema anormal de extensiones.

c) La optimización móvil de la ruta IPv6 puede funcionar con seguridad para igualar sin asociaciones predispuestas (pre-arranged) de la seguridad. Se espera que la optimización de la ruta se pueda desplegar en una escala global entre todos los nodos móviles y los nodos correspondientes.

d) El soporte también se integra en IPv6 móvil para permitir que la optimización de la ruta coexista eficientemente con los routers que realizan la "filtración del ingreso".

e) La detección de *vecindario inalcanzable* de IPv6 asegura accesibilidad simétrica entre el nodo móvil y el router por defecto en la localización actual.

f) La mayoría de los paquetes enviados a un nodo móvil mientras vienen de su red origen en IPv6 móvil se envían usando la cabecera de encaminamiento IPv6 en lugar de la encapsulamiento del IP, reduciendo la cantidad de gastos indirectos que resultaban comparándolo con IPv4 móvil.

g) IPv6 móvil se desacopla de cualquier capa de enlace particular. Pues utiliza el *Descubrimiento vecino* IPv6 en vez del *ARP*. Esto también mejora la robustez del protocolo.

h) El uso de la encapsulamiento IPv6 (y de la cabecera de ruteo) elimina la necesidad en IPv6 móvil de manejar el *estado del túnel.*

i) El *agente en casa* dinámico del mecanismo del descubrimiento de la dirección de lPv6 móvil devuelve una sola respuesta al nodo móvil. La difusión directa alcanzada usada en las respuestas IPv4 separa las respuestas desde cada *agente en casa*.

C. NUEVOS TIPOS DE MENSAJES ICMPv6 PARA MOVILIDAD

La movilidad en IPv6 también introduce cuatro nuevos tipos de mensajes ICMP. Dos para el uso del mecanismo de descubrimiento de la dirección dinámica del agente en casa y los dos restantes para la renumeración y configuración de mecanismos móviles (RFC3775).

1). Mensajes ICMPv6 para mecanismos de descubrimiento de direcciones dinámicas de agente en casa.

a) *Mensaje ICMP de Petición de descubrimiento de la dirección del agente en casa* (Home Agent Address Discovery Request).

El mensaje de petición de descubrimiento de la dirección de un agente en casa ICMP es usado por un nodo móvil para iniciar el mecanismo dinámico de descubrimiento de la dirección del *agente en casa*. El nodo móvil envía el mensaje de petición de descubrimiento de la dirección del *agente en casa* a la dirección anycast de agentes en casa de IPv6 móvil para su propio prefijo de subred de casa. El formato del mensaje se muestra en la figura 9.C.1.

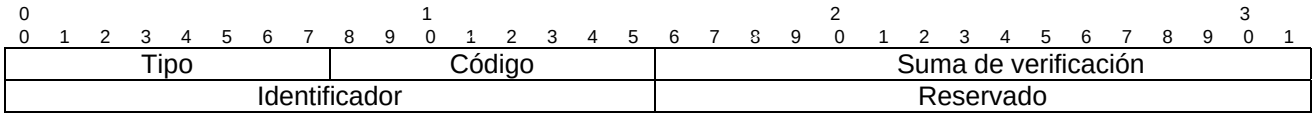


Figura 9.C.1: *Formato del mensaje ICMP para descubrimiento de la dirección del agente en casa.*

Campos ICMPv6:

- Tipo (type): 144
- Código (code): 0
- Suma de verificación (checksum): Se procede como se indica en el apartado 4.B.2.c.
- Identificador (identifier): Un identificador es utilizado para asociar una replica del mensaje del descubrimiento de la dirección del agente en casa.
- Reservado (reserved): Este campo es inutilizado. Debe ser inicializado a 0 por el emisor y debe ser ignorado por el receptor.

b) *Mensaje ICMP de respuesta de descubrimiento de la dirección de agente en casa* (Home Agent Address Discovery Reply).
El mensaje de respuesta del descubrimiento de la dirección del agente en casa es utilizado por un agente en casa para responder a un nodo móvil que utiliza el mecanismo dinámico de descubrimiento de la dirección del agente en casa. El formato de este mensaje se muestra en la figura 9.C.2:

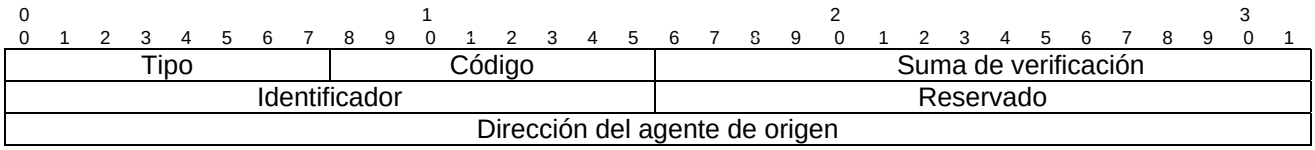


Figura 9.C.2: *Mensaje de respuesta de descubrimiento de la dirección del agente en casa.*

Campos ICMPv6 .

- Tipo (type): 145
- Código (code): 0
- Suma de verificación (checksum): Se procede como se indica en el apartado *4.B.2.c*.
- Identificador (Identifier): El identificador de la invocación del mensaje de descubrimiento de la dirección del agente en casa.
- Reservado (reserved): Este campo es inutilizado. Debe ser inicializado a 0 por el emisor y debe ser ignorado por el receptor.
- Dirección del agente en casa (Home Agent Addresses): Es una lista de direcciones de los agentes en casa dentro del enlace para el nodo móvil.

2). Mensajes ICMPv6 para la renumeración y configuración de mecanismos móviles.

a) *Solicitud del prefijo móvil* (Mobile Prefix Solicitation)
El mensaje de solicitud de los prefijos móviles es enviado por un nodo móvil a su agente en casa, mientras éste se encuentra fuera de su origen. El propósito de este mensaje es solicitar un aviso del prefijo móvil. Esto permitirá que el nodo móvil recopile información referente a su red de origen. Además esta información podría usarse para configurar y actualizar las

direcciones de origen acorde con los cambios de la información del prefijo proporcionada por el agente en casa. El formato del mensaje se muestra en la figura 9.C.3:

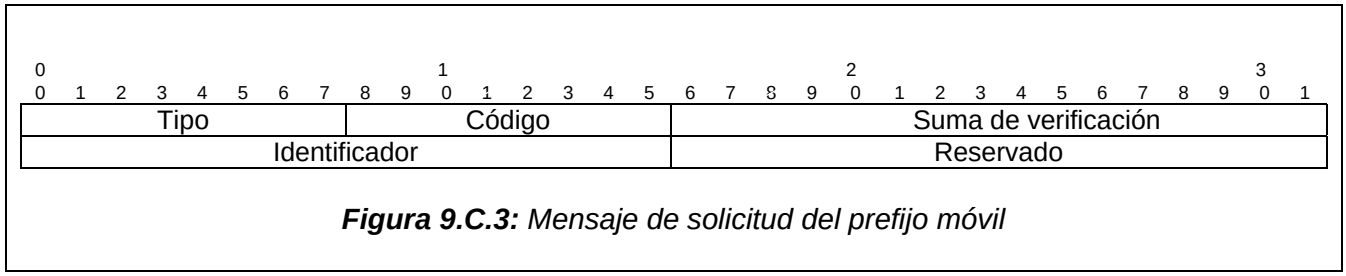


Figura 9.C.3: *Mensaje de solicitud del prefijo móvil*

Valores para los campos:

I. Campos IPv6:
- *Dirección destino:* Dirección de invitado del nodo móvil
- *Dirección de destino:* La Dirección del *agente en casa* móvil.
- *Limite de salto:* Se establece un valor inicial de límites de saltos, similar a cualquier paquete unicast enviado por un nodo móvil.
- *Opciones de destino:* Deben ser incluidas la opción de dirección de origen de destino.
- *Cabecera ESP:* Debe ser soportado por la cabecera IPsec. (Ver cap. 11)

II. Campos ICMPv6:
- *Tipo:* 146
- *Código: 0*
- *Suma* de *verificación:* Se procede como se indica en el apartado *4.B.2.c*.
- *Identificador:* Un identificador para facilitar la igualdad de un anuncio móvil futuro del prefijo a esta solicitud móvil del prefijo.
- *Reservado:* Este campo es inutilizado. Debe ser inicializado a cero por el emisor y debe ser ignorado por el receptor.

b) Mensaje de anuncio del prefijo móvil ICMPv6.

Un *agente en casa* envía un *anuncio del prefijo móvil* a un nodo móvil para distribuir la información del prefijo del enlace de origen, mientras el nodo móvil esta lejos de la red de origen. Esto ocurrirá en respuesta a una solicitud del prefijo móvil con un anuncio. El formato se muestra en la figura9.C.4.

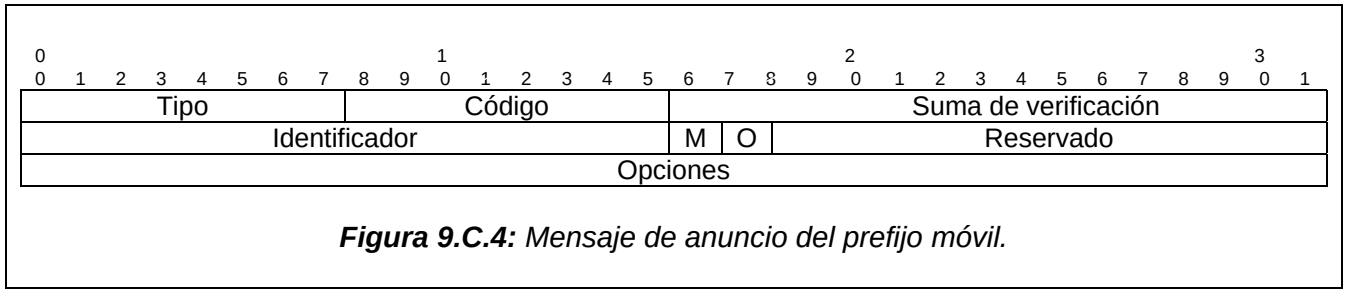


Figura 9.C.4: *Mensaje de anuncio del prefijo móvil.*

Valores para los campos:

I. Campos IPv6:
- *Dirección destino:* La dirección del *agente en casa* tal y como el nodo móvil.
- *Dirección de destino:* Este campo contiene el campo de la dirección origen de ese paquete.
- *Cabecera de ruteo:* Dos tipos de cabeceras de ruteo deberían ser incluidas.
- *Cabecera ESP:* Debe ser soportado por la cabecera IPsec. V*er* capitulo 11)

II. Campos ICMPv6:
- *Tipo:* 147
- *Código: 0*

- *Suma de verificación:* Se procede como se indica en el apartado *4.B.2.c.*
- *Identificador:* Un identificador para facilitar la igualdad de un anuncio móvil futuro del prefijo a esta solicitud móvil del prefijo.
- *Reservado:* Este campo es inutilizado. Debe ser inicializado a cero por el emisor y debe ser ignorado por el receptor.
- *M:* Bandera de 1 bit maneja la configuración de la dirección. Cuando están fijados, los hosts utilizan el protocolo con estado (stateful) administrado para la autoconfiguración de la dirección.
- O: Otra bandera de un bit de configuración con estado (stateful). Cuando están fijados, los anfitriones utilizan el protocolo con estado administrado para la autoconfiguración de la otra información (no direcciones).

D. PROCESO BASICO DE MOVILIDAD IP

El proceso de la movilidad en IPv6 es descrito a continuación:

1. Un nodo móvil utiliza direcciones permanentes. o sea la dirección de casa, cuando está alojado en su red de origen. Si un nodo envía un datagrama para un nodo móvil, éste lo envía a la dirección de casa del nodo móvil.
2. El nodo móvil recibe el datagrama en la red de casa.
3. Cuando un nodo móvil esta visitando una red, fuera de su red de casa, este adquiere por algún medio de la red que visita una dirección IP temporal, llamada la *dirección de invitado* (*care-of-address)*.
4. El nodo móvil registra esta *dirección de invitado (care-of-address)* con su agente en casa.
5. El nodo correspondiente conoce del nodo móvil solamente por su dirección de casa. Así envía un datagrama con la dirección de destino como la dirección de casa del nodo móvil.
6. El datagrama es reenviado hacia la dirección de casa, donde el *agente en casa* intercepta el datagrama y lo reenvía hacia el nodo móvil basándose en el reconocimiento del agente en casa de la *dirección de invitado* del nodo móvil, estando esta dirección situada en la red de visita. El nodo móvil recibe el datagrama.
7. Cuando el nodo móvil envía un datagrama para el nodo correspondiente, la dirección de origen del datagrama es la dirección de casa del nodo móvil, y lo envía directamente al nodo correspondiente.

Dicho proceso se detalla gráficamente en la figura *9.D.1.*

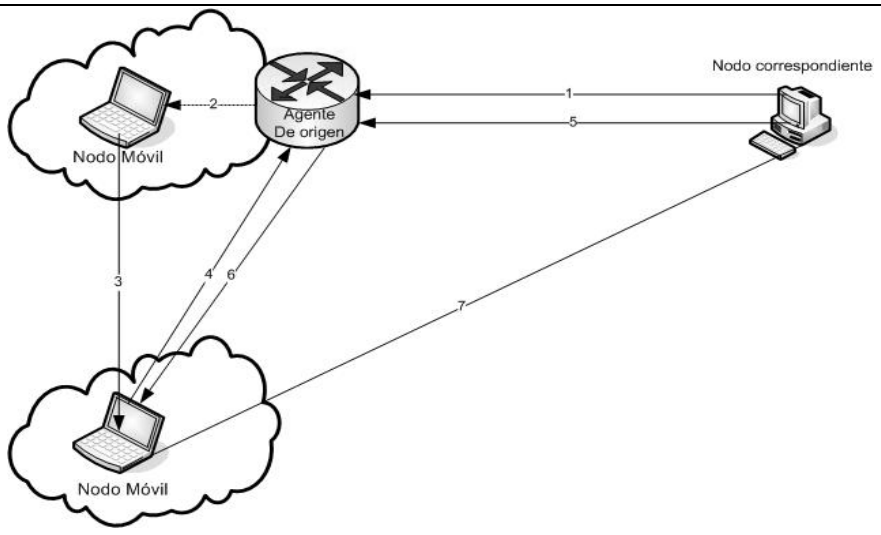


Figura 9.D.1: *Proceso básico de movilidad en IPv6.*

E. NODO MOVIL QUE ESTA LEJOS DE SU ORIGEN

Un nodo de móvil necesita saber cuándo se ha movido para comenzar a usar los funciones de movilidad IP. Un nodo se mueve cuando cambia su dirección IP. Para saber cuando éste se ha movido, un nodo compara su dirección de casa con la nueva dirección adquirida. Si las direcciones son iguales, entonces este se encuentra en su red de origen, de lo contrario este se encuentra visitando otra red. Un nodo móvil que visita una red adquiere una dirección IPv6 por medio de la autoconfiguración o DHCPv6. El nodo correspondiente conoce el nodo móvil por la dirección de casa. Por defecto, el nodo correspondiente envía el datagrama a la dirección de casa, el agente en casa intercepta la dirección del paquete de la dirección de casa del nodo móvil, encapsula esta dirección en un paquete IPv6, con la *dirección de invitado* del nodo móvil como la dirección de destino y entonces es enviado al nodo móvil que visita el sitio remoto. En la figura 9.E.1 se muestra un nodo enviando un paquete a una dirección de casa.

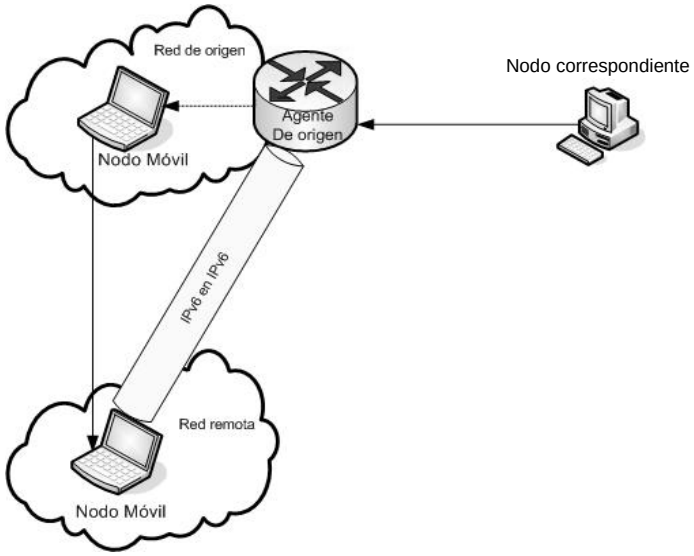


Figura 9.E.1: *Nodo correspondiente enviado un paquete a una dirección de casa.*

1) Nodo móvil contactando al agente de origen.

Después de adquirir la nueva dirección IP y descubrir que se encuentra de visita. El nodo móvil registra la nueva dirección IP con el agente en casa, a través de una secuencia de mensajes denominados *actualización del aseguramiento (Binding Update)*. Después que se ha realizado la *actualización del aseguramiento (Binding Update)* el agente en casa puede entonces reenviar cualquier paquete recibido para el nodo móvil a su nueva dirección IP, tal y como se muestra en la figura 9.E.1.

2) Nodo móvil contactando al nodo correspondiente.

La *actualización del aseguramiento* es también enviado para algunos nodos correspondientes para informarlos de la nueva dirección IP del nodo móvil. Después de recibir el mensaje de *actualización del aseguramiento,* el correspondiente nodo envía el paquete directamente a la nueva localización del nodo móvil, sin ir a través del agente en casa.

F. REDUCCIÓN DE LA CABECERA SOBRE ANCHOS DE BANDA LIMITADOS EN LA CAPA DE ENLACE.

La mayoría de los protocolos de tiempo real para voz y video sobre IP utilizan Protocolos de tiempo real (RPT) sobre UDP. Un datagrama RPT sobre UDP en IPv4 combinaba una cabecera de tamaño de 40 octetos repartidos de la siguiente manera: 20 octetos para la cabecera IPv4, 8 octetos para la cabecera UDP y 12 octetos para la cabecera RTP. En IPv6 esta combinación del tamaño de cabecera es de 60 octetos donde la cabecera IP es 20 octetos

más grande que la de IPv4. Para el caso de UDP y RPT el tamaño de la cabecera es el mismo. Si el tráfico de voz asciende a 50 datagramas por segundos. Entonces las cabeceras IPv6, UDP y RPT combinaran la cabecera de 60 octetos, es decir, 50x 60x8 = 24 bits/segundo. Considerando una voz típica sobre un datagrama IP tiene un tamaño entre 15 y 20 octetos de datos, la carga de la cabecera es muy grande para manejarlo. Especialmente considerando el limitado ancho de banda. Entonces es necesaria la reducción de la cabecera IP por las siguientes razones:

Tiempo de reacción mejorada

- Ancho de banda utilizado eficientemente para paquetes pequeños
- Latencia baja para paquetes pequeños
- Disminución del desbordamiento de cabeceras
- Reducción de paquetes perdidos

G. COMPORTAMIENTO DE TCP SOBRE ENLACES INALAMBRICOS.

El diseño del TCP para redes inalámbricas asume una pequeño tasa de bit de error. El flujo de control basado en la congestión de la red, no así, en la tasa de bit de error de la capa de enlace. El TCP retarda la tasa de transferencia de datos en caso de errores, en cada conexión TCP independientemente.
En un enlace inalámbrico la tasa de error es usualmente muy alta, se presenta en la mayoría de los casos en los paquetes perdidos. El comportamiento del TCP es como que si hubiera una congestión de red.
Cuando una conexión TCP es atravesada por una conexión inalámbrica y una red de área amplia tal y como se muestra en la figura 9.G.1, la tasa del bit de error en el enlace inalámbrico y control de la congestión dentro de la red amplia compiten y genera un doble problema en el algoritmo TCP.

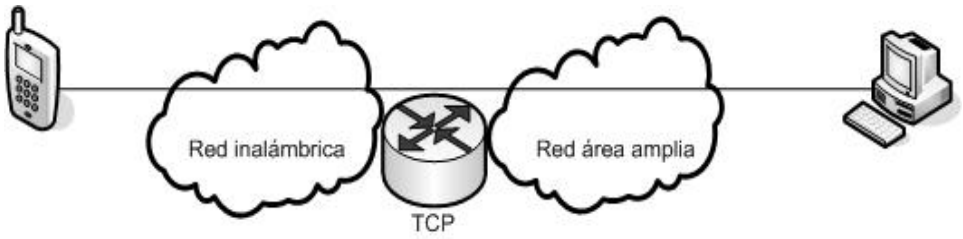


Figura 9.G.1: *TCP sobre redes inalámbricas y de área amplia.*

H. 3GPP

El programa de circuitos asociados de tercera generación (The third generation program - 3GPP) es el estándar para GSM/GPRS basado en redes 3G (RFC3314). Desde una visión del IP cada equipo móvil del usuario (*EQ*) debería, tal y como los teléfonos celulares, tener un enlace punto a punto para los nodos soportando pasarelas GRPS (GGSN), el próximo salto del router, sobre el servicios de radio de paquete general (General Packet Radio Services) en la red de aire es como se muestra en la figura 9.H.1.El enlace punto a punto utiliza el protocolo de datos de paquete (PDP) dentro de un contexto de negociación en el infraestructura subyacente. El enlace punto a punto es asignado a un prefijo de /64. Para mayor especificación ver el RFC3314 “Recommendations for IPv6 in Third generation Partnership Project (3GPP) Standards”.

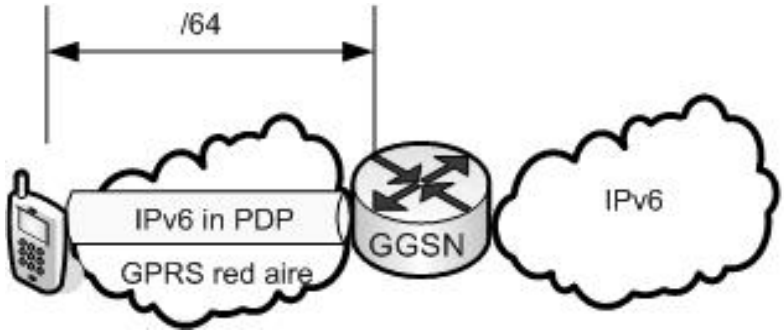


Figura 9.H.1: *Enlace IPv6 en 3GPP.*

10. PROTOCOLO DE SEGURIDAD EN IPv6 (IPsec)

A. INTRODUCCIÓN

Las computadoras, las redes, los sistemas operativos, las aplicaciones, los protocolos y los usuarios son componentes que forman un complejo sistema, cuando ellos interactúan entre si la seguridad debe ser aplicada a cada componente por separado, aunque es importante recalcar que la seguridad perfecta no existe. Pero si se deben prever los riesgos y prepararse para afrontarlos.

El propósito de este capítulo es enfocar la forma como se administra la seguridad en el nuevo protocolo de Internet IPv6, y como se proporcionan los servicios de seguridad a la capa de Internet IP y a todos los protocolos superiores basados en IP.

Es importante hacer notar que el protocolo de seguridad viene integrado en el nuevo protocolo de Internet IPv6.

B. PROTOCOLO DE SEGURIDAD IPsec

El estudio completo de las generalidades del protocolo de seguridad IPsec se encuentra publicado en el RFC2401. Este protocolo proporciona diferentes servicios de seguridad en la capa de Internet IP permitiendo seleccionar los siguientes componentes para garantizar la seguridad dentro de un sistema de red:

i. Determinación de los servicios de seguridad que se deben utilizar y en que combinaciones.
ii. Determinación del algoritmo a utilizar para los servicios de seguridad.
iii. Negociar cualquier criptografía de clave requerida para proporcionar los servicios solicitados.

Entre los servicios que proporciona el protocolo de seguridad IPsec se pueden mencionar los siguientes:

i. Control de acceso.
ii. Integridad sin conexión.
iii. Autenticación del origen de los datos.
iv. protección anti-reenvío (anti-replay) (una forma de integridad parcial de secuencia)
v. Confidencialidad (encriptación).
vi. Confidencialidad limitada del flujo de tráfico.

Además estos servicios pueden ser utilizados por cualquier protocolo de capa superior, por ejemplo, TCP, UDP, ICMP, BGP, etc.

1) Cómo trabaja IPsec

IPsec utiliza dos subprotocolos para proporcionar seguridad al tráfico de un sistema de red, y son los siguientes:

a) *La cabecera de Autenticación (AH):* Se utiliza para proporcionar integridad sin conexión, Autenticación del origen de los datos y un servicio opcional de protección anti-reenvío (anti-replay).

b) *La carga de seguridad encapsulada (ESP):* Se utiliza para proporcionar confidencialidad (encriptación), y confidencialidad limitada de flujo de tráfico, también proporciona integridad sin conexión, Autenticación del origen de los datos y un servicio de protección anti-reenvío (anti-replay).

2) Modos de utilizar IPsec

Cada uno de estos subprotocolos con los que trabaja IPsec soporta dos modos de uso:

i. Modo transporte
ii. Modo túnel

a) Modo transporte.

En este modo el contenido transportado dentro del paquete (utilizando cualquiera de los subprotocolos de seguridad) son los datos de la capa de transporte (TCP, UDP, etc.), por lo tanto la cabecera del protocolo de seguridad IPsec se inserta a continuación de la cabecera IPv6 y antes de los datos de la capa superior que se desean proteger. La ventaja de este modo es que garantiza la comunicación de extremo a extremo, siempre que los nodos que se estén comunicando utilicen IPsec. En la figura 10.B.1 se ilustra el funcionamiento del modo transporte.

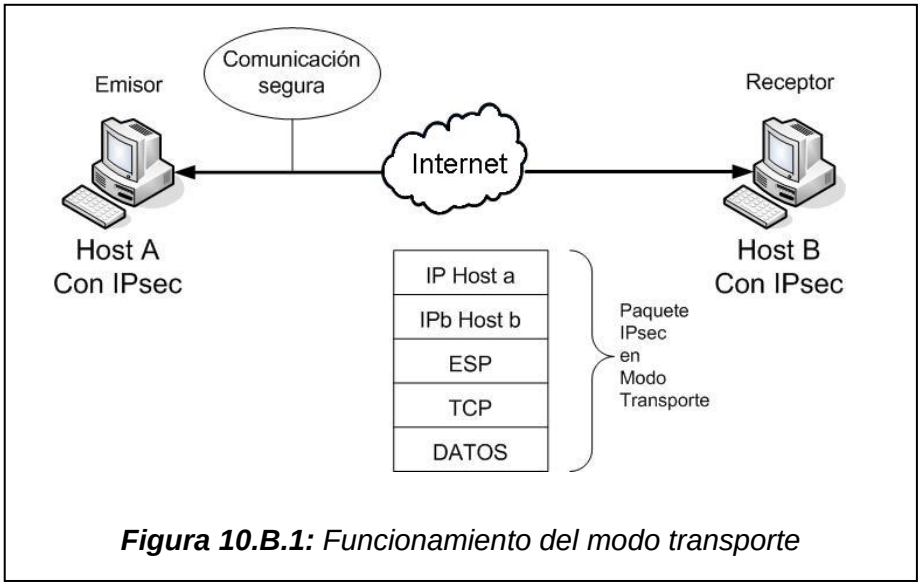


Figura 10.B.1: *Funcionamiento del modo transporte*

b) Modo túnel.

En este modo el contenido transportado dentro del paquete (utilizando cualquiera de los protocolos de seguridad) es el paquete IP completo. El procedimiento que se sigue para enviar un paquete entre dos nodos es el siguiente:

i. Se toma la cabecera IPv6 básica y luego como siguiente cabecera la cabecera AH o ESP
ii. Luego se añade una nueva cabecera IPv6 que es la que se utiliza para encaminar los paquetes a través de la red. Generalmente el modo túnel se utiliza cuando el nodo destino no utiliza IPsec.

El modo túnel es empleado por routers que se usan como cortafuegos (denominados pasarelas o gateway de seguridad), de tal forma que el encriptado se lleve acabo entre un host y la pasarela de seguridad. En la figura 10.B.2 se ilustra el funcionamiento del modo túnel.

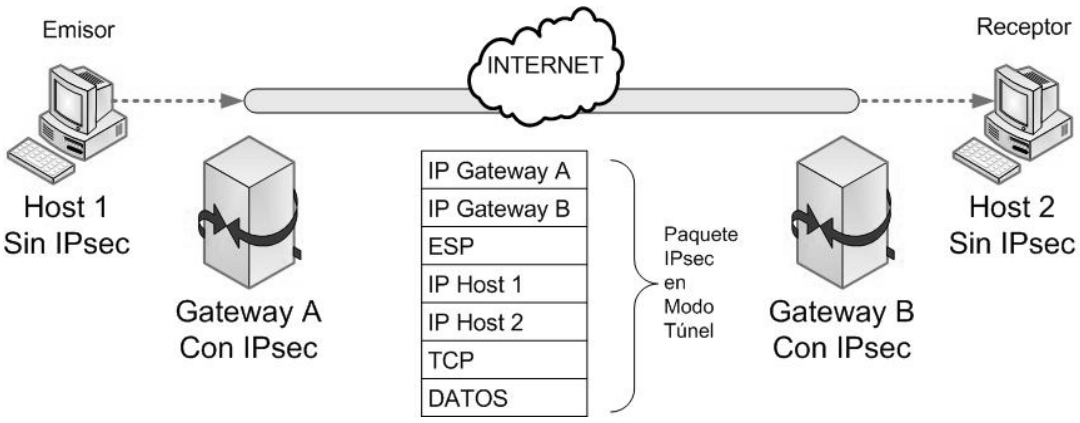


Figura 10.B.2: *Funcionamiento del modo Túnel*

En la ilustración de la figura 10.B.2 se puede ver que la comunicación se realiza a través de una red de datos pública entre un host que se encuentra en una LAN y otro que se encuentra en una red local remota es por eso que entre las pasarelas de seguridad o gateway se establece un túnel a través del cual viajan seguros los paquetes que se intercambian entre ambas redes sin embargo debemos hacer notar que tanto en el Host 1 y el Host 2 de la figura envían y reciben trafico como si estuvieran en la misma red.

El modo túnel también se ocupa para poder establecer Redes Privadas Virtuales (*VPN*) a través de redes públicas.

3) Asociaciones de seguridad

Una asociación de seguridad es una conexión unidireccional que ofrece servicios de seguridad al tráfico transportado por este, dicho servicio de seguridad es utilizado por el protocolo de seguridad de la Cabecera de Autenticación (AH) o bien por el de la Carga de seguridad encapsulada (ESP), pero no por ambos. Para que exista una comunicación bidireccional entre dos host o entre dos pasarelas de seguridad (gateway), se requieren dos asociaciones de seguridad (una en cada sentido).

Una asociación de seguridad se identifica por tres componentes:

a) Un índice de parámetros de seguridad (SPI): Es una cadena de bits asignada a la asociación de seguridad y que sirve como un puntero hacia la base de datos de esta.
b) Una dirección IP destino
c) *Un identificador de protocolo de seguridad:* Identifica que tipo de seguridad se usa en la asociación de seguridad y puede ser el subprotocolo AH o ESP

El conjunto de los servicios de seguridad ofrecidos por una asociación de seguridad depende del protocolo de seguridad seleccionado por lo que los servicios de seguridad principales ofrecidos por una asociación de seguridad son:

a) *Servicio de Autenticación:* Este servicio utiliza el protocolo de la Cabecera de Autenticación (AH).
b) *Servicio de Cifrado mas Autenticación:* Utiliza el protocolo de la carga de seguridad encapsulada.
c) *Una función de gestión de claves (IKE).*

4) Bases de datos de las asociaciones de seguridad.
Las asociaciones de seguridad de IPsec cuentan con dos bases de datos que son:

a) *Bases de datos de políticas de seguridad (SPD):* Que especifica las políticas que determinan el tratamiento de todo el trafico IP de un host o una pasarela de seguridad.
b) *Bases de datos de asociaciones de seguridad (SAD):* Contiene los parámetros que se asocian con cada grupo de seguridad activa.

C. LA CABECERA DE AUTENTICACION (AH).

El estudio completo de las generalidades de la Cabecera de Autenticación se encuentra publicado en el RFC 2402. Como se especificó anteriormente la cabecera de Autenticación proporciona los siguientes servicios de seguridad:

a) Servicio de integridad sin conexión
b) Autenticación del origen de datos para datagramas IP
c) Protección contra reenvíos (anti-replay)

Estos servicios se proporcionan a los datos de los protocolos de capas superiores.

El formato de la cabecera de Autenticación se ilustra en la figura 10.C.1:

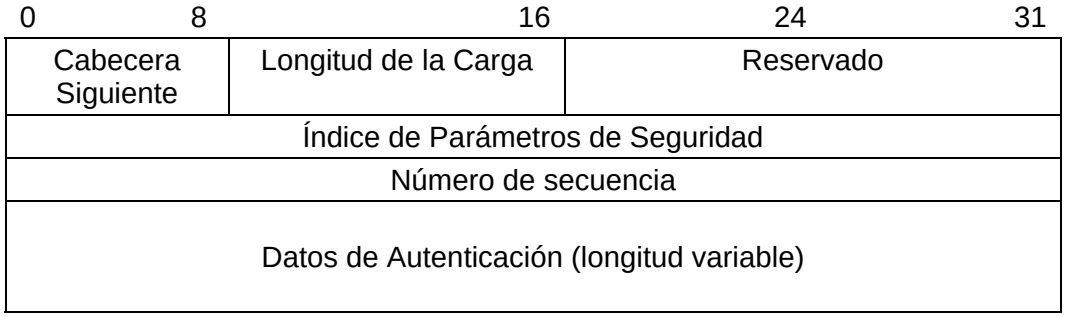


Figura 10.C.1: *Formato de la cabecera de autentificación (AH).*

Los campos de la cabecera de autentificación (AH) son los siguientes:

a) *Cabecera Siguiente (Next Header):* La cabecera siguiente es un campo de 8 bits que identifica la cabecera siguiente a la cabecera de autentificación.
f) *Longitud de la Carga (Payload Length):* Longitud de la cabecera AH.
g) *Reservado (Reserved):* Campo reservado para usos futuros.
h) *Índice de Parámetros de Seguridad (Index of parameters of security):* Este campo es un valor arbitrario de 32 bits, conjuntamente con la dirección IP destino y el subprotocolo de seguridad AH, identifican a la asociación de seguridad para el paquete.
i) *Número de Secuencia (Sequence Number):* El campo número de secuencia es un entero sin signo de 32 bits que contiene un valor creciente y único del contador de número de secuencia. Este campo es obligatorio y debe estar presente incluso si el receptor elige no habilitar el servicio de anti-reenvío (anti-replay) para una asociación específica. El procesamiento de este campo esta a criterio del receptor. Es decir, el emisor debe transmitir siempre este campo pero el receptor no necesita actuar sobre él. Este campo se inicializa a cero cuando se establece una asociación de seguridad.
j) *Datos de Autenticación (Authentification data):* Este campo es de longitud variable y contiene el valor de comprobación de integridad para el paquete (ICV), este campo debe contener un entero múltiplo de 64 bits de longitud. Por lo que incluye una opción de relleno para asegurar la longitud de la cabecera de autentificación.

D. PROCESAMIENTO DE LA CABECERA DE AUTENTICACIÓN (AH).

1) Localización de la cabecera de Autenticación

a) Localización de la AH en el Modo transporte.
En este modo la cabecera de autenticación se ve como carga de extremo a extremo, y debe aparecer después de las cabeceras de extensión: salto a salto, ruteo y fragmentación. Las cabeceras de opciones de destino podrán aparecer antes o después de la cabecera de autenticación. En la figura 10.D.1 se ilustra la localización de la cabecera de autenticación en el modo transporte.

a) Antes de emplear AH

Cabecera IP	Cabeceras extendidas (si están presentes)	TCP	DATOS

b) Después de emplear AH

Cabecera IP	Cabeceras extendidas (si están presentes)	AH	Opciones de Destino	TCP	DATOS

Figura 10.D.1: *Localización de la Cabecera de Autenticación en el modo transporte.*

b) Localización de la Ah en el modo túnel.
En este modo la cabecera de autenticación se emplea en host, pasarelas o gateway de seguridad. Para este modo la cabecera IP "interna" lleva la última dirección de origen y de destino, mientras que la cabecera IP "externa" puede contener distintas direcciones IP. En modo túnel, la cabecera de autenticación protege el paquete IP interno completamente, incluyendo la cabecera IP interna. En la figura 10.D.2 se ilustra la localización de la cabecera de autenticación en el modo túnel.

Nueva Cabecera IP	Cabeceras extendidas (si están presentes)	AH	Cabecera IP Original	Cabeceras extendidas	TCP	DATOS

Figura 10.D.2: *Localización de la cabecera de autenticación en el modo túnel.*

2) Algoritmo de Autentificación
El algoritmo de autenticación es utilizado para el cálculo del valor de comprobación de integridad (ICV) que se especifica en la Asociación de Seguridad. Para las comunicaciones extremo a extremo entre dos nodos que utilicen IPsec los algoritmos de autenticación aptos incluyen los siguientes componentes:

i. Claves con códigos de autenticación de mensajes (MACs).
ii. Algoritmos de encriptación simétricos o *funciones hash*[21] unidireccionales

Una implementación AH debe soportar obligatoriamente los siguientes algoritmos:

i. HMAC con MD5
ii. HMAC con SHA-1

[21] Funciones Hash: Es un método para resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Una hash o búsqueda es el resultado de dicha función o algoritmo.

El algoritmo de autenticación debe especificar las siguientes opciones:

i. La longitud del valor de comprobación de integridad (ICV)
ii. Las reglas de comparación
iii. Los pasos de procesamiento para la validación.

3) Procesamiento de paquetes salientes

a) Cálculo del valor de comprobación de integridad (ICV)
Los campos de la cabecera IPv6 se clasifican de la siguiente forma:

Campos Inmutables (Campos que no son modificados durante la transmisión):

i. Versión
ii. Longitud de la carga
iii. Cabecera siguiente (tiene el valor de 51)
iv. Dirección de origen
v. Dirección de destino (sin la cabecera de extensión de ruteo)

Campos mutables pero predecibles (Campos que son modificados durante el tránsito pero su valor en el receptor es predecible)

i. Dirección de destino (con la cabecera de extensión de ruteo)

Campos mutables (Campos que se modifican durante el tránsito y que sus valores se fijan a cero para el cálculo del ICV)

i. Clase
ii. Etiqueta de flujo
iii. Límite de saltos

Las cabeceras de extensión que contienen opciones (Salto a Salto y Opciones de destino) contienen un bit que indica que la opción puede o no cambiar de forma impredecible durante el tránsito. Si el bit indica que los campos son inmutables los campos se incluyen en el cálculo del valor de comprobación de integridad (ICV).

b) Relleno de los datos de autenticación.
El campo Datos de autenticación de la cabecera de autentificación incluye el relleno para asegurarse que la longitud de la cabecera de autentificación tenga un múltiplo de 64 bits. El tamaño del relleno de los datos de autentificación depende de la longitud del valor de comprobación de integridad (ICV) que determina el algoritmo de autenticación. El contenido del campo de relleno es seleccionado arbitrariamente por el nodo emisor

c) Fragmentación
Se tienen dos casos para aplicar la fragmentación a un paquete IP que este siendo procesado con IPsec. Y son los siguientes:

a) *Fragmentación en el modo transporte:* Esta fragmentación se realiza después de que es procesada la cabecera de autenticación puesto que esta es aplicada solamente al paquete IP completo no a los fragmentos. Un paquete IP al cual se le aplica la cabecera de autentificación se puede fragmentar en los routers de la ruta, y se debe reensamblar antes de la cabecera de autenticación sea procesada en el nodo receptor.
b) *Fragmentación del modo túnel:* La cabecera de autenticación se aplica a un paquete IP, el cual la carga puede ser un paquete IP fragmentado.

4) Procesamiento de paquetes entrantes

a) Reensamblaje
Si se requiere reensamblar un paquete IP se debe realizar antes de procesar la cabecera de autenticación por lo tanto cualquier paquete que se haya reensamblado y tenga en su cabecera extendida de fragmentación el campo de desplazamiento (offset) con un valor diferente a cero o el campo para la bandera de más fragmentos tenga un valor de 1 el nodo receptor debe desechar el paquete.

b) Buscar la asociación de seguridad
Cuando se recibe un paquete que contiene una cabecera de autentificación, el receptor determina la Asociación de seguridad unidireccional basándose en la dirección IP destino, el protocolo de seguridad AH.

Si no existe ninguna Asociación de seguridad para la sesión (el receptor no tiene la clave), el receptor debe desechar el paquete.

c) Verificación del valor de comprobación de integridad (ICV)
El nodo receptor calcula el ICV sobre los campos apropiados del paquete, usando el algoritmo de autenticación especificado, y verifica que sea el mismo que el ICV incluido en el campo Datos de autenticación de la cabecera de autenticación del paquete.

Si el ICV calculado y el ICV recibido coinciden, el paquete es valido y es aceptado. Si el control falla, el receptor debe descartar el paquete recibido.

En la figura 10.D.3 se ilustra todo el procesamiento de la cabecera de autenticación.

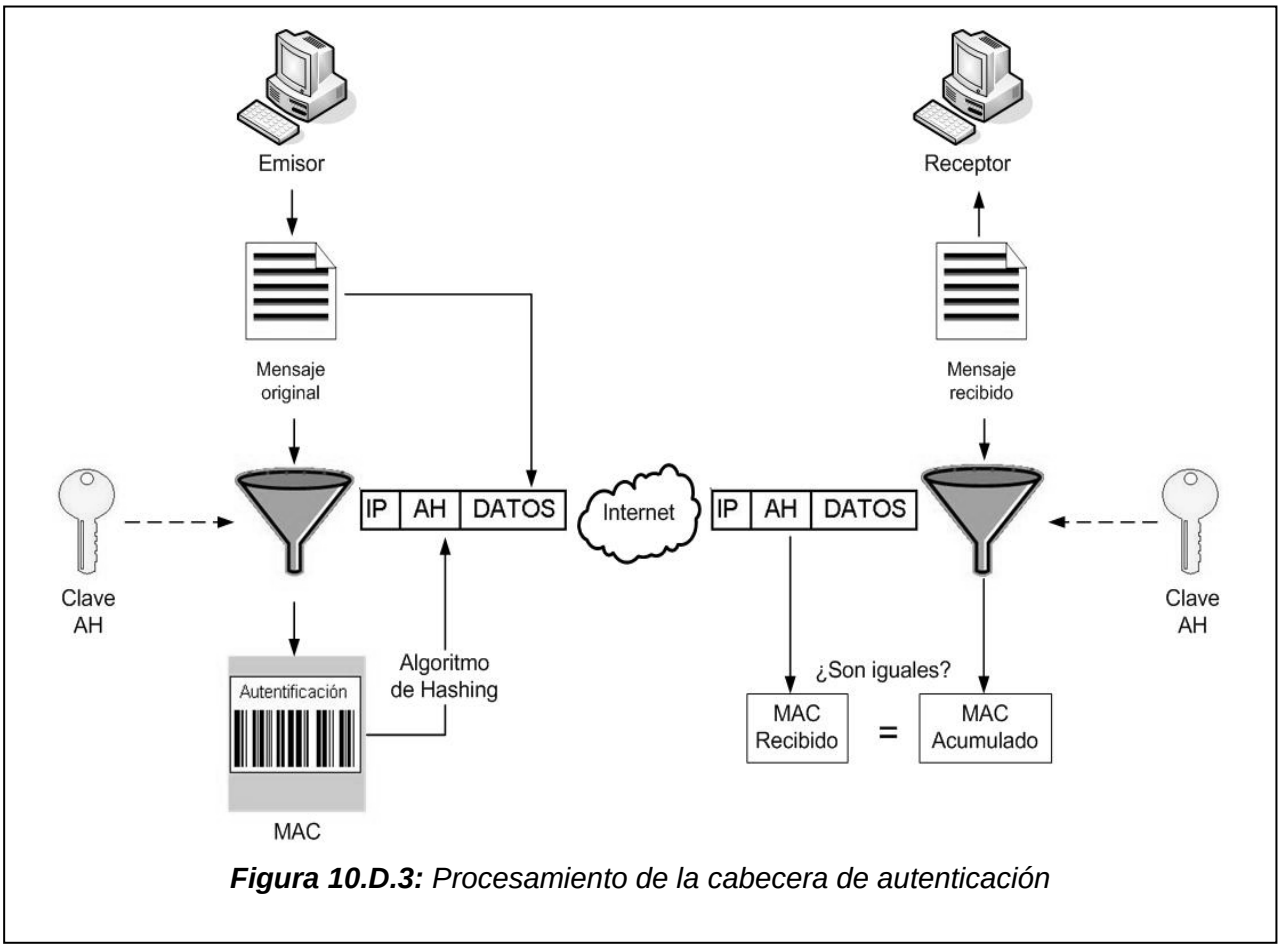


Figura 10.D.3: *Procesamiento de la cabecera de autenticación*

E. LA CABECERA DE LA CARGA DE SEGURIDAD ENCAPSULADA (ESP).

El estudio completo de las generalidades de la Cabecera de la carga de seguridad encapsulada se encuentra publicado en el estándar de Internet RFC 2406. La Cabecera de carga de seguridad encapsulada esta diseñada para proporcionar un conjunto de servicios de seguridad al nuevo protocolo de Internet IPv6, entre estos servicios podemos mencionar los siguientes:

a) Confidencialidad.
b) Autenticación del origen de los datos.
c) Integridad sin conexión.
d) Servicio de anti-reenvío (anti-replay)
e) Confidencialidad limitada al flujo de tráfico (Este servicio requiere de la selección del modo túnel y su efectividad depende de la pasarela o gateway de seguridad).

Todos estos servicios de seguridad se establecen en la asociación de seguridad (SA), otro aspecto importante de resaltar es que esta cabecera puede aplicarse también en combinación con la Cabecera de autenticación.

El formato de la cabecera de la carga de seguridad encapsulada se ilustra en la figura 10.E.1.

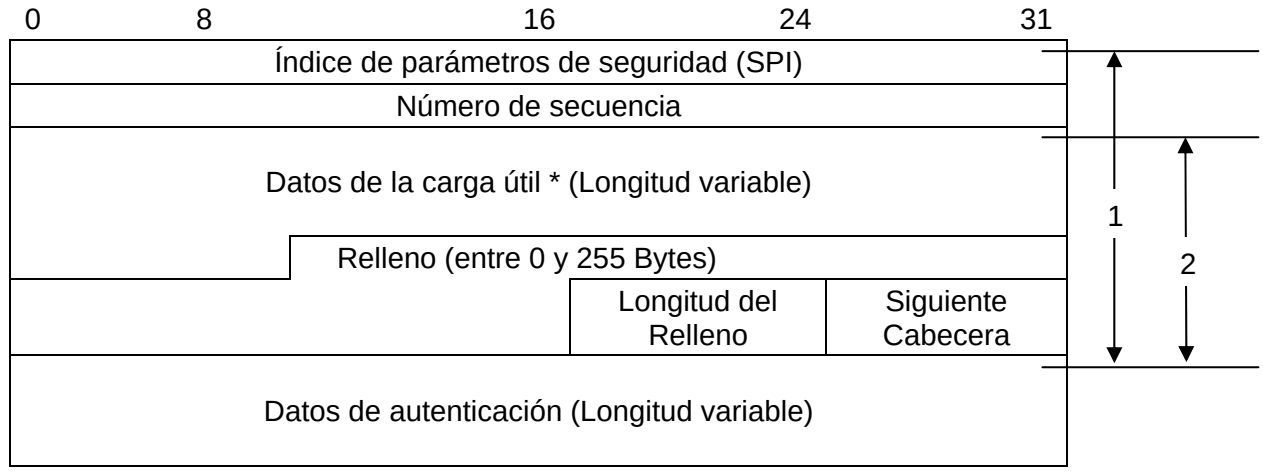


Figura 10.E.1*: Formato de la cabecera de la carga de seguridad encapsulada.*

1: Alcance de la autenticación
2: Alcance de la confidencialidad
*: Si se incluye en el campo Datos de la carga útil, los datos de sincronización criptográficos; por ejemplo un vector de inicialización.

Los campos de la cabecera de la carga de seguridad encapsulada son:

g) *Índice de parámetros de seguridad (Index of parameters of security):* Es un valor arbitrario de 32 bits que conjuntamente con la dirección destino IP y el protocolo de seguridad ESP identifica una asociación de seguridad (SA).
h) *Número de secuencia (Sequence Number):* Campo obligatorio de 32 bits sin signo que contiene un valor creciente y único del contador.
i) *Datos de la carga útil (Payload Data):* Es un campo obligatorio de longitud variable. Cuando el algoritmo usado para encriptar a la carga útil requiere de los datos de sincronización criptográficos. Estos datos se pueden llevar en este campo.
j) *Relleno (Padding):* Entre los factores que requieren o motivan el uso del campo relleno tenemos los siguientes:

i. Si se emplea un algoritmo de encriptación que requiere que el texto plano (El texto plano consta de los datos de la carga útil, la longitud del relleno y la siguiente cabecera) sea un múltiplo de cierto número de bytes. Se usa el relleno para completar los bytes que hagan falta.
ii. Si se requiere alinear correctamente los campos longitud de relleno y siguiente cabecera en una palabra de 4 bytes según lo ilustrado en la figura del formato de la cabecera ESP.
iii. Se puede utilizar para disfrazar la longitud real de la carga, en respaldo a la confidencialidad del flujo de tráfico. Sin embargo su uso debe hacerse con cautela para no tener implicaciones adversas en el ancho de banda.

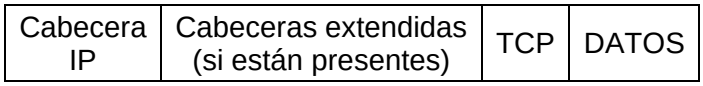
k) *Longitud del relleno (Pad Length):* Se indica el número de bytes de relleno que preceden a este campo, el rango de valores validos es de 0 a 255 bytes
l) *Siguiente cabecera (Next Header):* Identifica el tipo de datos contenidos en el campo datos de la carga útil que puede ser una cabecera de extensión IPv6 o un identificador de protocolo de capa superior
m) *Datos de autenticación (Authentication Data):* Este campo es de longitud variable y contiene el valor de comprobación de integridad (ICV). La longitud del campo es especificada en función de la autenticación seleccionada. Este campo es opcional y se incluye solamente si el servicio de autenticación se ha seleccionado para la asociación de seguridad (SA)

F. PROCESAMIENTO DE LA CABECERA DE LA CARGA DE SEGURIDAD ENCAPSULADA (ESP).

1) Localización de la cabecera de la carga de seguridad encapsulada (ESP)
Como la cabecera AH, la cabecera ESP puede ser empleado tanto en el modo transporte como en el modo túnel.

a) Localización de la cabecera ESP en el modo transporte.
En este modo la cabecera ESP se inserta después de la cabecera IP básica y antes del protocolo de capa superior. La cabecera ESP se ve como una carga útil extremo a extremo y por esta razón debe aparecer después de las cabeceras de extensión: salto a salto, ruteo, y fragmentación. Las cabeceras de opciones de destino podrán aparecer antes o después de la cabecera de Autenticación; sin embargo como la cabecera de seguridad encapsulada protege únicamente los campos que están después de ella generalmente es preferible colocar la cabecera de opciones de destino después de ella. En la figura 10.F.1 se ilustra la localización de la cabecera de la carga de seguridad encapsulada en el modo transporte.

a) Antes de emplear AH



b) Después de emplear AH

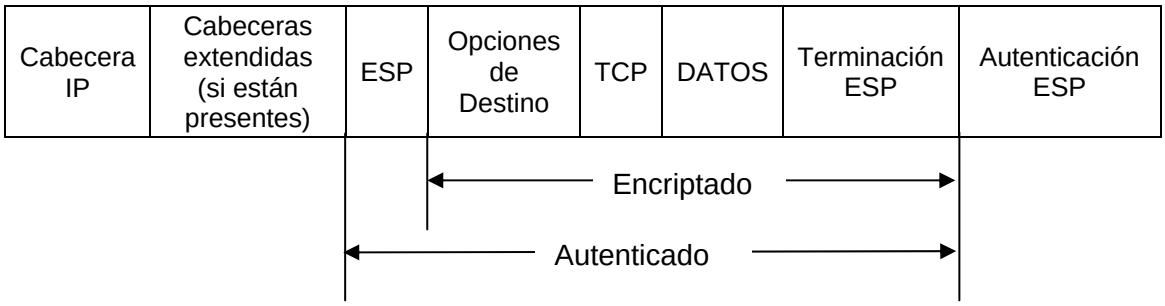


Figura 10.F.1: *Localización de la Cabecera de la carga de seguridad encapsulada en el modo transporte.*

b) Localización de la cabecera de ESP en el modo túnel.
En este modo la cabecera de la carga de seguridad encapsulada se emplea en hosts o en pasarelas o gateway de seguridad. En este modo la cabecera IP "interna" lleva la última dirección de origen y de destino, mientras que la cabecera IP "externa" puede contener distintas direcciones IP. En el modo túnel la cabecera ESP protege a todo el paquete, en figura 10.F.2 se ilustra la localización de la carga de seguridad encapsulada en el modo túnel.

