IPv6 protocolo de internet de siguiente generación

Autor: Fernando Martínez González

Tesina presentada para obtener el título de:
Ing. En Sistemas Computacionales

Nombre del asesor:
Edwin Castro Morales

UNIVERSIDAD VASCO DE QUIROGA

FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

"IPv6 Protocolo de Internet de Siguiente Generación"

TESINA

PARA OBTENER EL TÍTULO DE

INGENIERO EN SISTEMAS COMPUTACIONALES

Fernando Martínez González

ASESOR

Edwin Castro Morales

CLAVE: 16PSU0049F

ACUERDO: LIC000808

MORELIA, MICHOACÁN FEBRERO 2010

Dedicatoria

Dedico este trabajo a mi madre Ma. Concepción por su apoyo y sus consejos que me hicieron crecer como persona y como estudiante. Y por el apoyo que me brindo todo el tiempo para poder terminar este trabajo.

A mi papa y mi hermana por el apoyo económico, moral y la paciencia que me tuvieron durante este tiempo y por sus consejos para poder terminar esta tesina.

Le agradezco a isa por su apoyo y consejos para terminar la tesina.

ÍNDICE GENERAL

JUSTIFICACIÓN

El crecimiento de computadoras conectadas a la Internet se ha multiplicado en los últimos 20 años, donde la Internet se ha vuelto cada día más popular y por lo cual más requerida así día a día hay más dispositivos conectados a la Red Mundial. Esto nos conlleva a que en un futuro no muy lejano se van a ir agotando las direcciones IP disponibles para tener el acceso a Internet.

Cada equipo conectado a Internet debe contar una dirección IP única para poder navegar en la Red, ya que se están agotando, se han creado tecnologías que ayudan a que estas sean suficientes por el momento, una muy importante es NAT que hace posible que un grupo de computadoras de un Ruteador tenga acceso a una sola dirección IP.

Se tendrá la necesidad de migrar hacia el protocolo IPv6 debido a que IPv4 solo soporta 4, 294, 967,296 direcciones distintas, un número muy limitado si se quieres asignar una IP única a cada Auto, Teléfono fijo, Celular, PDA, PC. etc. Y los que nos ofrece el cambio hacia el nuevo Protocolo IPv6 soporta hasta 340,282,366,920,938,463,374,607,431,768,211,456 (340 sextillones) de direcciones diferentes.

La diferencia se hace notar ya que IPv4 utiliza 32 Bits para las direcciones mientras IPv6 utiliza 128 Bits de espacio para soportar más direcciones y así tener más niveles de jerarquía de direccionamiento y los nodos sean más direccionables.

OBJETIVOS

El objetivo principal es la comparativa del Protocolo de Internet IPv4 con la nueva generación de Protocolo IPv6 ya que es muy factible su uso en un futuro no muy lejano, así teniendo en cuanta las ventajas y desventajas que este nos ofrecerá y las forma en la nos ayudará para mejor el direccionamiento de direcciones, tomando en cuenta la seguridad que nos ofrece para poder tener un control y acceso a redes sociales e internas, sabiendo que la información que se envía o recibe va a hacerse de forma segura.

Así tomando en cuenta la viabilidad que nos permite para que las compañías u organizaciones hagan una migración paulatinamente hacia IPv6 tomando en cuenta los elementos esenciales sobre las ventajas que este protocolo ofrece y tener la posibilidad de migrar hacia IPv6 para cualquier empresa que requiera de una red o ya sea una red pequeña.

Objetivos Específicos

- Estudiar IPv4 para conocer su capacidad de direccionamiento IP.
- Estudiar IPv6 para conocer las mejoras implementadas, tomadas a partir de IPv4.
- Describir los cambios más importantes, como las principales mejoras y cambios fundamentales dentro de la cabecera IPv6.
- Cuáles son las opciones de para la transición de IPv4 a IPv6.

Capitulo 1 Introducción

1.0 Internet

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación. La idea de una red de computadoras diseñada para permitir la comunicación general entre usuarios de varias computadoras se ha desarrollado en un gran número de pasos. La unión de todos estos desarrollos culminó con la red de redes que conocemos como Internet. Esto incluía tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones.

Las más antiguas versiones de estas ideas aparecieron a finales de los años 50. Implementaciones prácticas de estos conceptos empezaron a finales de los 60 y a lo largo de los 70. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo. En los 90 se introdujo la World Wide Web (www), que se hizo común.

La infraestructura de Internet se esparció por el mundo, para crear la moderna red mundial de computadoras que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a información y comunicación sin precedentes, pero también una brecha digital en el acceso a esta nueva infraestructura. Internet también alteró la economía del mundo entero, incluyendo las implicaciones económicas de la burbuja de las .com.

Un método de conectar computadoras, prevalente sobre los demás, se basaba en el método de la computadora central o unidad principal, que simplemente consistía en permitir a sus terminales conectarse a través de largas líneas alquiladas. Este método se usaba en los años 50 por el Proyecto RAND para apoyar a investigadores como Herbert Simón, en Pittsburgh (Pensilvania), cuando colaboraba a través de todo el continente con otros investigadores de Santa Mónica (California) trabajando en demostraciones de teoremas automatizadas e inteligencia artificial.