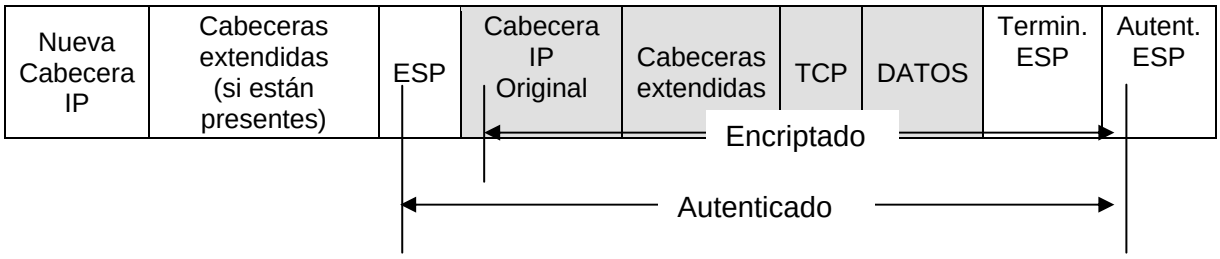


Figura 10.F.2: *Localización de la Cabecera de la carga de seguridad encapsulada en el modo túnel.*

2) Algoritmos
Los algoritmos que se deben implementar obligatoriamente en la transmisión de paquetes que utilizan la cabecera de seguridad ESP en cualquiera de los modos en los que se utiliza IPsec son:

a) *DES en modo CBC*
b) *HMAC con MD5*
c) *HMAC con SHA-1*
d) *Algoritmo de Encriptación:* Es empleado por la asociación de seguridad (SA). La cabecera ESP esta diseñada para usarse con algoritmos de encriptación simétricos. Debido a que los paquetes pueden llegar en desorden, cada paquete debe llevar algún dato que permita que el receptor establezca la sincronización criptográfica para la desencriptación.

e) *Algoritmo de Autenticación:* Es empleado para el cálculo del valor de comprobación de integridad (ICV) que esta especificado por la asociación de seguridad (SA), los algoritmos de autenticación incluyen los siguientes aspectos.
    i. Código de autenticación del mensaje (MAC)
    ii. Funciones hash unidireccionales (por ejemplo MD5 o SHA-1)

3) Procesamiento del paquete saliente

a) *Procesamiento de paquetes salientes para el modo transporte.*
En este modo el emisor encapsula la información del protocolo de capa superior en la cabecera ESP, y mantiene la cabecera IP básica y las cabeceras de extensión.

b) *Procesamiento de paquetes salientes para el modo túnel.*
En este modo las cabeceras IP básica y las cabeceras extendidas se construyen durante el proceso de encapsulación.

c) *Buscando la asociación de seguridad (SA).*
La cabecera de la carga de seguridad encapsulada se aplica solamente a un paquete saliente siempre que una implementación del protocolo de seguridad IPsec determine que el paquete esta asociado con una SA que requiera el procesamiento de la cabecera ESP

d) *Encriptación del paquete.*
Los pasos que realiza el nodo emisor son los siguientes:
    i. Encapsular dentro del campo Carga útil ESP
        - Para el modo transporte solo la información del protocolo de la capa superior.
        - Para el modo túnel el paquete IP completo.
    ii. Agregar el relleno si es necesario
    iii. Usando la clave, el algoritmo de encriptación de la asociación de seguridad y los datos de sincronización criptográficos se deben encriptar en los campos Datos de la carga útil, Relleno, Longitud del relleno, Siguiente cabecera.
    iv. Como se puede apreciar en la figura 10.F.1 y 10.F.2 los datos de autenticación ESP no están protegidos por la encriptación por lo que es necesario que un algoritmo de autenticación de claves sea empleado para calcular el valor de comprobación de integridad (ICV).

e) *Generación del número de secuencia.*
El contador del nodo emisor es inicializado a cero (0) al momento de establecer una asociación de seguridad (SA). Luego el emisor incrementa el valor del campo número de secuencia para que el primer paquete enviado usando una asociación de seguridad especifica tenga el valor del número de secuencia de 1.
Si se habilita el anti-replay (por defecto), el emisor establece un control para asegurarse que el contador no ha completado un ciclo antes de insertar el nuevo valor en el campo Número de Secuencia para evitar un desbordamiento del número de secuencia.

f) *Cálculo del ICV.*
El cálculo del valor de comprobación de integridad (ICV) de paquetes IP en donde se implementa la cabecera ESP es el mismo que el descrito en la cabecera de autenticación AH de la sección 10.D.3.a.

g) *Proceso de fragmentación.*
El proceso de fragmentación de paquetes IP en donde se implementa la cabecera ESP es el mismo que el descrito en la cabecera de autenticación AH de la sección 10.D.3.c.

4) Procesamiento del paquete entrante.

a) *Reensamblaje.*
El reensamblaje de la recepción de paquetes IP en donde se implementa la cabecera ESP es el mismo que el descrito en la cabecera de autenticación AH de la sección 10.D.4.a.

b) V*erificación del número de secuencia.*
La verificación del número de la recepción de paquetes IP en donde se implementa la cabecera ESP es el mismo que el descrito en la cabecera de autenticación AH de la sección 10.D.4.b .

c) Cálculo del ICV.
El cálculo del valor de comprobación de integridad (ICV) de la recepción de paquetes IP en donde se implementa la cabecera ESP es el mismo que el descrito en la cabecera de autenticación AH de la sección 10.D.4.c.

b) *Desencriptación del paquete.*
Los pasos que realiza el nodo receptor para desencriptar el paquete IP son los siguientes:

i. Usar la clave del algoritmo de encriptación indicado por la asociación de seguridad (SA) para desencriptar los datos de los campos carga útil de la cabecera ESP, Relleno, Longitud de relleno y Siguiente cabecera.
ii. Procesar cualquier relleno según las especificaciones del algoritmo de encriptación.
iii. Reconstruir el datagrama IP original.
    - Para el modo transporte: La cabecera IP original más la información del protocolo original de la capa superior dentro del campo carga útil ESP.
    - Para el modo túnel: La cabecera IP del túnel más el datagrama IP entero dentro del campo Carga útil de ESP.

En la figura 10.F.3 se ilustra todo el procesamiento de la cabecera de la carga de seguridad encapsulada.

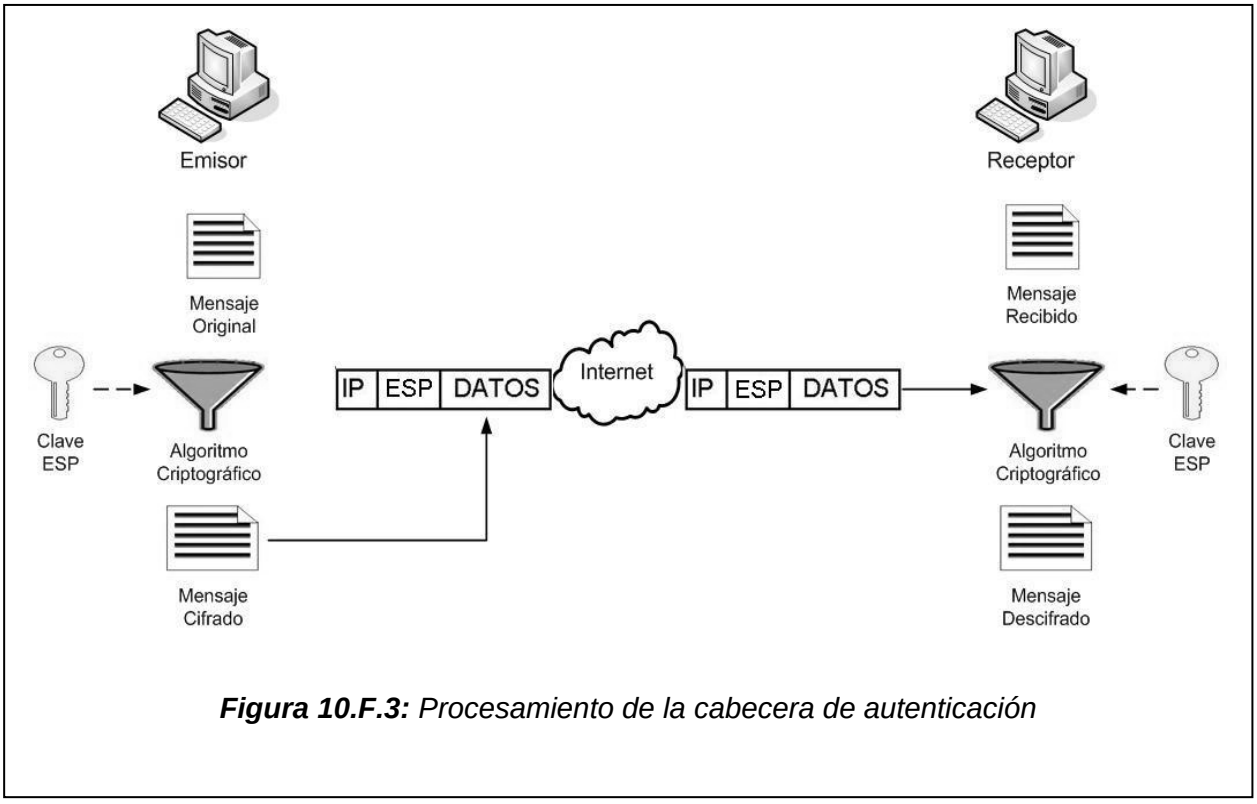


Figura 10.F.3: *Procesamiento de la cabecera de autenticación*

G. GESTIÓN DE CLAVES

El protocolo IKE (Internet Key Exchange) es el estándar por defecto para la gestión automática de claves para el protocolo de seguridad IPsec, así como el establecimiento de asociaciones de seguridad.

El objetivo principal del protocolo de gestión de claves IKE es establecer una conexión cifrada y autenticada entre dos nodos de un sistema de red para que se puedan negociar los parámetros necesarios para establecer una asociación de seguridad IPsec, dicha negociación se lleva a cabo en dos fases que son:

a) Fase 1. Fase común a cualquier aplicación: En esta fase se establece un canal seguro y autenticado mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene de un algoritmo de intercambio de claves Diffie-Hellman. Este método no garantiza la identidad de los nodos, para ello es necesario realizar un método adicional de autenticación, dos de los métodos de autenticación más usados son los siguientes:
   i. Autenticación basada en el conocimiento compartido de una cadena de caracteres que únicamente conocen los extremos que quieren establecer una comunicación IPsec. Mediante el uso de funciones hash cada extremo obtiene el valor de la cadena de caracteres sin revelarlo.
   ii. Autenticación basada en el uso de certificados digitales X509v3, el uso de estos certificados permite distribuir de forma segura una clave publica a cada nodo, de modo que estos nodos puedan demostrar su identidad mediante la posesión de una clave privada y ciertas opciones de criptografía publica.

b) Fase 2. Canal seguro IKE: Es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado.

El funcionamiento del protocolo IKE se ilustra en la figura 10.G.1.

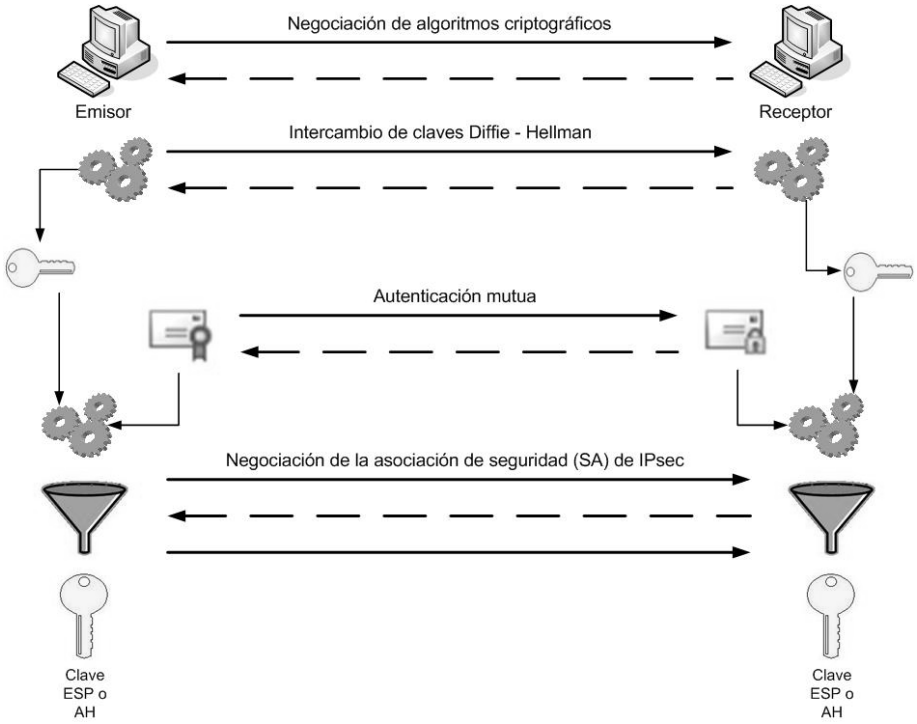


Figura 10.G.1: *Funcionamiento del protocolo de gestión de claves de Internet (IKE)*

H. APLICACIONES DE IPsec

Una de las principales aplicaciones del protocolo IPsec es el procedimiento de autenticación (fase 1) que permite al protocolo de descubrimiento de vecindario (ND) poder asegurar intercambios seguros entre los distintos routers, evitando la intercepción de los paquetes del tráfico.

Actualmente para la implementación de seguridad de Internet se emplean los *cortafuegos* o *firewalls* que son maquinas intermedias que mediante un sencillo conjunto de reglas no permiten el acceso directo de los host de una Intranet a Internet con el objetivo de filtrar todo el trafico que se da entre estos sistemas de red.

El protocolo de seguridad IPsec propone una nueva configuración que consisten en realizar un túnel virtual seguro de forma que dos cortafuegos o firewalls estén virtualmente conectados a través de Internet de una forma transparente para los usuarios. De esta forma el intercambio e información que se es regulado por la comunicación entre los dos firewalls mediante datagramas IPv6 sean encapsulados en datagramas IP autenticados y cifrados. Esta configuración es conocida como Red Privada Virtual (VPN). La ilustración de la configuración VPN en el tráfico entre dos cortafuegos o firewall se muestra en la figura 10.H.1.

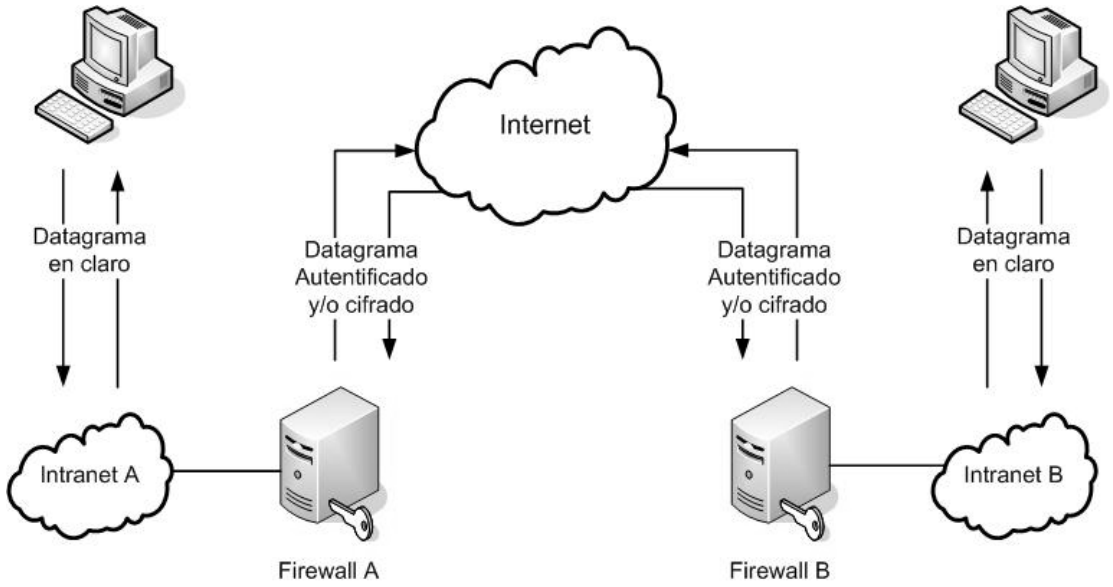


Figura 10.H.1: *Configuración VPN entre dos cortafuegos de las redes A y B*

11. PROTOCOLOS DE TRANSPORTE

A. INTRODUCCIÓN

Los protocolos de transporte no han cambiado desde IPv4 hacia IPv6, sin embargo, la suma de verificación (*checksum*) en la cabecera de transporte ahora es obligatoria. Aunque IPv6 es un nuevo diseño de la capa de red, un requerimiento de este diseño es la reutilización de los protocolos de la capa de transporte. Los protocolos de transporte existentes son:

a) Protocolo de Control de Transmisión de Flujo (SCTP).
b) Protocolo de Control de Transmisión (TCP).
c) Protocolo de Datagramas de Usuario (UDP).

Como se explicó en el capitulo 1, el protocolo IP es el encargado de enviar paquetes individuales por la red hacia un nodo destino, y el protocolo de control de transmisión (TCP) es el que se encarga de prever una regulación del flujo de los paquetes enviados, asegurando que lleguen a su destino de una forma correcta y ordenada. Para aquellas aplicaciones que no requieran un control tan estricto se ha desarrollado el protocolo de datagramas de usuario (UDP) que al igual que el TCP, utiliza los servicios del protocolo IP, pero sin dar confiabilidad. SCTP es una nueva alternativa que tiene ventajas sobre TCP.

B. PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

El protocolo TCP no ha sufrido cambios en IPv6, sin embargo paralelo al trabajo que se realiza en IPv6, el protocolo TCP ha sido objeto de numerosos estudios y también ha evolucionado, presentando actualmente las siguientes mejoras:

a) Opciones de notificación de recepción selectiva en TCP (SACK) [RFC2018]
b) Notificación de Congestión Explicita (ECN) [RFC 3168]

El estudio completo del protocolo TCP se encuentra publicado en el estándar de Internet RFC793.

El protocolo de control de transmisión (TCP) esta diseñado para ser un protocolo de host a host y proporcionar un servicio de entrega confiable y ordenada al destino.

1) Funciones del protocolo TCP

Basándose en las diferentes capas del modelo TCP/IP, se puede afirmar que los protocolos asociados a la capa de aplicación necesitan que la comunicación entre equipos distantes sea confiable, y dado que la capa IP aporta un servicio de entrega de paquetes no confiables (sin confirmación), el protocolo de transporte TCP añade las siguientes funciones para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe:

a) Comunicación libre de errores.
b) Ordenar los paquetes recibidos.
c) Evitar la pérdida de paquetes.
d) Evitar la duplicación de los paquetes.

2) Servicio de entrega confiable en el protocolo TCP

El servicio de entrega de flujo confiable garantiza que la entrega de los datos de un nodo a otro se de sin pérdida o duplicación. Para realizar este servicio el protocolo TCP utiliza una técnica conocida como *Acuse de Recibo (ACK)*. Esta técnica requiere que un host receptor se comunique con el origen y le envíe un mensaje ACK conforme reciba los datos. El nodo transmisor guarda un registro de cada paquete que envía y espera un ACK antes de enviar el siguiente paquete.

Cuando se pierde o corrompe un paquete el nodo transmisor arranca un temporizador después de enviar el paquete. Cuando termina el tiempo el nodo transmisor asume que el paquete se ha

perdido y lo vuelve a enviar. Aunque esta acción podría causar la duplicación de algún paquete, el protocolo TCP detecta esta duplicación debido a que asigna a cada paquete un número de secuencia y obliga al nodo receptor a recordar que número de secuencia recibe.

Los protocolos de acuse de recibo (ACK) envían los números de secuencia dentro de los acuses de recibo, para que el receptor pueda asociar correctamente los ACK con los paquetes.

En la figura 11.B.1 se ilustra como el protocolo TCP se vale de reconocimientos o mensajes de *acuse de recibo* positivo (ACK).

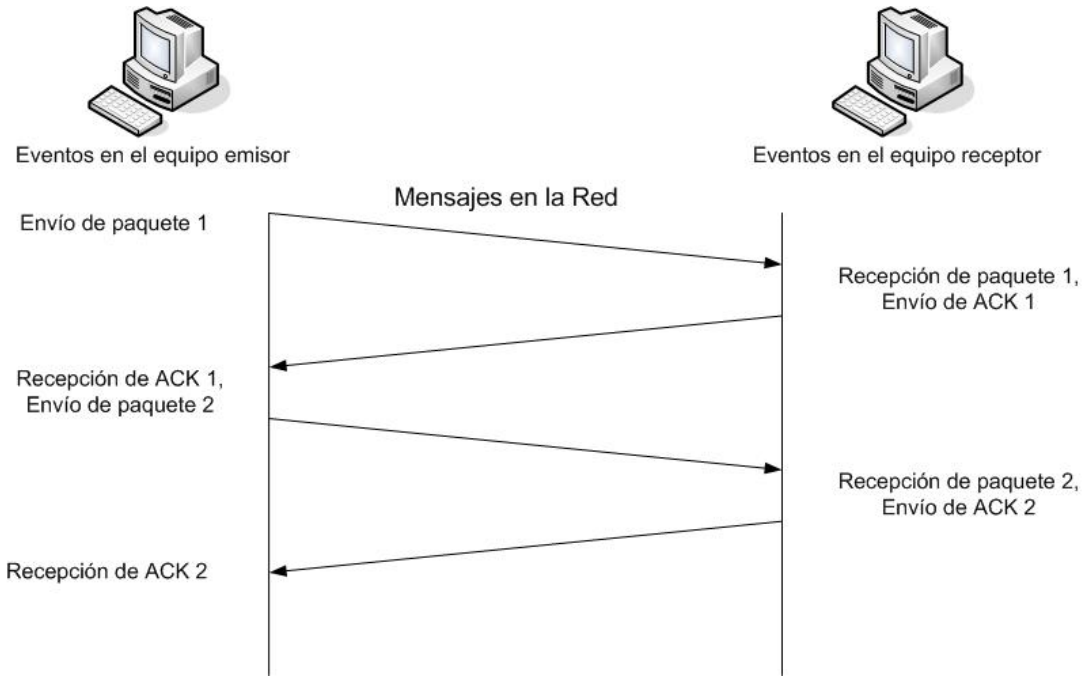


Figura 11.B.1: *Un protocolo que se vale de reconocimiento o acuses de recibo positivos, con retransmisión, en la cual el emisor espera un acuse de recibo para cada paquete enviado. La distancia vertical bajo cada equipo representa el incremento en el tiempo y las líneas que cruzan la diagonal representan la transmisión de paquetes de red.*

3) Las ventanas deslizantes

Al analizar la figura 11.B.1 podemos observar que el protocolo que utiliza los mensajes de *acuse de recibo* usa una buena cantidad de su ancho de banda disponible, puesto que la red estará inactiva debido a que se retrasará el envío de un nuevo paquete hasta que se reciba un *acuse de recibo* (ACK) del paquete anterior. Para dar solución a este problema se emplea en la comunicación entre dos equipos el uso de la técnica llamada *Ventana Deslizante* que permite al equipo transmisor enviar varios paquetes sin esperar un *acuse de recibo*. El protocolo TCP opera con *ventanas deslizantes* a nivel de octetos, enumerando dichos octetos del flujo de datos de manera secuencial, y el transmisor guarda tres apuntadores asociados con cada conexión utilizando dos de ellos para delimitar las fronteras de la ventana deslizantes del protocolo. El otro apuntador se utiliza para definir el octeto más alto en la secuencia que se puede enviar antes de recibir más *acuses de recibo*.

Los punteros que delimitan las fronteras de la ventana deslizante dividen la secuencia de los octetos del flujo en tres partes:

a) Paquetes a la izquierda de la ventana fueron transmitidos, se recibieron y acusaron exitosamente.

b) Paquetes dentro de la ventana están en proceso de transmisión.
c) Paquetes a la derecha de la ventana no se han transmitido.

El equipo receptor debe tener una ventana similar para ensamblar de nuevo el flujo, debido a que las conexiones TCP son de tipo *Full duplex* (el flujo TCP/IP permite la transferencia concurrente en ambas direcciones), se llevan a cabo dos transferencias al mismo tiempo en cada conexión.

Es importante recalcar que el protocolo TCP permite que el tamaño de la ventana varíe esto con el fin de poder eliminar el tiempo ocioso de la red.

4) Especificaciones del Protocolo de Control de Transmisión (TCP)

El protocolo TCP permite que varios programas de aplicación en un host se comuniquen de manera concurrente y realiza el ordenamiento de los paquetes del trafico TCP entrante entre los programas de aplicación. El protocolo TCP utiliza los números de *Puertos de Protocolo* para identificar el destino final dentro de un host. Cada puerto de protocolo tiene asignado un número entero pequeño utilizado para identificarlo.

El protocolo TCP utiliza la conexión de los puntos extremos para asegurar la comunicación entre dos equipos. Un punto extremo es la combinación de la dirección IP del anfitrión y el puerto del protocolo, es decir que en el mismo host se puede compartir un número de puerto puesto que el TCP utiliza la conexión de los puntos extremos.

Debido a que el protocolo TCP esta orientado a la conexión este requiere que en ambos puntos los programas de aplicación deben estar de acuerdo en participar en dicha conexión. Para hacer esto, el programa de aplicación en un extremo realiza una función de *Apertura pasiva* en la cual solicita al sistema operativo que acepte una conexión entrante y que le asigne un número de puerto TCP a su extremo de la conexión. El programa de aplicación en el otro extremo realiza la operación de *Apertura activa* para establecer una conexión y que los programas de aplicación puedan comenzar a transferir datos.
La estructura de un segmento TCP se ilustra en la figura 11.B.2.

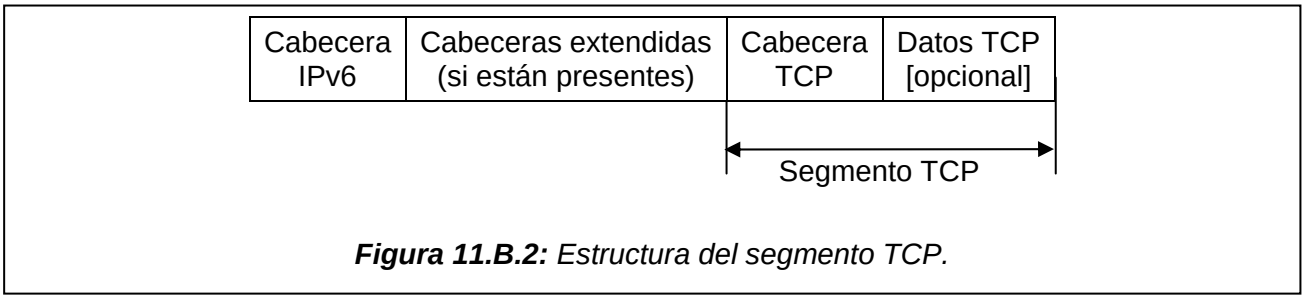


Figura 11.B.2: *Estructura del segmento TCP.*

El formato de la cabecera TCP se muestra en la figura 11.B.3.

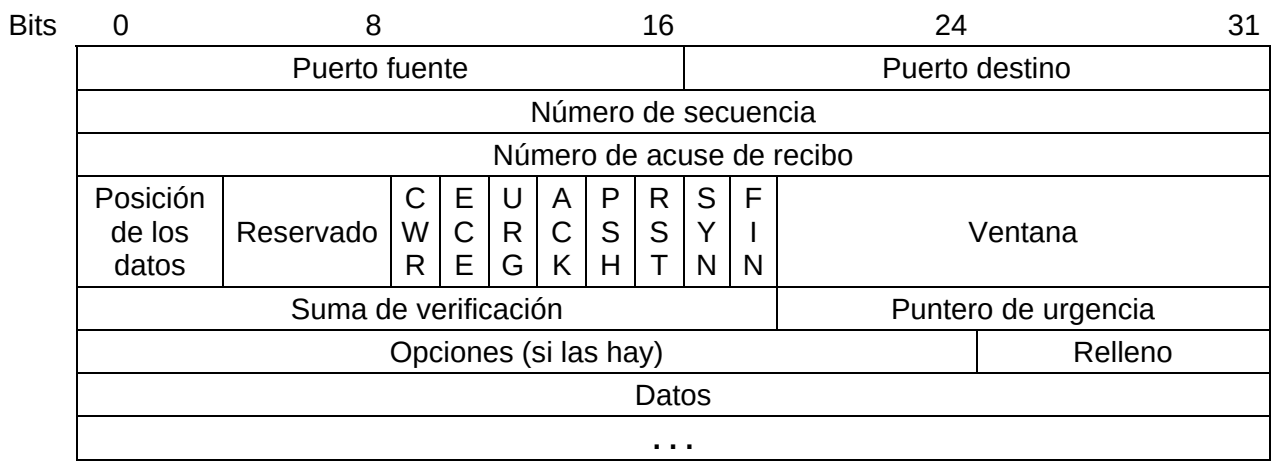


Figura 11.B.3: *Formato de la cabecera TCP.*

Los campos de la cabecera del protocolo TCP son los siguientes:

a) *Puerto de origen (Source Port):* Campo de 16 bits que especifica el número del puerto de origen.

b) *Puerto destino (Destination Port):* Campo de 16 bits que especifica el número del puerto de destino.

c) *Número de secuencia (Sequence Number):* Campo de 32 bits que indica el número de secuencia del primer octeto de datos del segmento (excepto cuando el indicador SYN esté puesto a uno). Si SYN está puesto a uno es el número de secuencia original y, entonces, el primer octeto de datos es ISN+1.

d) *Número de acuse de recibo (Acknowledgment Number):* Campo de 32 bits. Si el bit de control ACK está a puesto a uno, este campo contiene el valor del siguiente número de secuencia que el emisor del segmento espera recibir. Una vez que una conexión queda establecida, este número se envía siempre.

e) *Posición de los datos (Data Offset):* Campo de 4 bits. El número de palabras de 32 bits que utiliza la cabecera TCP. Este número indica dónde comienzan los datos.

f) *Reservado (Reserved):* Campo de 6 bits que esta reservado para usos futuros.

g) *Bits de control:* Campo se 6 bits que contienen las banderas encargadas de especificar los diferentes estados de la comunicación. Así mismo, también validan los valores de los distintos campos de la cabecera de control. Pueden haber simultáneamente varios bits de control activados. Las banderas de control son las siguientes.

   i. URG: Valida el campo “Puntero urgente”
   ii. ACK: Valida el campo “Número de acuse de recibo”.
   iii. PSH: Función de entregar datos inmediatamente”
   iv. RST: Reiniciar la conexión
   v. SYN: Sincronizar los números de secuencia.
   vi. FIN: Últimos datos del emisor

h) *Ventana:* Campo de 16 bits que indica el número de octetos de datos, a contar a partir del número indicado en el campo “Número de acuse de recibo”, que el emisor de este segmento está dispuesto a aceptar.

i) *Suma de de verificación (Checksum)*: Se procede como se indica en el apartado *4.B.2.c.*

j) *Puntero de urgencia (Urgent Pointer)*: Campo de 16 bits que indica el valor actual del puntero urgente, el puntero urgente apunta al número de secuencia del octeto al que seguirán los datos urgentes. Este campo es interpretado únicamente si el bit de control URG está establecido a uno.

k) *Opciones (Options):* Campo de longitud variable pero siempre de una longitud múltiplo de 8 bits que nos permiten especificar de forma opcional características extras a la comunicación. Un ejemplo de las opciones es el MSS (Maximum Segment Size), que especifica el tamaño máximo de datos que el emisor desea recibir. Esta opción se indica al inicio de la comunicación (flag SYN activado).

l) *Relleno (Padding):* Campo de longitud variable y se utiliza para asegurar que la cabecera TCP finaliza, y que los datos comienzan, en una posición múltiplo de 32 bits. El relleno está compuesto por ceros.

5) Establecimiento de una conexión TCP.

Para establecer una conexión el protocolo TCP utiliza una operación de saludo *Handshake* de tres etapas que son las siguientes:

a) *Etapa 1:* El equipo emisor selecciona un número aleatorio de secuencia (X). a continuación activa la bandera de control SYN.

b) *Etapa 2:* El equipo receptor recibe la petición y almacena el número de secuencia (X). elige un número aleatorio (Y) que utilizara como número de secuencia, a continuación activa las banderas de control SYN y ACK, finalmente envía un segmento con el número de secuencia elegido y con una confirmación del valor recibido más uno (ACK + 1).

c) *Etapa 3:* El equipo emisor almacena el número de secuencia (Y). activa la bandera de control ACK. Y finalmente envía una confirmación del número recibido más uno (ACK + 1).

En la figura 11.B.4 se ilustran las tres etapas para establecer una conexión.

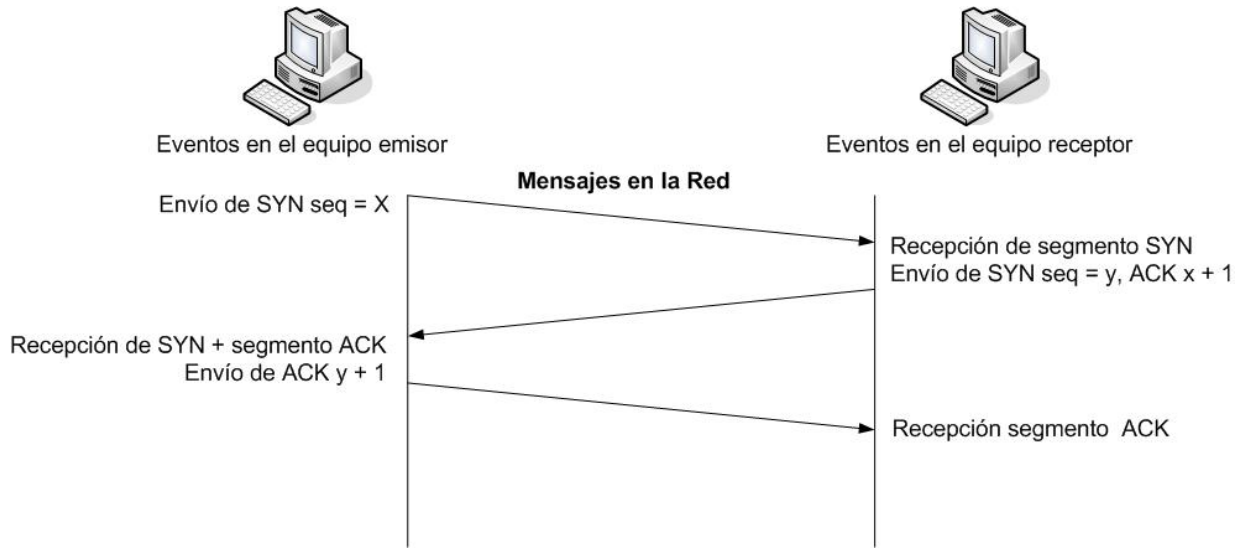


Figura 11.B.4: *Etapas para el establecimiento de conexión TCP*

6) Terminación de una conexión TCP.

Dos programas que utilizan el protocolo TCP pueden terminar la comunicación valiéndose de la operación *Close* para terminar la conexión. Esta operación consta de cuatro etapas que son:

a) *Etapa 1:* El equipo emisor decide finalizar la comunicación en su sentido. Envía al equipo receptor una señal de FIN con un número de secuencia

b) *Etapa 2:* El equipo receptor recibe esta señal y responde con un reconocimiento de acuse de envió (ACK). Enviando el número de secuencia recibido más uno.

c) *Etapa 3:* El equipo receptor decide finalizar la conexión en su sentido y envía una señal de finalización (FIN) de conexión al equipo emisor.
d) *Etapa 4:* El equipo emisor acepta la petición de finalizar la conexión respondiendo con un ACK y enviando el número de secuencia recibido más uno. En esta etapa se da la finalización TCP.

En la figura 11.B.5 se ilustran las cuatro etapas para terminar una conexión.

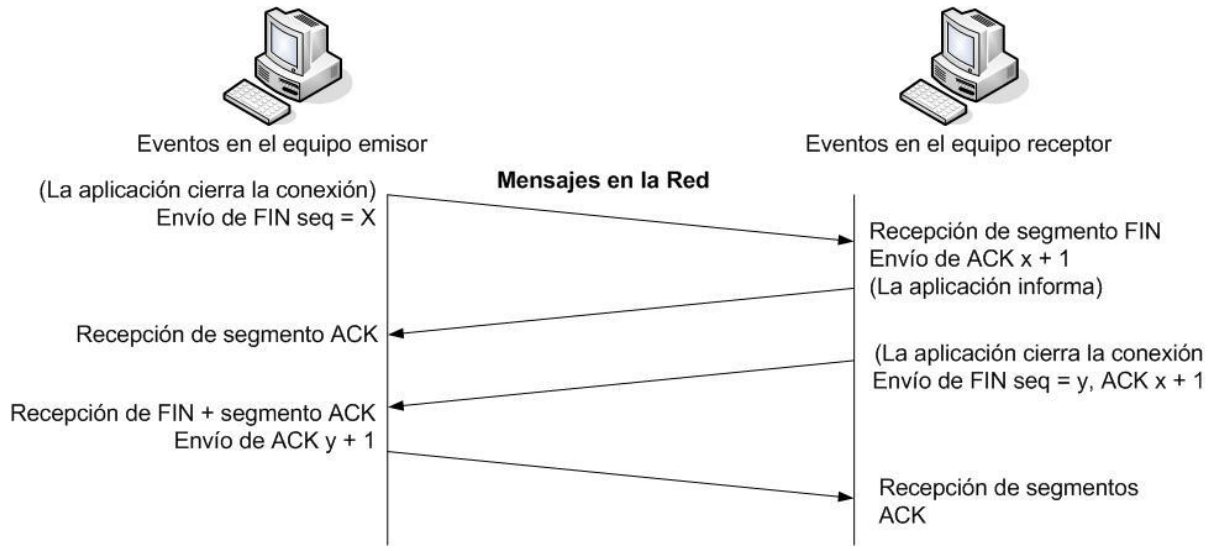


Figura 11.B.5: *Etapas para terminar una conexión TCP*

Debido a la posibilidad de que cualquiera de los dos extremos implicados en la comunicación pueda enviar y/o recibir datos, tenemos la posibilidad de que cualquiera de los dos extremos finalice la comunicación (enviando una señal FIN) hacia su sentido. Una vez que la conexión se ha cerrado en una dirección dada, el protocolo TCP rechaza más datos en esta dirección. Mientras tanto los datos pueden continuar fluyendo en la dirección opuesta hasta que el emisor se cierre. Cuando ambas direcciones se han cerrado el software TCP en cada punto extremo borra sus registros de la conexión.

7) Notificación de la congestión explicita (ECN)

Es una de las nuevas optimizaciones que posee el protocolo TCP, el cual es un mecanismo de administración de colas activas, tal y como la detección temprana aleatoria, permite al router detectar la congestión antes de que la cola se desborde haciendo que todos los paquetes subsecuentes se pierdan. ECN es una manera de cómo los router señalan la congestión, basada en la detección temprana de ellos, para nodos terminales antes de que los routers comiencen a perder paquetes. La señalización de desbordamiento es hecha a través de bits tanto por la cabecera IP como por la cabecera TCP. Los bits que representan los valores ECN se detallan en la tabla 11.B.1 (RFC3168).

Valores	Descripción
00	No capacitado para ECN
10	Nodo capacitado para ECN
01	Nodo capacitado para ECN
11	Router que advierte congestión a nodos capacitados para ECN

Tabla 11.B.1: *Valores ECN en el campo de clase de tráfico.*

Un nodo capacitado para ECN pone '10' en el bit ECN del campo de clase de tráfico de la cabecera IPv6 cuando es enviado un paquete. Mientras tanto un nodo no capacitado para ECN pone '00' en el campo de clases de tráfico. Un router detectando una congestión temprana dentro de su cola activa modifica la cabecera IPv6 fijando el bit ECN en '11'. El bits ECN también es definido en la cabecera TCP. En la figura 11.B.6 se muestra el proceso que lleva una red IPv6 con nodos capacitados para ECN llamados N1 y N2 y router capacitados para ECN llamado R1.

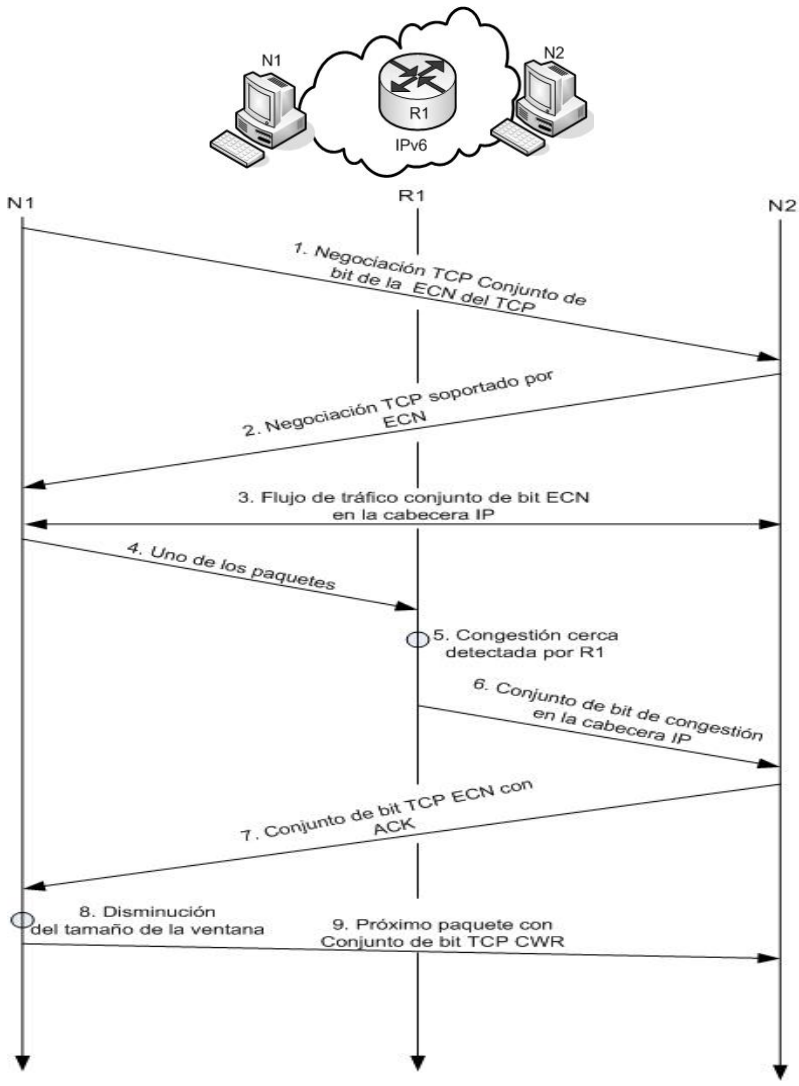


Figura 11.B.6: *Proceso en una red IPv6 soportando ECN*

N1 reconoce en N2 la recepción de la señal de la congestión por la configuración del bit TCP CWR, después de eso, el mecanismo normal de la congestión del TCP se aplica.

C. PROTOCOLO DATAGRAMA DE USUARIO (UDP).

No existe ninguna modificación que se haya realizado en UDP para IPv6, excepto que ahora la suma de verificación es obligatoria, no así en IPv4. Como se sabe el protocolo de datagrama de usuario (RFC768) proporciona un mecanismo primario que utilizan los programas de aplicación como por ejemplo http, para enviar datagramas a otros programas de aplicación. Cada mensaje UDP contiene tanto el número de puerto origen como el número de puerto destino. Esto hace posible que el programa UDP en el destino entrege el mensaje al receptor correcto obteniendo además una respuesta de este. El UDP utiliza el protocolo de Internet subyacente para transportar un mensaje de una máquina a otra, no emplea acuses de recibo (ACK) como lo hace TCP, ni controla la velocidad a la que fluye la información entre los nodos en comunicación, esto hace que los mensajes UDP puedan ser perdidos, duplicados y llegar en desorden a su receptor.
El estudio completo del protocolo UDP se encuentra publicado en el estándar de Internet RFC768.

1) Formato del mensaje UDP.
En la figura 11.C.1 se muestra el formato de un mensaje UDP.

Puerto fuente	Puerto destino
Longitud del mensaje	Suma de verificación
Datos	
….	

Figura 11.C.1: *Formato de mensajes UDP.*

Los campos de la cabecera del protocolo UDP son los siguientes:

a) *Puerto fuente (Source Port):* Es un campo opcional, cuando se utiliza, este especifica el puerto donde deben enviarse las respuestas, de lo contrario este debe tener un valor de cero.
b) *Puerto destino (Destination Port):* Tiene un significado dentro del contexto de una dirección de destino de Internet particular.
c) *Longitud del mensaje (Length):* Es la longitud en octetos del datagrama de usuario incluyendo la cabecera de este y los datos.
d) *Suma de verificación (Checksum):* Se procede como se indica en el apartado *4.B.2.c*.

2) Interfaz IP
El módulo UDP debe poder determinar las direcciones del Internet de origen y destino y el campo del protocolo de la cabecera de Internet. Una posible interfaz UDP/IP retorna el datagrama del Internet completo incluyendo la cabecera de Internet completa en respuesta a una operación de la recepción.

D. PROTOCOLO DE CONTROL DE TRANSMISIÓN DE FLUJO (SCTP).

1) Definición
Como se señaló en la introducción de este capítulo, se han desarrollado los protocolos TCP y UDP que son los mas comunes en su aplicación, pero existe otro protocolo que es una alternativa mas para el transporte de los datos en redes de computadores denominado Protocolo de Control de Transmisión de Flujo (SCTP), el cual es desarrollado en el RFC2960. El SCTP esta diseñado para transportar mensajes con señales de *PSTN* (Public Switched Telephone Networks) sobre redes de IP, pero este es capaz de usos más amplios.

El SCTP es un protocolo de transporte confiable que funciona sobre redes de paquetes sin conexión tal como IP. Este ofrece los servicios siguientes a sus usuarios (RFC2960):

a) Transferencia no duplicada, reconocimiento de error en los datos del usuario.
b) Fragmentación de los datos en concordancia con el tamaño descubierto de la *MTU de la ruta* del paquete.
c) Entrega ordenada de los mensajes del usuario dentro de flujos múltiples, con una opción para la entrega de orden de llegada de los mensajes individuales del usuario.
d) El entrelazado opcional de los mensajes múltiples del usuario en un solo paquete de SCTP.
e) Tolerancia por defecto del nivel de red a través del soporte de multiasentamiento (multihoming) en cada uno o en ambos extremos de una asociación.

El TCP ha desarrollado una inmensa gama de servicios como los medios de transferencia de datos confiables en redes IP. Sin embargo, un número creciente de aplicaciones recientes han encontrado que TCP es demasiado limitado, y han incorporado sus propios protocolos de transferencias de datos confiables en la cima de UDP. Las limitaciones que los usuarios han deseado evadir incluyen las siguientes:

a) El TCP provee tanto una transferencia de datos confiables como una entrega de datos en estricto orden de transmisión. Algunas aplicaciones necesitan una transferencia confiable sin mantenimiento de secuencia, mientras otras serian satisfechas con un ordenamiento parcial de los datos. En ambos casos la cabeza del bloqueo de línea ofrecido por TCP ocasiona retardos innecesarios.
b) La naturaleza orientada al flujo de TCP es a menudo un inconveniente. Las aplicaciones deben añadir su propia marca de registro para delinear sus mensajes, y debe hacer uso explícito de las facilidades de *empuje* para asegurar que el mensaje completo es transferido en un tiempo razonable.
c) Los sockets TCP de ámbitos limitados complican la tarea de proveer disponibilidad alta de capacidad de transferencia de datos utilizando host multiasentados (multihomed*)*.
d) TCP es relativamente vulnerable a los ataques de *negación de servicio*, tales como los ataques SYN.

El transporte de Señalización PSTN a través de la red IP es una aplicación para la cual todas estas limitaciones de TCP son relevantes. Mientras esta aplicación directamente motiva el desarrollo de SCTP, otras aplicaciones pueden encontrar en SCTP que se ajusta perfectamente a sus requerimientos.

2) Arquitectura

STCP es visto como una capa entre la aplicación del usuario SCTP y el servicio de red de paquetes sin conexión como IP. Este servicio es desarrollado dentro del contexto de una *asociación* entre dos puntos finales SCTP.

La naturaleza de SCTP es orientada a la conexión, Mas sin embargo la *asociación SCTP* es un concepto más amplio que la conexión TCP. SCTP provee los medios para que cada punto final SCTP provea al otro punto final (durante el inicialización de la *asociación*) con una lista de direcciones de transporte (es decir, direcciones IP múltiples en combinación con un puerto SCTP) a través de la cual ese punto final puede ser alcanzado y desde el cual se originaran las paquetes SCTP. En la figura 11.D.1 se muestra una *asociación SCTP.*

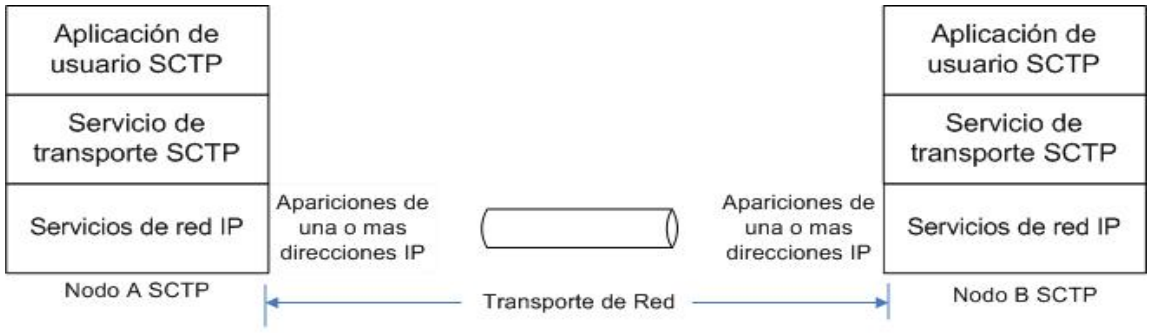


Figura 11.D.1: *Una asociación SCTP.*

3) Formato de cabecera SCTP

En la figura 11.D.2 se muestra el formato de la cabecera común SCTP.

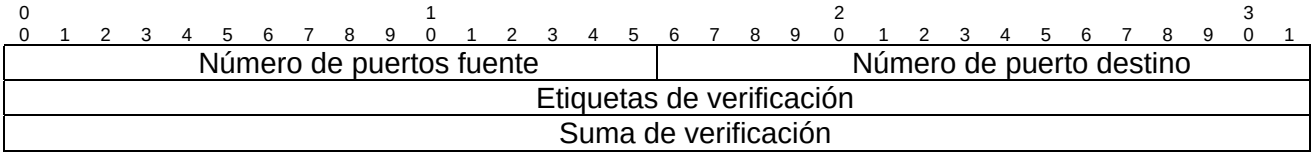


Figura 11.D.2: *Formato de la cabecera común SCTP.*

Donde:

Número de puertos fuente (Source Port Number): Entero de 16 bits, que indica el número de puertos de los emisores SCTP.

Número de puerto destino (Destination Port Number): Entero de 16 bits, que indica el número de puertos a los cuales se destinan los paquetes SCTP.

Etiquetas de verificación (Verification Tag): Entero de 32 bits que se utiliza para validar el emisor del paquete SCTP.

*Suma de verificación (Checksum): S*uma de verificación de CRC 32 bits (ver RFC3309).

4) Formato del paquete SCTP

Un paquete SCTP esta compuesto por una cabecera común y trozos. Un trozo contiene tanto información de control como datos de usuario

En la figura 11.D.3 se muestra el formato del paquete SCTP.

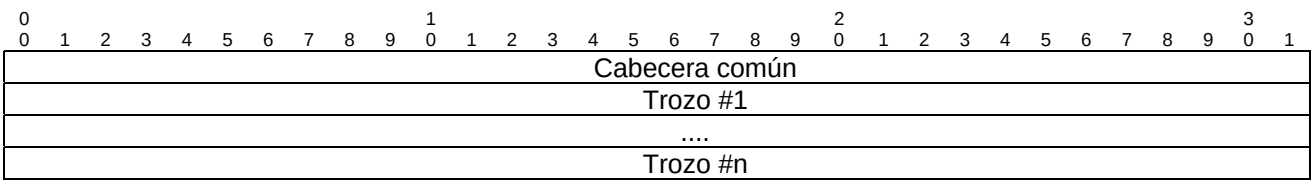


Figura 11.D.2: *Formato de la cabecera común SCTP.*

12. IPv6 SOBRE ALGUNAS TECNOLOGÍAS DE ENLACE

A. INTRODUCCIÓN

IPv6 al igual que su antecesor IPv4 es implementado sobre diversas tecnologías de enlace, en la tabla 12.A.1 se muestran algunas de los protocolos de capa de enlace donde es implementando el protocolo IPv6.

Protocolo	RFC
Ethernet	2464
Point to Point Protocol (*PPP*)	2472
FDDI	2467
Token-Ring	2470
Non-Broadcast Multiple Access (*NBMA*)	2491
ATM	2492
ARCnet	2497
Frame-Relay	2590
IEEE 1394	3146
MAPOS	3572

Tabla 12.A.1: *Protocolos de capa de enlace implementados en IPv6.*

En este capitulo se desarrollan algunos de los protocolos de capa de enlace para IPv6.

B. IPv6 SOBRE ENLACES ETHERNET

1). Unidad máxima de transmisión (MTU)
Por defecto el tamaño de una MTU para un paquete IPv6 dentro de una Ethernet es de 1500 octetos. Dicho tamaño puede ser reducido por los avisos del router, conteniendo una opción de la MTU que especifica un tamaño más pequeño o ya sea por la configuración manual de cada nodo. En el caso de que recibiera un anuncio del router dentro de una interfaz Ethernet, especificando en la opción de la MTU un tamaño más grande que 1500 octetos o un valor grande configurado manualmente, esta opción debería ser notificada al administrador del sistema; en caso contrario debe ser ignorado.

2). Formato de trama (Frame format)
Los paquetes IPv6 son transmitidos en tramas estándar Ethernet[22]. La cabecera Ethernet contiene la dirección de destino y origen y el tipo de código Ethernet, cada uno debe contener el valor hexdeciamal de 86DD. El campo de datos contiene la cabecera IPv6 seguida inmediatamente por la carga útil y un posible relleno de octetos para satisfacer el tamaño mínimo de la trama en el enlace Ethernet. En la figura 12.B.1 se muestra el formato del marco estándar Ethernet.

[22] RFC2464:Transmission of IPv6 Packets over Ethernet Networks

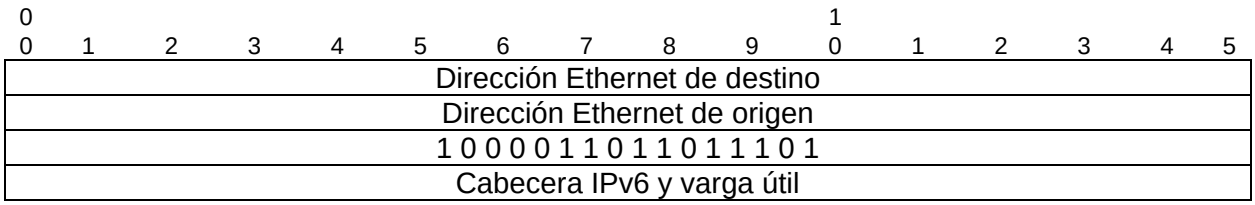


Figura 12.B.1: *Formato de trama estándar Ethernet*

En la figura 12.B.2 se muestra el identificador de trama Ethernet para IPv6.

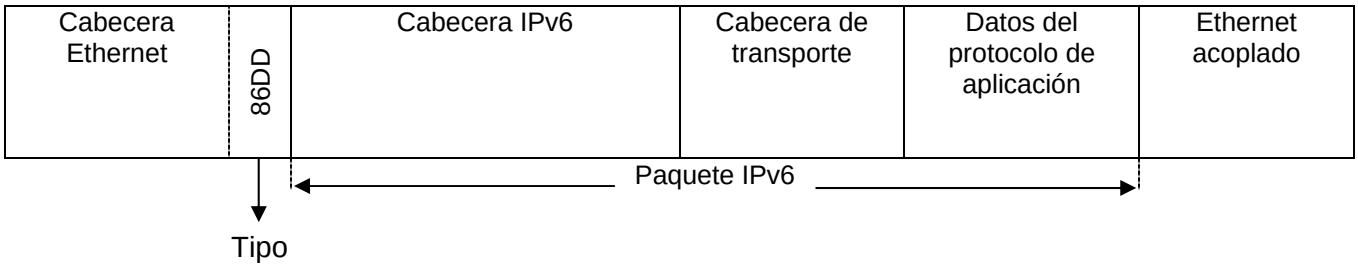


Figura 12.B.2: *Identificador de trama Ethernet para IPv6.*

3). Autoconfiguración sin estado

El identificador de interfaz para una interfaz Ethernet es basado en el identificador EUI-64, desarrollado en la capitulo 3 direccionamiento IPv6, esta se deriva de una interfaz construida con una dirección de 48 bits. Una dirección Ethernet es representada por 6 campos escritos como octetos en formato hexadecimal con un campo separador "-" tal y como lo muestra la figura 12.B.3

00-11-22-33-44-55

Figura 12.B.3 *Formato de direcciones Ethernet.*

4). Dirección local de enlace

La dirección local de enlace IPv6 para una interfaz Ethernet es formada añadiendo el identificador de interfaz para el prefijo FF80::/64. E formato se muestra en la figura 12.B.4.

10 bits	54 bits	64 bits
1111111010	Ceros	Identificador de interfaz

Figura 12.B.4: *Formato de la dirección de enlace local en Ethernet para IPv6.*

5). Trazado de direcciones Unicast

El procedimientos de trazado de direcciones unicast en enlaces Ethernet es especificado en el RFC 2461. El origen y el destino de la dirección de capa de enlace deben tener la siguiente forma si se encuentra en un enlace Ethernet. El formato se muestra en la figura 12.B.5.

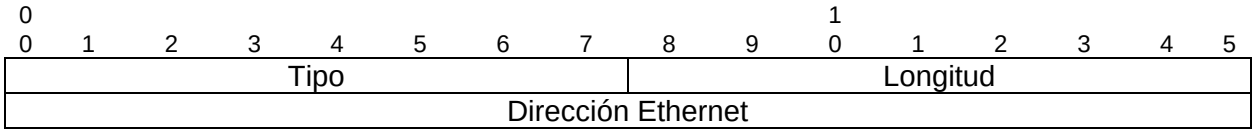


Figura 12.B.5 *Formato de trazado de direcciones unicast en enlaces Ethernet.*

Opciones de los campos:

Tipo (type): 1 para la dirección origen de la capa de enlace
2 para la dirección destino de la capa de enlace

Longitud (length): Una unidad de 8 octetos, que especifica el tamaño del paquete

Dirección Ethernet (Ethernet Address): Dirección de 48 bits según el estándar IEEE 802.

C. IPv6 SOBRE ENLACES PPP (PROTOCOLO PUNTO A PUNTO)

El protocolo *PPP* provee un método estándar de encapsulación de información de protocolo de capa de red, sobre enlaces punto a punto. PPP también es definido como un protocolo de control de enlace y propone una familia de protocolos de control de red NCPS, para establecer y configurar diversos protocolos de capa de red.

1). Partes principales del protocolo PPP[23]

PPP posee tres componentes principales:

- Un método para encapsulación de datagramas sobre enlaces seriales
- Un protocolo de enlace PCL para estabilizar, configurar y testear la conexión de datos de enlace.
- Una familia de protocolos de control de red NCPS para estabilizar y configurar diferentes protocolos de capa de red.

En la figura 12.C.1 se muestra el formato de una trama PPP en IPv6.

[23] RFC2472: IP Version 6 over PPP

Identificador del protocolo	Carga útil	Rellenando

Figura 12.C.1: *Formato de trama en enlaces PPP.*

En la figura 12.C.2 se muestra el formato de un paquete PPP.

0057	Cabecera IPv6	Carga útil IPv6

Figura 12.C.2: *Formato de un paquete PPP en IPv6.*

Para establecer comunicaciones sobre enlaces PPP, cada extremo del enlace del PPP debe primero enviar los paquetes de LCP para configurar y para probar la transmisión de datos. Después de que se haya establecido el enlace y facilitar las opciones deben ser negociadas según lo necesitado por el LCP, el PPP debe enviar los paquetes de *NCP* para elegir y para configurar uno o más protocolos de capa de red. Una vez los protocolos elegidos de la capa de red se ha configurado entonces los datagramas de cada protocolo de la capa de red se puede enviar sobre el enlace.

2). Enviando datagramas IPv6

Antes de que cualquier paquete IPv6 pueda ser enviado, el PPP deberá alcanzar la fase del protocolo de la capa de red y el protocolo del control IPv6 debe alcanzar un estado abierto.
IPv4 es manejado por el protocolo de control IPCP y los paquetes IPv4 son puestos en el campo de carga útil del marco PPP haciendo uso del protocolo id 0x0021. Mientras que IPv6 es manejado por el protocolo de control IPv6CP y los paquetes IPv6 son puestos en el campo de la carga útil del marco PPP con el protocolo id 0x0057.
Un paquete IPv6 se encapsula exactamente en el campo de información de la trama de capa de transmisión de datos del PPP donde el campo del protocolo indica el tipo hexadecimal 0057 (versión 6 del Protocolo de Internet).
La longitud máxima de un paquete IPv6 transmitido sobre un enlace del PPP es igual que la longitud máxima del campo de información de la trama de capa de transmisión de datos del PPP.
Los enlaces del PPP que soportan IPv6 deben permitir un campo de información por lo menos tan grande como el tamaño mínimo de la MTU del enlace requerido para IPv6.

3). Protocolo del control de la red del PPP para IPv6
El protocolo del control IPv6 (IPV6CP) es responsable de configurar, de permitir, y de inhabilitar los módulos del protocolo IPv6 en ambos extremos del enlace punto a punto. IPV6CP utiliza el mismo mecanismo del intercambio del paquete que el protocolo del control de enlace (LCP), los paquetes de IPV6CP no pueden ser intercambiados hasta que el PPP ha alcanzado la fase del protocolo de capa de red, los paquetes de IPV6CP recibidos antes de que se alcance esta fase deben ser desechados sin dar previos avisos.

4). Opciones de configuración IPv6CP

Las opciones de la configuración de IPv6CP permiten la negociación de los parámetros deseables IPv6. IPv6CP utiliza el mismo formato de la opción de la configuración definido para LCP, con un sistema separado de opciones. Si una opción de la configuración no se incluye en el paquete de solicitud de configuración, el valor prefijado para esa opción de la configuración es asumido. Los valores actualizados del tipo campo de la opción de IPv6CP se especifican en el RFC2472. Se asignan los valores actuales como sigue:

a) Identificador de interfaz:

Esta opción de configuración proporciona una manera de negociar un interfaz única de 64 bits más para ser utilizado para la autoconfiguración de la dirección en el extremo del enlace local Una solicitud de configuración debe contener exactamente un instancia de la opción del identificador de interfaz. Dicho identificador de interfaz debe ser único dentro del enlace PPP.
Los siguientes son métodos para elegir el identificador tentativo del interfaz en orden de preferencia:

- Si un identificador de interfaz global IEEE (48 bits o 64 bits) es habilitado en cualquier nodo, este debería ser usado para construir el identificador de interfaz tentativo esto es debido a que presenta características de unicidad. La única transformación desde un identificador EUI-64 es convertir el bit u (bit universal/local, ver capitulo 3 direccionamiento). Por ejemplo para un identificador único global EUI-64 el formato se muestra en la figura 12.C.3.

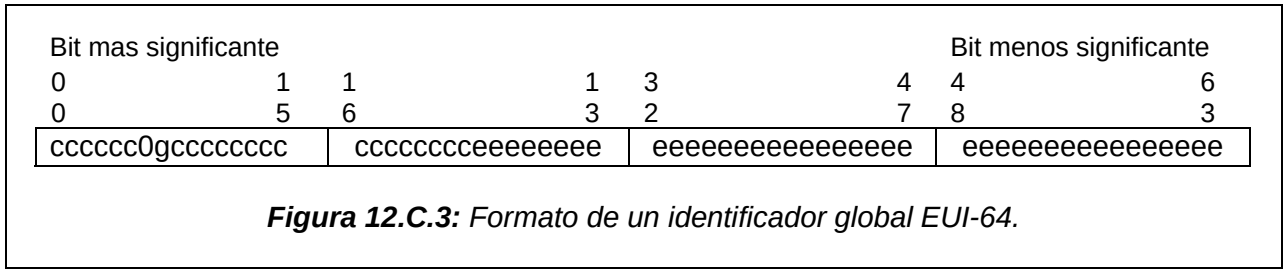


Figura 12.C.3: *Formato de un identificador global EUI-64.*

Donde los bits “c” que representa el identificador de la compañía, “0” es el valor del bit universal/local para indicar alcance global, “g” es el bit de grupo/individual, y “e” es los bits del identificador de la extensión.

- Si un identificador global de IEEE no está disponible en diferentes fuentes de unicidad este debe ser utilizado. Las fuentes sugeridas de la unicidad incluyen direcciones de la capa de enlace, números de serie de la máquina, etc. En este caso el bit de “u” del identificador del interfaz se debe fijar en cero (0).
- Si una buena fuente de unicidad no puede ser encontrada, se recomienda que un número al azar sea generado. En este caso el bit “u” del identificador del interfaz se debe fijar a cero (0). Las buenas fuentes de unicidad o de la aleatoriedad se requieren para la negociación del identificador de interfaz puedo ocurrir. Si ningún número único o un número al azar puede ser generado se recomienda que un valor cero sea utilizado para el identificador de interfaz transmitido en la solicitud de Configuración.

b) Protocolo de la compresión IPv6:

Esta opción de configuración proporciona una manera de negociar el uso de un protocolo específico de la compresión del paquete IPv6. La opción de la configuración del Protocolo de la compresión IPv6 se utiliza para indicar la capacidad de recibir los paquetes comprimidos. Cada extremo del enlace debe solicitar por separado esta opción si se desea que la compresión sea bidireccional. Por defecto la compresión no es habilitada. La compresión IPv6 negociada con esta opción es específica para los datagramas IPv6 y no debe ser confundida con la compresión resultante de las negociaciones vía el Protocolo del Control de Compresión (CCP), que potencialmente efectúan todos los datagramas. El formato de la

opción de la configuración de protocolo de compresión IPv6 se demuestra en la figura 12.C.4. Los campos se transmiten de izquierda a derecha.

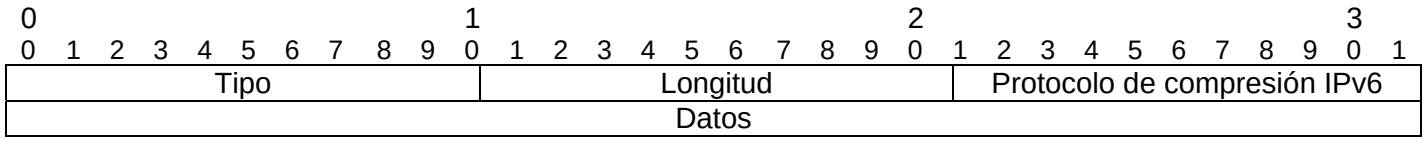


Figura 12.C.4: *Formato de la opción del protocolo de compresión de IPv6.*

Campos:

Tipo (type): 2

Longitud (length): 4

Protocolo de compresión IPv6 (IPv6-Compression-Protocol): El campo del protocolo de compresión IPv6 contiene dos octetos e indica el protocolo de la compresión deseado. Los valores para este campo son siempre iguales que el campo del protocolo de capa de enlace de datos del PPP. No se han asignado ningún valor al campo de protocolo de compresión IPv6 actualmente. Las asignaciones específicas serán hechas en los documentos que definen algoritmos específicos de la compresión.

Datos (data): El campo de datos es cero o más octetos y contiene datos adicionales según lo determinado por el protocolo de compresión particular.

5) Consideraciones de seguridad

La extensión del protocolo de control IPv6 para PPP puede ser usada por todas las definiciones PPP de autenticación y mecanismos de encriptación.

D. IPv6 SOBRE ENLACES ATM (MODO DE TRANSFERENCIA ASÍNCRONA)

El uso de una red ATM para transportar paquetes IPv6 puede ser relativamente simple o muy complejo, dependiendo de cómo se utiliza a si misma la red ATM[24].

Muchas ofertas comerciales para los WANs de ATM (redes de área amplia) ofrecen un servicio basado en PVCs (conexiones virtuales permanentes) y una red de redes entre las redes locales y la red de área amplia puesta en ejecución a través de las routers. Este método que usa ATM no presenta problemas particulares porque las routers ven PVCs como canales *punto a punto*. Este acercamiento se elige con frecuencia cuando:

- Los tamaños de la red de redes son significativos
- Los medios heterogéneos de la transmisión se utilizan, haciendo el uso de una tecnología de red única imposible.
- Las razones de la confiabilidad imponen una tecnología parcialmente indentada, también con medios heterogéneos de la transmisión.

SVCs (conexiones virtuales cambiadas), hacen a ATM una red multiaccesos, es decir, una red en la cual el resto de los usuarios de la red puedan ser alcanzados desde cualquier punto de la conexión.

[24] RFC2492: IPv6 over ATM Networks

Un manejador de ATM IPv6 como mínimo conformará el soporte al modo de operación del PVC (servicio punto a punto). Un manejador de ATM IPv6 que soporta el modo completo del SVC (servicio punto a multipunto).

1). Entornos PVC

Cuando una red ATM es usada en un modo PVC, cada PVC conecta exactamente dos nodos y el uso del descubrimiento de vecindario y de otras características IPv6 son limitados. Las interfaces ATM IPv6 poseen únicamente un vecindario en cada enlace. Ya que los enlaces ATM del PVC no utilizan direcciones de la capa de enlace, las opciones de la dirección de la capa de enlace no se deben incluir en ningún mensaje ND. Si una opción de la dirección de la capa de enlace está presente en un mensaje del ND, entonces la opción debe ser ignorada.

2) Entornos SVC

a) Puntos de código específicos del SVC

- Encapsulación de la capa de la adaptación de ATM para entornos SVC

  El proceso de encapsulación es ejecutado mediante el uso de direcciones unicast y paquetes multicast a través de enlaces SVC.

- Encapsulación de paquetes unicast

  La encapsulación de paquetes unicast IPv6 por defecto es como sigue:

  $$[0\times AA-AA-03][0\times 00-00-00][0\times 86-DD][PaqueteIPv6]$$

- Encapsulación de paquetes multicast

  La encapsulación de paquetes unicast IPv6 por defecto es como sigue:

  $$[0\times AA-AA-03][0\times 00-00-5E][0\times 00-01][pkt\$cmi][0\times 86DD][paqueteIPv6]$$

- Encapsulación nula opcional

  Los manejadores ATM IPv6 pueden también apoyar la encapsulación nula como opción configurable. La encapsulación nula será utilizada solamente para pasar los paquetes IPv6 a partir de un manejador de ATM IPv6 a otro. Si se permite la encapsulación nula, el paquete IPv6 se pasa directamente a la capa AAL5. Ambos extremos del SVC deben acordar utilizar la encapsulación nula durante la fase de la configuración de llamada. El SVC no estará disponible para uso de protocolos con excepción de IPv6.

- Mensajes de control de descubrimiento de vecindario

  La opción de la dirección de capa de enlace del ND para manejadores ATM IPv6 posee los subcampos serán codificados de la manera siguiente: Ver figura 12.D.1.

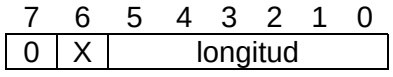


Figura 12.D.1: *Formato de mensaje de ND sobre enlaces ATM en IPv6.*

El bit más significativo es reservado y se debe fijar a cero. El segundo bit significativo (x) es una bandera que indica en si el número de la ATM está:

Formato del foro AESA de ATM $X=0$

Formato nativo E.164 $X=1$

Los 6 bits del fondo representan un valor del entero sin signo que indica la longitud del campo de dirección asociado a ATM en octetos.

3). Autoconfiguración de direcciones
El problema de la autoconfiguración de las direcciones IPv6 asociado a las interfaces de ATM es complicado por la carencia de un mecanismo nativo del multicast que permita el uso del procedimiento duplicado de la detección de la dirección, pero también por la presencia del concepto de interfaz de la lógica en enlaces de tipo ATM. De hecho, en una tabla de red de ATM, muchos interfaces lógicas de ATM se pueden configurar, obviamente teniendo diversas direcciones (símbolo de interfaz, según la terminología IPv6). La autoconfiguración local de la dirección del enlace por lo tanto llega a ser más compleja que en el caso de LANs donde 48 bits de la direcciones del MAC se utilizan como símbolo del interfaz. Esta edición soluciona tanto el problema de usar un número de bits suficientes para identificar la interfaz, como evitar direcciones duplicadas y el problema de usar un número de bits suficientes para el prefijo de red. Este problema no había tenido una solución general hasta ahora. Una propuesta limitada al caso de NHRP se describe en el RFC 2491 (IPv6 over NBMA networks).

4) Servidor de resolución de direcciones multicast (MARS)
El MARS es una extensión del servidor de ATMARP estandarizado para IPv4 en RFC 1577. Pone una entidad de almacenamiento en ejecución en qué direcciones del multicast de la capa 3 se asocian a los interfaces del enlace ATM que pertenecen al grupo de multicast. Los mensajes de MARS permiten la distribución de la información sobre la composición de los grupos multicast así como la adición o la cancelación de un nodo o desde un grupo del multicast. Un servidor de MARS administra un VC a múltiples puntos con todos los nodos que deseen recibir una ayuda del multicast.

E. IPv6 SOBRE ENLACES FRAME RELAY (RETRANSMISIÓN DE TRAMAS)

1). Unidad de transmisión máxima
Los dispositivos FRAME RELAY se configuran generalmente para tener un tamaño de trama máximo de por lo menos de 1600 octetos. Por lo tanto, el tamaño de la MTU por defecto IPv6 para un interfaz FRAME RELAY debe ser de 1592. Un adecuado tamaño tanto de la MTU IPv6 y del tamaño de la trama FRAME RELAY pueden ser configurados para evitar la fragmentación. El tamaño máximo de la trama es controlado por los mecanismos de la generación del CRC empleados en el nivel del HDLC. CRC16 proveerá cobertura a tramas hasta de 4096 octetos de longitud, que reduce el tamaño máximo eficaz de la trama en aproximadamente 4088 octetos. Un tamaño deseado más grande de la trama (tal como es utilizado por FDDI o token ring), requeriría el mecanismo CRC32, que no es todavía ampliamente utilizado y no es obligatorio para los sistemas FRAME RELAY.

2). Trama IPv6 en FRAME RELAY[25]
La encapsulación de la trama IPv6 para FRAME RELAY (para PVCs y SVCs) permite que un VC lleve los paquetes IPv6 junto con otros paquetes del protocolo. Se utiliza el formato de la trama de NLPID, en el cual el IPv6 NLPID tiene un valor de 0x8E.

3). Autoconfiguración sin estado
Un identificador del interfaz para una interfaz FRAME RELAY IPv6 debe ser único en un enlace FRAME RELAY, y debe ser único en cada uno de los enlaces virtuales representados por el VCs terminando en la interfaz. El identificador del interfaz para un enlace FRAME RELAY es localmente generado por el módulo IPv6.

[25] RFC2590: Transmission of IPv6 Packets over Frame Relay Network Specification

Cada circuito virtual (VC) en una red del FRAME RELAY es identificado únicamente en una interfaz FRAME RELAY por un DLCI. Además, un DLCI se puede ver como una identificación del punto final de un circuito virtual en un interfaz FRAME RELAY. Puesto que cada VC FRAME RELAY se configura o se establece por separado y actúa como un enlace virtual independiente del otro VCs en la red o dentro de la interfaz, enlaces o alambre de fibra.
Para alcanzar las ventajas descritas arriba, los mecanismos especificados en este documento sugieren construir el identificador de interfaz FRAME RELAY a partir de 3 campos distintos (ver figura 12.E.1).

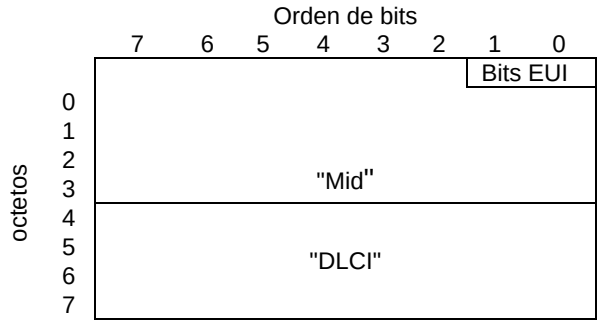


Figura 12.E.1:*Campos para construir el identificador de interfaz en FRAME RELAY*

a) *"El campo de los bits de EUI":* Bit 7 y 6 del primer octeto, representando el EUI-64 local/Universal y respectivamente el grupo/individual de bits convertido al uso de IPv6. El anterior se fija a cero para reflejar que el valor del identificador de interfaz de 64 bits tiene significación local. El último se fija a 0 para reflejar la dirección del unicast.
b) *"El campo Mid":* Un campo de 38 bits que se genera con el propósito de la adición de unicidad al identificador del interfaz.
c) *"El campo DLCI":* Campos de 24 bit que podría ser tanto 10, 17, o 23 bits del valor DLCI este debe ser ampliado con 0 a 24 bits. Un DLCI basado en el identificador del interfaz que contiene un DLCI válido de ser generado como resultado de éxito de establecer un PVC VC o un SVC.

Puesto que los DLCIs son locales a un nodo FRAME RELAY, es posible tener circuitos virtuales distintos del FRAME RELAY dentro de una red del enlace FRAME RELAY identificada con los mismos valores de DLCI.

4). Enviar mensajes de descubrimiento de vecindario sobre enlaces FRAME RELAY
Las redes FRAME RELAY no proporcionan mecanismos nativos de la multidifusión de la capa de enlace. Para el funcionamiento correcto de los mecanismos vecinos del descubrimiento de vecindario, la multidifusión de la capa de enlace debe ser emulada. Para emular la multidifusión para el descubrimiento de vecindario el nodo debe enviar las tramas que llevan los paquetes multicast de ND a todo el VCs en un interfaz FRAME RELAY. Esto se aplica a las direcciones de los mensajes del ND tanto para todos los nodos y direcciones multicast de solicitud de nodo. Este método trabaja muy bien con PVC.

5). Recepción de mensajes de descubrimiento vecinos en FRAME RELAY
Si un mensaje de solicitud del descubrimiento de vecindario recibido por un nodo contiene la opción de la dirección de la capa de enlace de la fuente con un DLCI, el mensaje debe experimentar el proceso previo específico del enlace FRAME RELAY requerido para la interpretación correcta del campo durante el proceso del manejo del protocolo de ND. Esto procesamiento se hace antes de que el mensaje del descubrimiento de vecindario sea procesado por el manejo del protocolo del descubrimiento de vecindario (ND).

6). Consideraciones de seguridad en enlaces FRAME RELAY

Los mecanismos definidos en este documento para generar un identificador de interfaz FRAME RELAY IPv6 se han pensado para proporcionar unicidad en el circuito virtual (VC) del nivel de enlace. La protección contra la duplicación es otra vez alcanzada por mecanismos de detección de direcciones duplicadas mediante la autoconfiguración de direcciones sin estado IPv6. La protección de la seguridad contra la falsificación o el accidente en el nivel de los mecanismos proporcionada por los medios de seguridad IPv6, por ejemplo IPsec, Autenticación IPsec , ESP IPsec aplicado al descubrimiento de vecindario ND o al descubrimiento inverso de vecinos mensajes IND.

13. TRANSICIÓN A IPV6.

A. INTRODUCCIÓN.

Transición y *migración* son términos técnicos que se pueden emplear indistintamente en el lenguaje cotidiano. Pero se puede precisar una diferencia práctica en estos dos términos, ya que se puede definir la *migración* como la primera meta hacia el manejo de una red en un entorno IPv6 que no implica una interrupción de las operaciones corrientes con IPv4, en un ámbito inicial reducido. Mientras que, *transición* sería la acción global y el efecto generado al cambiar un entorno prevaleciente en IPv4 a uno completamente en IPv6, donde todo el soporte a IPv4 fuese desechado. El caso de la *migración* sería lo que se puede dar en el momento actual en una empresa o institución que inicia un proceso como éste, mientras que el caso de la *transición* comprendería un escenario hipotético que se puede dar a través de un despliegue gradual de IPv6 hasta llegar a cubrir el ámbito completo tratado, tal como se observa en la Figura 13.A.1.

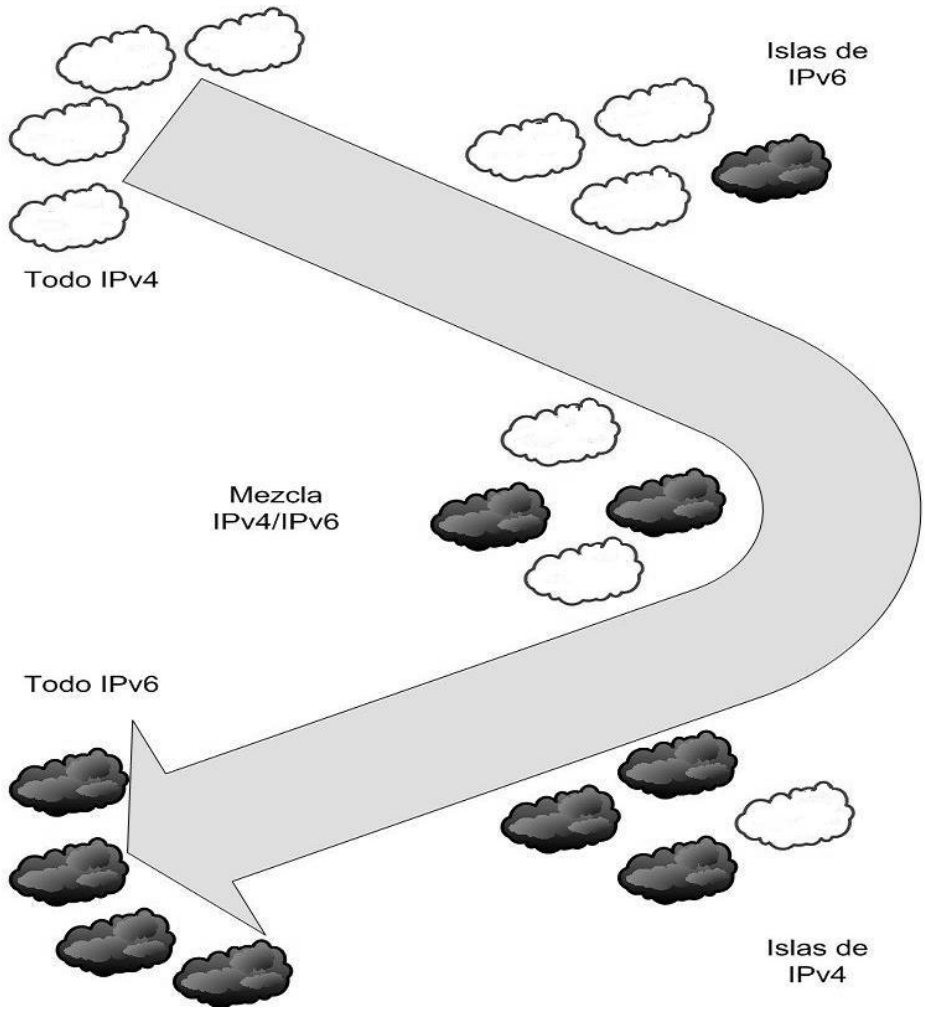


Figura 13.A.1: *Estados hipotéticos de la transición de IPv4 a IPv6*

Una vez hecha esta aclaración, puede dejarse este aspecto para describir concretamente distintos escenarios que se pueden dar durante el ínterin de una *transición*, en lo referente a las estrategias tecnológicas que se pueden emplear dependiendo del estado de la *transición* misma. Luego, será necesario establecer en términos generales, una posible planificación para llevar a cabo una *transición a IPv6* ordenada y satisfactoria.
La acción de migrar de IPv4 a IPv6 es una tarea institucional que debería llevarse a cabo bajo una concepción de proyecto persiguiendo metas como cualquier otro proyecto de TIC[26], y en el que la gerencia de TIC podría incluir todas o algunas, con o sin variantes, de las siguientes tareas sucesivas:

1) Creación de un módulo de laboratorio dentro del área institucional que contenga todo tipo de dispositivos de red, servidores y clientes que simulen la red completa.
2) Consentimiento para que personal de TIC aprenda sobre las capacidades de IPv6 y se distribuyan dentro del laboratorio para utilizar todo tipo de *herramientas de transición* y así ganen experiencia que sirva para dar soporte a los recursos corporativos.
3) Diseminación de conocimientos sobre IPv6 a todo el personal de TIC, trabajando con ellos para que desarrollen sus propios *procesos y estrategias de transición*.
4) Actualizar DNS para soportar direcciones IPv6 y, si es posible, proveer resolución DNS sobre un transporte IPv6.
5) Habilitación de IPv6 en la estructura de red a través de toda la empresa, asegurándose que no haya impacto en servidores, clientes o procesos de negocios en curso.
6) Instalación de pilas duales IPv4/IPv6 en servidores internos de tal manera que corran ambos protocolos, y asegurándose que todas las aplicaciones soportan IPv6.
7) Instalar pilas duales IPv4/IPv6 en clientes internos.
8) Despliegue de IPv6 internamente con la ayuda de registros DNS que permitan a clientes con capacidad para IPv6 utilizar servicios IPv6. Seguramente IPv4 será el protocolo más común fuera del cortafuego (firewall), de tal manera que la pila dual IP será requerida para la comunicación externa.
9) Una vez que la prueba de aplicaciones, sistemas y redes esté completa, se comienzan a mover servicios a la infraestructura habilitada para IPv6. A medida que la aceptación de IPv6 se incremente, será necesario dar soporte a IPv6 más allá del cortafuego.
10) Remoción de configuraciones IPv4 remanentes y contratos de soporte a IPv4, habilitación completa de servicios IPv6 y operación integral de una red IPv6 pura.
11) Evaluación y auditoria de los procesos de transición efectuados con el fin de actualizarlos continuamente.

En consecuencia, los aspectos más esenciales relacionados con esto se tratan en detalle en las secciones siguientes.

B. ESTRATEGIAS DE TRANSICIÓN.

Como una premisa hay que aclarar que las estrategias de transición se plantean para el uso de IPv6 en un entorno unicast. La migración de IPv4 a IPv6 en entornos multicast no ha sido considerada. Asimismo, la migración se visualiza como un proceso celular aplicado red tras red. Las estrategias para hacerlo tampoco son únicas y tienen que ser adaptadas o creadas por completo de acuerdo a las características de la red tratada.
Existen tres grupos de *herramientas o mecanismos* que permiten a IPv6 convivir dentro de distintos escenarios junto a IPv4 basados en el Internet o en intranets. Estos *mecanismos o herramientas* o traducen entre ambos protocolos o transportan vía túnel a uno en el otro. Tampoco hacen una migración completa de IPv4 a IPv6 para todo el Internet, simplemente pueden ser parte de una evolución eventualmente realizada. Estas herramientas han sido ampliamente tratadas por el grupo de trabajo *NGTRANS* de *IETF* y se compilan a continuación según su orientación[27].

[26] TIC: Tecnologías de Información y Comunicaciones.
[27] Aunque se ha tratado de incluir todas, siempre habrán nuevas propuestas para la transición.

1) Herramientas de traducción.

Habilitan la comunicación entre nodos IPv4 e IPv6.

*a) Traducción de Dirección de Red - Traducción de Protocolo (**NAT-PT**)*

El mecanismo NAT-PT, definido en el RFC2766, maneja la comunicación entre un host solo IPv6 y un host solo IPv4. La comunicación es realizada utilizando un dispositivo dedicado que hace la traducción entre las direcciones IPv4 y las direcciones IPv6, manteniendo el estado durante el tiempo de la sesión. El dispositivo NAT-PT también incluye una pasarela de capa de aplicación para hacer posible la traducción entre peticiones y respuestas DNS tanto en IPv4 como en IPv6.
NAT-PT utiliza una pila de direcciones IPv4 para asignarlas a nodos IPv6 en una base dinámica en la medida que se inicializan las sesiones en las fronteras entre IPv4 e IPv6. Las direcciones IPv4 se asumen que son globalmente únicas. NAT-PT vincula direcciones de la red IPv6 con direcciones de la red IPv4 y viceversa para proveer ruteo transparente para los datagramas atravesando entre entornos de direcciones. Los puertos TCP/UDP de IPv6 son traducidos en puertos TCP/UDP de la dirección IPv4 registrada.
Su ámbito de aplicación es a nivel de sitio.

Operación básica de NAT-PT es como sigue:

i) Comunicación de IPv6 a IPv4 (Figura 13.B.1)

NAT-PT tiene una pila de direcciones incluyendo la de la subred IPv4 presente. Las direcciones IPv4 en la pila de direcciones podrían ser asignadas una a una a las direcciones IPv6 en los nodos terminales IPv6; en tal caso se necesita tantas direcciones IPv4 como nodos finales IPv6. Así, si el nodo A IPv6 quiere comunicarse con el nodo C IPv4 entonces se genera un paquete con la dirección IPv6 del nodo A como la dirección fuente y con la dirección IPv4 del nodo C como la dirección destino, siendo encaminado por la pasarela NAT-PT donde es traducido a IPv4.

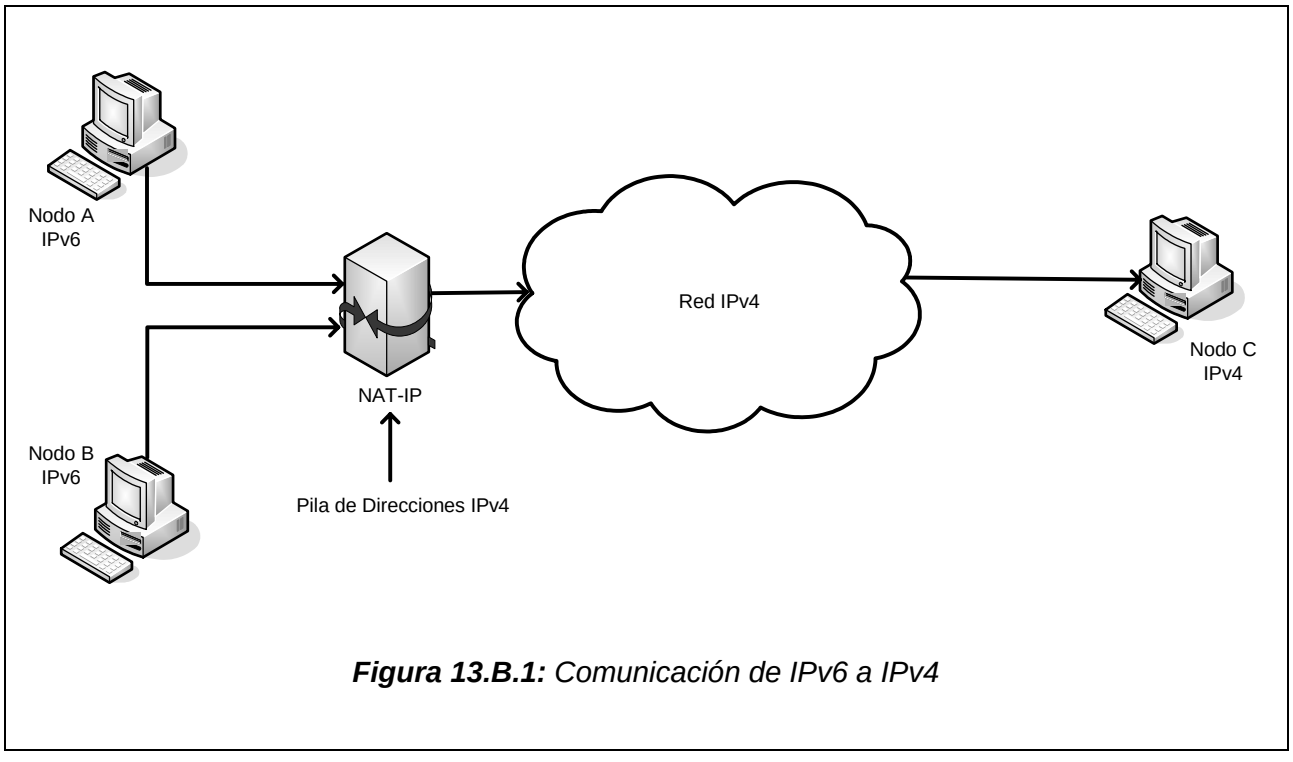


***Figura 13.B.1:** Comunicación de IPv6 a IPv4*

ii) Comunicación de IPv4 a IPv6 (Figura 13.B.2)

NAT-PT tiene una pila de direcciones incluyendo la de la subred IPv4 presente. Cuando el resolvente (resolver) del nodo C IPv4 envía una petición de búsqueda de nombre para el nodo A IPV6, la consulta de búsqueda es dirigida al servidor DNS en la red IPv6. Tomando en cuenta que NAT-PT residiera en el router de frontera entre las redes IPv4 e IPv6, este datagrama de petición atravesaría dicho router. La *pasarela DNS de nivel de aplicación* (DNS-ALG) en el dispositivo NAT-PT modificaría las consultas DNS de registros A por las de registros *AAAA* o *A6*, y los registros *PTR IN_ADDR.ARPA* por los registros *IP6.ARPA* y viceversa.

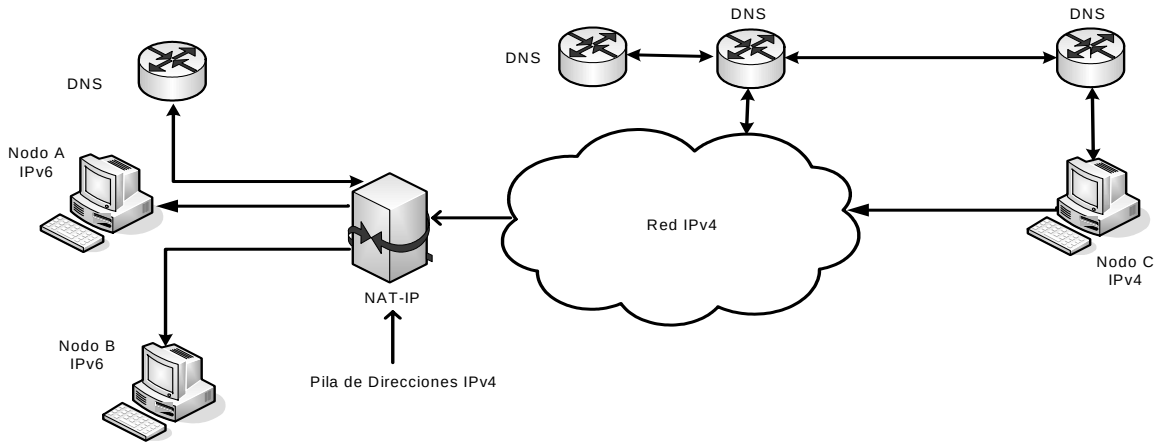


Figura 13.B.2: *Comunicación de IPv4 a IPv6*

*b) Algoritmo de Traducción Sin Estado para IP/ICMP(**SIIT**)*

El protocolo SIIT es un método descrito en el RFC2765 para traducir entre IPv6 e IPv4 con un ámbito a nivel de sitio. Este algoritmo puede utilizarse como parte de una solución que permita a hosts IPv6, que no tienen una dirección IPv4 permanentemente asignada, comunicarse con hosts solo IPv4. La traducción está limitada a la cabecera del paquete IP (incluyendo la cabecera ICMP). El traductor opera en un modo sin estado, lo cual significa que la traducción necesita hacerse para cada paquete.

Utilización básica de SIIT:

i) La figura 13.B.3 muestra como se utiliza SIIT en pequeñas redes, es decir subredes sencillas.

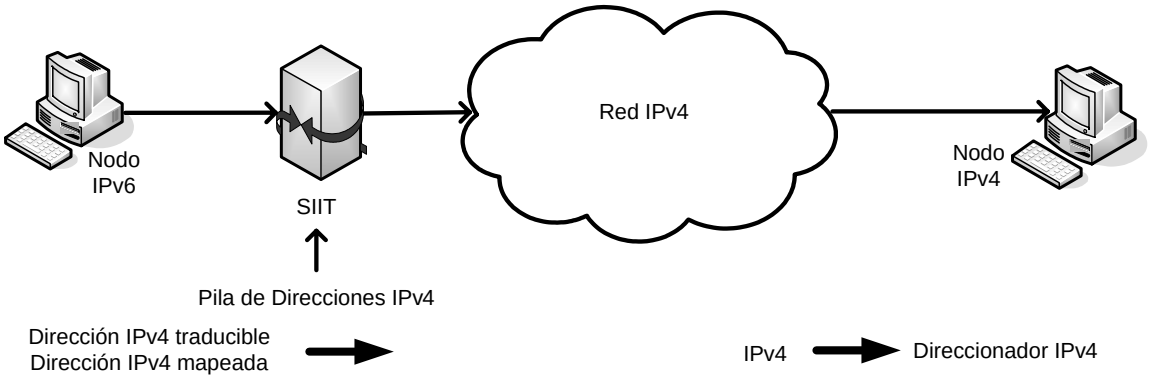


Figura 13.B.3: *Utilización de SIIT en una subred sencilla solo IPv6.*

ii) La figura 13.B.4 muestra como se utiliza SIIT en subredes solo IPv6 o en nube dual (p.ej. un sitio) que contiene tantos hosts solo IPv6 como hosts solo IPv4.

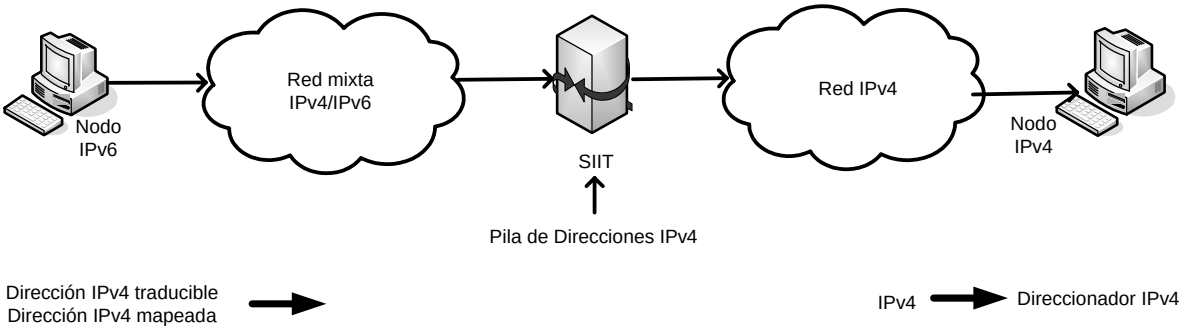


Figura 13.B.4: *Utilización de SIIT para una subred solo IPv6 o una nube dual.*

El nodo solo IPv6 que se comunica con un nodo IPv4 a través de un traductor ve una *dirección IPv4 mapeada* para el punto y utiliza una *dirección IPv4 traducible* para su dirección local en esa comunicación. Cuando el nodo solo IPv6 envía paquetes la *dirección IPv4 mapeada* indica que el traductor necesita traducir los paquetes.
Cuando el nodo IPv4 envía paquetes éstos se traducen para tener la dirección IPv4 traducible como un destino; no es posible utilizar una *dirección IPv4 mapeada o compatible con IPv4* como un destino puesto que encaminaría el paquete de regreso al traductor (para la dirección IPv4 mapeada), o bien, haría que el paquete sea encapsulado en IPv4 (para la dirección compatible con IPv4)
Estos usos asumen un mecanismo para que nodos IPv6 adquieran temporalmente direcciones de la pila de direcciones IPv4. El RFC no aclara un método para asignarlas.
Esto hará que SIIT no sea útil durante transiciones con escenario de mayoría IPv6 y solamente alguna islas IPv4.

*c) Traductor de Retransmisión de Transporte (**TRT**)*

La técnica de TRT, tratada en el RFC3142, posibilita a un host solo IPv6 intercambiar tráfico {TCP, UDP} con host solo IPv4. Cuando se despliega una red solo IPv6, todavía se desea obtener acceso a los recursos de red solo IPv4 afuera, tales como los servidores web solo IPv4. Un sistema TRT, ubicado en el medio, traduce {TCP, UDP}/IPv6 a {TCP, UDP}/IPv4, o viceversa, utilizando tan solo tecnologías existentes. Esto es lo que se llama un *traductor de retransmisión de transporte (TRT)* para la traducción de IPv6 a IPv4. Aunque la descripción común es aplicada a TCP, la implementación con UDP es similar.
Para el mapeo de direcciones, se reserva un prefijo IPv6 referido por C6::/64. Este debiera ser una parte del espacio de direccionamiento unicast IPv6 para el sitio. La información de ruteo debe ser configurada de tal modo que los paquetes a C6::/64 puedan ser encaminados hacia el sistema TRT. La figura 13.B.5 muestra la configuración de la red.

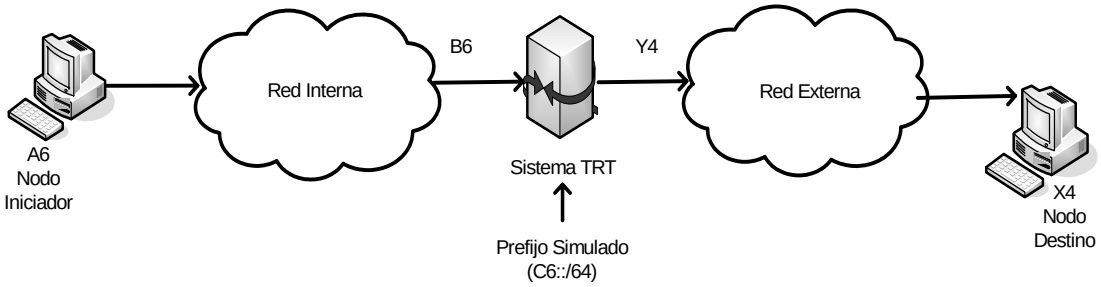


***Figura 13.B.5:** Configuración de red con un sistema TRT*

La subred denominada como *prefijo simulado* realmente no existe. También, se asume que el *nodo iniciador* sea solo IPv6, y que el *nodo destino* sea solo IPv4.
Cuando el host iniciador (cuya dirección IPv6 es A6) desea hacer conexión con el host destino (cuya dirección IPv4 es X4), requiere hacer una conexión TCP/IPv6 hacia C6::/64. El paquete es encaminado hacia el sistema TRT, y es capturado por este. El sistema TRT acepta la conexión TCP/IPv6 entre A6 y C6::X4 (dirección mapeada), y se comunica con el host iniciador, utilizando TCP/IPv6. Luego, el sistema TRT investiga los 32 bits menos significativos de la dirección destino (dirección IPv6 C6::X4) para obtener el destino real IPv4 (dirección IPv4 X4). Lleva a cabo una conexión TCP/IPv4 de Y4 a X4, y reenvía el tráfico a través de las dos conexiones TCP. Una es TCP/IPv6 y la otra es TCP/IPv4, en la fig. 13.B.5 es de A6 a B6 (como C6::X4), y de Y4 a X4, como sigue:

i) TCP/IPv6: el host iniciador (A6) → la dirección del sistema TRT (como C6::X4) en la cabecera IPv6

ii) TCP/IPv4: El sistema TRT (Y4) → la dirección del host destino (X4) en la cabecera IPv4

*d) **SOCKS64***

La herramienta *pasarela SOCKS*, tratada en el RFC3089, es una sistema pasarela que acepta conexiones SOCKS mejoradas desde hosts IPv4 y retransmitiendo a hosts IPv4 o IPv6. Especialmente para *sitios* orientados a SOCKS, que ya utilizan *clientes alerta (aware clients) SOCKS* y un *servidor SOCKS*, una *pasarela SOCKS* provee un modo fácil para dejar que hosts IPv4 se conecten a host IPv6. No se necesita hacer modificaciones al DNS o al mapeo de direcciones. Este principio también puede

utilizarse para que se conecten hosts IPv6 a hosts IPv4, hosts IPv4 sobre redes IPv6 y hosts IPv6 sobre redes IPv4. Este último caso se asemeja a las técnicas de tuneleado sin posibles problemas con la fragmentación o los límites de salto.
El mecanismo de pasarela IPv6/IPv4 basado en SOCKS está fundamentado en un mecanismo que retransmite dos conexiones terminadas IPv4 e IPv6 en la *capa de aplicación* (servidor SOCKS); sus características son heredadas de aquéllas del mecanismo de retransmisión de la conexión en la *capa de aplicación* y de aquéllas del mecanismo nativo SOCKS. La figura 13.B.6 muestra el mecanismo de pasarela basado en SOCKS.