Un pionero fundamental en lo que se refiere a una red mundial, J.C.R. Licklider, comprendió la necesidad de una red mundial, según consta en su documento de enero, 1960, Simbiosis Hombre Computadora (Man Computer Symbiosis).

1.1 IP

El Protocolo de Internet (IP) fue diseñado en los años 70 con el fin de interconectar redes entre sí. Los creadores de Internet, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en tan poco tiempo, en una gran multitud de lugares donde se puede utilizar. Las Tecnologías de la Información y Comunicación (TIC) han evolucionado de un modo mucho más explosivo de lo esperado.

Por esto que la versión actual de IPv4 (IP versión 4), está llegando a sus límites, con limitaciones que impiden un adecuando crecimiento de la red, y por tanto la creación e implementación de nuevas aplicaciones, con más posibilidades que las actuales. El nacimiento de IPv6 (IP versión 6) viene a resolver las limitaciones de IPv4, además de integrar nuevas características que permitan entregar seguridad y confiabilidad en la transmisión de la información. IPv6 define direcciones de 128 bits frente a las direcciones de 32 bits de IPv4, lo que nos da un espacio de direccionamiento prácticamente infinito. Para tener una idea de este alto número, ahora cada grano de arena del planeta puede ser direccionado vía IP.

Una característica muy importante de IPv6, ya que permite un mejor soporte al tráfico en tiempo real, como es el caso de videoconferencia ya que ahora es cada día más usado en el mundo además incluye etiquetado de flujos en sus especificaciones. También cuenta con seguridad intrínseca en sus especificaciones a través de IPsec. Que permite que se realice encriptación de la información y la autentificación del remitente de la información, incluye en su mecanismo conocido como PNP que facilita a los usuarios la conexión de sus equipos a la red, ya que la configuración se realiza automáticamente. Hoy en día muchas redes de investigación y educación en el mundo ya soportan este nuevo protocolo (IPv6) aunque aun dominados por IPv4 y que poco a poco va creciendo.

Dado que las empresas actuales y más vanguardistas y que ahora viven con la tecnología se han visto en la necesidad de contar con una mayor cantidad de aplicaciones multimedia y aplicaciones de red que consumen mucho ancho de banda, IPv6 es dedicado para que la viabilidad de redes empresariales y las redes públicas de Internet sigan creciendo.

A finales del año 2011[1] aproximadamente, se prevé que se produzca el agotamiento de las direcciones IPv4 que aún no han sido utilizadas. Ello implicaría que Internet no podría seguir creciendo con la facilidad que lo ha hecho hasta ahora y que se dificultaría la incorporación de nuevos usuarios, dispositivos, servicios, aplicaciones y en general la innovación en Internet.

Además incrementaría el coste del desarrollo de software y por tanto el coste asociado a la utilización de Internet para nuevos servicios y aplicaciones.

El despliegue de IPv6 es fundamental para evitar que lleguemos a esta situación y es la única solución que podemos calificar de prácticamente permanente para la problemática del agotamiento de IPv4.

1.2 Necesidad de cambio a IPv6

Unas de la principales consideraciones y mas importantes de la transición a IPv6 es cuando se adopto el IPv4 los Hosts se cambiaron a principios de 1983 y no había necesidad de cambio sino hasta el año 1984 cuando el numero de Hosts conectados Backbone rebasaron los 1000, ya que en esos años los usuarios de internet eran muy limitados y la mayoría eran expertos en el campo.

Para el año de 1999 existían 60, 000,000 Hosts fijos registrados en el DNS, y un número dinámico de Hosts asignados dinámicamente, desde entonces el número de Hosts en Internet ha rebasado la imaginación. Aunque muchos de los usuarios no tiene un conocimiento concreto más bien un poco o nulo de la telecomunicaciones, las computadoras, las redes, protocolos. La transición a IPv6 es un problema a de gran escala.

Una característica muy importante es el amplio y flexible número de direcciones en IPv6 con la habilitación de definición de arquitecturas de ruteo globales, flexibles y jerarquías, con varios niveles. Una arquitectura jerárquica de direcciones IPv6 se puede asignar a áreas geográficas utilizando los prefijos flexibles tipo CIDR (Classless Inter-Domain Routing).

El direccionamiento IPv6 puede ser enfocado de una manera que facilite la sumarización del ruteo y controle la expansión de las tablas de ruteo en los ruteadores de backbone.

A los proveedores de Internet tendrán suficientes direcciones para asignar a empresas medianas y a usuarios de dial up que necesiten direccionamientos globales para qua así puedan explorar al máximo el Internet. En lo que se refiere a la telefonía, el direccionamiento de Ipv6 permite a la industria conectada en red, ir más allá del sistema telefónico actual.

Pero se deben tener en cuenta varias consideraciones, la reducción de trabajo, la seguridad, el factor humano, el hardware y software y sobre todo, la simplicidad y estandarización del formato de Ipv6.

Ya que las tecnologías de la información han crecido a gran escala, para mejorar la calidad de vida de las persona. Esta nos proporciona un conjunto de servicios, redes, software y dispositivos para poder integrar dentro de un entorno de sistemas de información que ayuden a mejor y facilitar las tareas cotidianas, así como proveer el recurso o medios necesarios para el aprendizaje y desarrollo de las personas.