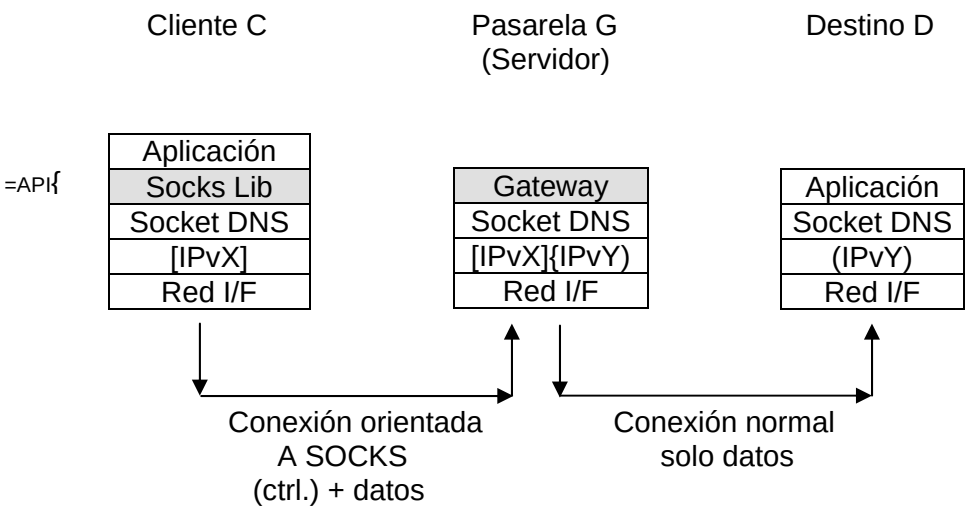


Figura 13.B.6: *Mecanismo de pasarela basado en SOCKS.*

En esta figura, el cliente C inicia la comunicación hacia el destino D. En este momento se agregan dos nuevos bloques funcionales a la pila creando el mecanismo.
El primer bloque, denominado *Socks Lib (Biblioteca de Socks)*, es introducida en el lado cliente (cliente C). Este procedimiento es llamado *socksificamiento (socksifying*). La *Socks Lib* se ubica entre la *capa de aplicación* y la *capa socket*, y puede remplazar las *APIs socket* de las aplicaciones y las *APIs* de resolución de nombres DNS (por ejemplo, *getnameinfo(), getaddrinfo(), etc*). Existe una tabla de mapeo en ella para una característica de *delegación de resolución de nombres DNS*. Cada *aplicación socksificada (socksified)* tiene su propia *Socks Lib.*
El otro, denominado *Gateway (Pasarela)*, está instalada en el nodo pila dual IPv6/IPv4 (pasarela G). Es un servidor SOCKS mejorado que habilita cualquier tipo de combinación de protocolos establecida entre el cliente C (IPvX) y el destino D (IPvY). Cuando la *Biblioteca de Socks* (*Socks Lib)* invoca una retransmisión, un proceso (hilo) de pasarela correspondiente es generado desde la *Pasarela (Gateway) matriz* para encargarse de la conexión de retrasmisión.
Los siguientes tipos de combinaciones de IPvX e IPvY son posibles en el mecanismo (Tabla 13.B.1):

	C -- G	G -- D	
TIPO	[IPvX]	[IPvY]	COMUNICACIÓN
A	IPv4	IPv4	Homogénea (Socks normal)
B	IPv4	IPv6	Heterogénea
C	IPv6	IPv4	Heterogénea
D	IPv6	IPv6	Homogénea

Tabla 13.B.1: *Tipos de combinaciones de IPvX e IPvY.*

El tipo A es soportado por el mecanismo SOCKS normal. Los tipos B y C son los objetivos principales del mecanismo de pasarela IPv6/IPv4 basado en SOCKS. Estos proveen comunicación heterogénea. El tipo D puede ser soportado por la extensión natural del mecanismo SOCKS, debido a que es una comunicación homogénea.

*e) Colisión en la Cola (**BIS**)*

El modelo BIS, desarrollado en el RFC 2767, permite el empleo de aplicaciones en IPv6 en hosts IPv4 para comunicarse con hosts solo IPv6. A la pila IPv4 se añaden tres módulos que intervienen entre la aplicación y la red, una extensión para el resolvente de nombres, un mapeador de direcciones y un traductor (Figura 13.B.7).

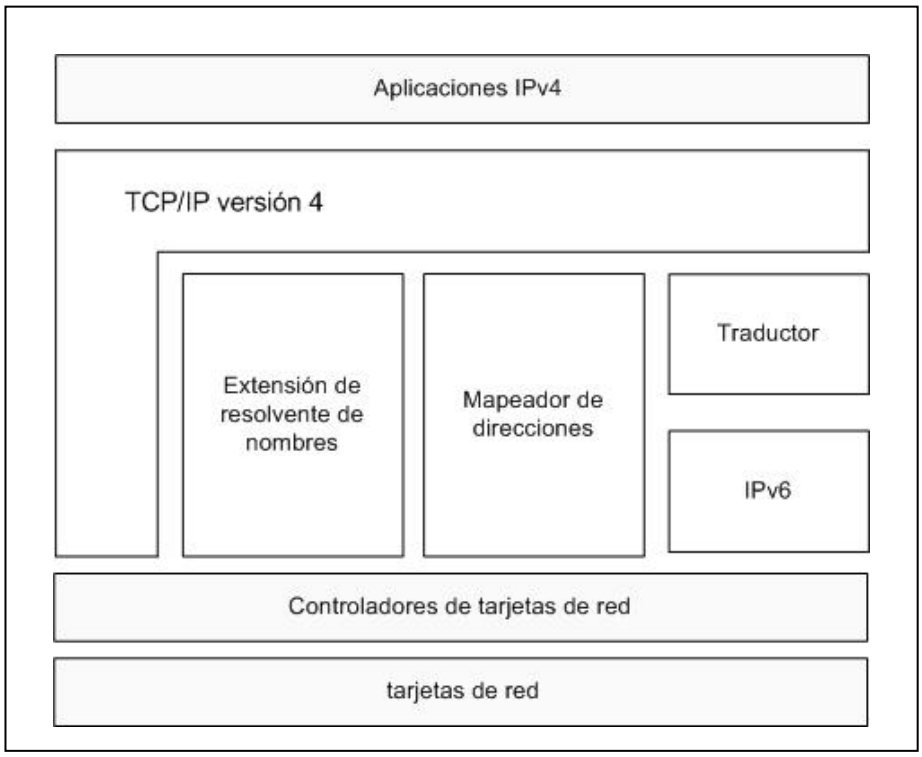


Figura. 13.B.7: *Estructura de host de pila dual empleando BIS*

La idea básica es que cuando una aplicación IPv4 necesite comunicarse con un host solo IPv6, la dirección IPv6 de ese host es mapeada dentro de una dirección IPv4 fuera de una pila o depósito local para los hosts de la pila dual. El paquete IPv4 generado para la comunicación es traducido en un paquete IPv6 de acuerdo al algoritmo SIIT.
BIS puede considerarse como una implementación particular de NAT-PT dentro de la pila IP de un host.

*f) Colisión en la API (**BIA**)*

El mecanismo BIA, desarrollado en el RFC3338, permite que hosts de pila dual se comuniquen con otros hosts IPv6 empleando las aplicaciones IPv4 existentes. El propósito de este mecanismo es el mismo que el del mecanismo BIS, solo que agrega un método de traducción entre las *APIs* IPv4 y las *APIs* IPv6, sin emplear una traducción de cabeceras IP.
La técnica BIA inserta un traductor de *API* entre el módulo *API socket* y el módulo TCP/IP en los hosts de pila dual, de tal modo que traduzca una función *API socket* IPv4 a una función *API socket* IPv6 y viceversa (Figura 13.B.8).

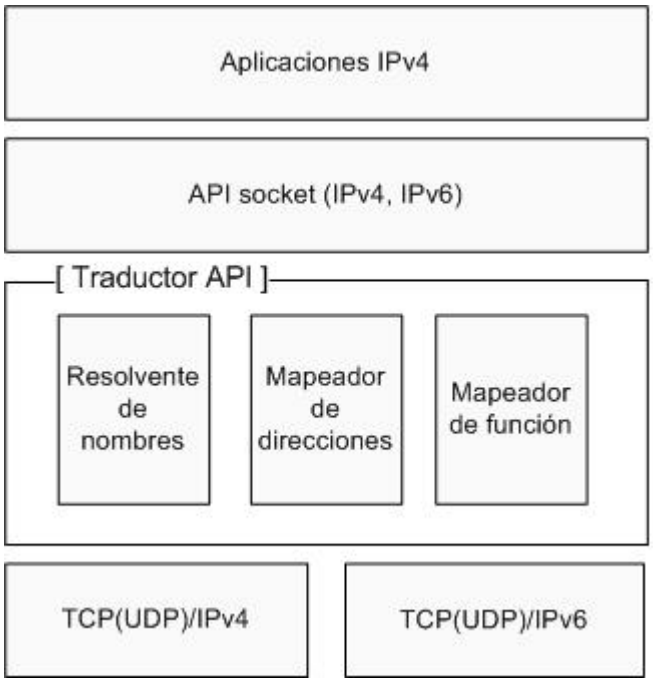


***Figura 13.B.8:** Arquitectura de un host de pila dual empleando BIA.*

2) Herramientas de Pila Dual.
Ambos protocolos son soportados igualmente a través de toda la infraestructura.

*a) Pila Dual (**Dual Stack**)*

En el modelo de *pila* dual, desarrollado en el RFC2893, todos los nodos IPv6, hosts o routers, son habilitados para pila dual (figura 13.B.9). De ese modo, la comunicación a nodos IPv4 se realiza con la pila IPv4 y la comunicación con los nodos IPv6 se realiza con la pila IPv6. La limitación de esta concepción es que se necesita colocar una dirección IPv4 en cada nuevo nodo IPv6.
Cuando se arranca una conexión con este esquema, una aplicación en un nodo de pila dual selecciona entre IPv4 o IPv6 basado las respuestas DNS y en su configuración propia.

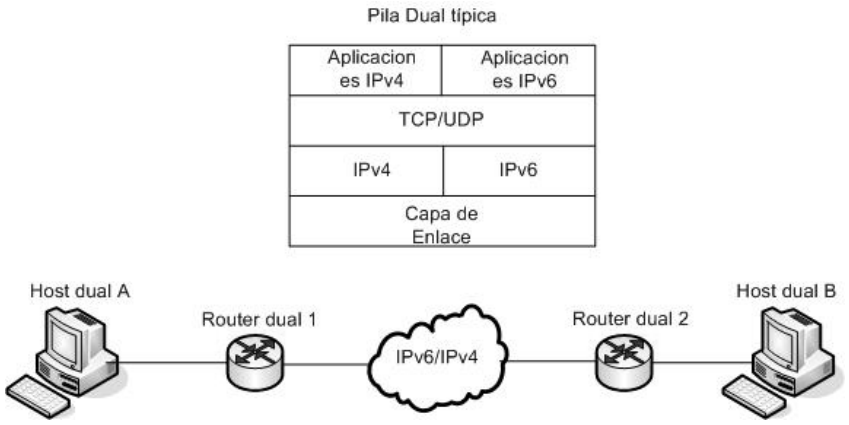


Figura 13.B.9: **Red con dispositivos configurados con pila dual**

*b) Mecanismo de Transición de Pila Dual (**DSTM**)*

El mecanismo DSTM, descrito en el borrador *draft-ietf-ngtrans-dstm-08*, provee un método para asegurar que hosts en redes IPv6 nativas puedan mantener conectividad con hosts y/o aplicaciones que solo pueden ser alcanzadas a través de IPv4. Esta conectividad se basa en el empleo de túneles IPv4 sobre IPv6 y la colocación temporal de una dirección IPv4 global a los hosts que requieren tal comunicación.
Una ilustración esquemática de DSTM se presenta en la figura 13.B.10.

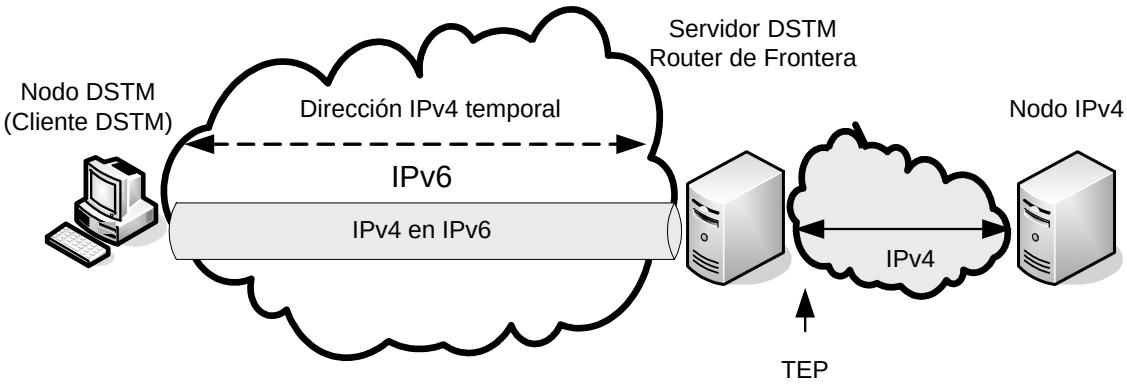


***Figura 13.B.10:** Componentes DSTM*

Donde:
TEP : Punto final de túnel. Destino de flujo IPv6 conteniendo paquetes IPv4.
Dominio DSTM: las áreas de red en una Intranet donde nodos IPv6 emplean DSTM para asegurar comunicación IPv4.
Nodo DSTM: nodo que implementa ambas pilas IPv4 e IPv6, tuneleado 4 sobre 6 y es un cliente DSTM.
Cliente DSTM: Un proceso en un nodo DSTM que maneja la dirección IPv4 temporal ubicada por el servidor DSTM.
Servidor DSTM: un proceso a cargo de manejar el espacio de direccionamiento IPv4 que será asignado a nodos DSTM.

Para que un nodo IPv6 pueda participar en DSTM debe tener una capa IP dual, manejando ambas pilas IPv4 e IPv6. DSTM hace uso de extensiones de DHCPv6 y su ámbito es de sitio. DSTM no es una solución para nodos solo IPv6.

3) Herramientas de Tuneleado.

Habilitan a islas IPv6 comunicarse sobre infraestructura IPv4.

*a) Túnel Configurado (**Configured Tunnel**)*

Los *túneles configurados manualmente o túneles estáticos*, descritos en el RFC2893, pueden emplearse para conectar hosts IPv6 sobre una infraestructura IPv4. Usualmente los túneles configurados se emplean en sitios donde en el tráfico se da un intercambio regularmente.

Esta técnica consiste en tunelear IPv6 sobre IPv4 donde la dirección de los puntos extremos del túnel IPv4 es determinada por información de configuración en el nodo IPv4 que encapsula los datagramas IPv6, y que al final debe almacenarla. Cuando un paquete IPv6 es transmitido sobre un túnel, la dirección de punto extremo del túnel configurada para ese túnel es utilizada como dirección destino por la cabecera de encapsulamiento IPv4. Esto puede visualizarse en la figura 13.B.11 y en la tabla 13.B.2.

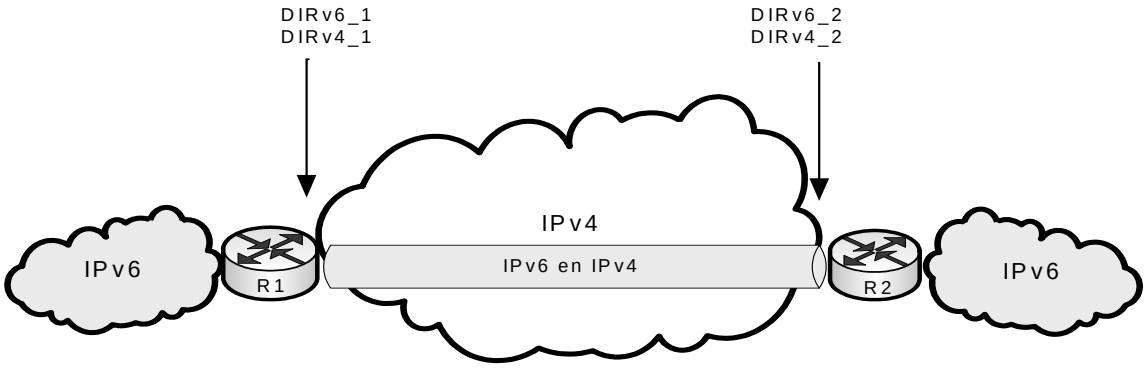


Figura 13.B.11:*Túnel configurado entre dos routers*

Parámetro de configuración	Router 1	Router 2
Dirección fuente IPv6	DIRv6_1	DIRv6_2
Dirección destino IPv6	DIRv6_2	DIRv6_1
Dirección fuente IPv4	DIRv4_1	DIRv4_2
Dirección destino IPv4	DIRv4_2	DIRv4_1

Tabla 13.B.2: *Configuración del túnel de Fig. 13.B.12 para ambos puntos extremos*

La determinación de cual paquete tunelear normalmente se hace mediante información de ruteo en el nodo encapsulador, el cual direcciona paquetes en base a su dirección de destino empleando la técnica de máscara de prefijo y apareo.

Estos túneles pueden ser tanto unidireccionales como bidireccionales. Los túneles configurados bidireccionales se comportan como enlaces virtuales punto a punto.

*b) Tuneleado Automático (**Automatic Tunneling**)*

Los *túneles automáticos*, descritos en el RFC2893, se utilizan como los túneles configurados para comectar hosts o redes IPv6 separados. Se crean cuando se necesitan y se disuelven cuando ya no más son necesarios. Los *túneles automáticos* típicos se emplean entre hosts individuales o entre redes donde solo incidentalmente hay una necesidad para intercambio de tráfico. Un pre-requisito para usar *túneles automáticos* es la existencia de direcciones compatibles con IPv4 para los hosts IPv6 que necesitan intercomunicación. Estas direcciones permiten a los hosts derivar las direcciones IPv4 de los puntos extremos del túnel de las direcciones IPv6.
En el *tuneleado automático*, la dirección del punto extremo de túnel se determina por la dirección de destino compatible con IPv4 del paquete IPv6 que se tunelea. El *tuneleado automático* permite que nodos duales IPv4/IPv6 se comuniquen sobre infraestructura de ruteo IPv4 sin túneles pre-configurados.
A nodos IPv4/IPv6 que soportan *tuneleado automático* le son asignados direcciones compatibles con IPv4 exclusivamente. Una dirección compatible con IPv4 se identifica por un prefijo de 96 bits todos ceros, y contiene una dirección IPv4 en los 32 bits menos significativos. La estructura de una dirección compatible con IPv4 se ilustra en la figura 13.B.12.

← 96 bits →	← 32 →
0:0:0:0:0:0	Dirección IPv4

***Figura 13.B.12:** Formato de dirección IPv6 compatible con IPv4.*

Un nodo debería ser configurado con una dirección compatible con IPv4, solamente si está preparado para aceptar paquetes IPv6 destinados a esa dirección encapsulada en paquetes IPv4 destinados a la dirección embebida en IPv4.

*c) Túnel 6a4 (**6to4**)*

La herramienta *6a4*, descrita en el RFC3056, es aplicable a la interconexión de dominios IPv6 aislados en un mundo dominado por IPv4. El router de frontera del dominio IPv6 crea un túnel al otro dominio. Los puntos extremos IPv4 del túnel se identifican en el prefijo del dominio IPv6. Este prefijo, reservado para este mecanismo 6a4, es de la forma *[2002]::/*16, el cual es completado por los 32 bits de la dirección externa del router de frontera del sitio y dando como resultado que se deriva automáticamente un prefijo de 48 bits para el sitio como se muestra en la figura 13.B.13.

2002	Dir. IPv4 externa del router de frontera		
← 16 →	← 32 →	← 16 →	← 64 →
← 48 →			

***Figura 13.B.13 :** Estructura de dirección 6a4.*

Con este mecanismo, los sitios pueden iniciar el despliegue de IPv6 sin tener que pedir espacio de direccionamiento IPv6 de algún registro. Es también invaluable que reduzca a cero la administración de túneles en ausencia de un Proveedor de IPv6 (ISP).
En la figura 13.B.14 se describe un ejemplo de un proceso 6a4 en el cual el host A envia un datagrama IPv6 al host B cuya dirección sería tal como *2002:DIRv4_2$_{16}$::/48*. Cuando el router 6a4 de frontera R1 recibe el datagrama con la dirección de destino *2002:DIRv4_2$_{16}$::/48*, la cual comienza con *2002*, se extrae la dirección IPv4 de los 32 bits siguientes a *2002* en la dirección destino, y luego reenvía el paquete IPv6 encapsulado en un paquete IPv4 a R2. La dirección IPv4 fuente del paquete encapsulado es la dirección de R1. R2 recibe el paquete IPv6 encapsulado en IPv4, lo desencapsula y lo reenvía al host B.

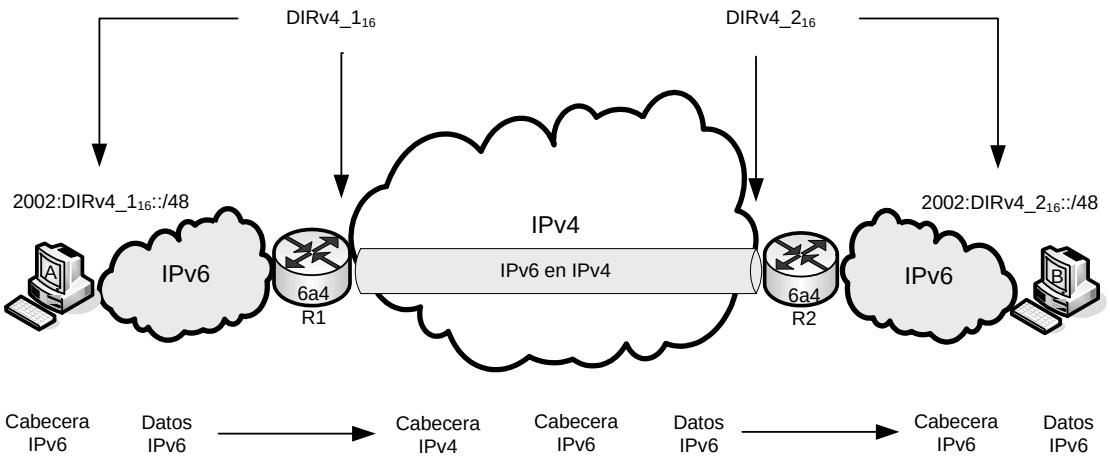


Figura 13.B.14: *Esquema de túnel 6a4 de router a router*

*d) Túnel 6sobre4 (**6over4**)*

El mecanismo 6sobre4, descrito en RFC (2529), se utiliza para interconectar hosts IPv6 aislados en un sitio a través del encapsulamiento de IPv6 en IPv4 sin el uso de túneles explícitos. Se crea un enlace virtual utilizando un grupo IPv4 multicast con un ámbito organizacional local. Las direcciones IPv6 multicast son mapeadas en direcciones IPv4 para ser capaces de realizar *Descubrimiento de vecinos.* Para rutear entre el Internet IPv6 y el dominio 6sobre4 en una organización, un router necesita ser configurado como 6sobre4 en al menos una interfaz.
Los paquetes IPv6 son transmitidos en paquetes IPv4 cuyas cabeceras contienen las *direcciones fuente y destino*. El cuerpo del paquete IPv4 contiene la cabecera IPv6 seguida inmediatamente por la *carga útil*. (Figura 13.B.15)

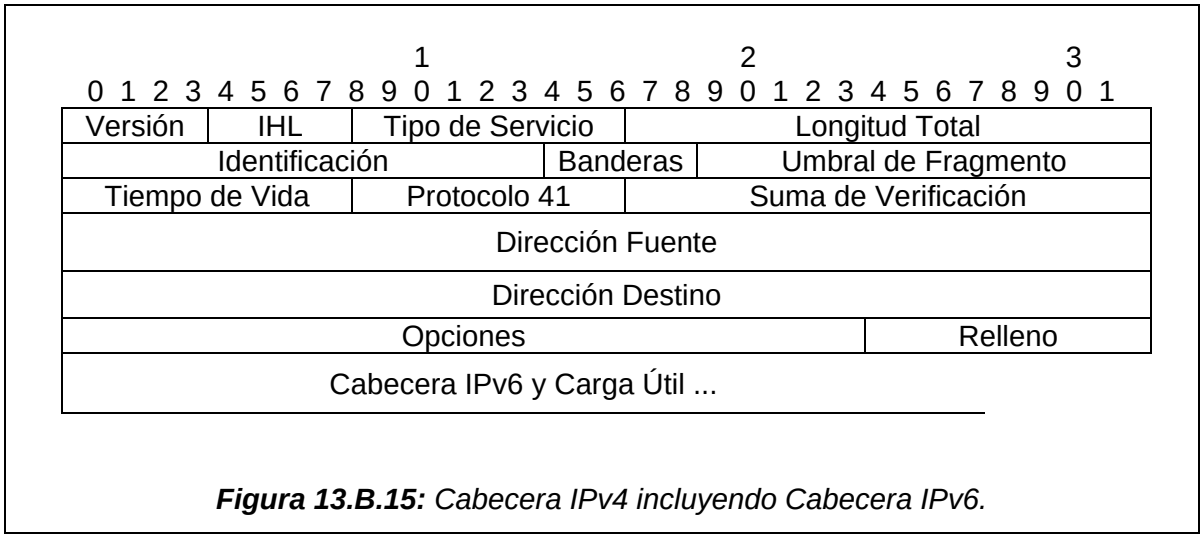


Figura 13.B.15: *Cabecera IPv4 incluyendo Cabecera IPv6.*

El procedimiento para mapear direcciones IPv6 en direcciones IPv4 virtuales de capa de enlace es el mismo que se describe en la sección 5.F.2 denominado como *determinación del próximo salto* y que al aplicarlo permite a un sitio operar con ambos protocolos en coexistencia, sin tener que configurar hosts IPv6 ya sea con direcciones compatibles con IPv4 o mediante túneles. La condición es que las interfaces tanto de hosts como de routers estén preparadas para este mecanismo. Hay que agregar que con esto no se resuelve el problema de conectar un usuario aislado al Internet global IPv6.

*e) Negociador de Túneles (**Tunnel Broker**)*

La configuración de túneles requiere cooperación de las dos partes que se comunican para fijar los puntos extremos correctos del túnel en cuestión. El modelo de *negociador de túneles*, que se desarrolla en el RFC3053, es un concepto para ayudar a la gente a recoger la información necesaria para configurar los túneles. Un *negociador de túneles*, que en la práctica es el papel que juegan servidores dedicados, puede ser visto como una conectividad ofrecida por un proveedor de IPv6 (ISP) a través de túneles de IPv6 sobre IPv4.

Las implementaciones más comunes son herramientas basadas en la web que permiten la configuración interactiva de un túnel IPv6 sobre IPv4. Al solicitar un túnel, el host obtiene una dirección IPv6 asignada fuera del espacio de direccionamiento del proveedor del túnel. El DNS será actualizado automáticamente. El túnel creado proveerá conectividad IPv6 entre el entorno IPv6 del proveedor del túnel y el host aislado.

El *negociador de túneles* se ajusta bien a pequeños sitios IPv6 aislados, especialmente hosts IPv6 aislados en el Internet IPv4, que desean conectarse fácilmente a una red IPv6 existente.

El modelo de *negociador de túneles* está basado en un conjunto de elementos funcionales representados en la figura 13.B.16.

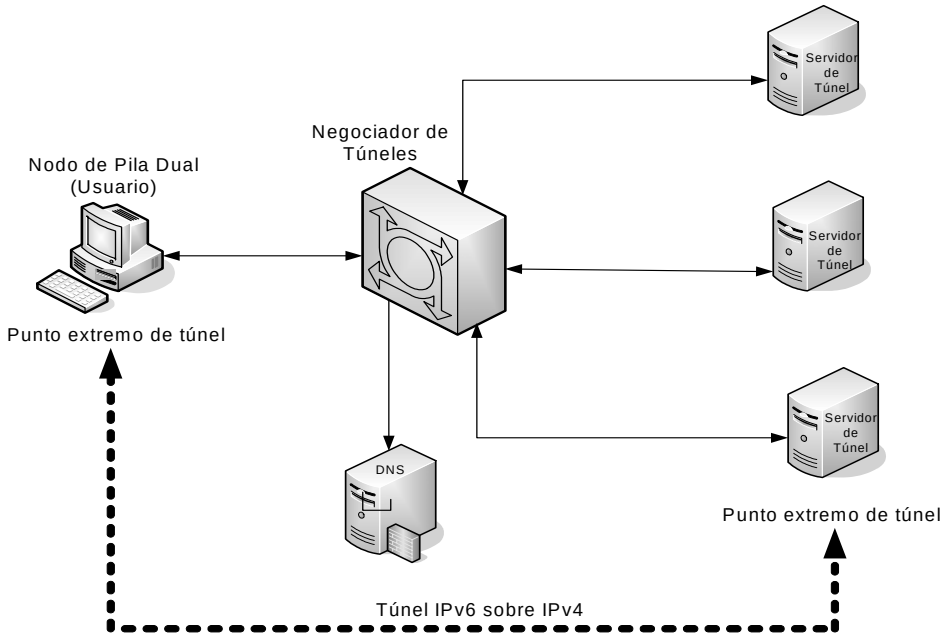


Figura 13.B.16: *El modelo de Negociador de Túneles.*

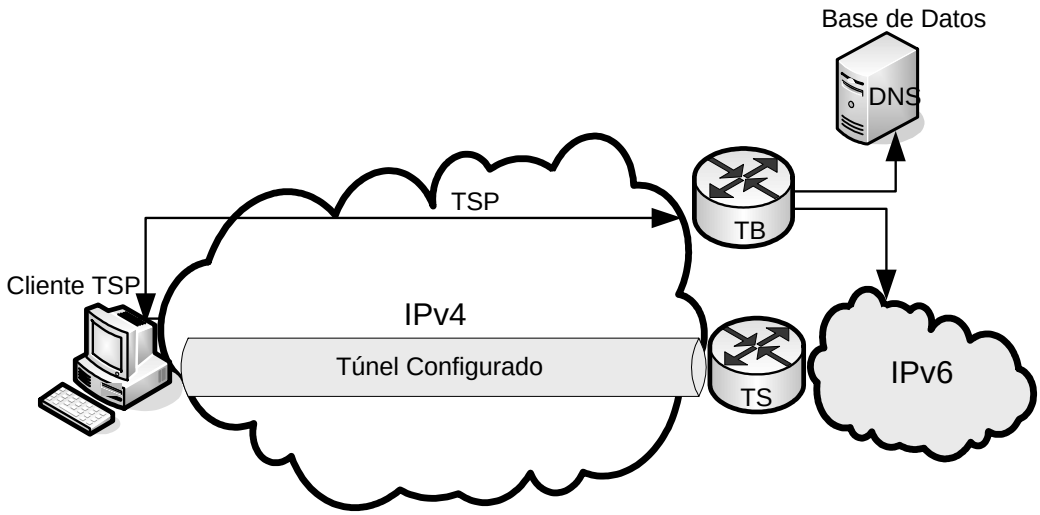
El *negociador de túneles* (TB) es el lugar donde el usuario se conecta para registrar y activar túneles. El TB gestiona la creación, modificación y supresión de túneles en representación del usuario.
Un servidor de túnel (TS) es un router de pila dual (IPv6 e IPv4) conectado al Internet global. En adición a recibir una orden de configuración del TB, crea modifica y borra el lado de servidor de cada túnel. También mantiene estadísticas de uso para cada túnel activo.

*f) Protocolo de establecimiento de túneles (**TSP**)*

Un *TB* con el *TSP* habilita el establecimiento de túneles de varios protocolos interiores tales como IPv6 o IPv4, dentro de varios paquetes de protocolo exteriores, tales como IPv4, IPv6 o UDP sobre IPv4 para NAT IPv4 transversal. El TSP[28], que es una versión mejorada del modelo TB, es usado por el cliente del túnel para tratar sobre el túnel con el negociador. Un nodo móvil implementando TSP puede ser conectado con ambas redes IPv4 e IPv6 aunque sea sólo para IPv4, IPv4 detrás de un NAT o sólo para IPv6. UN TB puede terminar los túneles en servidores de túnel remotos o en el mismo.
La conexión TSP puede ser establecida entre dos nodos, donde cada nodo puede controlar un punto extremo del túnel.
Los nodos involucrados en la estructura de trabajo son: (Figura 13.B.17)

i) El cliente TSP
ii) Punto extremo de túnel cliente
iii) El servidor TSP
iv) Punto extremo de túnel servidor

[28] Desarrollado en el borrador *draft-blanchet-v6ops-tunnelbroker-tsp-03.*



FFigura 13.B.17: *TSP usado en el modelo de Negociador de Túneles.*

En su modelo más simple, un nodo es el cliente configurado como un punto extremo de túnel y el segundo nodo es el servidor configurado como el otro punto extremo del túnel. Este modelo se ilustra en la figura 13.B.18.

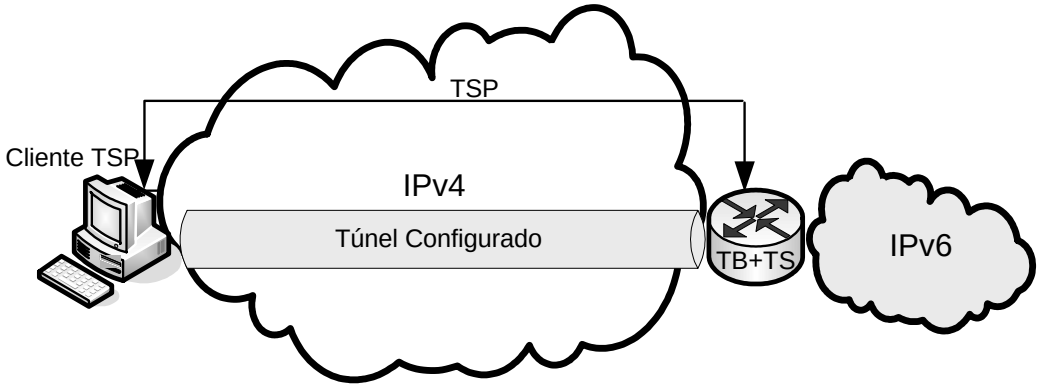


Figura 13.B.18: *TSP usado en el modelo de Servidor de Túnel.*

Desde el punto de vista de un sistema operativo, TSP es implementado como una aplicación cliente que es capaz de configurar parámetros del sistema operativo.

*g) Túnel BGP (**BGP Tunnel**)*

El propósito de esta propuesta[29], conocida como *Túnel BGP*, es interconectar islas IPv6 sobre una nube IPv4 habilitada para *Conmutación de Etiquetas Multi-Protocolo (MPLS)* (RFC 3031). Esta idea descansa en *routers de frontera de proveedor de IPv6 (6PE)*, los cuales son de pila dual con el objeto de conectar a islas IPv6 y a la red de núcleo *MPLS* que es requerida solamente para correr MPLS IPv4. Los routers *6PE* intercambian la información de alcanzabilidad transparentemente sobre el núcleo empleando el *Protocolo de Pasarela de Frontera Multi-Protocolo (MP-BGP)* sobre IPv4. Al hacer esto, se utiliza el campo *BGP* de *Próximo Salto* para transferir la dirección IPv4 del router *6PE* de tal manera que los caminos conmutados de etiquetas *MPLS* señalizados para IPv4 puedan usarse sin configuración de túnel explícito.
Una isla IPv6 es una red operando en IPv6 en forma nativa. Un típico ejemplo sería un sitio IPv6 de un cliente conectado a través de su propio router de frontera (*CE*) a uno o más routers de frontera de pila dual del proveedor de servicio IPv6 (*6PE*), los cuales están conectados a una red de núcleo *MPLS* IPv4 (Figura 13.B.19).

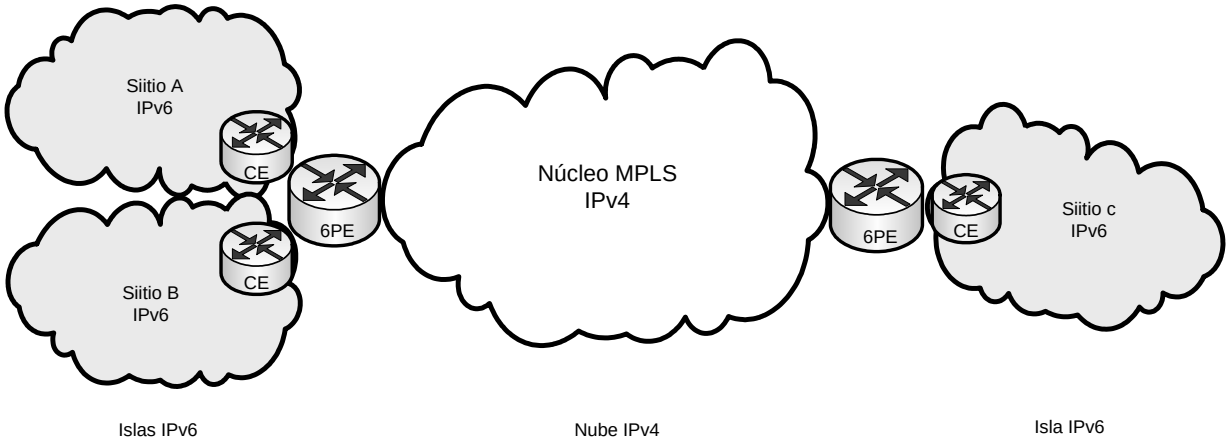


***Figura 13.B.19:** Ejemplo de interconexión aplicando el Túnel BGP.*

El método aplica a un proveedor (ISP) que tiene una red MPLS IPv4 y está familiarizado con *BGP* (posiblemente ofreciendo ya servicios VPN BGP/MPLS) y que desea ofrecer servicios IPv6 a algunos de sus clientes. Sin embargo, el proveedor puede no desear todavía actualizar su núcleo de red a IPv6 ni utilizar *tuneleado IPv6 sobre IPv4 (6sobre4)*. Con la propuesta *6PE*, el proveedor solamente tiene que actualizar algunos de sus routers de frontera (*PE*) para operaciones de pila dual de tal modo que se comporten como routers *6PE*.

*h) Protocolo de Direccionamiento de túneles automáticos dentro de un sitio (**ISATAP**)*

Mediante *ISATAP*, desarrollado en el RFC4214, se conectan automáticamente host y routers sobre redes IPv4 de un mismo sitio. *ISATAP* ve la red IPv4 como una capa de enlace para IPv6 y ve otros nodos en la red como potenciales hosts o routers IPv6. *ISATAP* soporta una abstracción de tuneleado automático similar al modelo de *Acceso Múltiple sin Difusión (NBMA)*.
El mecanismo requiere que la dirección IPv4 del nodo a conectarse, que puede o no ser global, sea embebida en los últimos 32 bits del identificador de interfaz de su dirección

[29] Desarrollada en el borrador *draft-ooms-v6ops-bgp-tunnel-06.*

IPv6. Como se observa en la figura 13.B.20 el formato de una dirección *ISATAP* está formado por 64 bits de prefijo, seguidos de 32 bits reservados por IANA para *ISATAP*, terminando con los 32 bits de la dirección IPv4 embebida.

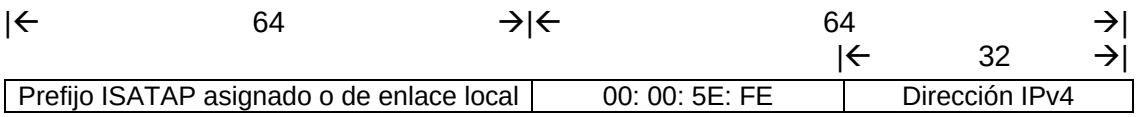


Figura 13.B.20: *Formato de dirección ISATAP.*

En la figura 13.B.21 se muestra un esquema de un ejemplo de implementación de *ISATAP* en un sitio. Los hosts A y B tienen el mismo prefijo de enlace y son de pila dual habilitados para *ISATAP*, mientras que C se encuentra en un entorno IPv6 y no está habilitado para *ISATAP*. El router por defecto es R1, el cual es de pila dual y está habilitado para *ISATAP*.

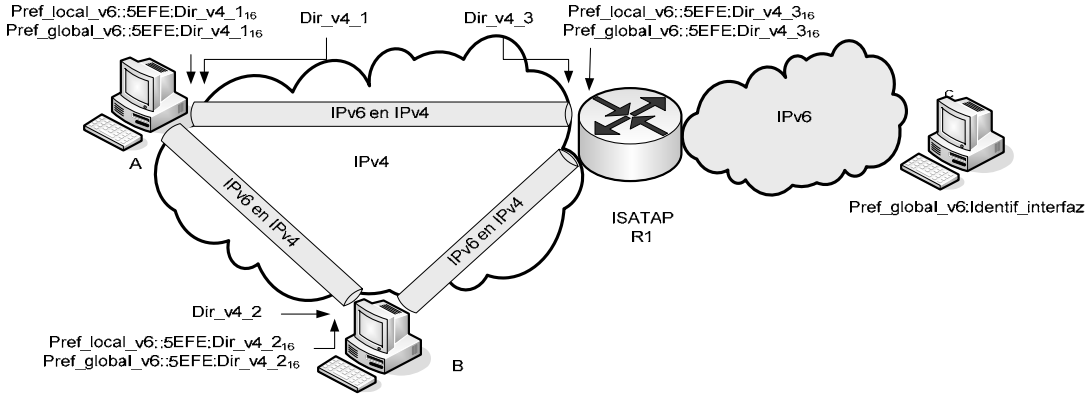


Fig. 13.B.21: *Ejemplo de aplicación de ISATAP*

A, B y R1 pueden formar un enlace virtual con direcciones de enlace local basadas en el formato *ISATAP*: Pref_local_v6::5EFE:Dir_v4_1_{16}, Pref_local_v6::5EFE:Dir_v4_2_{16}, Pref_local_v6::5EFE:Dir_v4_3_{16}. Con la cuales puede haber comunicación entre nodos en el mismo enlace a través del *descubrimiento de vecinos.* O bien, se le puede asignar una dirección global a todo el enlace virtual sobre la red IPv4 y crear un enlace virtual que incluye al nodo C no habilitado para *ISATAP*. Las direcciones globales de A, B y R1 siempre serían construidas al formato *ISATAP* y serían: Pref_global_v6::5EFE:Dir_v4_1_{16}, Pref_global_v6::5EFE:Dir_v4_2_{16}, Pref_global_v6::5EFE:Dir_v4_3_{16}. De esta manera, cualquier nodo, A o B, puede comunicarse con C con IPv6 sobre IPv4, siempre a través de *descubrimiento de vecinos.*

Es importante notar que se necesita un router como R1 conectado a la red IPv4 para alcanzar el resto IPv6 de un mismo sitio. Además de ser el router por defecto, debe ser configurado estáticamente en cada uno de los nodos habilitados para *ISATAP* en el sitio. Asimismo, los nodos en el entorno IPv4 deben ser de pila dual para poder formar un enlace virtual en IPv6. Hay que tener en cuenta que entre más nodos habilitados para *ISATAP* sean desplegados en un sitio menos escalable será. El método *ISATAP* no es aplicable para atravesar *NAT* en su camino.

i) ***TEREDO (Shipworm)***

Desarrollado en el RFC4380 y denominado *Teredo* por el nombre de un bicho de agua salada que horada la madera de los botes, es un servicio que posibilita que nodos ubicados detrás de uno o más *NATs* obtengan conectividad a IPv6 tuneleando paquetes sobre UDP.
Teredo se basa en un conjunto de componentes que interactúan entre sí, como se muestran en la figura 13.B.22.

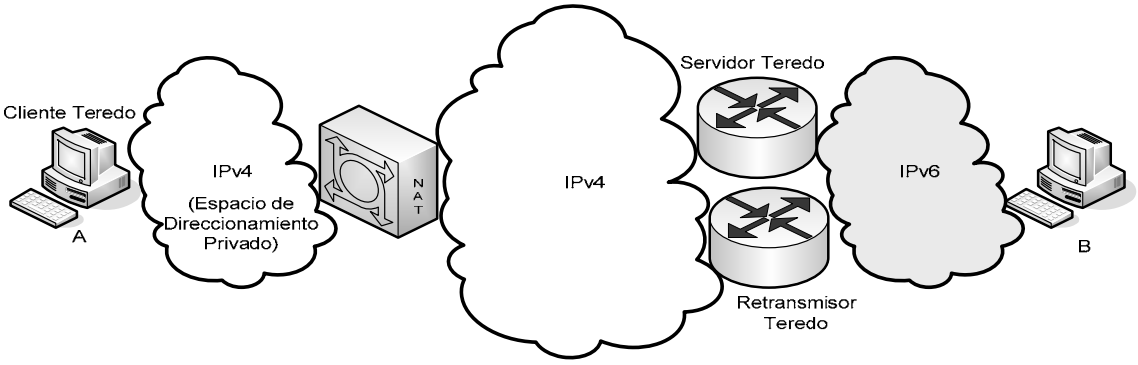


Figura 13.B.22: *Componentes Teredo.*

Donde:
i) *Cliente Teredo*: nodo que tiene algún acceso al Internet IPv4 y desea obtener acceso al Internet IPv6.
ii) *Servidor Teredo*: nodo que acceso al Internet IPv4 a través de una dirección ruteable globalmente, y que utilizado como un colaborador para proveer conectividad IPv6 a *clientes Teredo*.
iii) *Retransmisor Teredo*: router IPv6 que puede recibir tráfico destinado a *clientes Teredo* y reenviarlo utilizando el *servicio Teredo*.

Así como en el mecanismo 6a4, el *servicio Teredo* utiliza un prefijo especial para brindar una dirección IPv6 a los nodos, la cual tiene cinco componentes que se muestran en la figura 13.B.23.

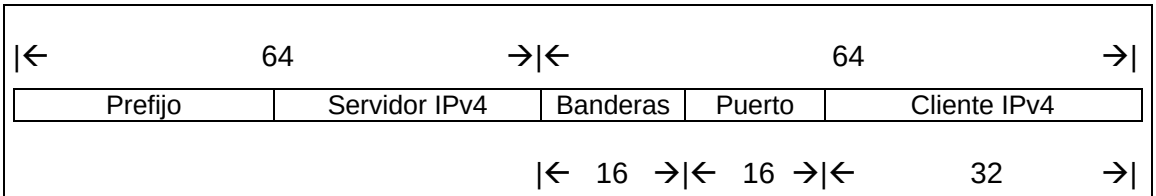


Figura 13.B.23: *Formato de dirección Teredo.*

Donde
i) *Prefijo*: prefijo de 32 bits del *servicio Teredo*.
ii) *Servidor IPv4*: dirección IPv4 del *servidor Teredo*.
iii) Banderas: conjunto de 16 bits que documenta el tipo de dirección y NAT.
iv) *Puerto*: puerto UDP mapeado del *servicio Teredo* en el cliente.
v) *Cliente IPv4*: dirección IPv4 mapeada del cliente.

Este servicio pretende encontrar un camino óptimo a los paquetes aún a través de NATs en la ruta. Los nodos IPv6 involucrados deben ser de pila dual, pues son los que implementan *Teredo*. La dirección IPv4 del *servidor Teredo* debe ser configurada estáticamente en todos los *clientes Teredo*.

C. PREPARACIÓN PARA LA TRANSICIÓN.

Lo primero que hay que hacer para llevar a cabo una transición exitosa es asegurarse de que todo el personal de TIC esté bien entrenado y que la empresa o institución tenga un lugar independiente para probar tanto el equipo como los conceptos alrededor del manejo de IPv6. Un adiestramiento adecuado no está demás aún para el personal más versado para IPv4.

1) Aprendizaje IPv6.

En buena parte de los conceptos, IPv4 e IPv6, son prácticamente similares y no serán extraños para los profesionales en redes. Conceptos tales como el formato y la generación de paquetes, ruteo y transporte de paquetes y otros. Pero hay también conceptos nuevos o replanteados que deberían ser revisados detenidamente para un uso ulterior adecuado. Conceptos como la autoconfiguración, el descubrimiento de vecinos y la planificación del direccionamiento y subneteo entre otros.

Por lo anterior, es una pérdida sustancial de tiempo y de esfuerzos, enfrentarse a una primera aproximación o a un despliegue inicial de IPv6 sin antes haber tenido un refuerzo de todos estos conceptos tanto teórico como experimentalmente, más si se piensa que en una empresa o institución deben cuidarse los escasos recursos con que a veces cuentan.

El entrenamiento en cuestión debe contar con el aporte de diferentes disciplinas, de tal manera que la comprensión sobre el diseño de redes IPv6 sea en todos los niveles: compresión general del protocolo, estrategias y métodos de transición, e instrucción especializada en algunos tópicos específicos como ruteo, DNS, y arquitectura de direccionamiento. En el caso del personal orientado al área administrativa de las redes, éste debe adquirir mucha experiencia práctica con los dispositivos de red: routers, switches, cortafuegos (firewalls), servidores, etc, de tal modo que pueda desenvolverse con los procedimientos de soporte y configuración de estos equipos.

2) Laboratorio de pruebas IPv6.

El área independiente donde el personal de TIC tendría que recibir entrenamiento sobre IPv6 debe seguir algunas pautas en su diseño. Debe considerarse su adecuación a los requerimientos del negocio y tratar de que el personal en entrenamiento pueda entender el manejo de los componentes y arquitectura usuales dentro de la empresa e institución, o bien, si se pretendiera una renovación y rediseño, el área de pruebas debiera así reflejarlo. Ante todo, el diseño de un laboratorio de pruebas de IPv6 debería cumplir con las siguientes características:

a) Flexibilidad: debe contarse con áreas independientes dentro del laboratorio de forma que puedan probarse diferentes componentes o versiones de software sin interferir otras pruebas.
b) Aislamiento: el laboratorio debería estar separado del entorno de producción, de tal manera que los continuos cambios de configuraciones no afecten el desempeño de la organización o viceversa.
c) Patrocinio comercial: si fuera posible se puede buscar patrocinio de algún proveedor de equipos o software con el objeto de probar su desempeño en redes IPv6 de prueba y así obtener beneficio mutuo.
d) Interoperatividad: deben probarse diferentes tipos de componentes de hardware y distintas versiones de software, de tal modo que se puedan visualizar sus fortalezas en operación sin una dependencia específica por un proveedor, y así

obtener patrones de implementación que se ajusten con las posibilidades y la naturaleza del negocio.

Las áreas especializadas que debe cubrir un laboratorio de esta naturaleza son:

a) Infraestructura de red: deberá incluir al menos un router de núcleo (pasarela), un router de frontera, dos o tres switches multicapas, y un cortafuego compatible con IPv6.
b) Sistemas operativos de red: además del S. O. en uso en la red institucional, debe incluirse otros para probar su interoperatividad. Sistemas tales como Linux en sus diferentes distribuciones, diferentes versiones de Windows y otros.
c) Servicios de red: se deben incluir servicios como DNS (estático y dinámico), DHCPv6, HTTP, Seguridad, y Administración de red entre otros.

D. PLANEACIÓN DE LA TRANSICIÓN.

La planeación es crucial para llevar a cabo una transición libre de problemas, en donde un sinnúmero de variables pueden presentarse, pero son dos las más importantes. Una es la planeación sobre la obsolescencia de los activos físicos y software que puedan afectar el paso de la transición y que hagan surgir la necesidad de compras para sustituir éstos. Esto afecta sensiblemente, pues dependiendo del estado de la transición y dependiendo de la estrategia tomada para hacerlo, en el camino pueda que se necesiten o no algunos componentes y se tenga que desechar algunos y sustituirse por otros. Así por ejemplo, si se emplean herramientas de traducción (p. ej. NAT-PT) al inicio, pueda ser que en un momento dado algunos componentes queden fuera de servicio y al sustituirse ya no sean necesarias las herramientas de traducción y se opte por una estrategia de tuneleado.