Capítulo 2 Redes y Protocolos

Los protocolos son muy importantes para realizar las conexión entre varias computadoras ya que son un conjunto de reglas que nos permite el flujo de información entre equipos o grupo de equipos que se manejan en distintos lenguajes por cual es necesario conocerles y estudiarles, es necesario conocer los principales protocoles de Red que hacen posible esa comunicación, definiendo en qué consiste una Red de computadoras y cuáles son sus componentes que permiten realizar el intercambio de información.

Los tipos de Red que existen y como permiten llevar a cabo el intercambio de información mediante métodos creados para realizar esa tareas. Proporcionando el tratamiento adecuado a la información asegurando una transferencia de datos segura.

2.0 Redes

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos).

Para simplificar la comunicación entre programas (uso de aplicaciones) de distintos equipos, se definió el Modelo OSI por la ISO, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

2.1 Tipos de Red

Red pública: Una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

Red privada: La red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

Red de área Personal (PAN): es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del interpersonal), o para conectar con una red de alto nivel y el Internet (un up link). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

Red de área local (LAN): Es la red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización. Es muy importante que para los propósitos administrativos, las LANs grandes se dividen generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroup es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN.

Red del área del campus (CAN): Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

Red de área metropolitana (MAN): una red que conecta las redes de un área dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Las rebajadoras múltiples, los interruptores y los cubos están conectados para crear a una MAN.

Red de área amplia (WAN): es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

2.2 Protocolos de Red

Protocolo de red o también Protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, el protocolo TCP/IP fue creado para las comunicaciones en Internet, para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación.

Pueden estar implementados bien en hardware (tarjetas de red), software (drivers), o una combinación de ambos.

Propiedades

- Detección de la conexión física sobre la que se realiza la conexión.
- Pasos necesarios para comenzar a comunicarse (Handshaking).
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos (corrección de errores).
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad (autentificación, cifrado).

2.3 Niveles de Abstracción

Modelo OSI

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI.

Según la clasificación OSI, la comunicación de varios dispositivos equipo terminal de Datos (ETD) se puede estudiar dividiéndola en 7 niveles, que son expuestos desde su nivel más alto hasta el más bajo:

Tabla 2- 1 Modelo OSI

NIVEL	NOMBRE	CATEGORIA
CAPA 7	NIVEL DE APLICACION	APLICACIÓN
CAPA 6	NIVEL DE PRESENTACION	
CAPA 5	NIVEL DE SESION	
CAPA 4	NIVEL DE TRANSPORTE	
CAPA 3	NIVEL DE RED	TRANSAPORTE DE DATOS
CAPA 2	NIVEL DE ENLACE DE DATOS	
CAPA 1	NIVEL FISICO	

A su vez estos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 3 capas superiores trabajan con problemas particulares a las aplicaciones y que solo se ejecutan solamente en software y las 4 capas inferiores se encargan de los problemas pertinentes al transporte de los datos y soporte físico. [2]

Ejemplos de protocolos de red dentro del modelo OSI

Capa 1: Nivel físico: Cable coaxial o UTP categoría 5, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232.
Capa 2: Nivel de enlace de datos: Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC.
Capa 3: Nivel de red: ARP, RARP, IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX.
Capa 4: Nivel de transporte: TCP, UDP, SPX.
Capa 5: Nivel de sesión: NetBIOS, RPC, SSL.
Capa 6: Nivel de presentación: ASN.1.
Capa 7: Nivel de aplicación: SNMP, SMTP, NNTP, FTP, SSH, HTTP, SMB/CIFS, NFS, Telnet, IRC, ICQ, POP3, IMAP.

Descripción de las 7 capas del modelo OSI

Capa 1: Capa Física.

Es la que se encarga de las conexiones físicas de la computadora hacia la red, medio físico (cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; otros medios como: radio, infrarrojos, microondas, láser y otras redes inalámbricas

Capa 2: Capa de enlace de datos.

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, un tránsito de datos fiable a través de un enlace físico. Se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Capa 3: Capa de red.

La capa de red hace que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea son encaminadores (Routers).

Capa 4: Capa de transporte.

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red

Capa 5: Capa de sesión.

Esta capa establece, gestiona y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha).
- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (checkpoints), que sirven para que ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

Capa 6: Capa de presentación.

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC) sonido o imágenes, los datos lleguen de manera reconocible.

Capa 7: Capa de aplicación.

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros (FTP).

2.4 Protocolo TCP/IP

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI, que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

2.4.1 TCP

Protocolo de Control de Transmisión (TCP): El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP y SSH.

2.4.2 Funciones de TCP

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y dado que la capa IP aporta un servicio de datagramas no fiable

(sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe: libre de errores, sin pérdidas y con seguridad.