La otra variable sería la necesidad de implementar una decisión arquitectónica sobre flujos de tráfico en la red en transición, que tiene que ver con los servicios como el ruteo, correo electrónico y otros, y que implique un sinnúmero de validaciones y políticas en el manejo de la red. Todo esto implica que los administradores estén suficientemente capacitados para anticipar el surgimiento de estas dificultades, y como todo buen proyecto de TIC, la planificación es fundamental para llegar a la meta.

E. MIGRACIÓN A IPV6.

La migración es el punto de partida del proyecto de transición. Es el momento en que la empresa o institución está lista para comenzar el proceso gradual de la transición de una red IPv4 a una red completamente IPv6. El propósito es llevar la transición sin interrumpir las operaciones corrientes en IPv4. Los siguientes pasos forman parte de un proceso lógico para estar listos para iniciar la migración a IPv6:

1) Actualización del entorno DNS.
   Debe tenerse en cuenta que algunas implementaciones de DNS para IPv6 proveen soporte para los registros AAAA y A6 pero no responden consultas DNS a través del protocolo IPv6 sino IPv4. Esto limita la capacidad del cliente para seleccionar que dirección utilizar para este proceso. Esto puede ser un problema cuando el estado de la transición avanza y el entorno cambia, por lo que este es un aspecto a tener en cuenta.
2) Actualización de la estructura de red.
   Todos los componentes de la estructura de la red institucional deben ser actualizados para operar tanto en IPv6 como en IPv4 durante el proceso de transición, lo cual debe ser delineado con anticipación y verificado en el camino
3) Esquema del plan.
   Debe delinearse el plan de transición de manera que pueda ser sometido a evaluación al inicio de la migración como una lista de verificación de actividades a completar.
4) Obtención de componentes actualizados.
   Una vez el plan está en su punto, deben colectarse todos los componentes y el software necesario de acuerdo a los requerimientos del plan.

F. TRANSICIÓN A IPV6.

Este es el punto de quiebre, en el que la red verdaderamente está lista y concretiza el proceso de transición a una red con capacidad para manejar tanto IPv4 como IPv6. En este momento lo que surge del plan concebido a iniciar la migración es una calendarización de las actividades a realizar, dejando especificado cuál sería el plan de contingencia que se tomaría en caso de no completar una actividad La ejecución que se tienen que realizar en esta fase final se llevaría a cabo de la siguiente manera:

a) Habilitar una pila dual (IPv4/IPv6) en todos los servidores.
Una vez cubiertas las etapas anteriores, se está listo para habilitar IPv6 en los sistemas operativos de todos los servidores en adición a IPv4, así como verificar que todas las aplicaciones disponibles en los servidores sean compatibles y configuradas adecuadamente. En una red empresarial típica se debe reservar un bloque de direcciones de su esquema de direccionamiento para la configuración estática de servidores en el DNS, dejando a los clientes que utilicen autoconfiguración.

b) Desplegar clientes habilitados para IPv6.
Ya cubierto lo anterior, las nuevas estaciones de clientes deberán irse desplegando con solo soporte IPv6, mientras que la estaciones antiguas continuarían operando con entradas para IPv4 e IPv6 en el DNS.

c) Desplazar IPv4.
Con el tiempo, las estaciones antiguas se irán retirando ordenadamente para evadir conflictos, hasta efectuar la transición completa. Los ingenieros de TIC encargados monitorearán la red institucional hasta certificar la finalización del proceso, tiempo en el cual todos los servidores serían nativos de IPv6 y así todos los dispositivos de la red, a excepción de los routers o pasarelas de frontera que todavía enlacen con redes IPv4.

14. EJEMPLO PRÁCTICO DEL PROTOCOLO IPv6.

A. INTRODUCCION.

En el presente capitulo se muestra un ejemplo práctico de la configuración del protocolo de Internet TCP/IP versión 6; los sistemas operativos seleccionados para realizar la implementación del nuevo protocolo de Internet IPv6 son Red Hat Enterprise Linux 3 y Microsoft Windows XP.

El ejemplo práctico consta de un sitio sencillo de 3 redes IPv6 en el cual se han configurados como routers para administrar y distribuir el tráfico entre dichas redes dos equipos que tienen instalados el sistema operativo Red Hat Enterprise Linux 3 y que poseen dos tarjetas de red para conectar dos redes distintas. También se han configurado a los extremos de las redes dos equipos que tienen instalados el sistema operativo Windows XP y que funcionan como hosts.

Uno de los routers ha sido configurado como el router de frontera y en el se han instalado los servicios de Encaminamiento, Resolución de Nombres de Dominio, Web, Transferencia de Archivos. Mientras que el otro router solo posee el servicio de Encaminamiento.

A continuación se detallan todos los procedimientos necesarios para la configuración del protocolo de Internet TCP/IP versión 6 en los equipos que funcionan como routers y como en hosts.

B. DISEÑO DE LA RED.

1) Asignación de la dirección global de enlace.
Para este ejemplo se utilizara la dirección IPv6 global de enlace:

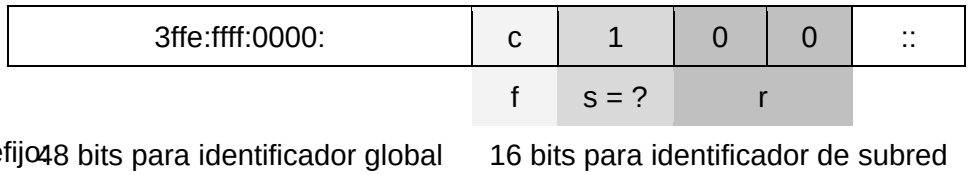
3ffe:ffff:0000:c000:0000:0000:0000:0000/52 de tipo Unicast

Simplificando los campos de la dirección IPv6 podemos especificar la dirección de la siguiente forma:

3ffe:ffff:0:c000::/52

2) Subredes del sitio.
Para el sitio que se propone en este ejemplo se necesitan crear 3 subredes, según el procedimiento detallado en el *apartado 3.I del capitulo de Direccionamiento* en este apartado se plantea el siguiente procedimiento par la determinación de subredes.

1. Determinar el número de bits a utilizar en el subneteo.



Donde:
f = Número de bits del prefijo de la dirección fijados por el nivel previo en la jerarquía.
s = Número de bits utilizados para subnetear el nivel en cuestión de jerarquía.
r = Número de bits remanente para el próximo nivel hacia abajo en la jerarquía.

2. Enumeración de prefijos de la dirección subneteada.

a. Se calcula *f* que es el número de bits dentro del identificador de subred que ya ha sido fijado:
f = m – 48
f = 52 – 48
f = 4

b. Se calcula *s* que es el número de bits utilizados para subnetear; Para un máximo de 3 subredes según la tabla 3.I.1 que hace referencia a los indicadores del número de bits utilizados para subnetear según el número de subredes requeridas. Se tiene que s = 2

c. Se calcula el valor del incremento entre cada identificador de subred sucesivo.
$i = 2^{16 - (F + S)}$.
$i = 2^{16 - (4 + 2)}$.
$i = 2^{16 - 6.}$
$i = 2^{10}$.
i = 1024
Expresado en notación hexadecimal.
$i = 0 \times 400_{16}$

d. Se calcula la longitud de los nuevos prefijos de la dirección subneteada.
p = m + s
p = 52 + 2
p = 54
F = 0 x c000

3. Según los datos obtenidos se genera la tabla de subredes:

Nº de Subred	**Prefijo de dirección subneteado**	**Rango de direcciones de hosts**
1	3FFE:FFFF:0:**C000**::/54	3FFE:FFFF:0:C000::1 - 3FFE:FFFF:0:C000:FFFF:FFFF:FFFF:FFFF
2	3FFE:FFFF:0:***C400***::/54	3FFE:FFFF:0:c400::1 - 3FFE:FFFF:0:C400:FFFF:FFFF:FFFF:FFFF
3	3FFE:FFFF:0:***C800***::/54	3FFE:FFFF:0:c800::1 - 3FFE:FFFF:0:C800:FFFF:FFFF:FFFF:FFFF
4	3FFE:FFFF:0:***CC00***::/54	3FFE:FFFF:0:cc00::1 - 3FFE:FFFF:0:CC00:FFFF:FFFF:FFFF:FFFF

3) Diagrama de Red.
En la figura 14.B.1 se detalla el diagrama de red utilizado en este ejemplo práctico.

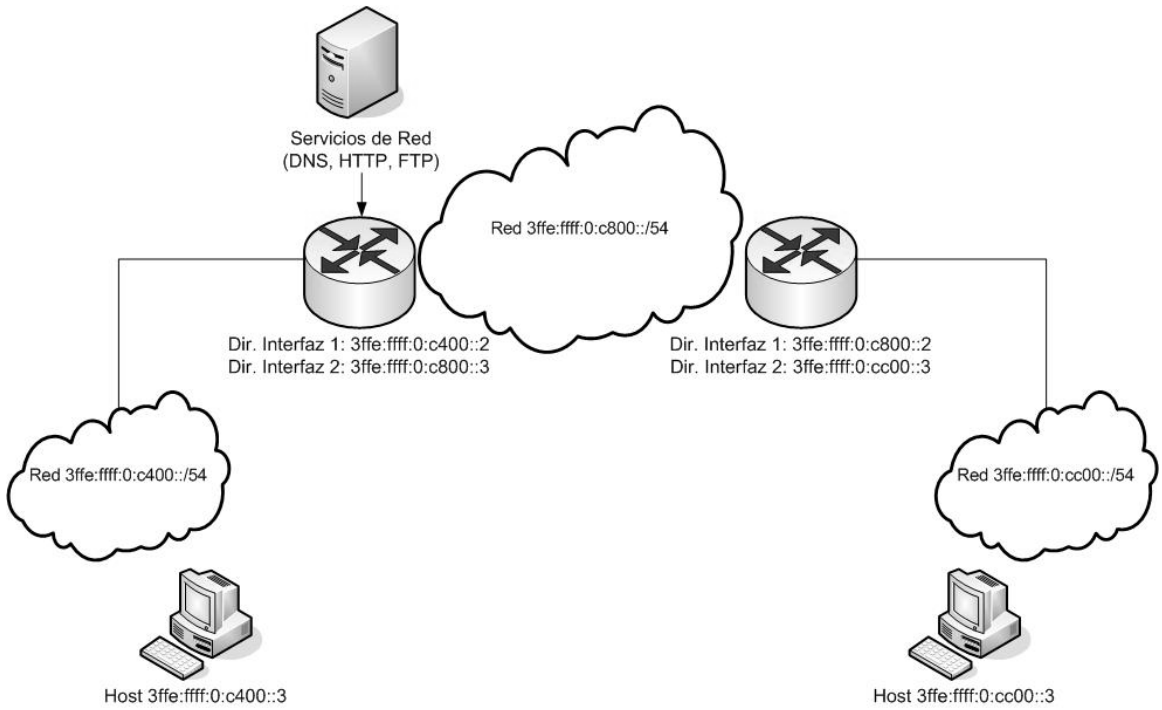


Figura 14.B.1: *Diagrama de red del ejemplo práctico.*

C. COMPROBACIÓN DEL SOPORTE DE IPv6 EN EL SISTEMA OPERATIVO.

El procedimiento a seguir con el sistema operativo *Red Hat Enterprise Linux 3* para comprobar el soporte del protocolo IPv6 es como sigue:

1. Debe asegurarse que el sistema operativo cuente con los siguientes paquetes para configurar el protocolo IPv6 y los diferentes servicios del trabajo en red:
   a. *Ifconfig*
   b. *Iproute2*
   c. *Servidor de Nombres de Dominio DNS*
   d. *Servidor Web*
   e. *Servidor FTP*

   Todas estas herramientas están incluidas en los CD's de instalación del sistema operativo Red Hat Enterprice Linux 3; si no están instalados basta con añadir las aplicaciones en el menú configuración del sistema del menú Inicio de Red Hat.

2. Se comprueba que el núcleo o kernel del sistema operativo soporta el trabajo con el protocolo IPv6. Este paso se realiza digitando el siguiente comando desde cualquier consola de Linux; si existe esta entrada quiere decir que el sistema operativo esta preparado para trabajar con este protocolo.

```
# modprobe ipv6
```

3. Para que Linux cargue de forma automática el protocolo IPv6 cuando se demande este servicio, es necesario editar el siguiente archivo.

```
alias net-pf-10 ipv6
```

4. Se verifica que se encuentren activados los valores de la cabecera IPv6 básica y extendidas así como también los diferentes protocolos con los que trabaja el estándar de Internet versión 6. Estos datos se detallan en el archivo **/etc/protocols**, y definen los valores que puede contener el campo *Siguiente Cabecera* de la cabecera IPv6. Después de abrirlo se prueban los siguientes datos.

```
# Valor que indica que la siguiente cabecera es para realizar túneles en IPv6.
ipv6            41      IPv6

# Valor que indica que la siguiente cabecera es de ruteo.
ipv6-route      43      IPv6-Route

# Valor que indica que la siguiente cabecera es de fragmentación.
ipv6-frag       44      IPv6-Frag

# Valor que indica que la siguiente cabecera es de encriptación.
ipv6-crypt      50      IPv6-Crypt

# Valor que indica que la siguiente cabecera es de autenticación.
ipv6-auth       51      IPv6-Auth

# Valor que indica que indica que la siguiente cabecera es un mensaje ICMPv6.
ipv6-icmp       58      IPv6-ICMP

# Valor que indica que no existe otra cabecera.
ipv6-nonxt      59      IPv6-NoNxt

# Valor que activa las opciones de cabecera.
ipv6-opts       60      IPv6-Optes
```

D. CONFIGURACIÓN DE LAS DIRECCIONES IPv6 EN LAS INTERFACES DE LOS EQUIPOS QUE FUNCIONAN COMO ROUTERS.

Los pasos realizados para configurar las tarjetas de red en el equipo que funciona como router, para que trabaje con direcciones IPv6 y asignarle direcciones unicast globales, son:

1. Se debe habilitar el trabajo en red con el protocolo IPv6 y definir una puerta de enlace para el router que se está configurando. Este paso se ejecuta añadiendo al archivo **/etc/sysconfig/network** las siguientes líneas.

```
NETWORKING_IPV6=yes
IPV6_GATEWAYDEV=eth1
```

2. Se habilita el protocolo IPv6 en cada tarjeta de red que conectará a cada interfaz con las que trabajará nuestro router y se asigna una dirección IP fija a cada una de ellas. Este paso se lleva a cabo añadiendo al archivo **/etc/sysconfig/networking/devices/ifcfg-eth0** las siguientes lineas:

```
IPV6INIT=yes
IPV6ADDR=3ffe:ffff:0:c400::2/54
```

3. Se edita el archivo **/etc/sysconfig/networking/devices/ifcfg-eth1** y se agrega las siguientes líneas:

```
IPV6INIT=yes
IPV6ADDR=3ffe:ffff:0:c800::2/54
```

4. En el directorio /**etc/sysconfig/network-scrpts** habrá un archivo para cada interfaz de red que se ha habilitado en las tarjetas de red al momento de cargar el sistema operativo, por lo que se debe agregar en cada archivo las siguientes líneas:
    a. Se edita el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0** y se agregan las siguientes líneas, para trabajar con la red 3ffe:ffff:0:c400::/54:

    ```
    IPV6INIT=yes
    IPV6ADDR=3ffe:ffff:0:c400::2/54
    ```

    b. Se edita el archivo **/etc/sysconfig/network-scripts/ifcfg-eth1** y se agregan las siguientes líneas, para trabajar con la red 3ffe:ffff:0:c800::/54:

    ```
    IPV6INIT=yes
    IPV6ADDR=3ffe:ffff:0:c800::2/54
    ```

    c. Se edita el archivo **/etc/sysconfig/network-scripts/ifcfg-lo** para configurar la dirección de autoretorno y se agregan las siguientes líneas:

    ```
    IPV6INIT=yes
    IPV6ADDR=::1
    ```

5. Para guardar los cambios realizados se debe reiniciar la computadora o reiniciar el servicio de red. Este último proceso se hace digitando el siguiente comando.

```
# service network restart
```

6. Se verifica que todos los cambios realizados en el sistema operativo se almacenaron satisfactoriamente, esta operación se hace introduciendo el siguiente comando.

```
# ifconfig
```

Se obtiene la siguiente respuesta de la configuración de las interfaces de red del equipo:

```
eth0        Link encap:Ethernet  HWaddr 00:A0:C9:D6:8C:20
            inet addr:172.17.2.27  Bcast:172.17.2.255  Mask:255.255.255.0
            inet6 addr: 3ffe:ffff:0:c400::2/54 Scope:Global
            inet6 addr: fe80::2a0:c9ff:fed6:8c20/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:0 (0.0 b)  TX bytes:744 (744.0 b)
            Interrupt:10 Base address:0xec00 Memory:df8ff000-df8ff038

eth1        Link encap:Ethernet  HWaddr 00:0D:87:E2:F7:97
            inet addr:172.17.3.27  Bcast:172.17.3.255  Mask:255.255.255.0
            inet6 addr: 3ffe:ffff:0:c800::2/54 Scope:Global
            inet6 addr: fe80::20d:87ff:fee2:f797/64 Scope:Link
```

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:744 (744.0 b)
          Interrupt:11 Base address:0xd400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:360 errors:0 dropped:0 overruns:0 frame:0
          TX packets:360 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28081 (27.4 Kb)  TX bytes:28081 (27.4 Kb)
```

De la información obtenida con este comando se destacan los siguientes puntos:

a. La dirección de MAC de las tarjetas de red del equipo.
   MAC de Eth0 = 00:A0:C9:D6:8C:20
   MAC de Eth1 = 00:0D:87:E2:F7:97

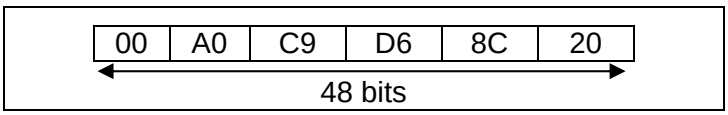
b. La dirección unicast IPv6 global para cada interfaz donde esta activado el protocolo IPv6.
   Dirección global para Eth0 = 3ffe:ffff:0:c400::2/54
   Dirección global para Eth1 = 3ffe:ffff:0:c800::2/54

c. La dirección unicast IPv6 para identificar interfaces en un enlace.

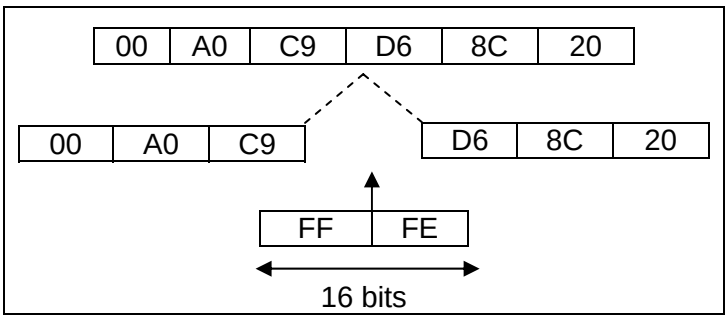
   Dirección de enlace para Eth0 = fe80::02a0:c9ff:fed6:8c20/64

   El proceso de composición del identificador de interfaz para formar una dirección MAC IPv6 es como sigue:

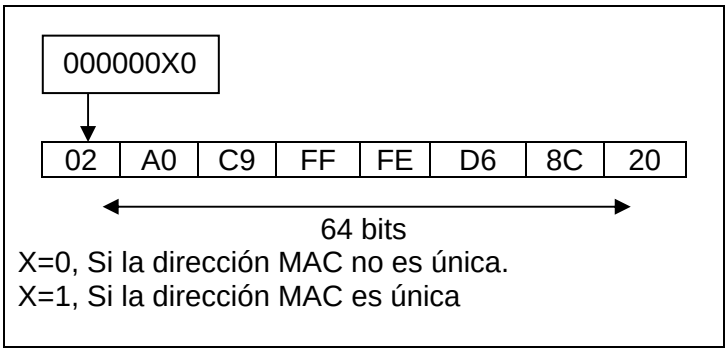
   - Dirección MAC de 48 bits.



   - Conversión de una dirección MAC de 48 bits a una dirección de 64 bits.
     En medio de la dirección de 48 bits se insertan los 16 bits (FFFE) que da una dirección de 64 bits.



- Unicidad de bit.
  El segundo bits del octeto más significativo a la izquierda sirve para declarar que la dirección MAC es única.



  Por lo tanto, se concluye que como el segundo bits del octeto más significativo es 2_{16} que tiene un valor igual a 0010_2 la dirección MAC es única.

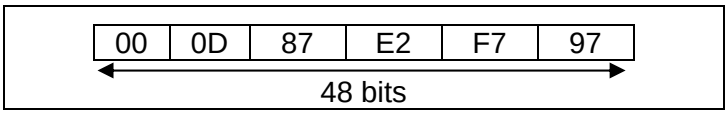
- Una vez que se tiene el identificador de interfaz se añade el prefijo de la dirección de enlace y se obtiene la siguiente dirección:

  Dirección para el identificador de interfaz = fe80::02a0:c9ff:fed6:8c20/64

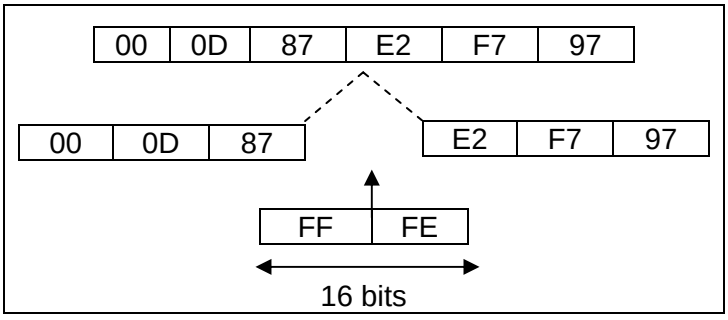
Dirección de enlace para Eth1 = fe80::020d:87ff:fee2:f797/64

El proceso de composición del identificador de interfaz para formar una dirección MAC IPv6 es como sigue:

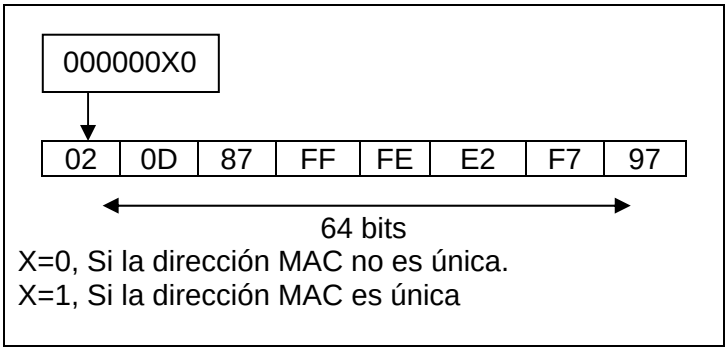
- Dirección MAC de 48 bits.



- Conversión de una dirección MAC de 48 bits a una dirección de 64 bits.



- Unicidad de bit.



Por lo tanto, se establece que como el segundo bits del octeto más significativo es 2_{16} que tiene un valor igual a 0010_2 la dirección MAC es única.

- Una vez que se tiene el identificador de interfaz se agrega el prefijo de la dirección de enlace y obtiene la dirección:

  Dirección para el identificador de interfaz = fe80::020D:87ff:feE2:F797/64

d. La máxima cantidad de datos (MTU) que se pueden transferir por unidad a través de las tarjetas de red es de 1500 octetos.

e. Dirección de autoretorno.
lo = ::1/128

7. El siguiente paso es enviar a cada una de las direcciones globales asignadas a cada interfaz de red del equipo un mensaje petición de eco (Mensaje de diagnóstico de la función Ping para determinar si un host que posee una dirección IP esta conectado a una red; este mensaje tiene un valor de 128 en el campo *Tipo* de la cabecera ICMPv6). El comando en el sistema operativo Red Hat es Ping6 <dirección de la interfaz>; se comprueba si se tiene un mensaje de respuesta a la petición de eco del comando ping6 en cada dirección IPv6 de la siguiente forma.
   a. Petición de eco para la dirección de autoretorno

```
# ping6 ::1
```

Se obtiene la siguiente respuesta

```
64 bytes from ::1: icmp_seq=0 ttl=64 time=0.057 ms
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.066 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.057/0.061/0.066/0.009 ms, pipe 2
```

Que confirma que se está trabajando correctamente.

   b. Petición de eco para la dirección de la interfaz eth0

```
# ping6 3ffe:ffff:0:c400::2
```

Se obtiene la siguiente respuesta.

```
PING 3ffe:ffff:0:c400::2(3ffe:ffff:0:c400::2) 56 data bytes
64 bytes from 3ffe:ffff:0:c400::2: icmp_seq=0 ttl=64 time=0.071 ms
64 bytes from 3ffe:ffff:0:c400::2: icmp_seq=1 ttl=64 time=0.065 ms

--- 3ffe:ffff:0:c400::2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.065/0.068/0.071/0.003 ms, pipe 2
```

Que confirma que se está trabajando correctamente.

c. Petición de eco para la dirección de la interfaz eth1

```
# ping6 3ffe:ffff:0:c800::2
```

Se obtiene la siguiente respuesta.

```
PING 3ffe:ffff:0:c800::2(3ffe:ffff:0:c800::2) 56 data bytes
64 bytes from 3ffe:ffff:0:c800::2: icmp_seq=0 ttl=64 time=0.066 ms
64 bytes from 3ffe:ffff:0:c800::2: icmp_seq=1 ttl=64 time=0.086 ms

--- 3ffe:ffff:0:c800::2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.066/0.076/0.086/0.010 ms, pipe 2
```

Que confirma que se está trabajando correctamente.

E. CONFIGURACIÓN DEL RUTEO ESTÁTICO EN LA RED.

Los pasos realizados para configurar el servicio de ruteo en el sistema operativo del equipo que se utiliza como router son los siguientes:

1. El sistema operativo Red Hat Enterprise Linux 3 no trae habilitado por defecto el servicio de ruteo por lo que lo es necesario establecer el parámetro correspondiente al ruteo del kernel de Linux. Para realizar esta acción digitamos la siguiente linea de comando.

```
# echo “1”> /proc/sys/net/ipv6/conf/all/forwarding
```

2. Posteriormente se añaden las rutas de las dos redes a las que se conectan las interfaces habilitadas en el router.
   a. Se agrega la ruta de la red que conecta la interfaz eth0 con el siguiente comando.

```
# route -A inet6 add 3ffe:ffff:0:c400::/54 dev eth0
```

   b. Se añade la ruta de la red que conecta la interfaz eth1

```
# route -A inet6 add 3ffe:ffff:0:c800::/54 dev eth1
```

3. Para este ejemplo se tiene un segundo router que tiene una interfaz que se conecta una de nuestras redes y que tiene la dirección 3ffe:ffff:0:c800::3/54 y también tiene otra interfaz que conecta lo otra subred y tiene la dirección 3ffe:ffff:0:cc00::2/54 por lo que se debe agregar la dirección de este enlace a la tabla de ruteo y además utilizar como dirección de puerta de enlace hacia esa subred la dirección de la interfaz que esta conectada a nuestra red. Para ello se utiliza el siguiente comando.

```
# ip -6 route add 3ffe:ffff:0:cc00::/54 via 3ffe:ffff:0:c800::3 dev eth1
```

4. Se verifican que las rutas se hayan agregado a la tabla de ruteo del router con el siguiente comando.

```
# route -A inet6
```

Se obtiene la siguiente respuesta.

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
::1/128	*	U	0	46	30	lo
3ffe:ffff:0:c400::/128	*	U	0	0	0	lo
3ffe:ffff:0:c400::2/128	*	U	0	13	13	lo
3ffe:ffff:0:c400::/54	*	U	0	0	0	eth0
3ffe:ffff:0:c800::/128	*	U	0	0	0	lo
3ffe:ffff:0:c800::2/128	*	U	0	16	14	lo
3ffe:ffff:0:c800::/54	*	U	0	0	0	eth1
3ffe:ffff:0:cc00::/54	3ffe:ffff:0:c800::3	U	1	0	0	eth1
fe80::/128	*	U	0	0	0	lo
fe80::20d:87ff:fee2:f797/128	*	U	0	1	0	lo
fe80::2a0:c9ff:fed6:8c20/128	*	U	0	0	0	lo
fe80::/64	*	U	256	0	0	eth0
fe80::/64	*	U	256	0	0	eth1
ff00::/8	*	U	256	0	0	eth0
ff00::/8	*	U	256	0	0	eth1

5. El router de la subred se configura de la siguiente forma.
   La dirección que se asignará la interfaz eth-1 es 3ffe:ffff:0:c800::3/54
   La dirección que se asignará a la interfaz eth-0 es 3ffe:ffff:0:cc00::2/54
   Se reinicia el servicio de red.
   Se habilita el servicio de ruteo.
   ```
   # echo “1”> /proc/sys/net/ipv6/conf/all/forwarding
   ```
   Se añade la ruta de la subred a la que se conecta la interfaz de red eth0
   # route -A inet6 add 3ffe:ffff:0:cc00::/54 dev eth0
   Se agregan las siguientes entradas a la tabla de ruteo y se asignan a la interfaz de red eth1
   # ip -6 route add 3ffe:ffff:0:c800::/54 via 3ffe:ffff:0:c800::2 dev eth1
   # ip -6 route add 3ffe:ffff:0:c400::/54 via 3ffe:ffff:0:c800::2 dev eth1

Cuando se tienen configurados estos parámetros en cada router de las dos subredes se está listo para encaminar el tráfico de datos de una subred a la otra, por ejemplo comprobamos desde el router de frontera si se puede obtener una respuesta de eco desde la dirección IPv6 de la interfaz de red 3ffe:ffff:0:cc00::2; los pasos para realizar esta petición son los siguientes:

1. Verificar que las tablas de rutas estáticas tengan las siguientes entradas.

Router de frontera		
Prefijo de red: 3FFE:FFFF:0:***c400***::/54		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
3ffe:ffff:0:c400::2	Local	0
3ffe:ffff:0:c800::3	3ffe:ffff:0:cc00::/54	1

Router de subred		
Prefijo de red: 3FFE:FFFF:0:***cc00***::/54		
Bits signif: 57		
Prox. Salto.	Enlace	Costo
3ffe:ffff:0:cc00::2	Local	0
3ffe:ffff:0:c800::2	3ffe:ffff:0:c800::/54	1
3ffe:ffff:0:c800::2	3ffe:ffff:0:c400::/54	1

2. Petición de eco a la dirección 3ffe:ffff:0:cc00::2

```
# ping6 3ffe:ffff:0:cc00::2
```

3. Al evaluar la petición del mensaje de diagnóstico de red enviado, se observa que la dirección destino se encuentra en una subred distinta a la propia. El procedimiento que se sigue para enviar el mensaje es el siguiente:
   a. Verificar que la dirección de la red donde se encuentra la dirección IPv6 destino se encuentra en la tabla de ruteo.
   b. Se procesa el paquete que se enviará a la dirección IPv6 destino y se construye un paquete que tendrá el formato que se muestra en la figura 14.E.1.

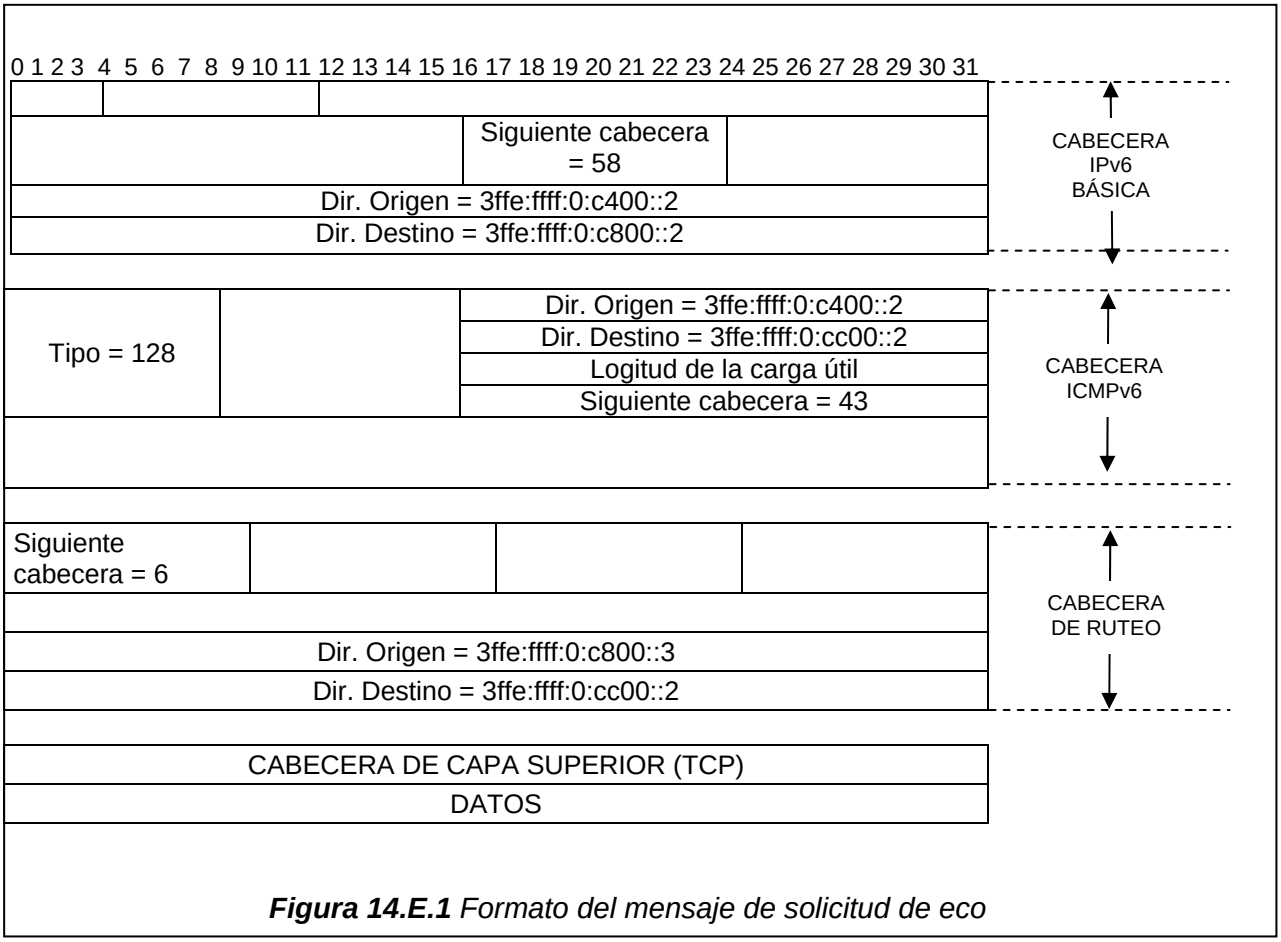


Figura 14.E.1 *Formato del mensaje de solicitud de eco*

4. Cuando el router de frontera tiene listo el paquete lo examina, y procesa primero la cabecera IP, luego la cabecera ICMPv6 y a continuación la cabecera de ruteo. En esta cabecera extendida el router cambia la primera dirección que es la del siguiente router en el camino por la dirección destino de la cabecera IP tal como se muestra en la figura 14.E.2. A continuación el router de frontera envía el paquete al router de la subred.

Paquete IPv6

Cabecera IP	Origen	3FFE:FFFF:0:***c400***::2
	Destino	3FFE:FFFF:0:***c800***::3
Cabecera ICMPv6	Origen	3FFE:FFFF:0:***c400***::2
	Destino	3FFE:FFFF:0:***cc00***::2
Cabecera de Ruteo	DirDestino	3FFE:FFFF:0:***c800***::3
	DirDestino	3FFE:FFFF:0:***cc00***::2
	Datos	

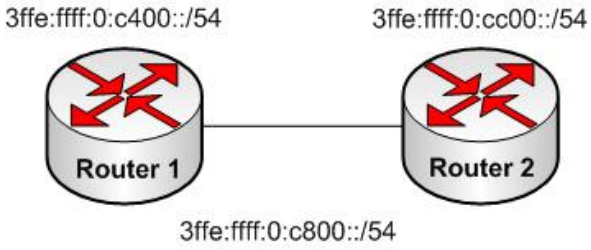


Figura 14.E.2: *Procesamiento del paquete enviado entre los routers*

5. Finalmente el router de la subred recibe el paquete y después de examinar la cabecera IP y la cabecera extendida las procesa, y luego intercambia la ultima dirección de la cabecera de ruteo por la dirección destino de la cabecera IP, y como el destino se encuentra en su mismo enlace envía directamente la petición de eco a la interfaz solicitada.

Los siguientes comandos son útiles para la administración de una red como la de este ejemplo:

1. Enviar un mensaje UDP para trazar la ruta de un paquete.

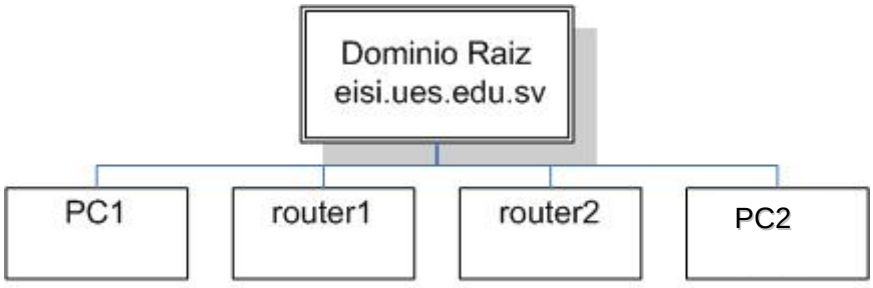
```
# traceroute6 <nombre de dominio del equipo>
```

2. Enviar un mensaje UDP para trazar el camino de un paquete desde su origen a su destino

```
# tracepath6 <nombre de dominio del equipo>
```

F. CONFIGURACIÓN DEL SERVIDOR DE NOMBRES DE DOMINIO (DNS).

El ejemplo se ha basado en la siguiente jerarquía de dominios para el sitio planteado:



Los pasos ejecutados para configurar el servidor de nombres de dominio en el equipo utilizado como router son los siguientes:

1. Configurar el servicio BIND para DNS, esto se hace editando el archivo **etc/named.conf** y agregando las siguientes zonas de configuración de servicio DNS.

```
zone "3ffe.ip6.arpa" in {
        type master;
        file "3ffe.ffff.0.zone";
        allow-transfer { any; };
};

#El formato para el DNS inverso se obtiene bit a bit. Por lo que se toma el prefijo IPv6
#invirtiendo el orden de los números y colocando un punto entre cada uno de ellos.
zone "0.f.f.f.f.e.f.f.3.ip6.int" in {
        type master;
        file "3.f.f.e.f.f.f.f.0.zone";
        allow-transfer { any; };
};

#Se proporciona el servicio DNS para el dominio eisi.ues.edu.sv
zone "eisi.ues.edu.sv" in {
        type master;
        file "eisi.ues.edu.sv.zone";
        allow-transfer { any; };
};
```

Para que BIND pueda escuchar las direcciones IPv6 se agrega el parámetro *any*.

2. Se crean los archivos de zona para añadir todos los nombres de las maquinas de la red ejemplo. Se accede al directorio **/var/named** y se generan los siguientes archivos.

    a. Se crea el archivo eisi.ues.edu.sv.zone y se edita su contenido a lo siguiente:

```
$TTL 2d
@       IN SOA          eisi.ues.edu.sv.        root.eisi.ues.edu.sv. (
                        2006062201      ; serial
                        3h              ; refresh
                        1h              ; retry
                        1w              ; expiry
                        1d )            ; minimum

# el router1 es el router de frontera y el router2 es un router de núcleo
# NS = servidor autoritario de nombres de dominio
# A = Asocia un nombre de dominio a una dirección IPv4
# AAAA = Asocia un nombre de dominio a una dirección IPv6
# CNAME = Nombre canónico para un alias utilizado al acceder a recurso
# MX = Intercambio de correo para el dominio
eisi.ues.edu.sv.        IN NS           router1.eisi.ues.edu.sv.
IN                      IN NS           router1.eisi.ues.edu.sv.
IN                      IN A            172.17.3.27
IN                      IN AAAA         3ffe:ffff:0:c800::2
IN                      IN MX           10 mail.router1.ues.edu.sv.
www                     IN CNAME        router1.eisi.ues.edu.sv.
mail                    IN CNAME        router1.eisi.ues.edu.sv.
ftp                     IN CNAME        router1.eisi.ues.edu.sv.
router1                 IN AAAA         3ffe:ffff:0:c800::2
router1                 IN A            172.17.3.27
router2                 IN AAAA         3ffe:ffff:0:c800::3
router2                 IN A            172.17.3.29
```

```
# Router1 conectada al  enlace local
IN                      IN NS           router1.eisi.ues.edu.sv.
IN                      IN A            172.17.2.27
IN                      IN AAAA         3ffe:ffff:0:c400::2
IN                      IN MX           10 mail.router1.ues.edu.sv.
www                     IN CNAME        router1.eisi.ues.edu.sv.
mail                    IN CNAME        router1.eisi.ues.edu.sv.
ftp                     IN CNAME        router1.eisi.ues.edu.sv.
router1                 IN AAAA         3ffe:ffff:0:c400::2
router1                 IN A            172.17.2.27
pc1                     IN AAAA         3ffe:ffff:0:c400::3
pc1                     IN A            172.17.2.28

# Nodo que pertenece al enlace de Router2
pc2                     IN AAAA         3ffe:ffff:0:cc00::3
pc2                     IN A            172.17.4.28
```

b. Se crea el archivo 3.f.f.e.f.f.f.f.0.zone y se edita su contenido a lo siguiente:

```
$TTL 2D
@           IN SOA      eisi.ues.edu.sv.      root.eisi.ues.edu.sv. (
                                2006062200      ; serial
                                3H              ; refresh
                                1H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

0.f.f.f.f.e.f.f.3.ip6.int.      IN NS           router1.eisi.ues.edu.sv.
```

c. Se crea el archivo 3ffe.ffff.0.zone y se edita para que contenga los siguiente:

```
$ORIGIN 3ffe.ip6.arpa.
      $TTL 2D
      @             IN SOA      eisi.ues.edu.sv.      root.eisi.ues.edu.sv. (
                          2006062104      ; serial
                          3H              ; refresh
                          1H              ; retry
                          1W              ; expiry
                          1D )            ; minimum

      IN NS router1.eisi.ues.edu.sv.

      # PTR = Puntero a otra parte del espacio de nombres de dominio
      \[x00010000000000000001/80] IN PTR router1.eisi.ues.edu.sv.
      \[x00010000000000000002/80] IN PTR router2.eisi.ues.edu.sv.


      \[x00010000000000000003/80] IN PTR pc1.eisi.ues.edu.sv.
      \[x00010000000000000004/80] IN PTR pc1.eisi.ues.edu.sv.
```

3. Finalmente se inicia el servidor de nombres de donimio DNS con el siguiente comando.

```
# service named start
```

Para comprobar que el Servidor de Nombres de Dominio se encuentra trabajando correctamente se ejecuta una petición de eco, pero en lugar de ponerle la dirección IPv6 se le asocia a la función ping6 el nombre de dominio de un equipo conectado a la red y que se encuentre especificado en la base de datos de los nombres de dominio. Este proceso se realiza digitando el siguiente comando.

```
# ping6 pc1.eisi.ues.edu.sv
```

La primera operación que se realizara es la traducción o resolución del nombre de dominio en una dirección IPv6 que pueda entender el mensaje de petición de eco. Este proceso se efectúa de la siguiente forma:

1. Se envía al servidor DNS raíz una petición para la dirección IPv6 de pc1.eisi.ues.edu.sv
2. El servidor Raíz de nuestro sitio posee la información respectiva para resolver el nombre pc1.eisi.ues.edu.sv por lo que asocia el nombre con su respectiva dirección IPv6.
3. El servidor DNS retorna la dirección IPv6 a la petición de eco realizada.
4. La petición de eco obtiene la siguiente respuesta.

```
PING pc1.eisi.ues.edu.sv(3ffe:ffff:0:c800::3) 56 data bytes
64 bytes from 3ffe:ffff:0:c800::3: icmp_seq=0 ttl=64 time=0.066 ms
64 bytes from 3ffe:ffff:0:c800::3: icmp_seq=1 ttl=64 time=0.086 ms

--- pc1.eisi.ues.edu.sv ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.066/0.076/0.086/0.010 ms, pipe 2
```

Lo que indica que el Servidor de Nombres de Dominio se encuentra trabajando correctamente.

G. CONFIGURACIÓN DEL SERVIDOR WEB HTTP

Se establece el servidor web Apache2 editando el archivo **/etc/httpd/conf/httpd.conf** de la siguiente forma.

1. Para que el servidor web Apache escuche la dirección de la puerta de enlace de nuestro router se edita la siguiente línea del archivo *httpd.conf*.

```
Listen [3ffe:ffff:0:c800::2]:80
```

2. Se escribe el correo electrónico del administrador de la red para enviar correos electrónicos en caso de algún problema con el sitio. Esta acción se realiza editando la siguiente línea en el archivo de configuración del servidor Web.

```
ServerAdmin jhony_mikel@hotmail.com
```

3. Como el router se utilizará como el servidor de nombres de dominio de la red ejemplo, se le agrega un host virtual al servidor web, el cual se empleará posteriormente si se cambia el nombre del equipo o incluso se le asigna otro dominio a la red. Para crear el host virtual se le agrega las siguientes lineas al archivo:

```
<VirtualHost [3ffe:ffff:0:c800::2]:80>
        ServerName router1.eisi.ues.edu.sv
        ServerSignature email
        DirectoryIndex  index.php index.html index.htm index.shtml
        LogLevel  warn
        HostNameLookups off
```

```
</VirtualHost>
```

4. Finalmente se incia el servidor de Web Apache2 con el siguiente comando.

```
# service httpd start
```

H. CONFIGURACIÓN DEL SERVIDOR DE TRANSFERENCIA DE ARCHIVOS (FTP).

Se configura el servidor VSFTPD editando el archivo **/etc/vsftpd/vsftpd.conf** de la siguiente forma.

1. Para que el servidor escuche la dirección de la puerta de enlace del router se edita la siguiente línea del archivo *vsftpd.conf*:

```
listen_ipv6=YES
```

2. Finalmente se inicia el servidor de de transferencia de archivos con el siguiente comando:

```
# service vsftpd start
```

I. CONFIGURACION DEL PROTOCOLO IPv6 EN EQUIPOS HOST CON EL SISTEMA OPERATIVO WINDOWS XP

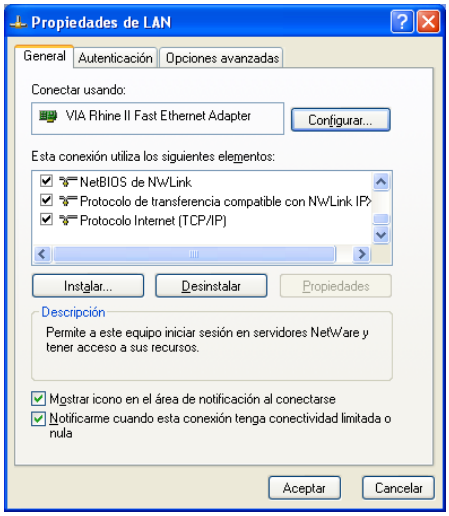
Los pasos para configurar el protocolo de Internet IPv6 en equipos con Windows XP y que funcionen como host en la red son:

1. Se debe asegurar que el sistema operativo Windows XP tenga instalado el Servipack2 y que se esté trabajando en una sesión con privilegio de administrador.

2. Dar un clic en el menú Inicio.

3. Dar un clic derecho en el icono Conexiones de Red y seleccionar la opción Propiedades en el menú emergente que aparece.

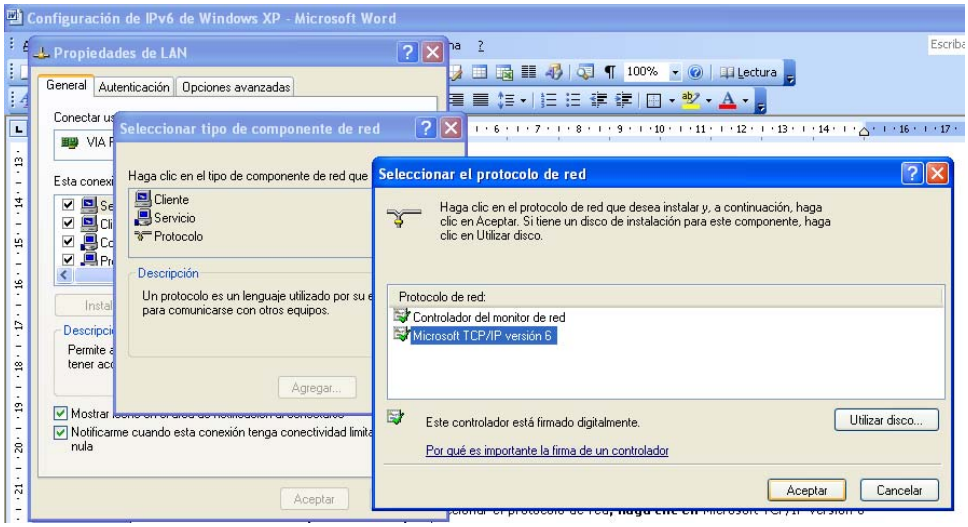
4. Seleccionar el dispositivo de red del equipo (el nombre que tiene la interfaz de red es *Conexión de área local*), luego se debe dar un clic derecho sobre este icono y se selecciona la opción *Propiedades*. Al realizar este procedimiento aparecerá la siguiente ventana.



5. Haga clic en Instalar.

6. En el cuadro de diálogo: Seleccionar tipo de componente de red, haga clic en *Protocolo* y, a continuación, en *Agregar*.

7. En el cuadro de diálogo: Seleccionar el protocolo de red, haga clic en *Microsoft TCP/IP versión 6* y, a continuación, *Aceptar*



8. Para finalizar la instalación haga clic en *Cerrar* para guardar los cambios en la conexión de red.

1) Agregar una dirección IPv6 de forma estatica.

Los pasos para agregar una dirección IPv6 de forma estática en el equipo son los siguientes:

1. Se debe dar un clic en el botón de *Inicio*

2. Luego se da un clic en la opción *ejecutar* y escribimos *cmd* para trabajar en modo consola DOS y luego presiona el botón Aceptar. Una vez cargado el símbolo del sistema se puede observar si la configuración de los dispositivos es correcta. Esto se logra digitando la siguiente línea de comando.

```
C:\> netsh interface ipv6 show interface
```

3. Para configurar la dirección IPv6 en nuestra interface de red se escribe la siguiente línea de comando.

```
C:\> netsh interface ipv6 add address “Conexión de área local” 3ffe:ffff:0:c800::3
```

2) Establecer una puerta de enlace.

Para comunicarse con equipos que pertenecen a la misma red se envía tráfico a la interfaz del router por defecto de esta red y este luego envía los paquetes a la dirección destino del paquete. Pero para comunicarse con equipos que pertenecen a otra red se necesita configurar como puerta de enlace la dirección de la interfaz del router que conecta a las otras redes y a la cual se le han agregado las entradas de la tabla de ruteo. Esto se hace escribiendo la siguiente línea de comando.

```
C:\> netsh interface ipv6 add route 3ffe:ffff:0:/48 “Conexión de área local”
nexthop=3ffe:ffff:0:c800::2 publish=yes
```

3) Establecer un Servidor de Nombres de Dominio
Finalmente queda configurar el acceso al servidor de nombres de dominio, Este procedimiento se realiza digitando la siguiente línea de comando.

```
C:\> netsh interface ipv6 add dns “Conexión de área local” 3ffe:ffff:0:c800::2
```

4) Probar los servicios de red configurados.
Se prueba el servicio de Nombres de Dominio instalado en el router de frontera y el servicio de encaminamiento instalados en los dos routers de la red. Para ello se envía un mensaje de petición de eco desde el host de la red 3ffe:ffff:0:c400::/54 al host de la red 3ffe:ffff:0:cc00::/54, este último ha sido asignado con el nombre de dominio pc2.eisi.ues.edu.sv y corresponde a la dirección IPv6 3ffe:ffff:0:cc00:3. Se escribe el siguiente comando en la ventana de símbolo de sistema de Windows.