2.4.3 Formato de los Segmentos TCP

En el nivel de transporte, los paquetes de bits que constituyen las unidades de datos de protocolo o PDU (Protocol data Unit) se llaman segmentos. El formato de los segmentos TCP se muestra en el siguiente esquema:

+	0 - 3	4 - 7	8- 15	16 - 31
0	Puerto origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	Longuitud de cabecera TCP	reservado	Flags	Ventana
128	Suma de Verificación (Checsum)			Puerto Urgente
160	Opciones + Relleno (Opcional)			
224	Datos			

Figura 2- 1 Formato de los Segmentos TCP

2.4.4 Segmentos TCP

Las aplicaciones envían flujos de bytes a la capa TCP para ser enviados a la red. TCP divide el flujo de bytes llegado de la aplicación en segmentos de tamaño apropiado (normalmente esta limitación viene impuesta por la unidad máxima de transferencia (MTU) del nivel de enlace de datos de la red a la que la entidad está asociada) y le añade sus cabeceras. Entonces, TCP pasa el segmento resultante a la capa IP, donde a través de la red, llega a la capa TCP de la entidad destino. TCP comprueba que ningún segmento se ha perdido dando a cada uno un número de secuencia, que es también usado para asegurarse de que los paquetes han llegado a la entidad destino en el orden correcto. TCP devuelve un asentimiento por bytes que han sido recibidos correctamente; un temporizador en la entidad origen del envío causará un tiempo fuera si el asentimiento no es recibido en un tiempo razonable, y el presuntamente desaparecido paquete será entonces retransmitido. TCP revisa que no haya bytes dañados durante el envío usando un checksum; es calculado por el emisor en cada paquete antes de ser enviado, y comprobado por el receptor.

Los protocolos TCP/IP se caracterizan por estar basados o definidos por la combinación de 4 capas (ver figura 2-2).

Las cuales se definen a continuación:

Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).

Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

Internet o Red: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

Enlace: es la encargada de que los sistemas operativos puedan enviar y recibir información, esta también se denomina capa de datos o capa de acceso a la red.

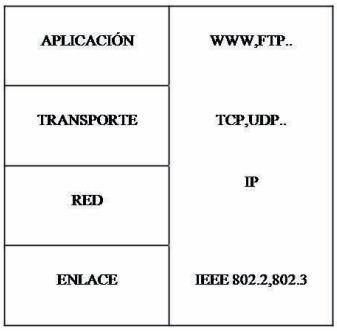

Figura 2- 2 Estructura de cuatro capas

2.5 PROTOCOLOS TCP/IP

Algunos de los protocolos son mostrados (ver figura 2 - 3) en la capa donde funcionan y realizan sus tareas.

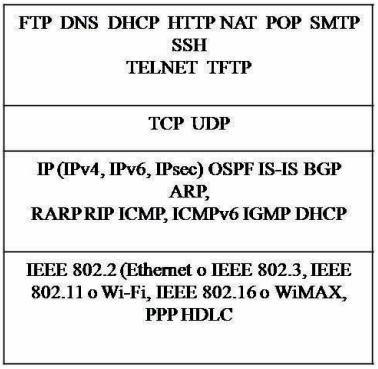

Figura 2- 3 Protocolos TCP/IP

Conexión entre dos computadoras

Las capas del modelo hacen que la comunicación entre dos computadoras sea por medio de las capas, haciendo cada capa independiente a la otra así facilitando cambio o mejoras en los modelos. Cada capa en modelo añade información en los encabezados de los paquetes enviados, es decir, en el encabezado se almacena la información de tipo protocolo, el número de paquete a quien va dirigido y de quien viene.

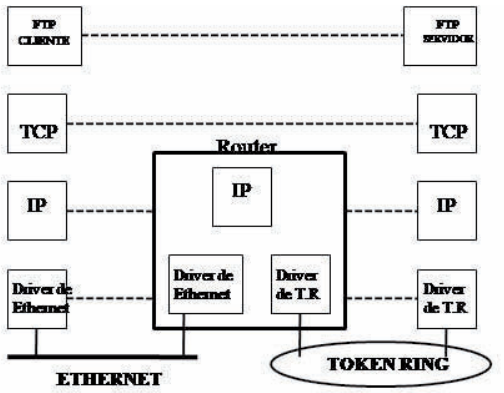

Figura 2- 4 Esquema de conexión entre dos equipos en Internet

Cuando se envía información en el encabezado se pone la información de cada capa y se pasa a la capa inferior hasta que se llega a la capa inferior de quien envía los datos a través de la red, cuando se recibe información pasa exactamente lo inverso.

Para que cada equipo se comunique con otro en Internet, el modelo genera paquetes los cuales viajan a través de la red por los equipos conectados que son encargados de hacer la conmutación de paquetes hasta llegar a su destino, existen dos tipos de equipos conectados a Internet, los que envían paquetes de información (Hosts) y los que hacen la

conmutación para que los paquetes generados lleguen a su destino (Router, Gateway, bridge).

2.6 Negociación en tres pasos

Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normalmente una de ellas abre un socket en un determinado puerto TCP y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete SYN inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese puerto. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit RST activado, lo que significa el rechazo del intento de conexión.

En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión.

Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas (spoofing).

Establecimiento de la conexión (negociación en tres pasos).

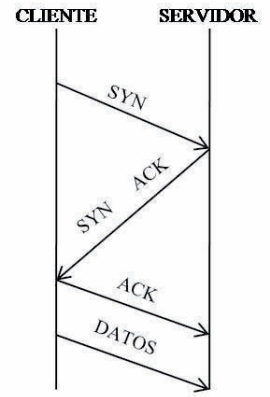

Figura 2- 5 Figura 2 0-1 Negociación tres pasos

2.7 Transferencia de datos

Durante la etapa de transferencia de datos, una serie de mecanismos claves determinan la fiabilidad y robustez del protocolo. Entre ellos está incluido el uso del número de secuencia para ordenar los segmentos TCP recibidos y detectar paquetes duplicados, checksum para detectar errores, y asentimientos y temporizadores para detectar pérdidas y retrasos.