```
C:\> ping6 pc2.eisi.ues.edu.sv
```

Se obtiene la siguiente respuesta al mensaje ICMPv6 de petición de eco.

```
PING pc2.eisi.ues.edu.sv(3ffe:ffff:0:cc00::3) 56 data bytes
64 bytes from 3ffe:ffff:0:cc00::3: icmp_seq=0 ttl=64 time=0.066 ms
64 bytes from 3ffe:ffff:0:cc00::3: icmp_seq=1 ttl=64 time=0.086 ms

--- pc2.eisi.ues.edu.sv ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.066/0.076/0.086/0.010 ms, pipe 2
```

Lo que indica que el Servidor de Nombres de Dominio se encuentra trabajando correctamente y que el servicio de encaminamiento y entrega de paquetes entre ambos routers de las subredes de nuestro sitio se están comunicando correctamente.

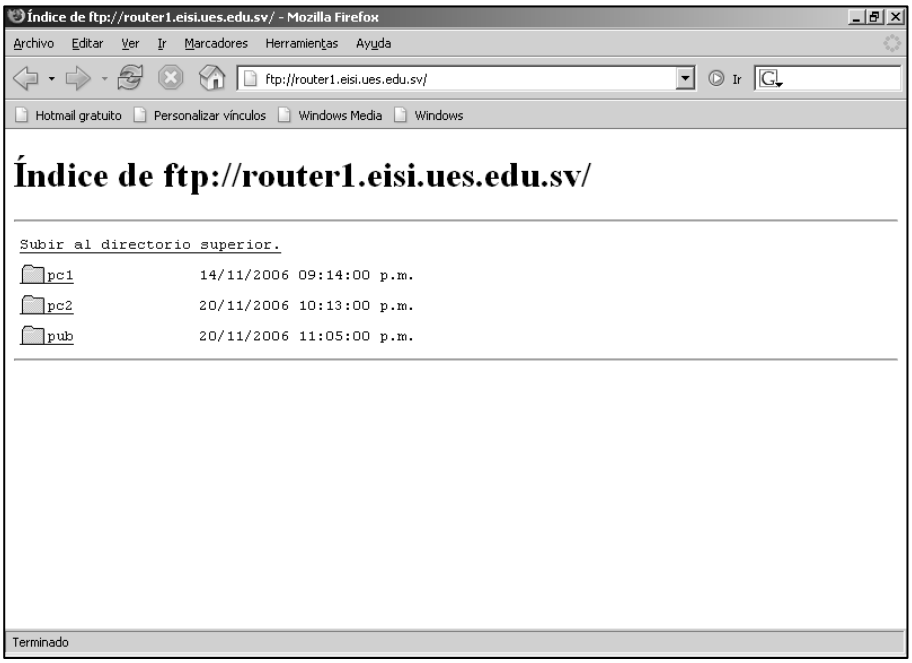
Para este ejemplo, por motivos de incompatibilidad del navegador Internet Explorer versión 6 con el protocolo de Internet versión 6, se utilizó el navegador Mozilla Firefox versión 5.0 para Windows.

Se prueba el servidor Web que se ha configurado con IPv6 realizando los siguientes pasos:

1. Abrir el Navegador Web Mozilla Firefox.
2. En la barra de búsqueda se indica al navegador que se trabajará con el protocolo de transferencia de hipertexto digitando *http://* luego el nombre del servidor Web que es **router1.eisi.ues.edu.sv/** y luego del Web sitio alojado en el servidor que es *Mikel.*
3. Nos carga el sitio Web alojado en el servidor.

Se prueba el servidor FTP que se ha configurado con IPv6 realizando los siguientes pasos:

1. Abrir el Navegador Web Mozilla Firefox.
2. En la barra de búsqueda se indica al navegador que se trabajará con el protocolo de transferencia de archivos digitando *ftp://* luego el nombre del servidor ftp que es **router1.eisi.ues.edu.sv**
3. Se carga el sitio *FTP* alojado en el servidor.



METODOLOGIA PARA IMPLEMENTAR EL PROTOCOLO DE INTERNET VERSION 6 EN EMPRESAS O INSTITUCIONES CON REDES OPERANDO APLICACIONES BASADAS EN EL PROTOCOLO DE INTERNET VERSION 4.

1. INTERFAZ SOCKET.

Los protocolos de capa superior en la pila TCP/IP (FTP, HTTP, DNS, etc.) establecen como una aplicación interactúa con los protocolos de la capa de transporte (TCP, UDP, etc.), de manera tal que dicha aplicación pueda enlazarse con un destino externo a la red. Los software de protocolo residen en el sistema operativo empleado, el cual determina los componentes y la operación de la interfaz requerida por un programa de aplicación y su conexión de transporte para alcanzar un destino fuera de la red de su enlace. Estas interfaces, conocidas como *sockets*, se definen como la combinación de la dirección IP del enlace, el número de puerto asignado y el protocolo de transporte seleccionado. Una interfaz *socket* está constituida por los siguientes componentes:

-Funciones de núcleo de *socket*
-Estructuras de datos de dirección
-Funciones de traducción de nombre a dirección
-Funciones de conversión de dirección

La *interfaz socket* es una abstracción de cómo un sistema operativo accede a redes para uso de las aplicaciones. Los *sockets* son creados de manera similar por los sistemas operativos mediante la invocación de rutinas que devuelven resultados que luego pueden ser interpretados para un objetivo. En una invocación a un *socket* se necesitan identificar los siguientes parámetros:

-Familia de protocolos, AF_INET para IPv4 y AF_INET6 para IPv6
-Tipo de *socket*, SOCK_STREAM para *sockets* orientados a la conexión y SOCK_DGRAM para *sockets* sin conexión
-Tipo de protocolo, IPPROTO_TCP o IPPROTO_UDP.

Para la pila de protocolos TCP/IP existen dos tipos de sockets:

Sockets orientados a la conexión o con conexión, que emplean conexiones TCP, y
Sockets sin conexión, para comunicaciones sobre UDP.

Para los sockets orientados a la conexión (TCP), hay dos lados: el lado del cliente, que hace la conexión activa, y el lado del servidor, que espera la conexión del lado del cliente pasivamente. La directiva Establecer conexión() es imprescindible para el lado del cliente. Las directivas Asociar puerto a socket(), Preparado para petición() y Aceptar conexión() son imprescindibles para el lado del servidor. Como se ilustra en la figura 1.1.

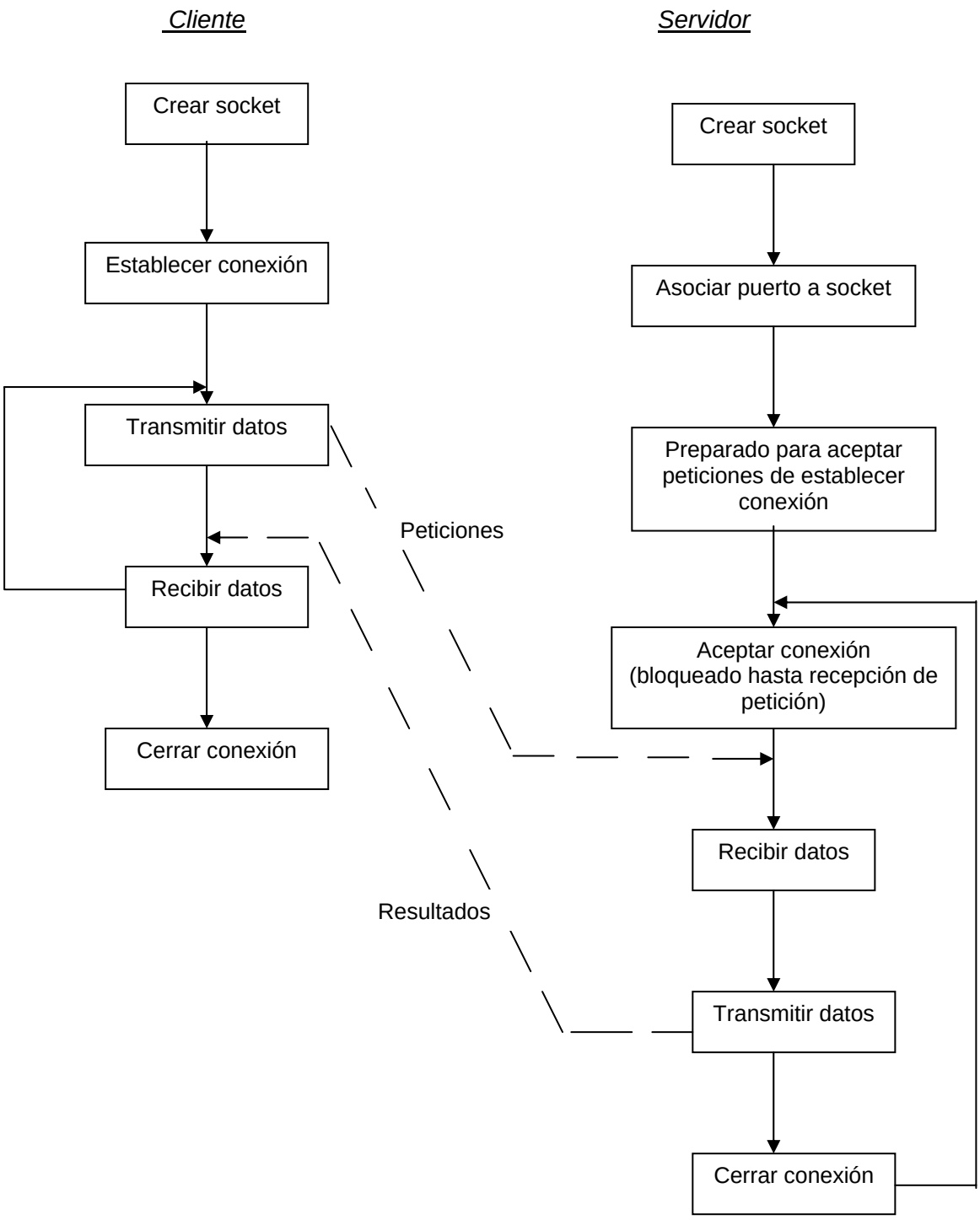


Figura 1.1: *Proceso de comunicación sobre socket orientado a la conexión.*

Para *sockets* sin conexión (UDP), la directiva *Establecer conexión()* no es obligatoria. Para recibir tráfico de otros puntos es imprescindible la directiva *Asociar puerto a socket()*. Como se ilustra en la figura 1.2.

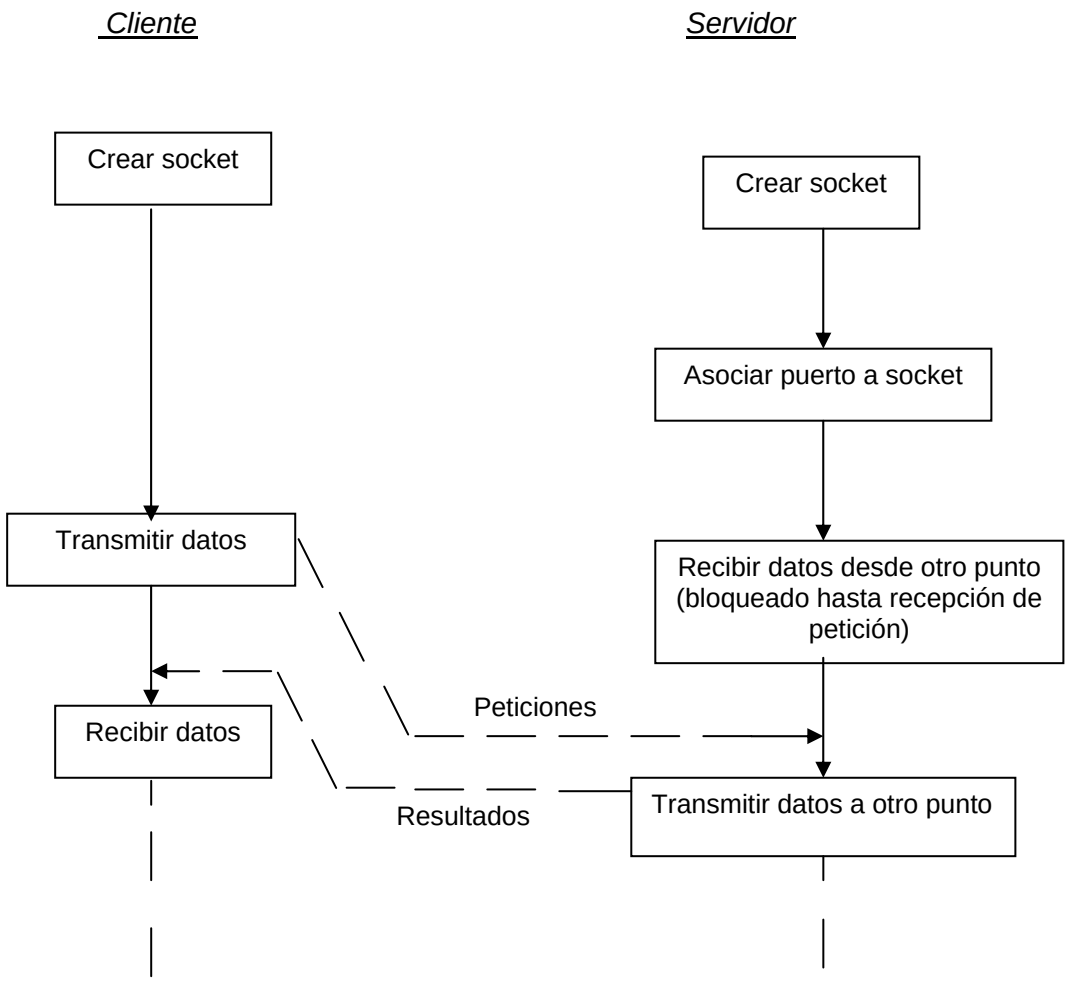


Figura 1.2: *Proceso de comunicación sobre socket sin conexión.*

Como puede observarse, hasta aquí no se ha introducido el objeto general de esta temática, la cual se refiere a la situación generada por la transición de un estado inicial con IPv4 a otro final con IPv6. Esto implica la actualización del software de routers y de sistemas operativos, así como el software relacionado con las aplicaciones de red (*sockets)*.

Básicamente los cambios a los que se refieren el final del párrafo anterior, son la adecuación que los *sockets* requieren para manejar direcciones de 128 bits en lugar de solo 32 bits. Esto no parece generar cambios conflictivos en los *sockets,* y solo parece enfocarse en cómo el sistema operativo realiza estos cambios. De acuerdo a esta aseveración la aplicaciones podrían ejecutarse si el sistema operativo en que corren, se encarga de efectuar estos cambios, ya que en el residen los protocolos involucrados. Es por ello que a continuación se hace una pequeña comprobación sobre la forma transparente en que una aplicación se ejecuta antes y después de la transición a IPv6.

2. PRUEBA OPERATIVA DE UNA APLICACIÓN TANTO EN IPv4 COMO EN IPv6

A. INTRODUCCION

En esta sección se realiza un ejemplo práctico de los pasos necesarios para realizar una migración hacia el nuevo protocolo de Internet IPv6 en un escenario sencillo compuesto de una sola red que posee dos equipos que tienen el sistema operativo Windows XP Profesional con ServiPack 2 y que trabajan como clientes. También se cuenta con un equipo que funciona como servidor de red y que posee el sistema operativo Windows 2003 Server, Edición Estándar, en la que se ejecutan los servicios de red http, DNS, Bases de datos, ruteo. También contiene una aplicación operativa desarrollada en ambiente Web que tiene acceso a una base de datos.

La estrategia de transición hacia el nuevo protocolo de Internet IPv6 empleada en todos los nodos de la red es la **PILA DUAL**.

Se han seleccionado estas plataformas en el ejemplo desarrollado por la incidencia que se ha observado que tienen en las empresas encuestadas y cuyos resultados se detallan en el siguiente capitulo.

El propósito que se persigue con este ejemplo es probar que cualquier institución que necesite realizar una migración para implementar el protocolo de Internet versión 6, en principio, no tendría ningún problema con sus aplicaciones basadas en el actual protocolo TCP/IP versión 4 al operarlas en IPv6. Además, este ensayo puede servir de modelo para el laboratorio de pruebas, que toda empresa que inicia un proceso de transición, necesita instalar para el aprendizaje de personal de TIC.

B. DISEÑO DE LA RED

1) Asignación de direcciones
Para este ejemplo se utilizan los siguientes datos:

Dirección IPv6 global de enlace.

3ffe:ffff:0000:1560:0000:0000:0000:0001/60

Después de simplificar los campos la dirección IPv6 de la siguiente forma

3ffe:ffff:0:156::1/60

Ya que el objetivo de este ejemplo es mostrar la facilidad con la que se realiza una transición hacia el protocolo IPv6 en una red LAN, no se utilizara procedimiento para crear subredes y se utilizará como prefijo de direccionamiento el asignado a la dirección global de enlace, trabajando solamente con el rango de direcciones asignadas a los host.

3) Escenario para la transición.
Suponiendo que tenemos el escenario hipotético que se ilustra en la figura 2.B.1 que es donde se realizará la transición al protocolo IPv6.

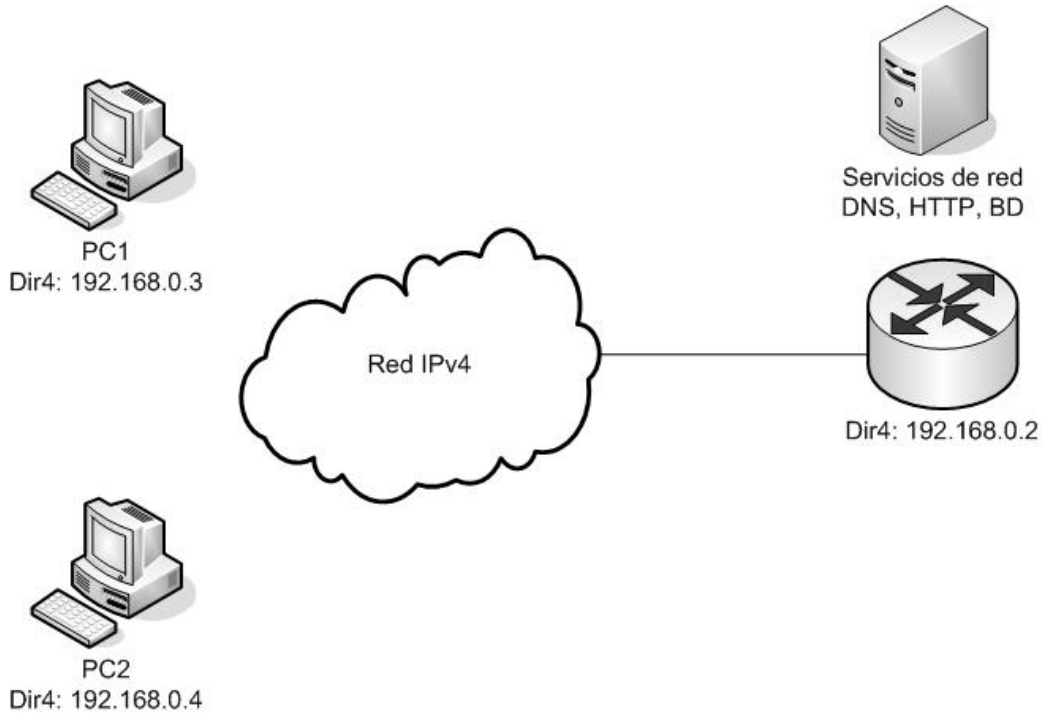


Figura 2.B.1: *Escenario para la transición al protocolo IPv6*

La infraestructura de pruebas para realizar la transición al protocolo IPv6 es la siguiente:

1. Un equipo que tiene el sistema operativo Microsoft Windows 2003 Server, Edición Estándar que posee los siguientes servicios de red.
    a. Servicio de ruteo en la red.
    b. Servidor de nombres de dominio (DNS).
    c. Servidor de aplicaciones Web (http, ftp): El servidor Web es IIS 6.0 y ejecuta una aplicación desarrollada en ASP.NET con acceso a bases de datos
    d. Servidor de Bases de Datos (BD): El gestor de bases de datos es MySQL para Windows, con el ODBC 3.51.
2. Dos equipos que se utilizan como clientes y poseen el sistema operativo Microsoft Windows XP Profesional Servipack 2 con soporte para el protocolo IPv6

2) Mecanismo de transición

Puesto que el protocolo IPv6 tiene un diseño que permite la coexistencia con su predecesor el protocolo IPv4. En el presente ejemplo se ha optado por utilizar el mecanismo de transición de Pila Dual, la descripción de este mecanismo se encuentra detallado en el capitulo de transición a IPv6 en el apartado 13.B.2 del *Manual de referencia del protocolo de Internet versión 6.*

Este mecanismo de transición será aplicado en primer lugar al servidor de la red y posteriormente en los equipos que funcionan como clientes.

Los clientes son los que deciden si la comunicación entre los nodos de la red se realiza con el protocolo IPv4 o IPv6. El diagrama resultante de aplicar el mecanismo de pila dual en la red se ilustra en la figura 2.B.2.

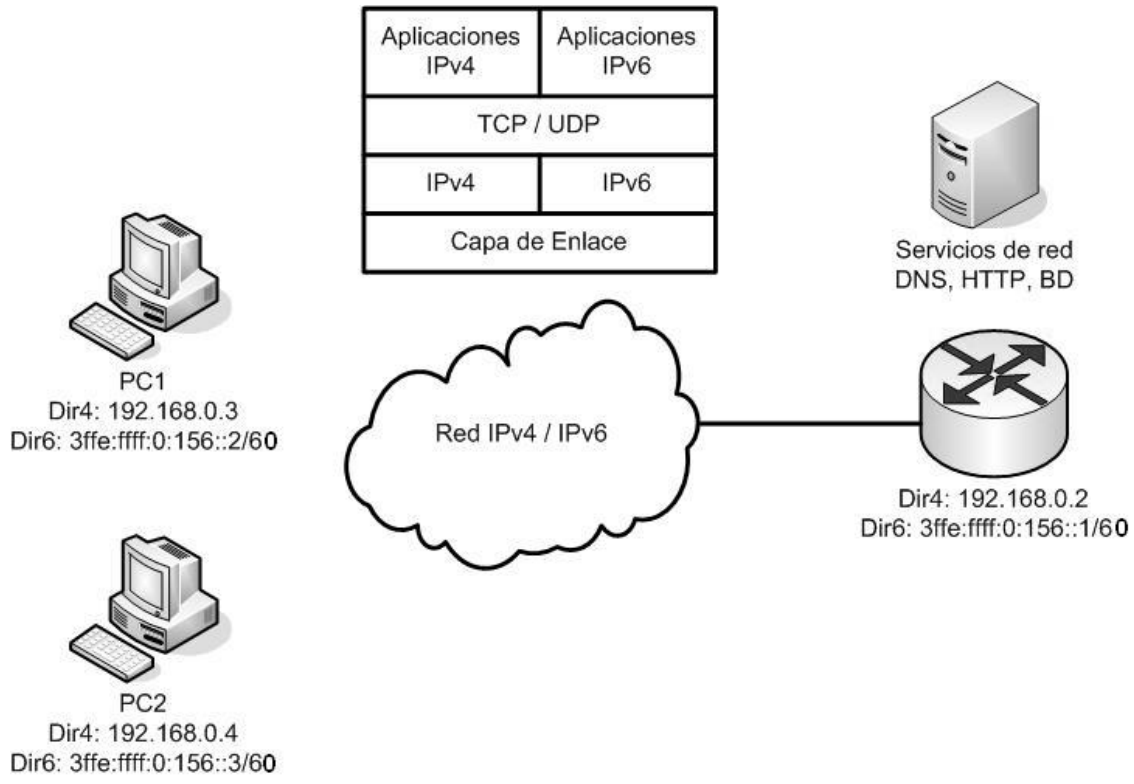


Figura 2.B.2: *Aplicación del mecanismo de pila dual en la infraestructura de red del escenario*

C. INSTALACION Y CONFIGURACIÓN DEL PROTOCOLO IPV6

Primero se instala el protocolo IPv6 en el equipo que tiene el sistema operativo Windows 2003 Server, Edición Estándar y posteriormente en los equipos que tienen el sistema operativo Windows XP Profesional SP2. Los pasos para instalar el modo IPv6 en estos sistemas operativos se detallan en el capitulo de Ejemplo practico de protocolo IPv6, apartado I, del *Manual de referencia del protocolo de Internet versión 6.*

D. IMPLEMENTAR LA PILA DUAL

En la infraestructura de red que funciona con IPv4 no se necesita realizar ningún cambio. Al agregar las direcciones IPv6 estáticas en cada nodo de la red queda habilitada la pila dual. También es importante hacer notar que los host que funcionan como clientes tienen la opción de comunicarse con el servidor utilizando el protocolo de Internet IPv4 o el protocolo IPv6. Esto gracias a que cada dispositivo tiene en su interface de red una pila que envía y recibe trafico con IPv4 y otra pila que envía y recibe trafico con IPv6 (idea central de la estrategia de pila dual).

En esta estrategia de transición es **MUY IMPORTANTE** que en la red donde se implementa este mecanismo de transición los nodos con capacidad para soportar pila dual deben tener a disposición un servidor de nombres de dominio con capacidad para tratar registros “A” que hacen referencia a las direcciones IPv4 y registros “AAAA” que hacen referencia a las direcciones IPv6.

El fin de que el servidor soporte estos tipos de registros es que los diferentes programas y software de protocolos de red con los que trabajan las aplicaciones que se ejecutan con los modelos cliente/servidor puedan utilizar en las funciones de bibliotecas de sockets administradas por el sistema operativo, el nombre de dominio para identificar a los nodos de la red. Lo que permite realizar una migración de cualquier servicio de red que trabaje con IPv4 a IPv6.

E. CONFIGURACIÓN DEL SERVIDOR DE NOMBRES DE DOMINIO

1) Jerarquía de dominio del sitio
En la figura 2.E.1 se ilustra la jerarquía de dominio para el sitio de prueba para la transición a IPv6.

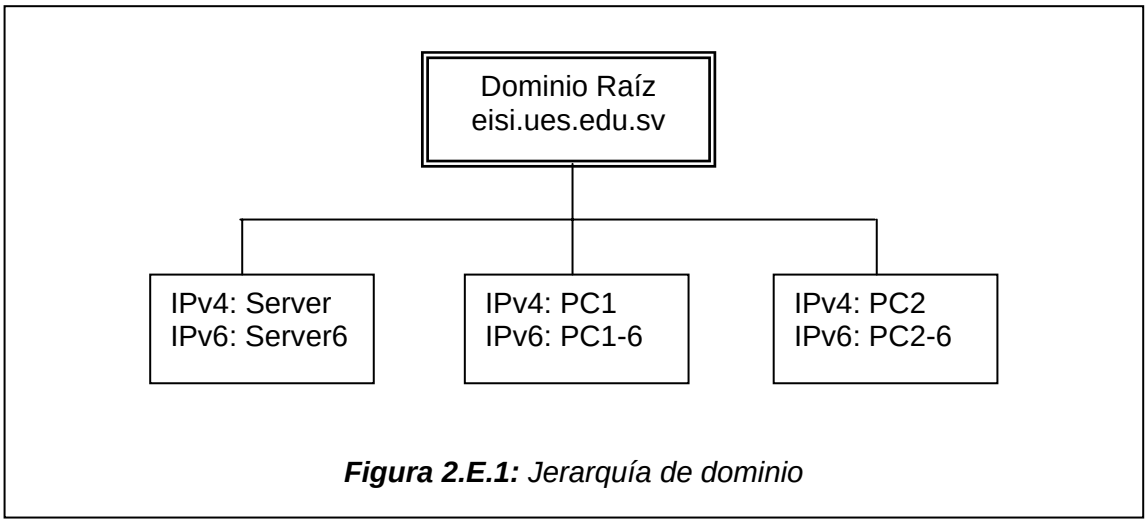


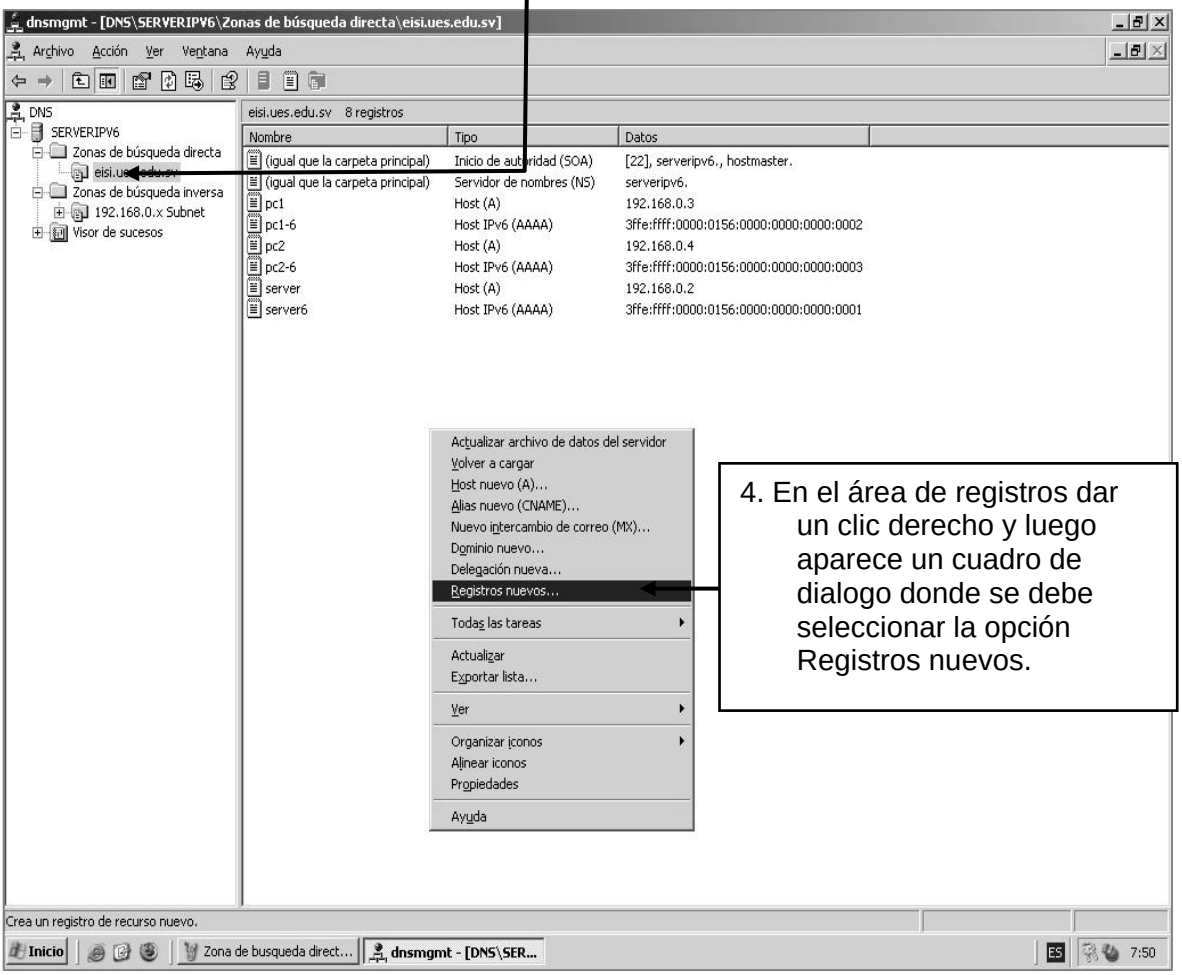
Figura 2.E.1: *Jerarquía de dominio*

2) Agregar registros "AAAA" a la zona de búsqueda directa
Se debe agregar al servidor DNS los registros que permitan asociar un nombre de dominio a una dirección IPv6. Estos registros son del tipo "AAAA", los pasos para agregar estos registros al servidor DNS del sistema operativo Windows 2003 Server, Edición Estándar son:

1. Dar un clic en el botón Inicio del Escritorio de trabajo.

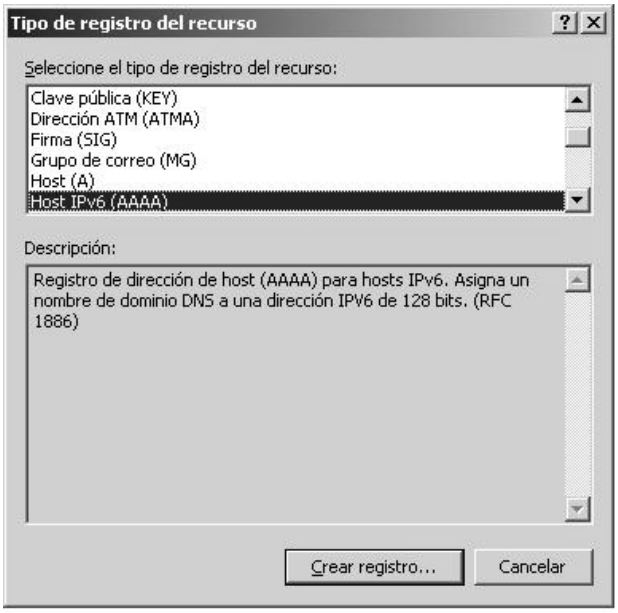
2. Seleccionar la opción Herramientas administrativas en el menú Inicio y a continuación dar un clic en el servicio DNS de Windows 2003 Server.

3. En la ventana del administrador DNS se debe seleccionar en el área de zonas del servidor DNS la zona de búsqueda directa eisi.ues.edu.sv

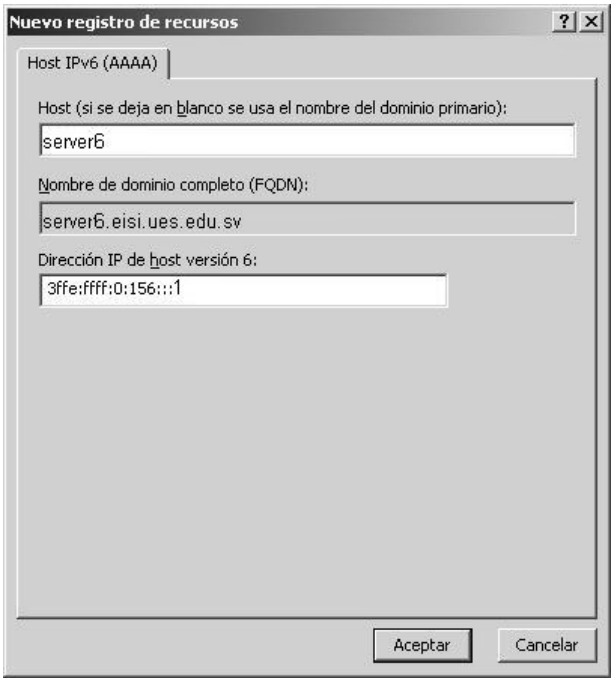


4. En el área de registros dar un clic derecho y luego aparece un cuadro de dialogo donde se debe seleccionar la opción Registros nuevos.

5. Se despliega el cuadro de dialogo Tipo de registro de recurso y luego se debe buscar y seleccionar el tipo de registro Host IPv6 (AAAA) y finalmente dar un clic en el botón Crear registro.



6. Luego aparece el cuadro de dialogo Nuevo registro de recurso, en este se debe digitar el nombre del host que se agregara al dominio y la dirección IPv6 de dicho host, y finalmente dar un clic en el botón Aceptar.



Con este procedimiento se deben agregar los siguientes registros al servidor DNS

Host	Nombre de dominio completo	Dirección IPv6
server6	Server6.eisi.ues.edu.sv	3ffe:ffff:0:156::1
Pc1-6	Pc1-6.eisi.ues.edu.sv	3ffe:ffff:0:156::2
Pc2-6	Pc2-6.eisi.ues.edu.sv	3ffe:ffff:0:156::3

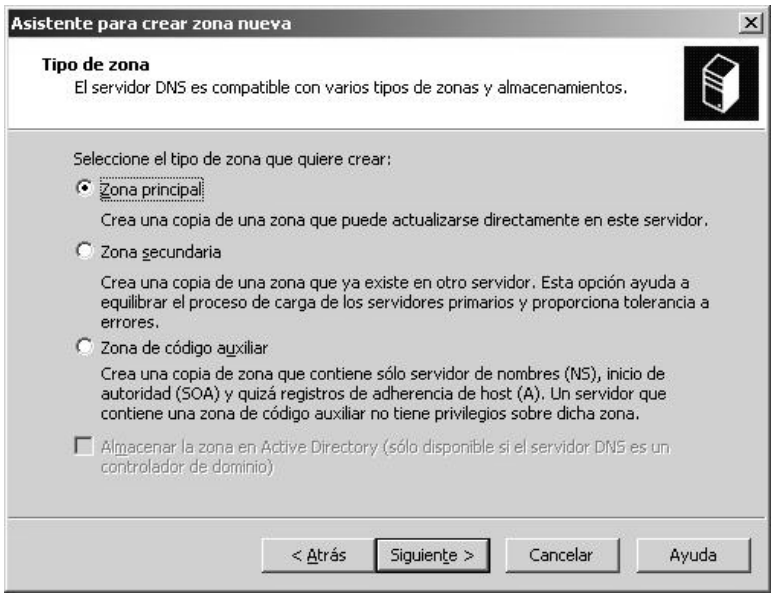
3) Agregar una zona de búsqueda inversa

Posteriormente se debe agregar al servidor un nuevo dominio para soportar búsquedas basadas en direcciones IPv6 con el siguiente procedimiento:

1. En el administrador DNS seleccionar el área de zonas de búsqueda inversa, luego dar un clic derecho sobre esta y en el menú emergente que aparece seleccionar la opción Nueva zona de búsqueda inversa.

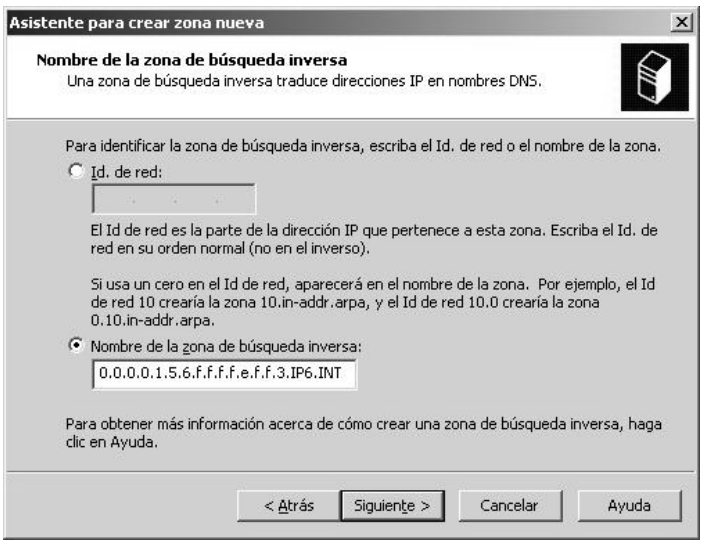
2. Se despliega un asistente para ayudar a crear la nueva zona, en dicho asistente se debe dar un clic en el botón siguiente.

3. En el cuadro de dialogo que aparece se debe seleccionar una zona principal para poder actualizar la base de datos DNS en el servidor, luego debemos dar un clic en el botón Siguiente.



4. En el cuadro de dialogo siguiente digitamos el nombre de la zona de búsqueda inversa (los detalles de cómo se forma el nombre de búsqueda inversa se encuentran en el capitulo DNS en el apartado 8.D.5 del *Manual de referencia del protocolo de Internet versión 6*). Para este caso el nombre de la zona de búsqueda inversa es:

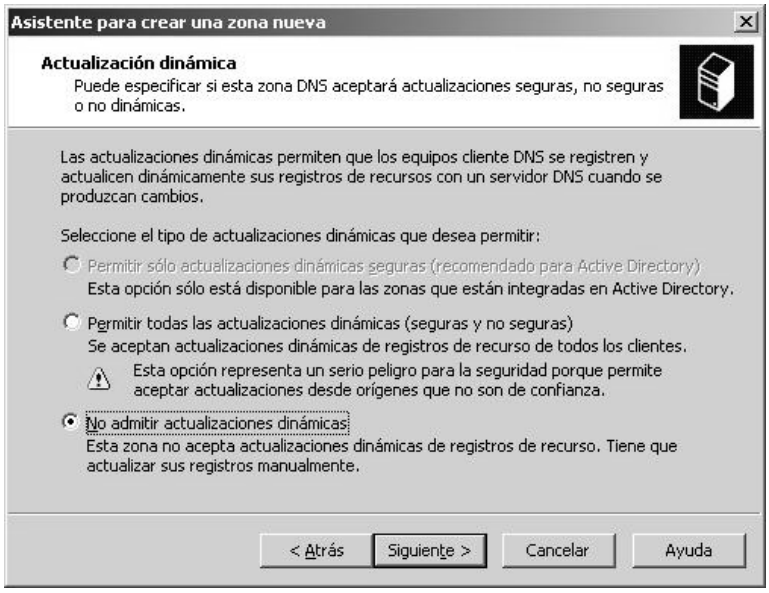
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.5.1.0.0.0.0.f.f.f.f.e.f.f.3.IP6.INT



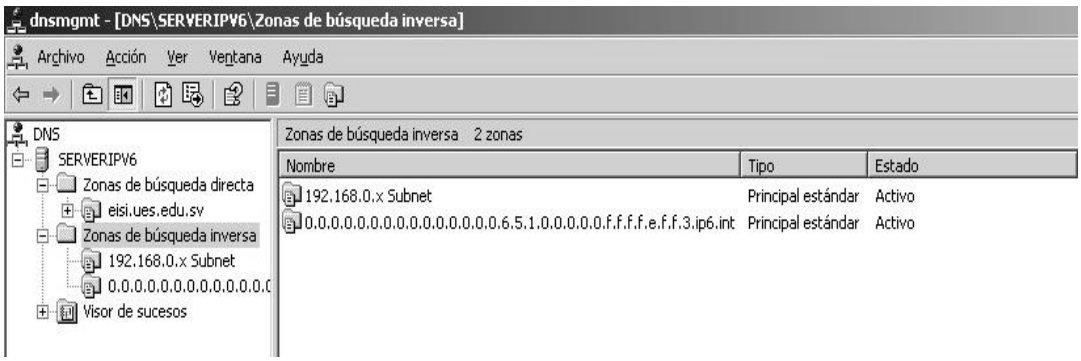
Es importante recalcar que el dominio basado en búsqueda de direcciones IP6.INT que vienen incluido en el sistema operativo Windows 2003 Server, Edición Estándar se basa en el estándar de Internet RFC 1886 y actualmente este RFC ha sido suplantado por el estándar RFC 3152 que especifica las consultas inversas utilizando el dominio IP6.ARPA.

Después de digitar el nombre de la zona de búsqueda inversa se debe dar un clic en el botón Siguiente.

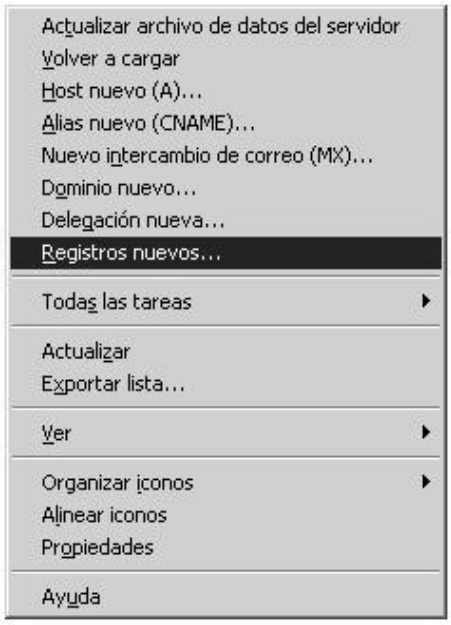
5. Luego se despliega el siguiente cuadro de dialogo donde se debe indicar al servidor DNS que la zona creada no aceptara actualizaciones dinámicas de los registros que almacenara.



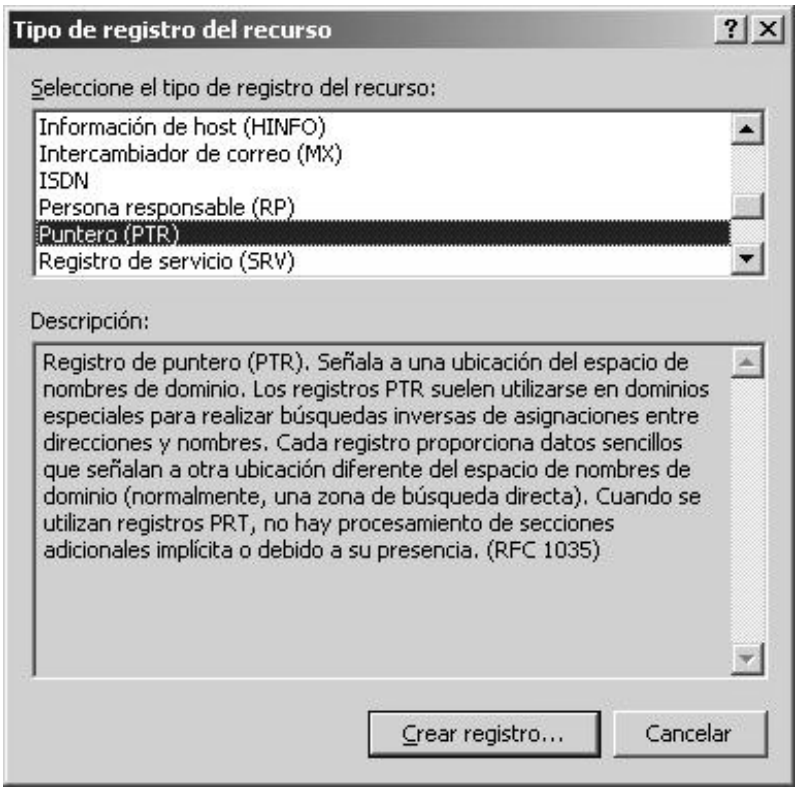
6. El ultimo cuadro de dialogo solo es para confirmar los datos introducidos a la zona de búsqueda inversa creada, si todos los datos son correctos damos un clic en el botón Finalizar, y finalmente se puede apreciar en la ventana del Administrador DNS el nombre de la zona de búsqueda inversa creada.



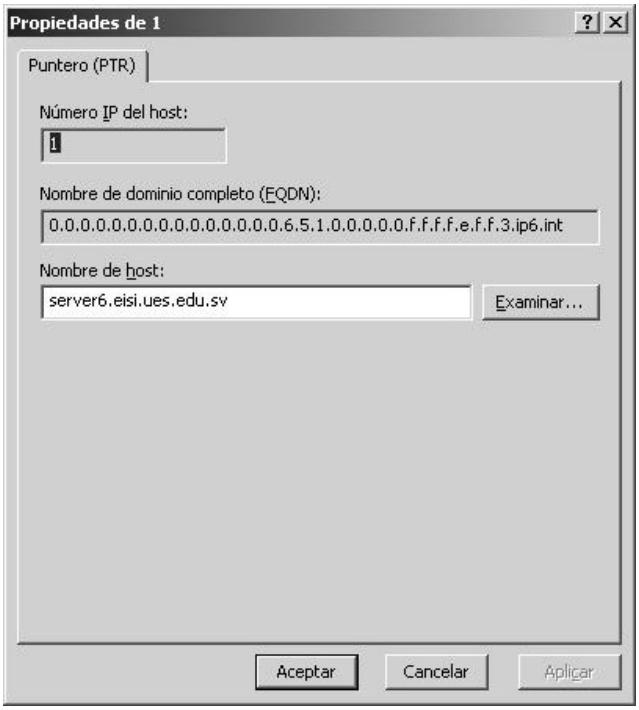
7. Una vez creada la zona de búsqueda inversa se deben agregar los registros de recurso de puntero PTR. Por lo que se debe seleccionar en el área de búsqueda de zonas del servidor el dominio 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.5.1.0.0.0.0.f.f.f.f.e.f.f.3.IP6.INT, y luego se debe dar un clic derecho en el área de los registros de la zona, luego se despliega un menú emergente en el que se debe seleccionar la opción Registros nuevos.



8. Luego se despliega el cuadro de dialogo Tipo de registro del recurso en donde se debe seleccionar la opción Puntero (PTR), luego dar un clic en el botón Crear registro.



9. En el cuadro de dialogo que aparece se debe digitar el identificador del host y su nombre correspondiente para finalmente dar un clic en el botón Aceptar.



Con este procedimiento se deben agregar los registros de recursos de puntero para cada nodo de la red al servidor DNS de la siguiente forma.

IP	Nombre de dominio completo	Nombre del host
1	1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.5.1.0.0.0.0.f.f.f.f.e.f.f.3.IP6.INT	Server6.eisi.ues.edu.sv
2	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.5.1.0.0.0.0.f.f.f.f.e.f.f.3.IP6.INT	Pc1-6.eisi.ues.edu.sv
3	3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.5.1.0.0.0.0.f.f.f.f.e.f.f.3.IP6.INT	Pc2-6.eisi.ues.edu.sv

4) Agregar un servidor DNS a los equipos cliente

Finalmente queda configurar el acceso al servidor de nombres de dominio en los equipos que funcionan como clientes en la red de prueba, esto se hace escribiendo la siguiente línea en la consola de comandos DOS.

Comando realizado desde el host PC1
C:\> netsh interface ipv6 add dns “Conexión de área local” 3ffe:ffff:0:156::1

5) Probar el servicio DNS

Para probar si el servidor de nombres de dominio se encuentra trabajando correctamente se debe seguir el siguiente procedimiento desde cualquiera de los equipos que están configurados para trabajar como clientes.

1. Verificamos desde cualquier equipo que funciona como cliente si se enlazó correctamente al servidor DNS. Esto se hace escribiendo el siguiente comando en la consola DOS.

Petición de información desde el host PC1 al servidor DNS
C:\> netsh interface ipv6 show dns

Se obtiene la siguiente respuesta.

```
Servidores DNS en la interfaz: Conexión de área local

Índ.   Servidor DNS
-----  ------------------------------------------------
   1  3ffe:ffff:0:156::1
```

2. Luego se envía una petición de información al servidor desde cualquier host que trabaja como cliente por medio de un mensaje ICMPv6 y en lugar de ponerle la dirección IPv6 se le digita el nombre de dominio del servidor para comprobar que se está resolviendo nombres de dominio en la red.

Petición de información enviada desde host PC1 al servidor DNS
C:\> ping6 server6.eisi.ues.edu.sv

Se obtiene la siguiente respuesta del servidor.

```
Haciendo ping server6.eisi.ues.edu.sv [3ffe:ffff:0:156::1]
de 3ffe:ffff:0:156::2 con 32 bytes de datos:

Respuesta desde 3ffe:ffff:0:156::1: bytes=32 tiempo=26ms
Respuesta desde 3ffe:ffff:0:156::1: bytes=32 tiempo=11ms
Respuesta desde 3ffe:ffff:0:156::1: bytes=32 tiempo<1m
Respuesta desde 3ffe:ffff:0:156::1: bytes=32 tiempo<1m

Estadísticas de ping para 3ffe:ffff:0:156::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 26ms, Media = 9ms
```

3. También se envía una consulta de búsqueda DNS al servidor para verificar las direcciones IPv4 e IPv6 y comprobar así el comportamiento de la pila dual, esto se hace digitando el siguiente comando en la consola DOS desde cualquier host que trabaja como cliente.

```
Comando que se ejecuta en el Equipo PC1
C:\>nslookup
```

Se obtiene la siguiente respuesta del servidor.

```
Servidor predeterminado:  server.eisi.ues.edu.sv
Address:  192.168.0.2

>
```

Luego se le envía como cliente DNS una petición para resolver el nombre de dominio del servidor y que nos envié la dirección IPv4 del servidor

```
> set type=a
> server.eisi.ues.edu.sv
```

El servidor raíz DNS envía la respuesta del nombre de dominio al cliente.

```
Servidor:  server.eisi.ues.edu.sv
Address:  192.168.0.2
```

Posteriormente se le envía la petición DNS para la dirección IPv6 del servidor

```
> set type=aaaa
> server6.eisi.ues.edu.sv
```

El servidor raíz DNS envía la respuesta del nombre de dominio al cliente.