Durante el establecimiento de conexión TCP, los números iníciales de secuencia son intercambiados entre las dos entidades TCP. Estos números de secuencia son usados para identificar los datos dentro del flujo de bytes, y poder identificar (y contar) los bytes de los datos de la aplicación. Siempre hay un par de números de secuencia incluidos en todo segmento TCP, referidos al número de secuencia y al número de asentimiento. Un emisor TCP se refiere a su propio número de secuencia cuando habla de número de secuencia, mientras que con el número de asentimiento se refiere al número de secuencia del receptor. Para mantener la fiabilidad, un receptor asiente los segmentos TCP indicando que ha recibido una parte del flujo continuo de bytes. Una mejora de TCP, llamada asentimiento selectivo (SACK, selective acknowledgement) permite a un receptor TCP asentir los datos que se han recibido de tal forma que el remitente solo retransmita los segmentos de datos que faltan.

Capítulo 3 El protocolo IP versión 4

En este capítulo describiré lo que es el protocolo IPv4 y como está definido dentro del funcionamiento de Internet, que trabajo realiza para llevar a cabo el direccionamiento. Así como la estructura del datagrama y describiré cada campo y funcionamiento de cada Bit. Aquí veremos los tipos de redes que existen y que capacidad de direcciones posibles se pueden asignar.

3.0 IPv4

El protocolo IP (*Internet Protocol*) es en el cual se basa la transmisión de datos en Internet, su definición se encuentra en el RFC 791[3], su base es la transmisión de datagramas a través de la Internet, lo cual hace por medio de un sistema *conectionless* y *unreliable* y da el servicio *best effort*, TCP provee las características de confiabilidad y de conexión e IP le delega ese trabajo para no hacer un retrabajo, los protocolos trabajan en conjunto pero cada uno haciendo lo que es necesario para que los datos lleguen con seguridad a su destino sin tener que ser enviados todos los datagramas por el mismo camino.

La capacidad de *best effort* de IP funciona de manera que si existe una falla en el enlace por el cual se están transmitiendo los datos, se tengan caminos alternos por los cuales se pueda transmitir la información por medio de un sistema muy sencillo de solución de errores.

El mecanismo de control de errores es controlado por el *Internet Control Message Protocol* (ICMP), si a un Ruteador le falla un enlace por el cual estaba transmitiendo los datos, elimina el datagrama y manda un mensaje de ICMP al equipo que está enviando los datos y se olvida del datagrama, no trata de retransmitirlo, el equipo que estaba transmitiendo, retransmite el datagrama, no teniendo la información de cual enlace está activo o no.

Cuando el datagrama llega al Ruteador él verá la manera de hacerlo llegar a su destino por otro enlace, lo que nos refleja éste tipo de servicio es que no implica fiabilidad y no conexión por un camino específico.

3.1 Estructura del datagrama IPv4

La estructura de un datagrama IP, se divide en bloques de 32 bits (4 bytes), comenzando de izquierda a derecha y de arriba hacia abajo, el primer bit es el bit 0, el orden es importante ya que dependiendo del equipo al que se está comunicando es su manera de guardar los bits en memoria. A ésta manera de transmitir los bits se le denomina *network byte order*.

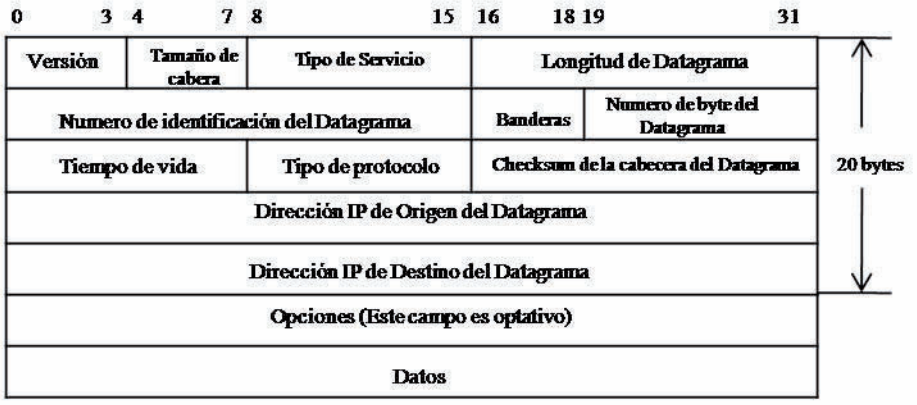

Figura 3- 1 Estructura Datagrama IPv4

Los datos del encabezado son importantes ya que son la manera de dar a conocer al Router o al otro *Host* lo que se está enviando. Para tener más claros los campos se detalla su contenido a continuación.

La ***versión*** (4 bits), sirve para identificar a que versión específica RFC 791 [4] hace referencia el formato del datagrama. Esta información sólo es utilizada por los Routers y capa IP de origen y final del datagrama. Esto permite la coexistencia de diferentes versiones del protocolo IP de una forma transparente al usuario. La versión actual es la 4 (conocida también cómo IPv4).

El ***tamaño de la cabecera*** (Header Length), son 4 bits (2^4 = 16 posiciones, 0...15) que indican el número de palabras de 32 bits que ocupa la cabecera. Estos 4 bits de tamaño máximo, nos limitan a un tamaño de cabecera máximo de 60 bytes (15 * 32 bits = 60 bytes). No obstante, el valor usual de este campo es 5 (5 * 32 bits = 20 bytes).

El campo de tipo de servicio son 8 bits, los primeros 3 no se usan, los siguientes 4 definen el tipo de servicio, el último bit no se utiliza pero debe de tener valor de 0 siempre, en los bits de tipo de servicio, solamente uno puede estar activo a la vez. El tipo de servicio se tiene para darle a entender al Ruteador la política de servicio que se debe de tener con el datagrama, minimizar el retraso, maximizar el rendimiento, maximizar la fiabilidad del transporte y minimizar el costo económico del transporte.

Tabla 3- 1 Valores de Tipo de Servicio

Tipo de servicio					
Tipo de aplicación	**Minimizar retraso**	**Maximizar rendimiento**	**Maximizar fiabilidad**	**Minimizar costo**	**Valor en hexadecimal**
TELNET	1	0	0	0	0x10
FTP	0	1	0	0	0x80
SMTP	0	1	0	0	0x80
DNS (UDP)	1	0	0	0	0x10
DNS (TCP)	0	0	0	0	0x00
ICMP	0	0	0	0	0x00
BOOTP	0	0	0	0	0x00

El campo de longitud del datagrama mide 16 bits y dice cuanto espacio se debe guardar en la memoria para la recepción de cada datagrama, también dice cuantos bytes se deben leer por datagrama, con esto se puede tener un control muy sencillo de si los datagramas llegan completos o no, también limita el tamaño máximo de los datagramas a 65515 bytes, el *Máximum Transfer Unit* (MTU) es 216 bytes 65525 – 20 bytes de encabezado.

Si el tamaño del datagrama, es mayor que el tamaño máximo del paquete de red (Ej. Datagrama de 32000 bytes enviado sobre una Ethernet, que tiene un tamaño máximo de paquete de 1500 bytes), se fragmenta en N trozos.

El campo de número de identificación del datagrama indica el número de paquete que se está recibiendo o enviando cuando se tiene que dividir en pedazos un paquete, así cuando se recibe el paquete se puede ordenar adecuadamente, mide 16 bits, por lo que un datagrama se puede dividir hasta en 65535 fragmentos.

El campo de banderas mide 3 bits y especifica diferentes actividades según el bit que esté encendido, si el primero está encendido quiere decir que el datagrama es parte de un datagrama mayor, si el segundo está encendido quiere decir que el datagrama no debe de ser fragmentado y el tercero no se utiliza, teniendo siempre el valor 0.

El campo de número de byte en el datagrama, indica cual es la posición en bytes que ocupan los datos en el datagrama original, obviamente solo se ocupa si el fragmento es parte de un paquete mayor, mide 13 bits y sirve para reconstruir el paquete original.

El campo de tiempo de vida mide 8 bits y es el que indica cuanto tiempo vivirá el datagrama en transición, es decir, cuánto tiempo tiene el datagrama para llegar a su destino para que los datagramas no circulen para siempre por la red, éste campo tiene un valor máximo de 255 y cada vez que pasa por un Router su valor se decrementa en uno, si el

valor llega a cero, el Router que le toca proporcionar ese valor, envía un ICMP al origen para que el datagrama sea retransmitido.

El campo de tipo de protocolo indica el protocolo superior que se está utilizando, ya sea TCP, UDP, ICMP, etc. El campo se ocupa ya que todos los protocolos de Internet utilizan IP como medio de transporte y al llegar al destino hay que entregarlo en los medios adecuados.

El campo de suma de comprobación ("checksum") del encabezado del datagrama se utiliza solo para verificar el encabezado, ya que tanto UTP, TCP y demás protocolos tienen su propio "checksum" y verificarán sus datos de manera autónoma, sirve para verificar que el encabezado llegue completo y no se descarte el datagrama por pérdida de información en el camino.

3.2 Direccionamiento IPv4

La dirección IP origen y la dirección IP destino son dos números de 32 bits, cada una. Cada equipo tiene un número específico, dentro del protocolo IPv4 se denominan 4 octetos de 8 bits separados por un punto para especificar cada equipo en la red. Existen varios tipos de redes los cuales se describen en la tabla.

Tabla 3- 2 Clases de direcciones IPv4 en Internet

CLASE	DESDE	HASTA
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Las clases de redes sirven para definir el tamaño de direcciones de las redes, como se vio en la figura anterior existen 5 clases de redes, en la figura (figura 3-2) se puede ver la cantidad de equipos que se pueden conectar a cada red:

Clase A	0	Identificador de Red (7bits)							Numero de Equipo (24 bits)																						
Clase B	1	0	Identificador de Red (14 bits)														Numero de Equipo (16 bits)															
Clase C	1	1	0	Identificador de Red (21 bits)																	Numero de Equipo (8 bits)										
Clase D	1	1	1	0	Identificador de Red (21 bits)																										
Clase E	1	1	1	1	0	Reservado para uso futuro (27 bits)																									

Figura 3- 2 Subdivisión de los 32 bits para las clases A, B, C, D Y E

Cabe mencionar que el número máximo en cada octeto es 255 ya que al ser de 8 bits (28=256) el rango es entre 0 y 255 para cada octeto.