```
Servidor:  server.eisi.ues.edu.sv
Address:  192.168.0.2

server6.eisi.ues.edu.sv AAAA IPv6 address = 3ffe:ffff:0:156::1
```

Las repuestas obtenidas del servidor nos indican que los nodos de la red están trabajando correctamente con el mecanismo de transición de pila dual.

F. CONFIGURACIÓN DEL SERVIDOR WEB

En el equipo que tiene instalado el sistema operativo Windows 2003 Server, Edición Estándar el servidor IIS 6.0 comienza automáticamente a implementar el protocolo IPv6 en su servicio después de instalarlo. Una práctica muy recomendable es reiniciar el servidor IIS para que este pueda atender a través de direcciones IPv6 las peticiones de sitios web de los clientes, a los sitios que tenia previamente alojados.

G. COMPROBACION DE OPERATIVIDAD DE LAS APLICACIONES

Ahora solo resta comprobar si las aplicaciones operan independiente al protocolo de Internet utilizado, es decir se ejecutan transparentemente tanto en IPv4 como después de realizada una transición a IPv6.

Para el presente ejemplo se utiliza en los equipos que funcionan como clientes el navegador Web Mozilla versión para Windows FireFox 2.0 porque este soporta el uso de direcciones IPv6.

Los detalles técnicos de la aplicación con la que se realiza la prueba de la transición al protocolo IPv6 se detallan a continuación:

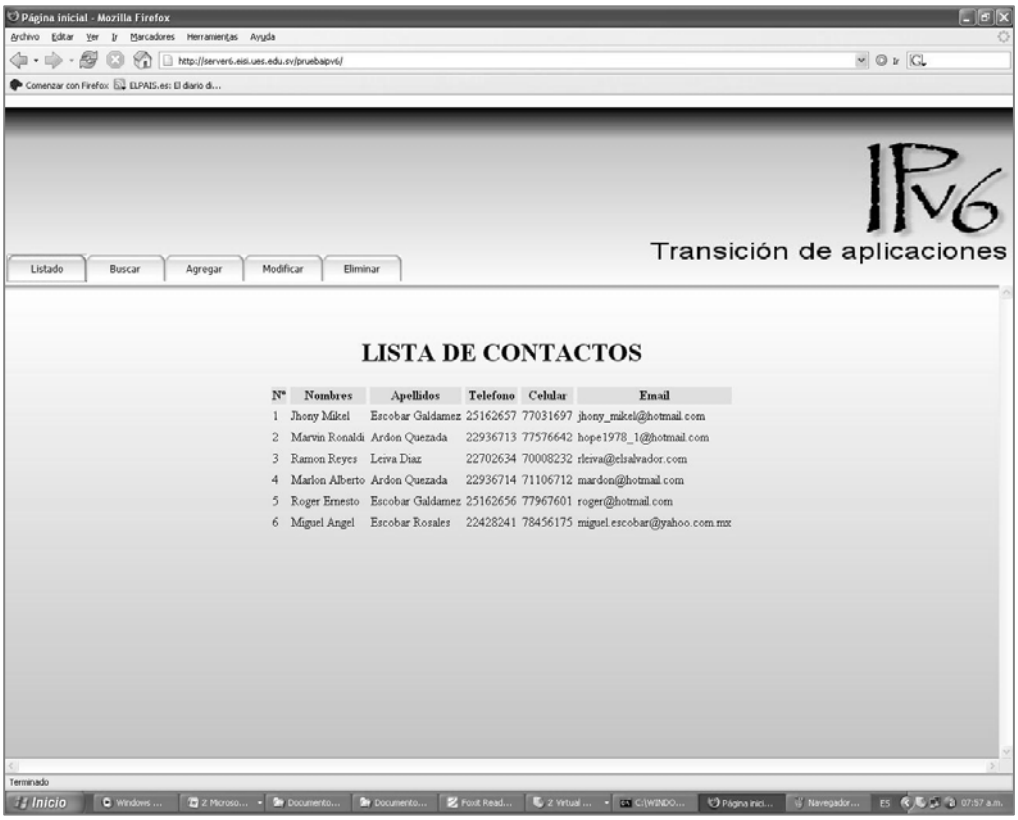
1. En el servidor IIS 6.0 se encuentra alojado un sitio Web que esta desarrollado en ASP.NET

2. El gestor de bases de datos con el que se trabaja en el servidor es MySQL 5.0.22 para Windows.

3. Un origen de conectividad a base de datos ODBC 3.51 para MySQL

Se abre el navegador Web Mozilla FireFox y se envía a través de la barra de direcciones una solicitud http al servidor utilizando la dirección IPv6 **http://[3ffe:ffff:0:156::1]:80/pruebaipv6** ó bien se envía una solicitud utilizando el nombre del dominio del servidor que actualmente trabaja con pila dual digitando en la barra de direcciones **http://server6.eisi.ues.edu.sv/pruebaipv6**, posteriormente visualizamos el siguiente sitio Web.

Para probar la independencia del protocolo IPv6 en la aplicación navegamos por el sitio y damos un clic en el enlace **Listado** para observar los datos almacenados en la base de datos y obtenemos la siguiente información.



Seguimos navegando y damos un clic en el enlace **Buscar** y digitamos uno de los nombres que aparecen en el listado para comprobar si se realizan consultas a la base de datos.

Se obtiene la siguiente respuesta del gestor de bases de datos.

En términos generales podemos concluir que no se presentan complicaciones que imposibiliten la operatividad de las aplicaciones al migrar de IPv4 a IPv6, por lo que podemos inferir que éstas son independientes del protocolo de Internet empleado.

3. INVESTIGACION DEL USO DE LAS APLICACIONES BASADAS EN EL PROTOCOLO TCP/IP POR EMPRESAS DE EL SALVADOR.

A. INTRODUCCIÓN

Con el fin de conocer el estado actual de las aplicaciones basadas en TCP/IP versión 4 y además conocer el conocimiento sobre IPv6 que poseen el personal de TIC de algunas empresas o instituciones en El Salvador del protocolo IPv6. Se tomaron a manera de referencia algunas empresas tipos, donde se realizó un estudio de campo.

B. SELECCIÓN DE LAS EMPRESAS A TOMAR EN CUENTA EN EL ESTUDIO

Las empresas que se tomaron en cuenta en este estudio son las que cumplen con los siguientes criterios de selección:

1. Poseer aplicaciones en operación basadas en el protocolo TCP/IP.

2. Contar con una arquitectura de red definida.

3. Administrar servicios de red en la institución o empresa.

4. Empresas tipo que representen cualquiera de los siguientes sectores:
   a) Gubernamental
   b) Servicios
   c) Financieras
   d) No gubernamental
   e) Educación

Para este estudio se visitaron 10 empresas representativas que cumplían con los criterios antes mencionados. Es importante recalcar que para conocer el uso que las aplicaciones operativas hacen de los protocolos TCP/IP, no es necesario buscar información de un gran número de empresas, ya que cualquiera que sea la arquitectura de red implementada y las plataformas que éstas utilicen, se siguen siempre los mismos lineamientos generales de los estándares (RFC) sobre estos protocolos.

C. RESUMEN DE INFORMACIÓN RECOPILADA

Se diseñó una entrevista para realizarla en cada una de las empresas o instituciones que fueron seleccionadas para el estudio. Las entrevistas efectuadas se detallan en el Anexo C.

En la tabla 3.C.1 se muestra el resumen del hardware de red que poseen las empresas encuestadas y en la figura 3.C.1 se ilustra el porcentaje del uso de diferentes modelos de switches para administrar el tráfico en las redes de dichas empresas.

Tipo de Hardware	Modelo o serie
Switch	Switch 3COM Switch 3COM 2250 Switch 3COM 3800 Switch 3COM 7200 Switch 3COM 3500 Switch 3COM 2250 Switch DELL PowerConnect Switch DELL PowerConnect Serie 5000 Switch de aplicación Nortel Alteon Switch de aplicación Nortel Alteon Serie 2208 Switch CISCO Catalyst Switch CISCO Catalyst Serie 2950 Switch CISCO Catalyst Serie 6500
Router	Router CISCO Router CISCO Series 2800 Router CISCO Series 3800 Router CISCO ASA Router CISCO ASA Serie 5500 Versión 8.0
Firewalls	Firewall Appliance Firewall Appliance Serie DFL-CP310

Tabla 3.C.1: *Información del hardware encontrado.*

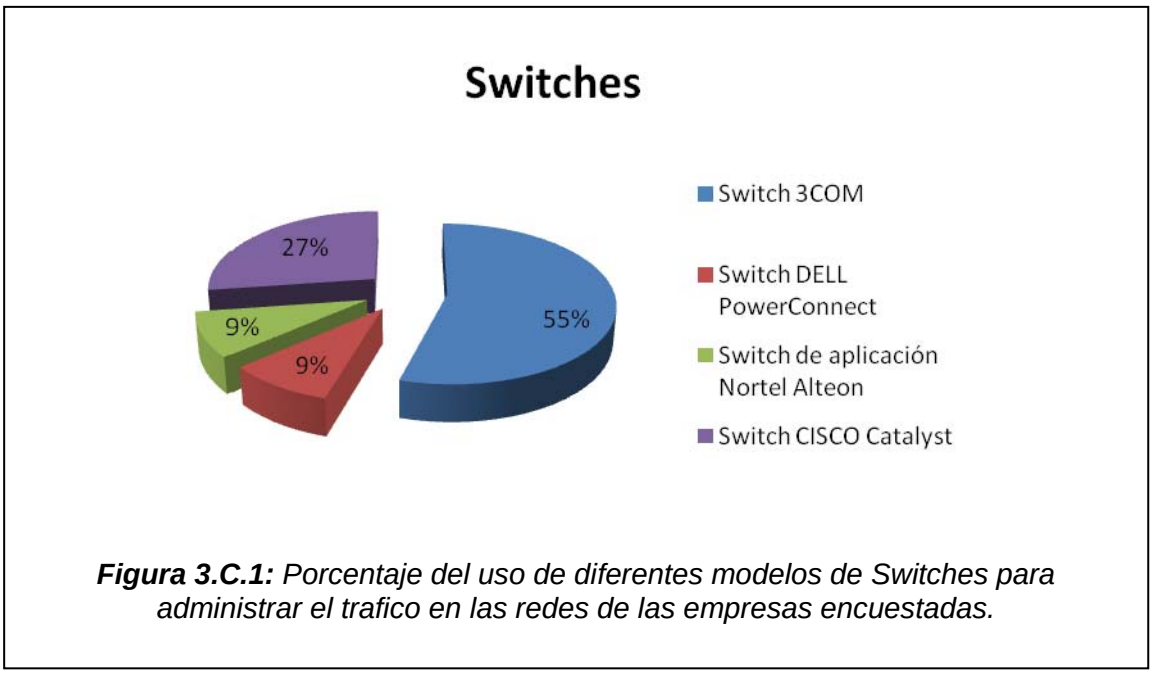


Figura 3.C.1: *Porcentaje del uso de diferentes modelos de Switches para administrar el trafico en las redes de las empresas encuestadas.*

En la tabla 3.C.2 se muestra la información detallada de las diferentes plataformas que utilizan las empresas encuestadas en sus equipos de red y en las figuras 3.C.2 y 3.C.3 se ilustra el porcentaje del uso de estas plataformas en equipos que funcionan como clientes y como servidores en las redes de dichas empresas.

Sistemas Operativos	Versiones
Windows	Windows 95 Windows 98 Windows 2000 Profesional Windows XP Profesional SP2 Microsoft Windows 2003 Server SP1 Microsoft Windows 2000 Server SP4
Linux	Linux RedHat Enterprise AS3 Linux Fedora Core 4.0 Linux Fedora Core 6.0 Linux SUSE 10

Tabla 3.C.2: *Información de las plataformas de red encontrados.*

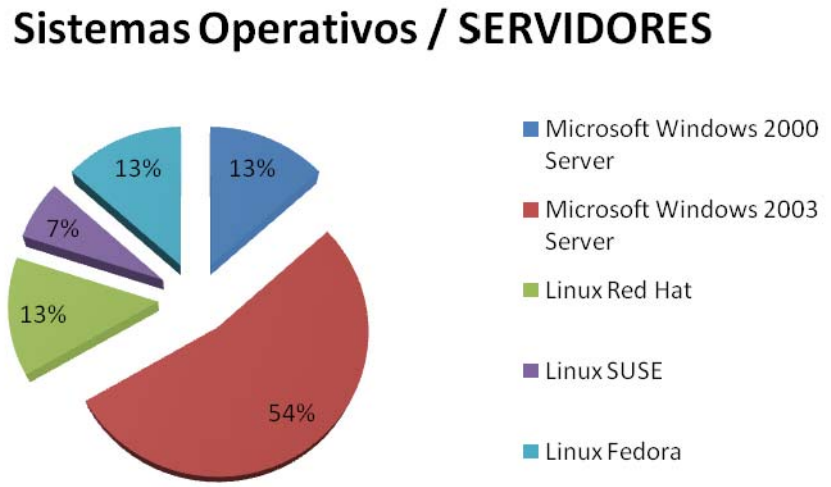


Figura 3.C.2: Porcentaje del uso de diferentes plataformas en equipos que *funcionan como servidores en las redes de las empresas encuestadas.*

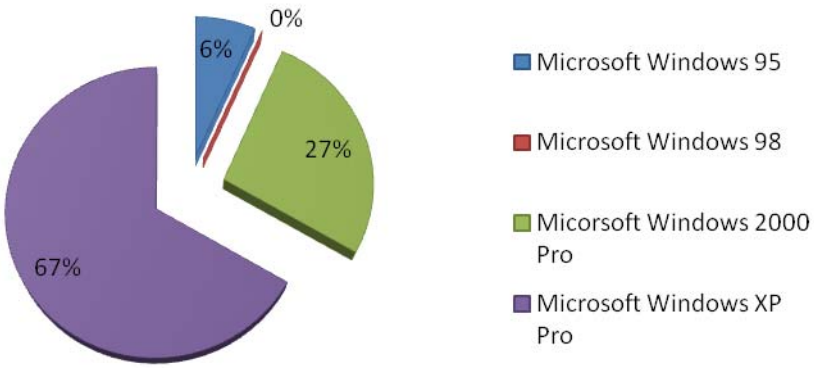


Figura 3.C.3: *Porcentaje del uso de diferentes plataformas en equipos que funcionan como clientes en las redes de las empresas encuestadas.*

En la tabla 3.C.3 se muestra la información detallada de los servicios de red y de las herramientas de software utilizadas para proporcionar estos servicios de red en las empresas encuestadas y en las figuras 3.C.4 y 3.C.5 se ilustra el porcentaje del uso de estas herramientas.

Tipos de servicios de red	Herramienta utilizada
WEB	Apache 2.0 IBM Lotus Notes versión 7.0
MAIL	Microsoft Exchange Server Postfix SendMail

Tabla 3.C.3: *INFORMACIÓN DE LOS SERVICIOS DE RED ENCONTRADOS.*

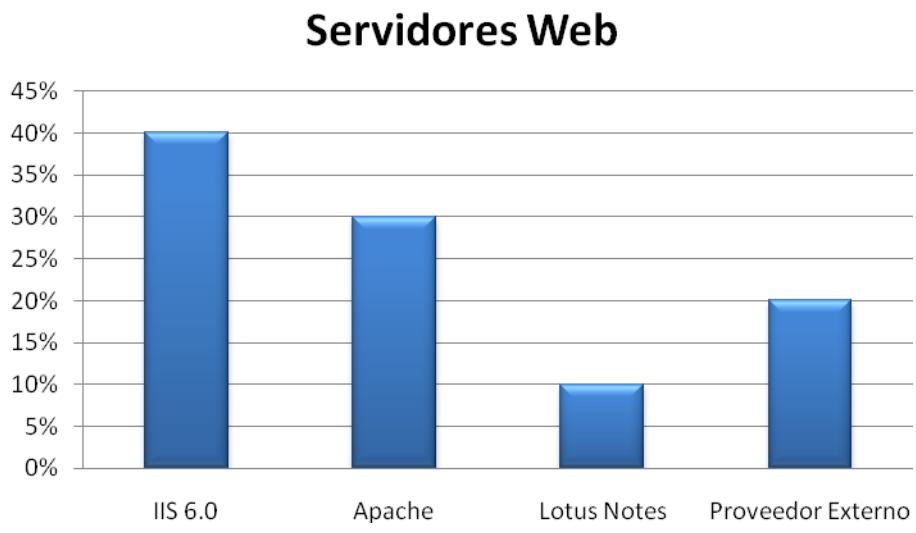


Figura 3.C.4: *Porcentaje del uso de herramientas de software utilizadas como servidores web.*

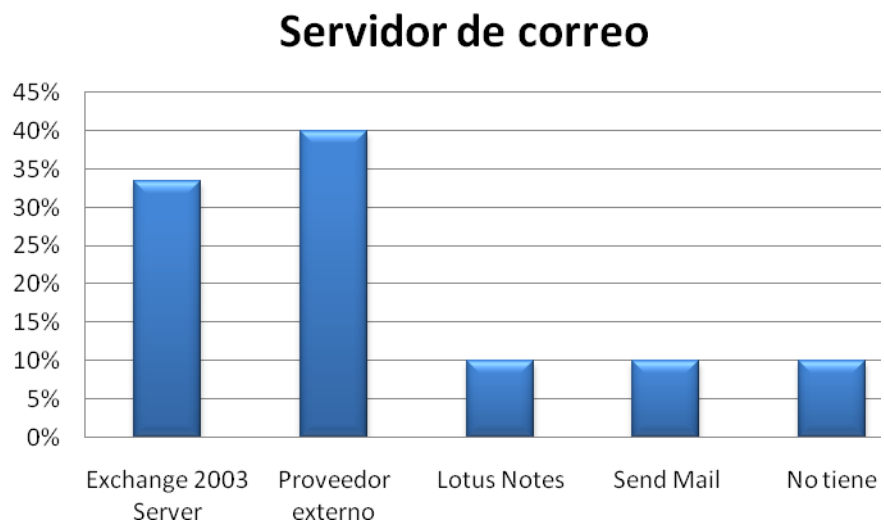


Figura 3.C.5: *Porcentaje del uso de herramientas de software utilizadas como servidores de correo electrónico.*

En la tabla 3.C.4 se detalla la información de los gestores de base de datos y el software para el desarrollo de las aplicaciones operativas que son utilizadas en las empresas del estudio y en

las figuras 3.C.6 y 3.C.7 se ilustra el porcentaje del uso de los gestores de bases de datos y de los lenguajes de desarrollo utilizados.

Gestores de bases de datos
Microsoft ACCESS XP Microsoft SQL Server 2000 Microsoft SQL Server 2005 MySQL Enterprise Server 5.0 DB2-IBM ORACLE 8i
Lenguajes de desarrollo
Fox para DOS JAVA Microsoft Visual Studio 6.0 Microsoft Visual Studio 2005 ASP.NET PHP 5.2.1

Tabla 3.C.4: *Información los gestores de bases de datos y lenguajes de desarrollo encontrados.*

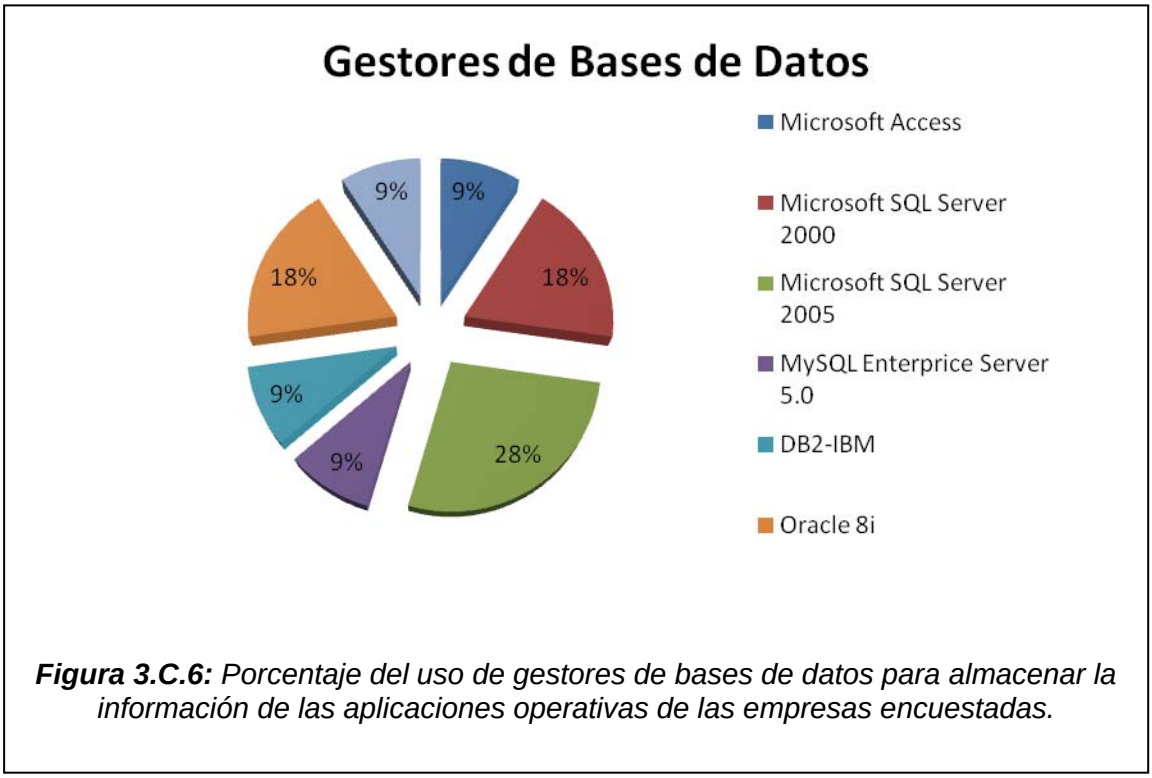


Figura 3.C.6: *Porcentaje del uso de gestores de bases de datos para almacenar la información de las aplicaciones operativas de las empresas encuestadas.*

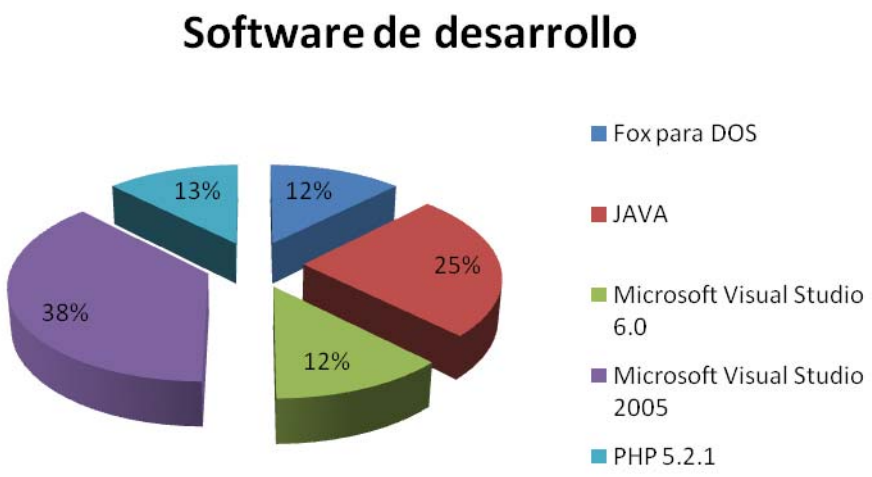


Figura 3.C.7: *Porcentaje del uso de herramientas de software utilizadas para el desarrollo de las aplicaciones operativas de las empresas encuestadas.*

Otra información que se recolectó en las entrevistas realizadas en las empresas fue punto de vista que los encargados de la administración de las redes corporativas de las instituciones o empresa tienen sobre la implementación de IPv6 en nuestro medio, por lo que en la tabla 3.C.5 se detallan algunos planteamientos expuestos por los entrevistados en este estudio.

Principales puntos de vista de los entrevistados en cuanto a la implementación de IPv6 en nuestro medio
1. Existe una falta de información organizada sobre IPv6 lo que dificulta conocer más a cerca de sus ventajas ante IPv4. 2. En la actualidad no se visualiza una necesidad marcada hacia la migración a IPv6, pero esto ira cambiando con el tiempo a causa del empuje del surgimiento de nuevas tecnologías de información y telecomunicaciones. 3. Se debe contar con personal capacitado en el tema para asesorar al personal de TIC de las instituciones en el conocimiento de este protocolo. 4. La falta de importancia que se le presta a las unidades de TIC en las empresas salvadoreñas, vendría a ser un obstáculo bien marcado en los intentos a una migración a IPv6.

Tabla 3.C.5: *Puntos de vista de las personas entrevistadas sobre la implementación del nuevo protocolo de Internet en nuestro medio*

4. METODOLOGIA PARA LA TRANSICION A IPv6

Metodología de migración a IPv6 (Ver *Manual de referencia del protocolo de Internet versión 6*, Capitulo de transición).

A. Preparación para la transición
   A.1 Evaluación del grado de conocimiento previo del personal
   A.2 Selección de estrategia de capacitación
   A.3 Creación de un laboratorio de prueba

B. Planeación de la transición
   B.1 Revisión de políticas de sustitución de equipos y actualización de software.
   B.2 Revisión de políticas de administración de red

C. Migración a IPv6
   C.1 Actualización del entorno DNS
   C.2 Actualización de la estructura de red
   C.3 Esquema del plan
   C.4 Obtención de componentes actualizados

D. Transición a IPv6
   D.1 Habilitar una pila dual (IPv4/IPv6) en todos los servidores
   D.2 Desplegar clientes habilitados para IPv6
   D.3 Desplazar IPv4

5. EJEMPLO DE IMPLEMENTACIÓN DE IPV6 EN UN MODELO DE MEDIANA EMPRESA.

A. DESCRIPCION DEL ESCENARIO DE IMPLEMENTACIÓN

En el siguiente escenario se requiere migrar a IPv6 todos los servicios de red.

Para dicho propósito se debe analizar las siguientes condiciones en que se encuentra la empresa en un estado inicial (IPv4). La situación esquemática de la red se puede visualizar en la figura 5.A.1.

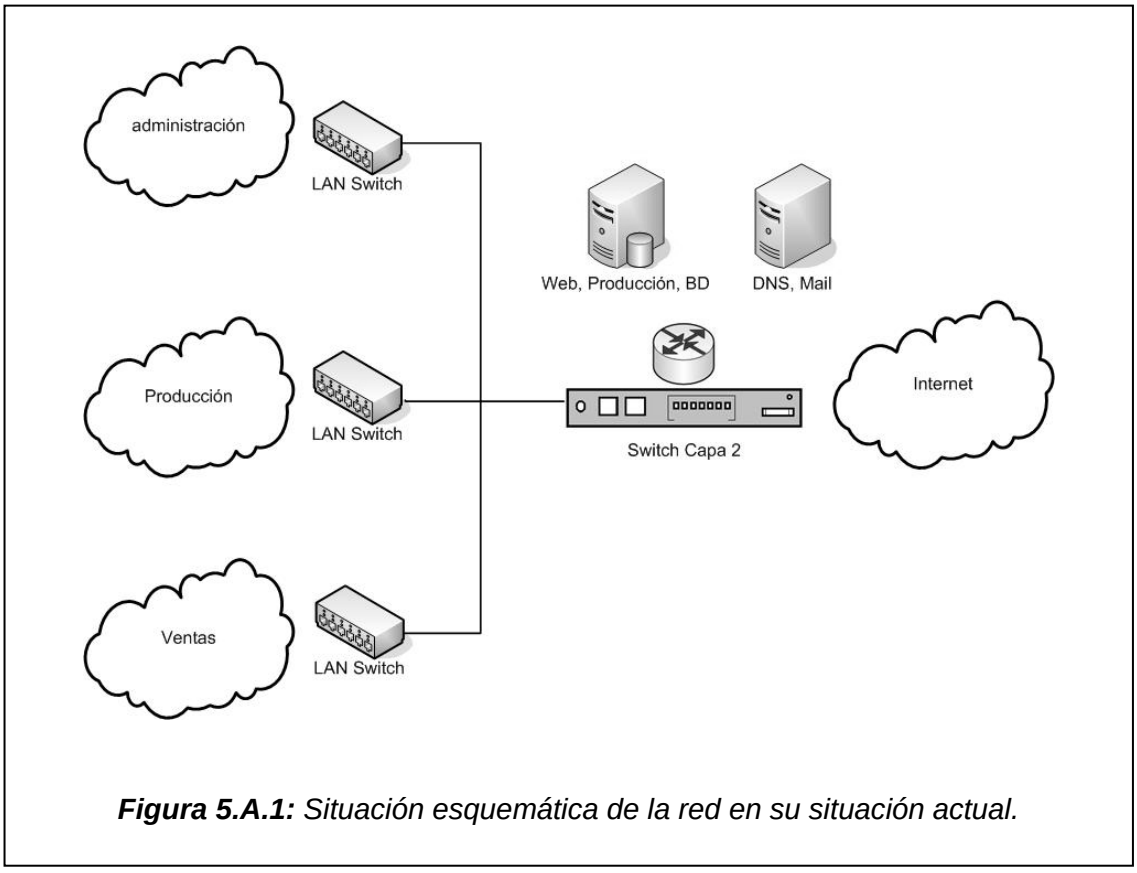


Figura 5.A.1: *Situación esquemática de la red en su situación actual.*

El detalle de la situación actual de la red es:

1. Un switch capa 2 para administrar el trafico en la red empresarial

2. El departamento de administración cuenta con un switch y posee 7 estaciones de trabajo

3. El departamento de producción cuenta con un switch y posee 3 estaciones de trabajo

4. El departamento de ventas cuenta con un switch y posee 4 estaciones de trabajo

5. Un servidor Linux Red Hat Enterprise AS 3, con los servicios DNS, las direcciones privadas han sido configuradas manualmente, se utiliza Sendmail para correo electrónico, Firewall de software.

6. Un servidor de producción Windows 2003 server, Edición Empresarial con SQL Server 2000 como gestor de bases de datos, IIS 6.0 como Servidor Web, Entorno de programación .NET para sus aplicaciones operativas, Un programa de Inventario de materiales y de producto terminado con base de datos en FOX.

B. PASOS PARA LA MIGRACIÓN A IPV6

1) Metodología de solución

En la figura 5.B.1 se ilustra con el diagrama de sistemas el proceso de transición de aplicaciones basadas en el actual protocolo de Internet versión 4 al nuevo protocolo de Internet versión 6

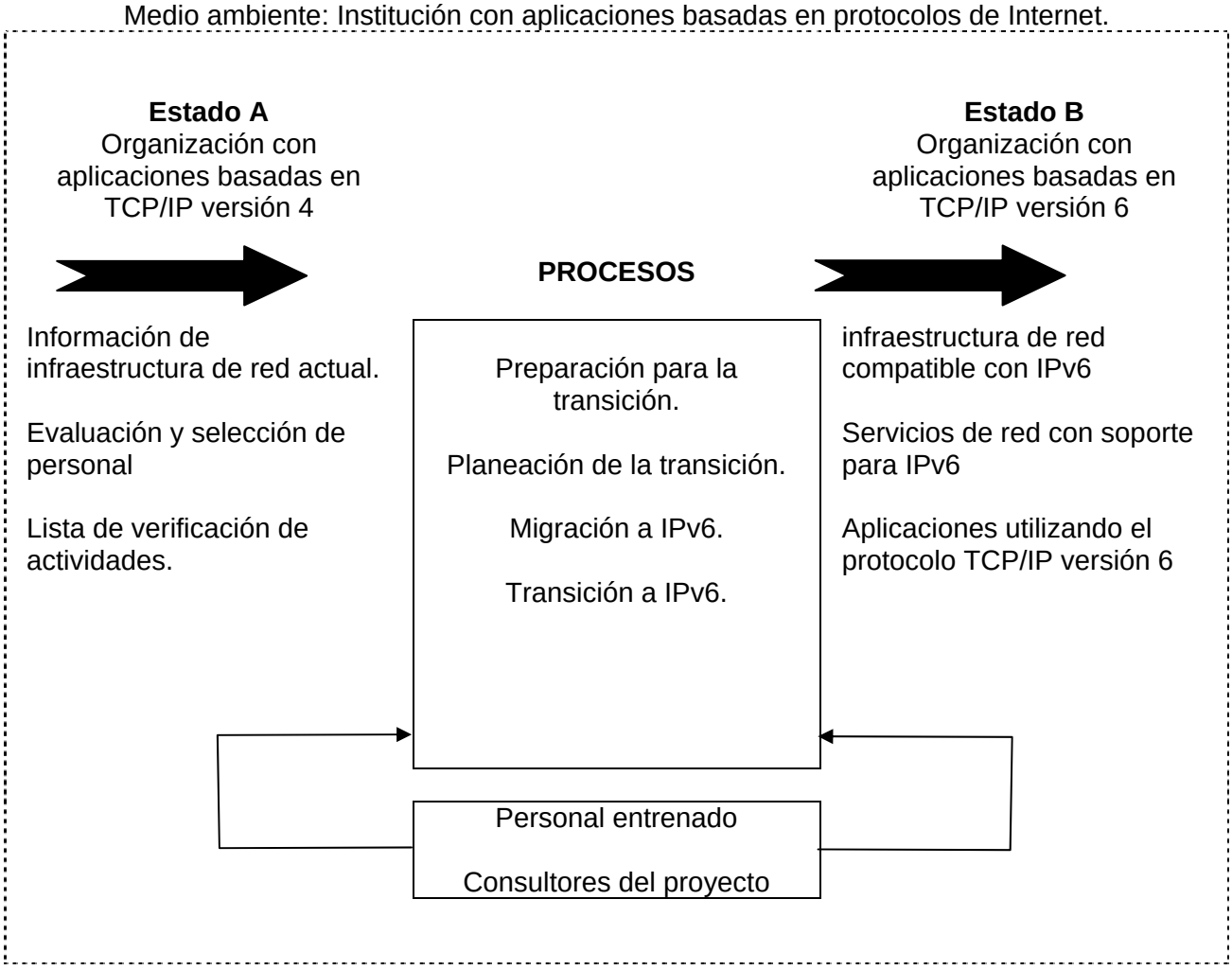


Figura 5.B.1: *Proceso de transición de aplicaciones basadas en el actual protocolo de Internet versión 4 al nuevo protocolo de Internet versión 6.*

2) Preparación

a) Aprendizaje IPv6
Se estima que al menos deberán emplearse cuatro meses para que todo el personal pueda cumplir un plan personalizado de aprendizaje.

Plan A:

Seleccionar un miembro del equipo para recibir entrenamiento sobre IPv6 y ponerlo al frente de la capacitación del todo el personal involucrado.

Plan B:

Asignar a un ente o personal fuera de la empresa para proporcionar un plan de capacitación de todo el personal sobre IPv6.

b) Laboratorio de pruebas IPv6
Instalar un área de prueba, aislada que comprenda al menos las características señaladas en el capitulo de transición, apartado 13.C.2 del *Manual de referencia del protocolo de Internet versión 6*, para facilitar la labor de aprendizaje del personal.

Se sugiere que se adelante la adquisición del equipo a sustituir con el fin de conformar el laboratorio de pruebas que se necesita. Una vez iniciada la transición dicho equipo desplazaría al obsoleto.

3) Planeación de la transición

Las variables a tomar en cuenta en la planeación de la transición a IPv6 en la institución son:

1. *Determinar la arquitectura de la red actual*.
   La infraestructura de red del escenario actual de la institución que se muestra en la figura 7.B.1 del presente capitulo, se resumen en la tabla 5.B.1.

DATOS DEL HARDWARE	
Switch	3COM serie 3800
Router	-
Firewalls	-
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Un equipo con Windows 2003 Server, Edición Empresarial Un equipo con Linux Red Hat Enterprise AS 3
Clientes	5 equipos con Microsoft Windows 98 9 equipos Microsoft Windows XP Profesional SP2
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Se realiza con el servidor Linux
Servidor DHCP	-
Servidor web	IIS 6.0
Servidor de correo electrónico	Send Mail
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	Visual FOX Pro 6.0 Visual Studio 2005

GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	Base de datos de Visual Fox Microsoft SQL 2000 Server
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	-
Proveedor ISP	TELECOM SA de CV

Tabla 5.B.1: *Tabla resumen de la situación actual (IPv4) de la red*

2. *Búsqueda de tecnologías TIC con soporte a IPv6*.
   Buscar con diferentes proveedores dispositivos de hardware y software que soporten IPv6.

3. *Evaluar las políticas de red*.
   Se debe tomar en consideración las políticas de red vigentes y adaptarlas al nuevo protocolo.

4. *Determinar el tiempo estimado para la migración a IPv6*.
   Evaluar con la dirección de la institución el tiempo en el que se debe desarrollar el plan de migración.

5. *Evaluar costos y beneficios de la migración a IPv6*.
   Se deben evaluar las diferentes opciones que ofrecen los proveedores de tecnologías TIC y seleccionar las más apropiadas.

4) Migración

a) Actualización DNS

En términos generales los servicios DNS necesitan de direcciones IPv4 actualmente. Se prevé que con un estado de transición del Internet hacia IPv6 mayoritariamente, se tengan que hacer cambios en el servicio DNS.

b) Actualizar la estructura de red

Según el recurso con que cuenta la compañía, en cuanto a la plataforma del servidor, basta con la modificación de los registro del DNS en el sistema operativo vigente ya que este posee soporte para IPv6, dicho procedimiento se describe ampliamente en el capitulo de transición, apartado 14.F del *Manual de Referencia del protocolo de Internet versión 6.*

Se tienen cinco estaciones de trabajo que operan bajo la plataforma Windows 98, y se recomienda que su hardware sea actualizado por la incompatibilidad con IPv6. En cuanto a las nueve estaciones restantes solo bastara con verificar si se cuenta con el soporte para IPv6 que brinda el ServiPack 2 de Windows XP Profesional, si no se posee este es necesario descargarlo del sitio WEB del proveedor.

En cuanto a los dispositivos de red, la institución posee un Switch 3COM serie 3800, se verifica con el proveedor y este equipo no posee soporte para IPv6, por lo que se recomienda evaluar la compra de un equipo compatible con IPv6.

c) Lista de verificación de actividades para realizar una transición al protocolo IPv6

ETAPAS PARA LA TRANSICION
A. PREPARACION PARA LA TRANSICION A.1 Evaluación del grado de conocimiento previo del personal ☐ Nulo ☐ Poco ☐ Medio ☐ Avanzado A.2 Selección de estrategia de capacitación ☐ Interna ☐ Externa A.3 Creación de un laboratorio de prueba ☐ Instalación ☐ En operación
B. PLANEACION DE LA TRANSICION B.1 Revisión de políticas de sustitución de equipos y actualización de software. ☐ SI ☐ NO (Adjuntar copia de documentos existentes) B.2 Revisión de políticas de administración de red ☐ SI ☐ NO (Adjuntar copia de documentos existentes)
C. MIGRACION A IPv6 C.1 Actualización del entorno DNS • Tipo de consultas: ☐ Solo IPv4 ☐ A elección del cliente C.2 Actualización de la estructura de red • Verificar y recomendar nueva Estructura de red: ☐ Hardware ☐ Software C.3 Obtención de componentes actualizados • Listado de componentes completo: ☐ SI ☐ NO
D. TRANSICION A IPv6 D.1 Habilitar una pila dual (IPv4/IPv6) en todos los servidores ☐ SI ☐ NO D.2 Desplegar clientes habilitados para IPv6 ☐ SI ☐ NO D.3 Desplazar IPv4 ☐ SI ☐ NO

d) Recolección del hardware y software actualizado

Debido a que algunos equipos no soporten la instalación de sistemas operativos más recientes y tampoco se tienen las licencias de éstos, se procede a detallar en las tablas 5.B.2 y 5.B.3 las sustituciones que deberán ejecutarse:

Equipo Actual	**Cambios para implementar IPv6**
Switch 3COM serie 3800	Switch 3COM serie 8100
5 PC Desktop, Pentium II, 450 MHz	5 PC Desktop, Pentium IV, 3.06 GHz

Tabla 5.B.2: *Sustituciones de Hardware que se deben ejecutar.*

Software Actual	**Cambios para implementar IPv6**
5 Licencias Windows 98	5 Licencias por volumen de Microsoft Windows XP Profesional SP2

Tabla 5.B.3: *Sustituciones de Software que se deben ejecutar.*

En el Anexo D del capitulo 10 se presenta una tabla que posee un listado sobre el soporte que diferentes plataformas tienen del protocolo IPv6. Con base a esta lista se determinan los requerimientos de hardware que dichos sistemas operativos necesitan.

5) Transición a IPv6

a) Cronograma de tareas necesarias para realizar la migración a IPv6

En la tabla 5.B.4 se presenta la propuesta de la calendarización de las tareas necesarias para realizar la migración del protocolo de Internet versión 4 al protocolo de Internet versión 6 en la institución.

Id	NOMBRE DE LA TAREA	FECHA INI.	FECHA FIN
1	Instalación y configuración del protocolo IPv6	02/05/2007	25/05/2007
	Diseño de la red IPv6.	02/05/2007	04/05/2007
	Instalar el protocolo IPv6 en todos los nodos de la red.	07/05/2007	09/05/2007
	Asignar direcciones IPv6 a todos los nodos de la red.	10/05/2007	11/05/2007
	Configurar el servicio de ruteo en la red.	14/05/2007	18/05/2007
	Pruebas de la configuración de la red	21/05/2007	25/05/2007
2.	Implementar la estrategia de transición de la pila dual.	28/05/2007	15/06/2007
	Definir una jerarquía de dominio.	28/05/2007	29/05/2007
	Agregar registros “AAAA” al servidor DNS.	30/05/2007	01/05/2007
	Agregar registros de zona inversa al servidor DNS.	04/06/2007	06/06/2007
	Configurar en los equipos cliente el acceso al servidor DNS.	07/06/2007	08/06/2007

Id	NOMBRE DE LA TAREA	FECHA INI	FECHA FIN
	Realizar pruebas de implementación de la pila dual.	11/06/2007	15/06/2007
3.	Actualizar los servicios de red.	18/06/2007	22/06/2007
4.	Probar la operatividad de las aplicaciones.	25/06/2007	27/07/2007
5.	Desplegar clientes habilitados para IPv6	25/06/2007	27/07/2007

Tabla 5.B.4: *Calendarización de tareas para realizar la migración al protocolo IPv6.*

En la figura 5.B.2 se ilustra con el diagrama de Gantt el cronograma de tareas necesarias para realizar la migración al protocolo de Internet IPv6 en la institución, dicho diagrama se encuentra distribuido por semanas.

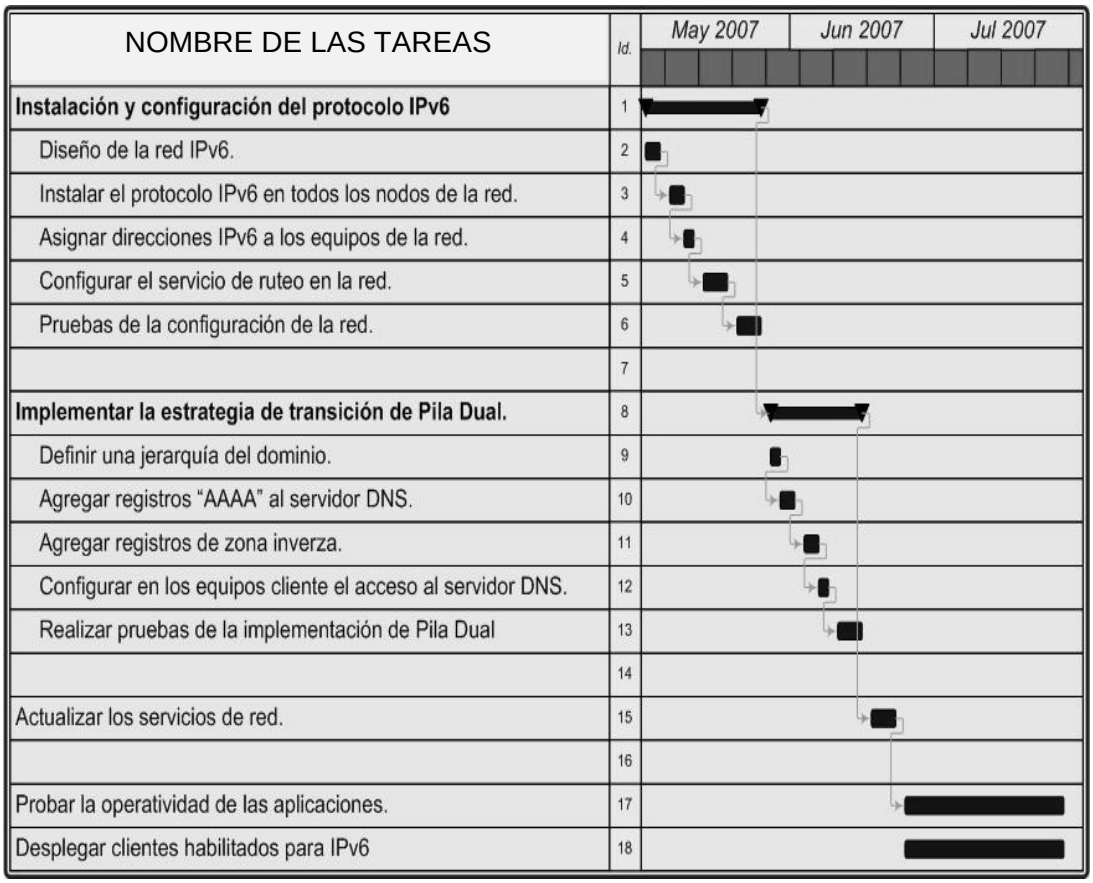


Figura 5.B.2: *Diagrama de Gantt del cronograma de actividades para realizar la migración al protocolo de Internet versión 6 en la institución.*

b) Desplazar IPv4

El desplazamiento completo de IPv4 se llevará a cabo solo cuando IPv4 ya no sea necesario. Por lo tanto este paso no es de cumplimiento radical por el momento.

CONCLUSIONES

Se verificaron algunas de las ventajas del protocolo de Internet versión 6 comparadas con su predecesor IPv4, entre las que se pueden citar las siguientes: un aumento notable en el espacio de direccionamiento, además de facilitar el control de las redes permitiendo crear redes de tamaño homogéneo y asignarlas de forma jerárquica, y que los servicios que en IPv4 son añadidos y adaptados, en IPv6 vienen integrados y son opcionales. Todo esto como producto de la simbiosis entre la teoría desplegada en los RFCs y el soporte efectivo brindado por el software y hardware de redes.

Los documentos establecidos como estándares que rigen la comunicación entre nodos, conocidos como RFCs, establecen el proceso de diseño de software basado en redes que deben seguir los desarrolladores para su correcta implementación. Solamente cuando los fabricantes de software se han apegado a las normas de un RFC se puede verificar que su producto permita al usuario lograr el fin perseguido en la normativa.

Se pudo comprobar mediante la investigación y la ilustración de una red ejemplo que en el protocolo IPv6 la base de datos distribuida DNS no ha presentado modificaciones en su estructura básica sino mas bien solo ha sido necesario extenderla para dar soporte a los registros propios de IPv6.

Al no modificarse los protocolos de la capa de transporte, a las aplicaciones en la capa superior no se les presentan mayores obstáculos para comunicarse con sus pares en otros destinos, pues son otros los protocolos de capas inferiores que manejan las direcciones de dichos destinos.

Debido a que IPv4 e IPv6 son similares en muchos aspectos, se podria intuir que la práctica en redes IPv6 nativas sería una tarea sencilla para un profesional en redes IPv4 nativas. Pero se ha podido verificar en algunas prácticas llevadas a cabo, que a pesar de las similitudes hay conceptos nuevos y estrategias propias de IPv6 que necesitan verificarse *in situ* para poder ser asimilados y debidamente adaptados, más aún cuando es difícil conseguir soporte de algún fabricante o distribuidor.

Partiendo del hecho que hay muchas implementaciones en IPv4 funcionando correctamente y que logran resolverse las necesidades más inmediatas en las redes que conforman Internet, y que además los costos elevados de su implementación marginan el uso de esta tecnología en los presupuestos de pequeñas y medianas empresas, hay que afirmar que el impulso que le dan grandes empresas o instituciones de alcance global que adopten IPv6 como su tecnología a corto o mediano plazo, ampliará la cobertura del soporte que pueden brindar fabricantes a IPv6 y esto conlleve a una reducción en los costos de su implementación para permitir que más usuarios de IPv4 migren a IPv6 sin utilizar recursos en exceso.

En términos generales, sólo después de haber avanzado la cobertura de IPv6 sobre el ambiente dominante de IPv4, en suficiente grado para ser perceptible, entonces se podría precisar cuándo podría prescindirse de IPv4. Es sumamente aventurado precisarlo en estos momentos.

De acuerdo a la experiencia lograda a través de la ejecución de este estudio se ha podido comprobar, que los cambios que puede traer la transición a IPv6, no traerían consigo grandes dificultades tecnológicas para usuarios de Internet que desearan migrar a ese protocolo por cualquier razón que les urgiera. Primero, porque ya los fabricantes de hardware están incorporando software compatible con IPv6. Segundo, los fabricantes de software están diseñando sus plataformas compatibles con IPv6. Tercero, las redes con uno u otro protocolo de Internet (IPv4 o IPv6), pueden convivir aunque no mezclarse. Y cuarto, se puede empezar a generar cuadros de personas capacitadas en la metodología de transición a IPv6 mediante la

utilización de laboratorios de aprendizaje y todo el material bibliográfico que se aporta en esta investigación.

Según se ha podido verificar, la cuestión de migrar o no a IPv6 es una cuestión de conveniencia, pues mientras las aplicaciones de las empresas puedan operar adecuadamente en IPv4 y el costo de la inversión en la actualización o sustitución de recursos para hacerlos compatibles con IPv6, no se perciba recuperable a través de los beneficios que pueda traer dicha migración, no cabría en los planes de empresas de nuestro medio decidirse por tal evento. Esta cuestión sólo se ve posible para aquellas empresas vanguardistas, que a través de una sustitución programada de sus equipos, su software, y una política permanente de capacitación de su personal de TIC, prácticamente estén preparadas en cuanto a esos recursos, y que al visualizar cambios globales en la conformación de la Red favorables a IPv6, perciban oportunas las circunstancias para ejecutar la transición sin ninguna situación traumática. Por lo demás, el resto de empresas tendrían que esperar a mejores condiciones para encontrar el momento justo, sin precisar el tiempo en que podría ocurrir.

RECOMENDACIONES

Se espera que el desarrollo de este estudio sirva como un buen precedente para futuras investigaciones en nuestro medio acerca del protocolo de Internet versión 6 con el fin de ampliar el conocimiento de esta nueva tecnología de comunicación de datos, y así hacer generar estrategias para hacer posible una migración a IPv6 adecuada con los recursos que se disponen.

Deben de hacerse esfuerzos por difundir este material de investigación con el fin de generar una discusión que conlleve a mayor grado de conocimiento sobre esta materia para enriquecer los resultados del presente estudio.

Ya que el Protocolo de Internet versión 6 es una tecnología nueva, se debe tener en cuenta que cualquier situación de transición al protocolo de Internet versión 6 en una red empresarial requiere sobretodo de la asesoría de personas capacitadas que puedan guiar a dicha empresa a través de cada paso en esta tarea.

GLOSARIO DE TERMINOS

ACK: ACKNOWLEDGEMENT (ACK) (Acuse de recibo), en comunicaciones entre computadoras, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si la terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

Agente en casa (Home agent): es un router en el enlace al que pertenece el nodo móvil y en donde ha registrado su actual *dirección de invitado*.

Algoritmo HMAC: Es un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto.

Ámbito (Scope): Representa un área dentro de la cual la dirección puede ser utilizada como identificador único de una o varias interfaces.

ARCnet: Arquitectura de red de área local desarrollado por Datapoint Corporation que utiliza una técnica de acceso de paso de testigo como el Token Ring. La topología física es en forma de estrella, utilizando cable coaxial y hubs pasivos (hasta 4 conexiones) o activos.

Aseguramiento (Binding): Es la asociación de la dirección origen un nodo móvil con una dirección de invitado para ese nodo móvil, junto con el remanente del tiempo de vida de esa asociación.

ATM: El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Autenticación (Authentication): En términos de seguridad de redes de datos, se puede considerar uno de los tres pasos fundamentales (AAA).

BGP4+: Protocolo usado para transferir información de ruteo entre diferentes Sistemas Autónomos.

Borrador (Draft): Documentos de trabajo de la Internet Engineering Task Force (IETF). Los borradores Internet Draft tienen una validez máxima de 6 meses. Pueden ser modificados, reemplazados o quedar obsoletos por otros documentos.

Buró de arquitectura de Internet (IAB): El Internet Architecture Board (IAB) es el comité cargado con del cuido del desarrollo técnico y de ingeniería del Internet por la sociedad de Internet (ISOC).

Cabecera de paquete (Packet header): Contiene la información que intercambian nodos, de tal manera que siempre sean valores válidos. Se visualiza a través de un formato y se utiliza como expresión del conjunto de reglas que definen un protocolo.

Canal completo (Full duplex): Es utilizado en las telecomunicaciones para definir a un sistema que es capaz de mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea.

Cliente DSTM (DSTM client): Un proceso en un nodo DSTM que maneja la dirección IPv4 temporal ubicada por el servidor DSTM.

Cliente Teredo (Teredo client): Nodo que tiene algún acceso al Internet IPv4 y desea obtener acceso al Internet IPv6.

Consulta DNS (DNS query): Son mensajes que pueden enviarse a un servidor de nombres para producir una respuesta.

Consulta DNS inversa (DNS Reverse Lookup): En lugar de suministrar un nombre y solicitar una dirección IP, el cliente DNS provee la dirección IP y pide el correspondiente nombre de dominio. Las *consultas inversas* son también conocidas como *búsquedas inversas (reverse lookups)*.

Cortafuegos (Firewall): Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Datagrama (Datagram): Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el ordenador receptor, de manera independiente a los fragmentos restantes.

DHCPv6: Es un mecanismo de configuración de host centralizado donde el servidor DHCPv6 contiene toda la información ya sea parte del identificador de red como la del identificador del host, así como también es capaz de enviar información adicional como el la dirección del DNS.

Direccion Anycast (Anycast address): El destino es un conjunto de anfitriones en donde todas comparten un solo prefijo de dirección.

Dirección de capa de enlace (Link-layer address): Es un identificador de capa de enlace para una interface.

Dirección de casa (home address): Es una dirección IP asignado al nodo móvil dentro de su prefijo de subred en su enlace origen.

Dirección de invitado (care-of-address): Son direcciones IP asociadas con el nodo móvil que tiene el prefijo de subred de un enlace en particular externo.

Direccion Multicast (Multicast address): El destino es un conjunto de anfitriones, posiblemente en múltiples localidades.

Direccion Unicast (Unicast address): La dirección de destino especifica una sola computadora (host o router), estas son las equivalentes a las direcciones IPv4.

Dominio (Domain): Es una rama del árbol y puede ubicarse en cualquier punto de la estructura del árbol DNS.

Dominio DSTM (DSTM Domain): Las áreas de red en una Intranet donde nodos IPv6 emplean DSTM para asegurar comunicación IPv4.

Encapsulamiento (Encapsulation): Proceso por el cual los datos que se deben enviar a través de una red se colocan en paquetes que se puedan administrar y rastrear. El encapsulado consiste entonces en ocultar los detalles de implementación de un objeto pero, a la vez, se provee una interface pública por medio de sus operaciones permitidas.

Encapsulamiento IPv6 (IPv6 Encapsulation): Radica principalmente en el aprovechamiento máximo de las redes ya existentes como ATM, con el manejo de ruteo de paquetes IPv6, que

también puede utilizarse para la distribución de estos paquetes dentro de un grupo de vecinos.

Encriptación (Encryption): Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.

EQ: Equipo móvil del usuario.

Espacio de nombres de dominio (Domain name space): Es una especificación para un espacio de nombres estructurado en forma de árbol y los datos asociados con los nombres, donde cada nodo y hoja del árbol del espacio de nombre de dominio denomina a un conjunto de información, y donde se procura realizar operaciones de consulta para extraer tipos específicos de información de un conjunto particular. En términos prácticos, se habla de que el espacio de nombres de dominio es una base de datos distribuida entre distintos medios de procesamiento y almacenamiento independientes (servidores).

Ethernet: Ethernet es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de ether.

Fragmentación (Fragmentation): E el tamaño del paquete más grande que esa red puede transmitir. Los paquetes más grandes que el MTU permisible se deben dividir en los paquetes más pequeños múltiples, o los fragmentos, para permitiros atravesar la red.

Función Hash: Es un método para resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash o búsqueda es el resultado de dicha función o algoritmo.

Host: A una máquina conectada a una red de computadores y que tiene un nombre de equipo (en inglés, hostname, es un nombre único que se le da a un dispositivo conectado a una red informática.

IANA: El Internet Assigned Numbers Authority, una organización que supervisa direcciones IP, dominio a nivel superior y las asignaciones del punto de código del protocolo de Internet.

ICMP: El Protocolo de Control de Mensajes de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP).

ICMPv6: El ICMP para IPv6 (versión 6 del Internet Control Message Protocol) es una parte integral de la arquitectura IPv6 y se debe apoyar totalmente por todas las puestas en práctica IPv6.

IDRPv2: Es un protocolo de basado en el vector de ruta definido en el ISO 10747. Al igual que BGP-4, el IDRP es utilizado entre sistemas autónomos, conocido como dominio de ruteo IDRP.

IEEE 1394: El IEEE 1394 o FireWire o i.Link es un estándar multiplataforma para entrada/salida de datos en serie a gran velocidad. Suele utilizarse para la interconexión de dispositivos digitales como cámaras digitales y videocámaras a ordenadores.

IEEE: IEEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricistas y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros en eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación.

IETF: Grupo de esfuerzo de Ingeniería de Internet.

IND: El descubrimiento inverso de vecinos es usado por los nodos (anfitriones y routers) para determinar las direcciones de la de capa de enlace para los vecinos conocidos para residir en acoplamientos de enlace y para purgar rápidamente los rangos de valores que llegan a ser inválidos.

Internet: Interconexión particular de computadoras, de carácter global y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales.

IP: Protocolo de Internet.

IPng: Protocolo de Internet de próxima generación, asi se le llamo inicialmente a IPv6 antes de en su camino a convertirse en estándar de Internet.

IPv4: Es la versión 4 del Protocolo IP (Internet Protocol). Fue la primera versión del protocolo que se implementó de forma extensa y forma la base de Internet.

IPv6: Es la versión 6 del Protocolo de Internet un estándar de la capa de red su función es dirigir y encaminar los paquetes a través de una red.

ISATAP: Mediante este mecanismo se conectan automáticamente host y routers sobre redes IPv4 de un mismo sitio.

IS-IS: Como el IS dual, es un protocolo de ruteo de estado de enlace que es muy similar al OSPF y que ha sido definido por la Organización Internacional para la Estandarización en el documento ISO 10589. Este protocolo de ruteo fue diseñado independiente del protocolo de la red. IS-IS fue adaptado fácilmente para IPv6 añadiendo unos cuantos valores de tipo y longitud.

Isla IPx (IPx island): una red operando en el protocolo IPx de forma nativa.

LSA (Anuncio de estado de enlace): consiste de un prefijo de dirección para la red y para cada router que es conectado y el costo asignado a estas redes.

MAC: En redes de computadoras la dirección MAC (Media Access Control address) es un identificador hexadecimal de 48 bits que se corresponde de forma única con una tarjeta o interfaz de red.

Mascara de red (Network mask): La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Sirve para que un ordenador (principalmente la puerta de enlace, router...) sepa si debe enviar los datos dentro o fuera de la red.

Métrica: Número que indica la distancia que existe hacia el destino final (número de saltos).

Migración (Migration): sería la acción global y el efecto generado al cambiar un entorno prevaleciente en IPv4 a uno completamente en IPv6, donde todo el soporte a IPv4 fuese desechado.

MLD: Protocolo que permite que cada router IPv6 descubra la presencia de escuchas multicast en los enlaces a los que están conectados directamente, utilizando mensajes ICMPv6.

Modelo OSI: El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos de comunicaciones de computadoras cumplen con los lineamientos del Modelo OSI.

MTU: Unidad máxima de transferencia (Maximum Transfer Unit - MTU) es un término de redes de computadoras que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.

NBMA: Es el termino usado para describir las redes que usan circuitos virtuales para su conectividad.

NCP: Network Control Program (NCP), se puede referir a: Conjunto original de protocolos de control de red de ARPANET, NetWare Core Protocol (Protocolo Principal Netware), en SNA es el programa que reside en la unidad de control de comunicaciones y el cual controla a la red que depende de esa unidad de control.

ND: Se focaliza en que todos los nodos (host o routers) que ocupen el nuevo protocolo de Internet IPv6 utilicen el descubrimiento de vecindario para determinar las direcciones de la capa de enlace de todos los otros nodos que se encuentran en la interfaz de red y verifiquen si estos nodos continúan siendo alcanzables.ARP: son las siglas en inglés de Address Resolution Protocol (Protocolo de resolución de direcciones).Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

Negociador de túneles (Tunnel Broker): Es el lugar donde el usuario se conecta para registrar y activar túneles.

Nodo (Node): Punto de intersección o unión de varios elementos que confluyen en el mismo lugar. Puede ser un enrutador.

Nodo correspondiente (Correspondent node): Es un nodo puntual con el cual el nodo móvil esta comunicándose. El nodo correspondiente puede se tanto móvil como estacionario.

Nodo DSTM: Nodo que implementa ambas pilas IPv4 e IPv6, tuneleado 4 sobre 6 y es un cliente DSTM.

Nodo móvil (Movil node): Es aquel cambia su punto de conexión de un enlace a otro, mientras aún es alcanzable mediante su dirección de casa.

Nombre de dominio (Domain name): Es más que una forma fácil de recordar una dirección IP y que está unívocamente asociada a ésta bajo una autoridad correspondiente.

Nube IPx (IPx cloud): Una red grande, posiblemente Internet, operando en el protocolo IPx de forma nativa.

Octeto (Octect): Es una unidad de medida que equivale a 8 bits y que es independiente del hardware.

OSPFv6: Es el protocolo de estado del enlace definido en el RFC2740 y designado para mantenimiento de la tabla de ruteo dentro de un sistema autónomo simple.

Paquete (Packet): Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo.

Ping: Valiosa herramienta de diagnóstico utilizada para determinar si un host particular está conectado a la misma red que cualquier otro host.

PPP: Protocolo punto a punto, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

Protocolo (Protocol): Es un conjunto de reglas expresadas a través de un software que permiten gestionar y establecer la comunicación entre computadoras conectadas en red. Estos mecanismos permiten que un programa de aplicación que utilice una red para intercambiar mensajes no interactúe directamente con el hardware de la red sino que lo haga indirectamente por medio del software de los protocolos de comunicación que se encargarán de ir llevando los mensajes por etapas o capas funcionales que componen el ejercicio de la comunicación entre computadoras.

Protocolo de Pasarela Exterior (EGP): Son protocolos que emplea vecinos exteriores para difundir la información de accesibilidad a otros sistemas autónomos.

Protocolo de Pasarela Interior (IGP): Son un conjunto de protocolos usados dentro de un sistema autónomo. Los protocolos IGP más utilizados son RIP, OSPF y IS-IS. IGP es un protocolo que genera tablas de enrutamiento dentro de un sistema autónomo.

Protocolo de ruteo interior (Interior routing protocol): Es aquel que intercambia información de ruteo entre routers dentro de un sistema autónomo.

Proveedores de servicios de Internet (ISP): Acrónimo en inglés de Internet Service Provider (Proveedor de Servicios de Internet), empresas dedicadas a conectar a Internet la línea telefónica de los usuarios, redes distintas e independientes o ambas.

Puerto (Port): Un puerto de red es una interfaz para comunicarse con un programa a través de una red.

PVC: Permanent virtual circuit (PVC). Un circuito virtual permanente (PVC) es una conexión lógica software-definida en una red tal como una red FRAME RELAY.

Red privada virtual (VPN): Una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Registro de recursos (Resource register): son archivos en la base de datos DNS que puede utilizarse para configurar un servidor de base de datos DNS.

Resolventes (Resolvers): Programas que extraen información de los servidores de nombre de dominio en respuesta a las peticiones de clientes DNS.

Retransmisor Teredo (Teredo relay): Router IPv6 que puede recibir tráfico destinado a clientes Teredo y reenviarlo utilizando el servicio Teredo.

RFC: Acrónimo inglés de Request For Comments (Requerimiento de comentarios). Conjunto de archivos de carácter técnico donde se describen los estándares o recomendaciones de cualquier estándar. Entre uno de ellos los de la propia Internet.

RIPng: Se basa en el protocolo de transporte UDP donde envían y se reciben paquetes UDP sobre el puerto número 521 (puerto RIP). Así también todas las comunicaciones entre los routers que usan el protocolo RIP son enviadas a este puerto al igual que los mensajes de actualización de ruteo.

Router (enrutador o encaminador): es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este

dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

RPT: Son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de aplicación (no de nivel de transporte, como su nombre podría hacer pensar) utilizado para la transmisión de información en tiempo real, como por ejemplo audio y video en una video conferencia.

Ruta (Route): Una ruta es la forma general de un nombre del archivo o de directorio, dando el nombre de un archivo y su localización única en un sistema de archivos.

Ruteo (Routing): En comunicaciones, el 'encaminamiento' (a veces conocido por el anglicismo ruteo o enrutamiento) es el mecanismo por el que en una red los paquetes de información se hacen llegar desde su origen a su destino final, siguiendo un camino o ruta a través de la red. En una red grande o en un conjunto de redes interconectadas el camino a seguir hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.

Ruteo IP (IP routing): Es proceso de envió de datagramas basados en la dirección IP de destino. El ruteo es realizado por medio de envíos de un host TCP/IP o de un router IP. Cualquiera que sea el caso, la capa de red en el envió del host o del router, debe decidir hacia donde enviar el datagrama, o sea la ruta hacia el destino final.

SCTP: Es un protocolo de comunicación de capa de transporte que fue definido por el grupo SIGTRAN de IETF en el año 2000. El protocolo está especificado en la RFC 2960, y la RFC 3286.

Servidor de túnel (Tunnel server): Es un router de pila dual (IPv6 e IPv4) conectado al Internet global.

Servidor DSTM (DSTM Server): Un proceso a cargo de manejar el espacio de direccionamiento IPv4 que será asignado a nodos DSTM.

Servidor Teredo (Teredo Server): Nodo que acceso al Internet IPv4 a través de una dirección ruteable globalmente, y que utilizado como un colaborador para proveer conectividad IPv6 a clientes Teredo.

Servidores de nombre de dominio (Domain name server): Programas especiales de servidor que almacenan registros de recursos e información acerca de la estructura de árbol del dominio, y que permiten contestar a las solicitudes de los clientes DNS, consultando para ello sus bases de datos de resolución de dominios.

Sistema Autónomo (AS): Es un conjunto de redes y dispositivos router IP que se encuentran administrados por una sola entidad (o en algunas ocasiones varias) que cuentan con una política común de definición de trayectorias para Internet.

Socket: Interfaz entre programas de aplicación y software de protocolo, y que es particular de un sistema operativo.

SOCKS: Una sistema pasarela que acepta conexiones SOCKS mejoradas desde hosts IPv4 y retransmitiendo a hosts IPv4 o IPv6.

SPI: Es una cadena de bits asignada a la asociación de seguridad y que sirve como un puntero hacia la base de datos de esta.

Subneteo (Subnetting): Proceso mediante el cual se subdividen las redes, creando así redes diferentes en sus parámetros de configuración como dirección IP, DNS e inclusive el gateway.

Suma de verificación (Checksum): Este campo de 16 bits se utiliza para detectar corrupción en los datos del mensaje ICMPv6 y de las partes de la cabecera IPv6.

SVC (Switched virtual circuit) (SVC): Es un circuito virtual temporal que se establece y se mantiene solamente para la duración de una sesión de la transferencia de datos.

TCP/IP: Es la base de Internet que sirve para comunicar computadoras que utilizan diferentes plataformas, las cuales pueden ser computadoras personales PC, minicomputadoras y servidores centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP: (TCP en sus siglas en inglés, Transmission Control Protocol que fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn) es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por ordenadores pueden usar TCP para crear *conexiones* entre ellos a través de las cuales enviarse datos.

TEREDO: Es un servicio que posibilita que nodos ubicados detrás de uno o más NATs obtengan conectividad a IPv6 tuneleando paquetes sobre UDP.

TIC: Tecnologías de Información y Comunicaciones.

Tipo de registro de recurso A6 (A6 resource register type): Este registro fue desarrollado en el RFC2874 y no ha podido desplazar al AAAA por su complejidad inherente, de tal manera que en el RFC3363 fue reclasificado a la categoría de experimental.

Tipo de registro de recurso AAAA (AAAA resource register type) : Este registro de recurso almacena una sola dirección IPv6 de 128 bits en el campo Datos de recurso (RDATA).

Tipo de Registro de Recurso para IPv6 (IPv6 resource register type): Son dos los registros de recursos definidos para mantener direcciones IPv6 y enlazarlas a nombres de dominio con diferente complejidad.

Traceroute: Es una herramienta de la red de ordenadores usada para determinar la ruta tomada por los paquetes a través de una red del IP. IPv6 una variante, traceroute6, está también extensamente disponible.

Trama (Frame): En telecomunicaciones una trama es una unidad de envío de datos. Viene a ser sinónimo de paquete de datos o paquete de red, aunque se aplica principalmente en los niveles OSI más bajos, especialmente en el Nivel de enlace de datos.

Transición (Transition): Es la primera meta hacia el manejo de una red en un entorno IPv6 que no implica una interrupción de las operaciones corrientes con IPv4, en un ámbito inicial reducido.

Tunel (Tunnel): Mecanismo que permite utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapulados en paquetes IPv4.

UDP: Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Vecindario (Neigborhood): Nodos adjuntados a un mismo enlace.
VLAN: Red conmutada particionada via software según las necesidades de una empresa sin importar la ubicación física de los usuarios.

Zona (Zone): Es una porción contigua de un dominio del espacio de nombres DNS cuyos registros de base de datos existen y son manejados en un archivo particular de base de datos DNS en uno o varios servidores DNS.

BIBLIOGRAFIA

A. Libros.

1) Loshin, Pete
IPv6: Theory, Protocol, and Practice. 2a. Edición.
Morgan Kaufmann Publishers (Elsevier, Inc.), 2004.

2) Blanchet, Marc
Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks.
John Wiley & Sons Ltd., 2006.

3) Comer, Douglas E.
Redes globales de Información con Internet y TCP/IP. 3a. Edición.
Prentice-Hall Hispanoamérica, S.A., 1996.

4) Wegner, J. D., Rockwell, Robert
IP Addressing and Subnetting including IPv6.
Syngress Media Inc., 2000.

5) Comer, Douglas E.
Computer Networks and Internets. 2a. Edición.
Prentice Hall International, Inc.1999.

6) Hagino, Jun-ichiro itojun
IPv6 Network Programming. 1a. Edición.
Elsevier, Inc. 2005.

B. Páginas web.

1) url: www.twnic.net.tw/download/seminar/ipv612a.ppt
archivo: ipv612a
tema: IPv4 to IPv6 Transition, Interoperability and Issues
autor: Shiao-Li Charles Tsao
fecha de acceso: Noviembre /2006

2) url: internetng.dit.upm.es/ponencias-jing/2001/david-fernandez.PDFarchivo: ipv612a
archivo: david-fernandez.pdf
tema: Introducción al Protocolo IPv6
autor: David Fernández Cambronero
fecha de acceso: Octubre /2006

3) url: www.ipv6.unam.mx/documentos/Taller-IPv6.pdf
archivo: Taller-IPv6.pdf
tema: IPv6. El protocolo para la nueva Internet
autor: Christian Lazo Ramírez, Azael Fernández Alcántara
fecha de acceso: Agosto /2006

4) url: www.cu.ipv6tf.org/pdf/DesarrolloAPI.PDF
archivo: DesarrolloAPI.pdf
tema: Desarrollo de Aplicaciones con Soporte IPv6
autor: Ing. Azael Fernández Alcántara
fecha de acceso: Octubre /2006

5) url: www.si.uji.es/bin/docs/projectes/ipv6/ipv6p.pdf
archivo: ipv6p.pdf
tema: IPv6 @ UJI – Rev : 22
autor: Luis Peralta
fecha de acceso: Mayo /2006

6) url: www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf
archivo: Tutorial%20de%20IPv6.pdf
tema: Tutorial de IPv6
autor: Jordi Pallet Martínez
fecha de acceso: Mayo /2006

7) url:www.microsoft.com/technet/itsolutions/network/evaluate/technol/tcpipfund/tcpipfund.mspx - 24k
archivo: TCPIP_Fund.pdf
tema: TCP/IP Fundamentals for Microsoft Windows
autor: Joseph Davies – Microsoft
fecha de acceso: Junio /2006

8) url: www.rediris.es/red/reuniones/IPv6practico.pdf
archivo: IPv6practico.pdf
tema: IPv6 Práctico
autor: José M. Femenía
fecha de acceso: Junio /2006

9) url: www.cu.ipv6tf.org/conf/tutorial-talleripv6.ppt
archivo: tutorial-talleripv6
tema: Tutorial IPv6. Una Aproximación Técnica de Implementación
autor: MSc.Jorge Daniel Villa Hernández
fecha de acceso: Noviembre /2006

10) url: amesthornton.com/redhat/linux/Enterprise/3/Reference-Guide/
tema: Chapter 10. Apache HTTP Server
autor: James Thornton
fecha de acceso: Noviembre /2006

11) url: www.ipv6.ernet.in/deepaksharma1.ppt
archivo: deepaksharma1
tema: IPv6 Host Configuration
autor: Deepak Sharma Network Engineer
fecha de acceso: Noviembre /2006

12) url: www.6sos.net/documentos/6SOS_Instalacion_IPv6_Windows_v4_0.pdf
archivo: 6SOS_Instalacion_IPv6_Windows_v4_0
tema: Instalación de IPv6 en plataformas Windows
autor: 6SOS
fecha de acceso: Noviembre /2006

13) url: http://www.gentoo.org/
enlace: Guía del router IPv6 en Gentoo
autor: Gentoo Fundation
fecha de acceso: Noviembre /2006

14) url: www.gulic.org/comos/LARTC
archivo: en linu
tema: Enrutamiento avanzado y control de tráfico en Linux
autor: Bert Hubert
fecha de acceso: Noviembre /2006

15) url: web.mit.edu/rhel-doc/3/rhel-rg-es-3/index.html
archivo: rhel-rg-es
tema: Red Hat Enterprise Linux 3: Manual de referencia
autor: Red Hat, Inc.
fecha de acceso: Noviembre /2006

16) url: http://www.linuxparatodos.net/geeklog/
tema: Configuración básica de Apache.
autor: Joel Barrios Dueñas
fecha de acceso: Noviembre /2006

17) url: www.6sos.net/documentos/6SOS_Instalacion_IPv6_Linux_v4_0.pdf
archivo: 6SOS_Instalacion_IPv6_Linux_v4_0
tema: instalación de IPv6 en plataformas linux
autor: 6SOS
fecha de acceso: Noviembre /2006

18) url: http://www.microsoft.com/windowsserver2003/technologies/ipv6
Tema: Microsoft Windows IPv6
Autor: ©2007 Microsoft Corporation
Fecha de acceso: Marzo de 2007

19) url: http://technet2.microsoft.com/windowsserver/es/library/
Tema: Comandos Netsh para la interfaz IPv6
Autor: ©2007 Microsoft Corporation
Fecha de acceso: Marzo de 2007

ANEXOS

A. Listado de RFCs y Borradores.

No.	RFC	Título	Capítulo
1	768	User Datagram Protocol	11 MR[30]
2	791	Internet Protocol	1 MR
3	793	Transmission Control Protocol	11MR
4	813	Window and Acknowledgement Strategy in TCP	11MR
5	1034	Domain Names - Concepts and Facilities	8 MR
6	1035	Domain Names – Implementation and Specification	8 MR
7	2080	RIPng for IPv6	7 MR
8	2136	Dynamic Updates in the Domain Name System	8 MR
9	2181	Clarifications to the DNS Specification	8 MR
10	2375	IPv6 Multicast Address Assignments	3 MR
11	2401	Security Architecture for the Internet Protocol	10 MR
12	2402	IP Authentication Header	10 MR
13	2450	Proposed TLA and NLA Assignment Rules	3 MR
14	2460	Internet Protocol, Version 6, Specification	2 MR
15	2461	Neighbor Discovery for IP Version 6	5 MR
16	2462	IPv6 Stateless Address Autoconfiguration	6 MR
17	2463	Internet Control Message Protocol for the Internet Protocol Version 6 Specification	4 MR
18	2464	Transmission of IPv6 Packets over Ethernet Networks	12 MR
19	2467	Transmission of IPv6 Packets over FDDI Networks	12 MR
20	2470	Transmission of IPv6 Packets over Token Ring Networks	12 MR
21	2472	IP Version 6 over PPP	12 MR
22	2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks	5/12 MR
23	2492	IPv6 over ATM Networks	12 MR
24	2497	Transmission of IPv6 Packets over ARCnet Networks	12 MR
25	2526	Reserved IPv6 Subnet Anycast Addresses	3 MR
26	2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels	13 MR
27	2535	Domain Name System Security Extensions	8 MR
28	2590	Transmission of IPv6 Packets over Frame Relay Network Specification	12 MR
29	2710	Multicast Listener Discovery for IPv6	4 MR
30	2732	Format for Literal IPv6 Addresses in URL's	3 MR
31	2740	OSPF for IPv6	7 MR
32	2765	Stateless IP/ICMP Translation Algorithm	13 MR
33	2766	Network Address Translation - Protocol Translation	13 MR
34	2767	Dual Stack Hosts using the Bump-In-the-Stack Technique	13 MR
35	2782	A DNS RR for specifying the location of services	8 MR

[30] MR : Manual de Referencia

No.	RFC	Título	Capítulo
36	2874	DNS Extensions to Support IPv6 Address Aggregation and Renumbering	8 MR
37	2893	Transition Mechanisms for IPv6 Hosts and Routers	13 MR
38	2894	Router Renumbering for IPv6	4 MR
39	2915	The Naming Authority Pointer DNS Resource Record	8 MR
40	2960	Stream Control Transmission Protocol	11MR
41	3007	Secure Domain Name System Dynamic Update	8 MR
42	3024	Reverse Tunneling for Mobile IP	9 MR
43	3031	Multi-Protocol Label Switching Architecture	13 MR
44	3053	IPv6 Tunnel Broker	13 MR
45	3056	Connection of IPv6 Domains via IPv4 Clouds	13 MR
46	3089	A SOCKS-based IPv6/IPv4 Gateway Mechanism	13 MR
47	3122	Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification	5 MR
48	3142	An IPv6-to-IPv4 Transport Relay Translator	13 MR
49	3146	Transmission of IPv6 Packets over IEEE 1394 Networks	12 MR
50	3152	Delegation of IP6.ARPA	8 MR
51	3168	The Addition of Explicit Congestion Notification to IP	11 MR
52	3177	IAB/IESG Recommendations on IPv6 Address Allocations to Sites	3 MR
53	3309	Stream Control Transmission Protocol Checksum Change	11 MR
54	3314	Recommendations for IPv6 in Third Generation Partnership Project Standards	9 MR
55	3315	Dynamic Host Configuration Protocol for IPv6	6 MR
56	3338	Dual Stack Hosts Using Bump-in-the-API	13 MR
57	3363	Representing Internet Protocol version 6 Addresses in the Domain Name System	8 MR
58	3364	Tradeoffs in Domain Name System Support for Internet Protocol version 6	8 MR
59	3493	Basic Socket Interface Extension for IPv6	1 MT[31]
60	3513	Internet Protocol Version 6 Addressing Architecture	3 MR
61	3572	Internet Protocol Version 6 over MAPOS	12 MR
62	3596	DNS Extensions to Support IP Version 6	8 MR
63	3775	Mobility Support in IPv6	9 MR
64	3810	Multicast Listener Discovery Version 2 for IPv6	4 MR
65	3845	DNS Security NextSECure RDATA Format	8 MR
66	3971	Secure Neighbor Discovery (SEND)	4 MR
67	4034	Resource Records for the DNS Security Extensions	8 MR
68	4065	Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations	4 MR
69	4214	Intra-Site Automatic Tunnel Addressing Protocol	13 MR
70	4286	Multicast Router Discovery	4 MR
71	4271	A Border Gateway Protocol 4	7 MR
72	4291	IP Version 6 Addressing Architecture	3 MR

[31] MT : Metodología de Transición.

No.	RFC	Título	Capítulo
73	4311	IPv6 Host-to-Router Load Sharing	5 MR
74	4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four	6 MR
75	4380	Teredo: Tunneling IPv6 over UDP through Network Address Translations	13 MR
76	4443	Internet Control Message Protocol for the Internet Protocol Version 6 Specification	4 MR
77	4460	Stream Control Transmission Protocol Specification, Errata and Issues	11 MR
78	4554	Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks	10 MR

No.	ID de Borrador	Título de Borrador	Capítulo
1	draft-ietf-ngtrans-dstm-08	Dual Stack Transition Mechanism	13 MR
2	draft-blanchet-v6ops-tunnelbroker-tsp-03	IPv6 Tunnel Broker with the Tunnel Setup Protocol	13 MR
3	draft-ooms-v6ops-bgp-tunnel-06	Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers	13 MR
4	draft-ietf-ngtrans-introduction-to-ipv6-transition-08	A Guide to the Introduction of IPv6 in the IPv4 World	13 MR

B. Formulario de LACNIC para solicitud de bloque de direcciones IPv6.