Se definieron los diferentes tipos de redes para hacer más fácil la ubicación de redes chicas, medianas y grandes, es decir:

- La red clase A es para redes grandes, se pueden tener 128 (2*7) redes de 16, 777,216 (224) equipos conectados en cada una.
- La red clase B es para redes medianas, se pueden tener 16,348 (2*14) redes de 65,535 (216) equipos conectados cada una.
- La red clase C es para redes chicas, se pueden tener 2, 097,154 (2*21) redes de 256 (28) equipos conectados.
- Las redes clase D y E son de Multicast y reservada respectivamente, también para futuros usos.

La numeración de las direcciones puede variar desde 0.0.0.0 hasta 255.255.255.255, entonces el aprenderse cada una de las direcciones para acceder a ellas sería muy difícil, pera ayudarnos a recordar las direcciones más fácilmente, existen los DNS (*Domain Name Server*), ellos hacen la traducción de la dirección en números a una dirección que se pueda recordar más fácilmente, por ejemplo una dirección 164.149.10.1 sería más fácil recordarla como www.uvaq.edu.mx.

La estructura también tiene una especificación definida, la última parte define por lo regular donde se encuentra la página, “.mx” es México, “.uk” es Inglaterra, “.es” es España, etc. El único país que no tiene definida una abreviación es Estados Unidos, ya que ellos generaron la terminología, para éste caso la última parte y en los demás en la penúltima parte, se define el tipo de red, “.gob” para empresas de gobierno, “.net” para empresas de telecomunicaciones, “.com” para empresas del ámbito general, “.mil” para militares y “.edu” para universidades o empresas educativas, se han agregado algunas como “.tv” para la televisión pero no están bien especificadas.

La segunda parte define el nombre de la empresa o la página a donde se quiere acceder.

La primera parte define por lo regular que se tiene acceso a una página de Internet (WWW), recientemente se ha desechado ésta parte ya que siempre es lo mismo y algunas empresas mejor la ocupan para diferenciar servidores.

Propuesta de Nuevo Protocolo

Se va requerir hacer una migran hacia el Protocolo IPv6 gracias a que no se previó la escasez de direcciones IP, por que se presento tan rápidamente la necesidad de direcciones ya nos está alcanzando por el del tiempo y no tardara en agotarse las direcciones y por eso se pensó en una nueva forma de direccionar. Por lo que causo preocupaciones al Internet Engineering Task Force que es la encargada de contribuir al crecimiento de la tecnología de Internet, así en 1991 comenzó una investigación del problema que esto causaría y así ofreciendo soluciones y encaminada a un proceso preliminar.

Porque fue elegido este protocolo:

- La más notable que es el gran numero de direcciones
- Una muy importante es porque este protocolo puede soportar IPv4 y así hacer facilitar y agilizar la migración.
- Su estructura más amigable para el direccionamiento.
- La fragmentación se realiza en el nodo origen y el reensamblado se realiza en los nodos finales, y no en los Routers como en IPv4.
- La estandarización de características de seguridad (IPsec).
- Se actualiza y crea nueva versión de mensajes de error, el cual incorpora MLD que sustituye a IGMP que era anteriormente utilizado por el IPv4.
- Auto-configuración de los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- Movilidad incluida en el estándar, que permitirá cambiar de red sin perder la conectividad.

Capítulo 4 Protocolo IPv6

Por que se dio el surgimiento o la necesidad de crear un nuevo protocolo que nos proporcione nuevas mejoras que el anterior, cuales son las mejoras que incorpora a partir de IPv4 y sus características que nos presenta llevar a cabo una migración de tecnología y utilizar esa tecnología actualmente o en un futuro que nos va alcanzando a una velocidad enorme.

Como está estructurado y si esta va poder coexistir con el anterior para llevar a cabo una migración más cómoda y rápida, mediante el direccionamiento, que tipo de direccionamiento se han incorporado para hacer mejor funcionamiento del protocolo así como en que nos ayuda y facilita la movilidad de entre Redes sin perder la estructura original ni la conectividad al hacer el salto de una Red a otra.

Se enlistan las diferencia más notables y que dominantes entre las versiones así como sus características que hacen de IPv6 una mejor opción y porque debe ser cambiado para mejor la comunicación entre redes. Por lo cual se está dando el agotamiento de direcciones por el uso de métodos de traductores tal como lo es NAT y sus problemas de comunicación.

4.0 Surgimiento de IPv6

A principios de la década de los 90's, en Julio de 1991, el *Internet Engineering Task Force* (IETF) comenzó a trabajar para desarrollar un nuevo protocolo que resolviera en primer lugar el problema de saturación de direcciones de IPv4 y además adicionar a este nuevo protocolo algunas características que no se contemplaron en el diseño de IPv4. En noviembre de 1992 surgió una nueva área de investigación llamada Internet *Protocol Next Generation* (IPng) comisionada por el IETF para formalmente estudiar las diferentes propuestas para el desarrollo de este nuevo protocolo.