```
#  Do not remove version number.
LACNIC IPV6 Template 20060503-2-EN

#  Send this request to hostmaster@lacnic.net

#  Information about the Organization.
#  If your organization already holds resources that are registered
#  with LACNIC, please provide the "OwnerID" and the Organization name
#  as it is registered in our system. If you do not know
#  your "OwnerID", please check a resource allocated to your
#  organization at LACNIC's WHOIS server:
#  http://whois.lacnic.net

0a. Organization ID. (OwnerID):
0b. Name of the Organization:
0c. Postal address:
0d. City:
0e. State:
0f. Country:
0g. ZIP Code:

#  Points of contact at the organization.
#  You must inform the technical, billing, and membership contacts.
#  The billing and membership contacts are internal and
#  therefore they are not visible through whois queries.
#  Inform only the contacts' "UserID" .
#  If you do not have points of contact, please create them at:
```

http://lacnic.net/newid/SP

1a. Technical contact ID. (UserID):
1b. Billing contact ID. (UserID):
1c. Membership contact ID. (UserID):

Provide information about the organization
requesting the IPv6 Block.

2a. Organization Overview:

Internet connection.
Specify service provider(s) name, postal address, ASN,
and status of provider's connection. If you have more than
one provider, copy the items below as many times as necessary.

3a. Service Provider Name:
3b. Postal Address:
3c. Service Provider ASN:
3d. Connectivity Status:

Provide information about expected date for deployment of IPv6
network, IPv6 address utilization plan, and plan for assigning IPv6
addresses to the organization's customers.

4a. Deployment Plan:
4b. Addressing Plan:
4c. Customer Assignment Plan:

Provide information about the IPv6 network structure
and the type of service that will be offered to the customers.
If you are requesting a prefix longer than a /32,
you must also provide information to justify this need.

5a. Additional information:

Do not remove this line.
End of template

C. ENCUESTAS REALIZADAS A EMPRESAS

Clasificación de la empresa según sector: NO GUBERNAMENTAL **Persona entrevista: Jefe de la unidad informática**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Medio
DATOS DEL HARDWARE	
Switch	Switch 3COM 3800
Router	Router CISCO 3500 Series
Firewalls	Firewall Appliance DFL-CP310
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Windows 2003 Server SP1

Clientes	Windows 2000 Windows XP SP2
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Se realiza a través de router
Servidor DHCP	Se realiza a través de router
Servidor web	IIS 6.0
Servidor de correo electrónico	Microsoft Exchange Server 2003
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	Microsoft Visual Estudio 2005
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	SQL Server 2005
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	Se realiza con el Firewall de la organización.
Proveedor ISP	TELECOM S.A. de C.V.
COMENTARIOS DE LA PERSONA ENTREVISTADA	

En la entrevista se comentó que la institución cuenta con políticas de actualización de hardware según las necesidades de software de la organización. Además que en promedio renueban sus TIC cada 3 años y que actualmente están analizando la opción de que los servicios básicos de red como lo son el servidor de correo electrónico y el servidor web se migren a software libre.

La persona entrevistada manifestaba que ha empezado a investigar por su cuenta sobre el nuevo protocolo de Internet IPv6 y las impresiones que posee de este son las siguientes:

1. Actualmente existe una falta de información organizada sobre este protocolo por lo que no es fácil conocer sobre IPv6.
2. Las empresas Salvadoreñas no ven la necesidad de migrar a este protocolo aunque esta persona si tiene el conocimiento que en otros países desarrollados ya se esta realizando esta migración y que tarde o temprano las instituciones de nuestro país tendrán la necesidad inmediata de realizar esta migración, por lo que a la hora de actualizar el hardware y software de la institución se toma en cuenta el soporte para el protocolo IPv6.

Tambien nos comento la persona entrevistada que si por ejemplo el año 2008 se tuviera la necesidad de migrar a este protocolo en nuestro país esta institución estaría preparada en cuanto a hardware y software pero se tendría la necesidad de buscar a la gente capacitada para realizar la migración a IPv6.

Clasificación de la empresa según sector: SERVICIOS **Persona entrevistada: Administrador de redes**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Medio
DATOS DEL HARDWARE	
Switch	Switch 3COM 2250
Router	-
Firewalls	Switch CISCO Catalyst Serie 2950
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Microsoft Windows 2003 Server Standard Edition
Clientes	Microsoft Windows XP Pro SP2
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Servicio DNS Windows 2003 Server
Servidor DHCP	Servicio DHCP Windows 2003 Server
Servidor web	IIS 6.0
Servidor de correo electrónico	Proveedor externo
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	Microsoft Visual Estudio 2005
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	SQL Server 2000
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	directivas de seguridad del servidor
Proveedor ISP	TELECOM S.A. de C.V.
COMENTARIOS DE LA PERSONA ENTREVISTADA	
En la entrevista se comento que en el caso de que se diera una migración al nuevo protocolo IPv6 lo único que se tendría que hacer es buscar proveedores ISP que hayan realizado la migración a este protocolo y que para el caso de esta institución que se dedica a la comercialización de hardware y software serian los proveedores de estos los encargados de actualizar sus productos, así que desde el punto de vista de la persona entrevistada los problemas que podrían enfrentar las instituciones para migrar a este protocolo serian los siguientes: 1. Las unidades informáticas de la mayoría de instituciones de El Salvador no se les da la importancia debida y por eso piensan 2 veces antes de invertir en actualizar las TIC de la institución. 2. Se necesita contar con una documentación detallada sobre la administración en todos los sentidos (seguridad, disponibilidad, infraestructura, operatividad, etc.) de las redes institucionales que trabajen sobre IPv6.	

Clasificación de la empresa según sector: FINANCIERA **Persona entrevistada: Jefe de la unidad informática**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Nulo
DATOS DEL HARDWARE	
Switch	DELL PowerConnect Serie 5000
Router	-
Firewalls	-
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Microsoft Windows 2000 Server SP4
Clientes	Microsoft Windows 98 Microsoft Windows XP Pro SP2
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Servicio DNS Windows 2000 Server
Servidor DHCP	Servicio DHCP Windows 2000 Server
Servidor web	Proveedor externo
Servidor de correo electrónico	Proveedor externo
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	ForT
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	ORACLE
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	directivas de seguridad del servidor
Proveedor ISP	-
COMENTARIOS DE LA PERSONA ENTREVISTADA	
No hubo comentarios.	

Clasificación de la empresa según sector: EDUCACION **Persona entrevistada: Jefe del departamento de redes**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Medio
DATOS DEL HARDWARE	
Switch	6 switch 3COM 3800
Router	CISCO 2800 Series
Firewalls	-
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Microsoft Windows 2003 Server
Gateway	Linux FEDORA 4
Clientes	Windows XP
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Se realiza con el router
Servidor DHCP	Se realiza con la plataforma Linux FEDORA 4
Servidor web	Apache 2.0
Servidor de correo electrónico	Hosting externo
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	PHP (para las aplicaciones web) Visual Basic 2005 (para aplicaciones de la institución)
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	MySQL (para las aplicaciones web) SQL Server 2005 (para aplicaciones de la institución)
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	-
Proveedor ISP	TELECOM
COMENTARIOS DE LA PERSONA ENTREVISTADA	
Dentro de la institución existen políticas para actualizar el hardware y el software que se emplea en la institución. Dichas políticas corresponden a las necesidades de Software y al tiempo de vida del hardware. Tabien se comento en la entrevista que dentro de la institución cuentan con el equipo que de soporte a IPv6 pero que por el momento no se ve la necesidad del porque preocuparse por realizar una migración, aunque nos expreso la persona entrevistada que el tema le llama mucho la atención y por lo que pudimos conversar con el conoce bastante del protocolo IPv6. Nos expresó también que según lo que él ha investigado en un dado caso se necesitara migrar al nuevo protocolo de Internet versión 6 las únicas inversiones que se realizarían seria solicitar el servicio IPv6 a un ISP, luego contactar al proveedor del router para que realice la actualización del sistema operativo del equipo de ruteo y finalmente contratar personas capacitadas que realicen las modificaciones pertinentes al equipo con el que cuentan.	

Clasificación de la empresa según sector: GUBERNAMENTAL **Persona entrevistada: Administrador del departamento de redes**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Medio
DATOS DEL HARDWARE	
Switch	NORTEL NETWORKS (Conectados en STACKER)
Router	CISCO 3800 (Filtrado por puertos)
Firewalls	CISCO 525 (Para controlar el trafico en la red) Watch Guard (Posee un Kernel de Linux)
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Windows 2003 Server (Active Directory para administrar el dominio de la red)
Gateway	Linux SUSE 10
Clientes	Windows 95, 98, XP
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Se realiza a través de router
Servidor DHCP	Se realiza a través de router
Servidor web	LOTUS NOTES
Servidor de correo electrónico	LOTUS NOTES
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	Poseen aplicativos en FOX para DOS que corren en Windows 95 Poseen aplicativos realizados en diversos lenguajes de desarrollo, aunque actualmente se encuentran desarrollando en JAVA
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	Base de datos de FOX Algunas aplicaciones trabajan con ACCESS La mayoría aplicativos trabajan con SQL Server 2000 Actualmente tienen el proyecto de integrar todas las bases de datos con el gestor DB2 de IBM
CONFIGURACION DE LA RED	
Configuración en VLANs	Poseen 5 VLANS administradas con Switches NORTEL los cuales son gestionados por direcciones MAC.
Configuración de seguridad	La corte suprema de justicia posee 6 oficinas departamentales que utilizan sus aplicativos la seguridad que se da en el trafico de información entre estas redes se administra por medio de VPN.
Proveedor ISP	INTERCOM

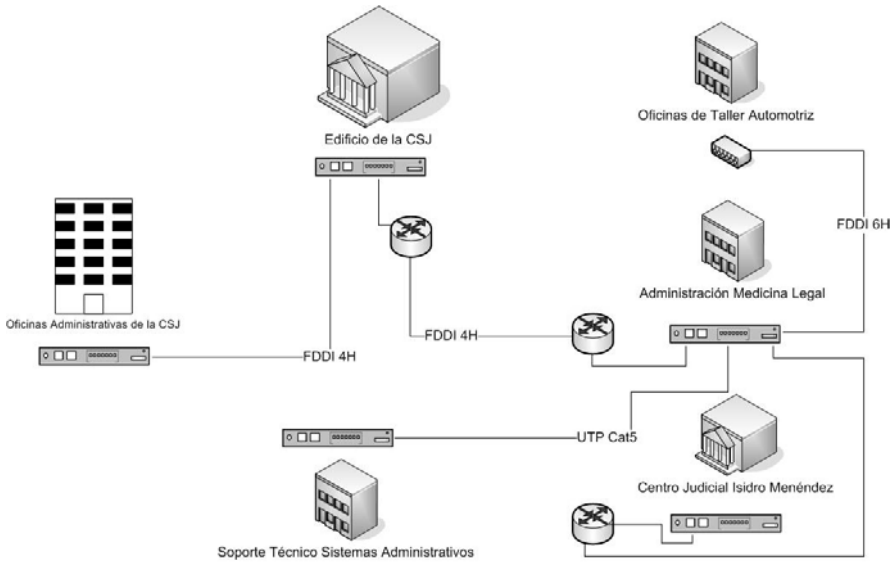
COMENTARIOS DE LA PERSONA ENTREVISTADA

Dentro de la institución existen políticas de actualización de Hardware y Software que corresponde a las necesidades de la institución.

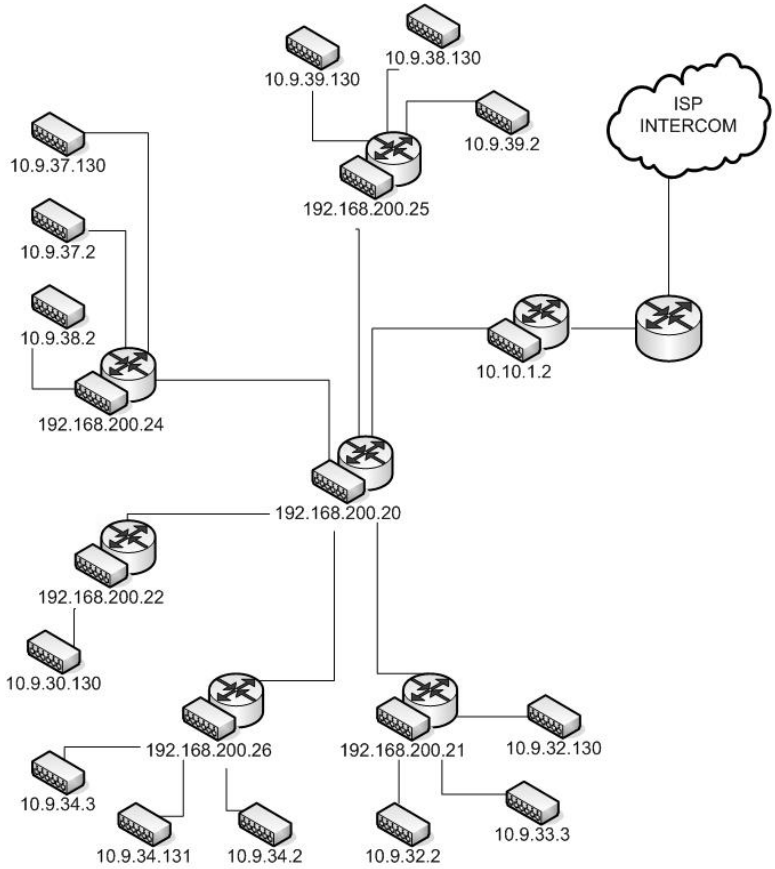
La persona entrevistada comentó que la institución posee algunos equipos que si soportan IPv6 pero que aun cuentan con algunos aplicativos, sobretodo los desarrollados para mecanizar los inventarios de la institución que son los que ocupan el Hardware y Software desactualizado, pero que como los equipos funcionan correctamente simplemente se les da mantenimiento preventivo y por otra parte los programas poseen una gran complejidad en cuanto al volumen de información y de transacciones por lo que mejor se ha optado por conservarlos así.

La infraestructura de red de la institución es la siguiente:

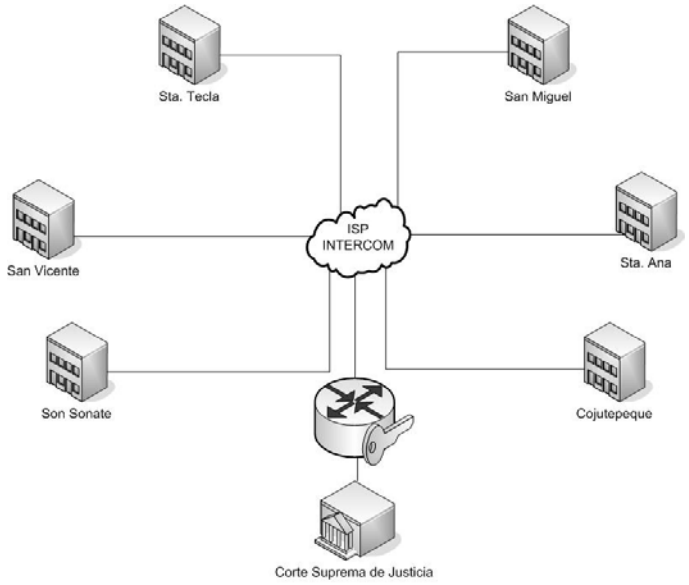
1. La red de la institución administra la información de 6 edificios que se conectan por medio de enlaces de fibra óptica. El diagrama de red es el siguiente.



2. Cada edificio que forma parte de la institución se gestiona por medio de VLANs que son administradas por Switches NORTEL que son conectados en STACKER (Configuración que sirve para asignar una sola dirección IP al grupo de Switches que gestionaran el trafico de cada VLAN, esto con el fin de conectar una mayor cantidad de equipos y administrarlos con una sola IP). Los Switches de cada VLAN administran los equipos por medio de direcciones MAC. El diagrama de esta configuración es la siguiente.



3. La seguridad es muy importante dentro de la institución por lo que se cuenta con un router CISCO 525 que se encarga de administrar el tráfico en la red y controla el acceso a esta. También la institución cuenta con 6 oficinas departamentales que tienen acceso a cierta información de la red. Por este motivo se han creado enlaces VPN para administrar la seguridad de la información entre las oficinas de la institución y las oficinas departamentales. El diagrama es el siguiente.



Clasificación de la empresa según sector: GUBERNAMENTAL **Persona entrevistada: Jefe de la unidad informática**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Nulo
DATOS DEL HARDWARE	
Switch	Switch de 24 pto. 10/100/1000 Catalyst 2950 CISCO
Router	CISCO 3800 Series
Firewalls	-
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Windows 2000 Server
Clientes	Windows 2000 Pro. Windows XP Pro SP2
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Servicio DNS Windows 2000 Server
Servidor DHCP	Servicio Windows 2000 Server
Servidor web	Configurado en CRN oficinas centrales
Servidor de correo electrónico	-
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	Java
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	Oracle 8i
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	-
Proveedor ISP	-
COMENTARIOS DE LA PERSONA ENTREVISTADA	
Según políticas de la institución la actualización de los equipos PCs se realiza cada 3 años y la de los elementos de red se realiza en periodos no mayores a los 6 años. La seguridad del tráfico en la red se realiza a través del servicio de autenticación de Windows (Usuarios registrados en el servidor). La persona entrevistada comentó que su conocimiento del nuevo protocolo de Internet IPv6 es bastante general y que como actualmente no existe la necesidad inmediata de contar con un procedimiento que le permita realizar una migración a este protocolo no ha realizado ninguna investigación sobre ello.	

Clasificación de la empresa según sector: GUBERNAMENTAL **Persona entrevistada: Administrador de redes**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Nulo
DATOS DEL HARDWARE	
Switch	Modelo 3COM 2500
Router	Router Cisco series 1600
Firewalls	-
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Linux FedoraCore 6 Linux Red Hat 8.0
Clientes	Windows XP, Windows 2003 Server
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Red Hat 8.0
Servidor DHCP	-
Servidor web	Apache 2.0 para Red Hat Linux
Servidor de correo electrónico	Linux FedoraCore 6 configurado con Sendmail
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	-
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	-
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	Linux FedoraCore 6
Proveedor ISP	-
COMENTARIOS DE LA PERSONA ENTREVISTADA	
Según lo discutido en la entrevista no se ven inconvenientes en una eminente migración a IPv6, se cuenta con personal especializado en materia y con recursos económicos, La persona entrevistada comentó que si en el caso de implementar IPv6 lo harían por la vía del software libre, por ejemplo, Fedora Core 6 que actualmente esta siendo utilizado en la empresa, cuyo sistema operativo esta listo para IPv6.	

Clasificación de la empresa según sector: SERVICIOS **Persona entrevistada: Administrador de redes**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Medio
DATOS DEL HARDWARE	
Switch	Catalyst 6500 16-Port
Router	Router MWR 1900
Firewalls	A través de router
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Linux Red Hat Enterprise 3.0
Clientes	Windows XP, 2000, 2003 Server
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	A través de router
Servidor DHCP	-
Servidor web	Apache 2.0 Red Hat Enterprise AS 3
Servidor de correo electrónico	Microsoft Exchange
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	-
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	-
CONFIGURACION DE LA RED	
Configuración en VLANs	Puertos de comunicación e ip, utilizando equipos de comunicación capa 2 y 3.
Configuración de seguridad	Red Hat Enterprise AS 3.
Proveedor ISP	-
COMENTARIOS DE LA PERSONA ENTREVISTADA	
No se ven problemas en la migración a IPv6, comentaba la persona entrevistada que si los clientes están bajo el protocolo y esos son sus requerimientos apostaremos a esa tecnología. Actualmente se posee la política de evaluación de cambios de equipos cada año y medio.	

Clasificación de la empresa según sector: GUBERNAMENTAL **Persona entrevistada: Jefe de la unidad informática**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Nulo
DATOS DEL HARDWARE	
Switch	Switch 3COM 3800
Router	
Firewalls	-
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Windows 2003 Server
Clientes	Windows XP, 98
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Proveedor externo
Servidor DHCP	-
Servidor web	Proveedor externo
Servidor de correo electrónico	Proveedor externo
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	-
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	-
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	-
Proveedor ISP	-
COMENTARIOS DE LA PERSONA ENTREVISTADA	
Principales aspectos relacionados a la migración: 1. Algunos equipos cambiaran (Equipos de telecomunicaciones, router, switches, etc). 2. Presupuesto pro migración 3. Capacitación del Recurso humano	

Clasificación de la empresa según sector: SERVICIOS **Persona entrevistada: Jefe de la unidad informática y Administrador de redes**	
RECURSO HUMANO	
Estado del conocimiento sobre IPv6	Medio
DATOS DEL HARDWARE	
Switch	Switch 3COM 7200
Router	Router CISCO 2800 - 7200 Series
Firewalls	Información confidencial
PLATAFORMAS O SISTEMAS OPERATIVOS	
Servidores	Microsoft Windows 2003 Server Enterprise Edition
Clientes	Microsoft Windows XP Pro SP2
SERVICIOS DE RED	
Servidor NAT	-
Servidor DNS	Se realiza con el servidor
Servidor DHCP	Se realiza con el router
Servidor web	Se realiza con el router
Servidor de correo electrónico	Microsoft Exchange Server
SOFTWARE DE DESARROLLO	
Software para desarrollo de aplicaciones	Microsoft Visual Estudio 2005 (Aplicaciones desarrolladas en .NET)
GESTORES DE BASES DE DATOS	
Servidor de bases de datos para aplicaciones	Microsoft SQL Server 2005
CONFIGURACION DE LA RED	
Configuración en VLANs	-
Configuración de seguridad	Información confidencial
Proveedor ISP	-
COMENTARIOS DE LA PERSONA ENTREVISTADA	
En cuanto a la configuración de las redes se comentó en la entrevista que se ha realizado una distribución de las direcciones IP empleando el método de estratificación de la red en subredes y también nos comento que en otros países donde poseen sucursales si tienen implementadas la configuración de VLANs en sus redes pero que en nuestro país no han requerido de realizar este tipo de configuración. El equipo de cómputo en la institución se actualiza dependiendo de los requerimientos que demande el software con el que trabajan y también del periodo de obsolescencia que tengan. Actualmente han estandarizado el software que ocupan en la institución migrando todas sus aplicaciones y plataformas a Microsoft. Otro aspecto importante de reclacar según los entrevistados es que al trabajar de esta forma estandarizando sus equipos y el software de la institución no le ve ningún problema para realizar una migración al nuevo protocolo de Internet, por lo que si esto se necesitara se esperaría que la única inversión a realizar es la de actualizar sus dispositivos de comunicación y la de contratar a gente que capacite a su personal de TIC.	

D. Estado del soporte de algunas plataformas[32]

En la tabla 10.B.1 se muestra el soporte que las plataformas más utilizada

Sistema Operativo	Estado
NetBSD	Soporte IPv6 desde versión 1.5 Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-NetBSD
Open BSD	Soporte IPv6 desde versión 2.7 Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-OpenBSD
Free BSD	Soporta IPv6 desde versión 4.0 Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-FreeBSD
BSD/OS	Soporta IPv6 desde versión 4.1
MAC OS X	Soporta IPv6 desde versión 10.2 Configurar IPv6 en url: http://www.ipv6day.org/action.php?n=Es.Configuration-MAC
Windows 95/98/Me	No soporta IPv6
Windows 2000	No soporta IPv6, hay una descarga experimental de una pila IPv6
Windows XP	Soporta IPv6, pero hay que habilitarlo Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-WindowsXP-SP1OrLater
Windows 2003 Server	Soporta IPv6 desde la versión 2.2 Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-Windows2003
Linux	Soporta IPv6 desde versión 2.7 Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-Linux
Solaris	Referencia url, sobre la configuración de IPv6 en esta plataforma: http://www.ipv6day.org/action.php?n=Es.Configuration-Solaris

[32] Más datos sobre sistemas operativos, Jun-ichiro itojun Hagino.