En diciembre de 1993 fue distribuido el RFC 1550 [5], el cual invitaba a todas las partes interesadas a participar dando sus comentarios acerca de cualquier requerimiento específico que consideraran pertinente incluir durante el proceso de selección de IPng. Veintiuna respuestas fueron recibidas, las cuales contenían puntos de vista de diferentes

tipos de industrias, tales como la industria celular, televisión por cable y seguridad, solo por mencionar algunas. En el RFC 1726 [6], el grupo de investigación IPng definió un conjunto de 17 criterios que serían usados para el proceso de evaluación del IPng y eran los siguientes:

- Escalabilidad: El nuevo protocolo debería ser capaz de identificar y direccionar por lo menos 1012 sistemas finales y 109 redes individuales.
- Flexibilidad topológica: La arquitectura de enrutamiento y protocolos para IPng debían permitir utilizar muchas topologías distintas de red.
- Rendimiento: Para IPng los Host deberían ser capaces de transferir datos a tasas comparables a las alcanzadas con IPv4 utilizando niveles similares de recursos máquina.
- Servicio robusto: El servicio de red junto con los protocolos de control y enrutamiento para IPng deberían ser suficientemente robustos.
- Transición: Debían existir mecanismos para realizar la transición de IPv4 hacia IPng de manera transparente para los protocolos y aplicaciones de las capas superiores.
- Independencia del medio: Este nuevo protocolo debe de trabajar a través de una Internet con diferentes medios LAN, WAN y MAN, así como distintas velocidades de conexión, que van desde algunos bits/segundo hasta cientos de giga bits/segundo.
- Servicio de datagramas no confiables: En nuevo protocolo debía soportar un servicio no confiable de entrega de datagramas.
- Configuración, Operación y Administración: Este nuevo protocolo también debía permitir conexiones fáciles, además de operación y configuración ampliamente distribuida. También debía permitir la configuración automática de Host y enrutadores.
- Operación segura: IPng también debía proveer una capa de red segura (IPSec).
- Acceso y documentación: Los protocolos que definen a IPng, sus protocolos asociados y protocolos de enrutamiento deberían ser publicados en los RFC's[7], así como estar disponibles libremente y no requerir licencia para su implementación.

- Nombrado único: IPng debía asignar a todos los objetos de la capa IP de manera global nombres de Internet únicos.

- Multicast: IPng debía soportar transmisión de paquetes Unicast y Multicast.
- Extensibilidad: IPng debía ser capaz de evolucionar para cubrir las necesidades futuras del Internet. Así mismo, conforme este evolucione, debería permitir diferentes versiones de él, que puedan coexistir sobre la misma red.
- Servicio de red: IPng debía permitirle a la red asociar paquetes con clases de servicio en particular y proveerlas con los servicios especificados por esas clases.
- Movilidad: El protocolo debía soportar huéspedes, redes e Inter redes móviles [8].
- Protocolo de control: El protocolo debía incluir soporte elemental para probar y depurar redes.
- Redes privadas: Por último, IPng debía permitir a los usuarios construir redes privadas sobre la infraestructura básica de red, soportando ambas, redes basadas ó no basadas en IP.
- Arquitectura Común para el Protocolo de Internet de la Siguiente Generación (CATNIP).
- Protocolo de Internet Simple Plus (SIPP).
- TCP/IP con Direcciones más Grandes (TUBA).

SIPP. Por su parte proponía una evolución a IPv4, por esto, todas las funciones de IPv4 que les parecieron buenas fueron mantenidas en su nueva propuesta, también fue aumentado el tamaño de las direcciones de 32 a 64 bits de longitud y lo mejor de todo, su instalación sería como una actualización de software. SIPP además sería interoperable con IPv4. En cuanto a esta propuesta, los revisores decidieron que SIPP cumplía con diez de los criterios clave, dos criterios no eran cumplidos y no tenían una conclusión acerca de los criterios restantes. [9]

TUBA. Proponía remplazar IPv4 con CLNP, lo cual traía consigo dos beneficios inmediatos: incremento en el espacio de direcciones y permitir a protocolos de la capa de transporte operar de manera transparente. Los revisores de TUBA determinaron que esta propuesta cumplía con cinco de los criterios clave, no cumplía un criterio y no tenían una conclusión acerca de los criterios restantes. [10]

Como resultado de las revisiones a estas tres propuestas se decidió elegir a SIPP, incorporarle direcciones de 128 bits de longitud y hacer algunas otras modificaciones. El

resultado final a todas estas modificaciones es lo que se conoce actualmente como IPv6 ó IPng.

4.1 Características principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionables.
- Header. Algunos campos del Header IPv4 se quitan o se hacen opcionales.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los Routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del Router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar Paquetes pertenecientes a un flujo de tráfico particular, que requieren manejo especial por los Routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real.

Muchas mejoras en los servicios Multimedia.

- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el Router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los Hosts por lo tanto la asignación es más simple.
- Remuneración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad. [11]

- ❖ Ruteo más eficiente en el Backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation. Calidad de servicio (QoS) y clase de servicio (CoS).
- ❖ Capacidades de autentificación y privacidad. Las direcciones pasan de los 32 a 128 bits, o sea de 2^32 direcciones.

4.2 El protocolo de IPv6

El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4).

La nueva estructura de la cabecera del protocolo IP versión 6 se caracteriza principalmente por dos particularidades:

1. Direcciones de 128 bits. Se ha creado una nueva estructura de direccionamiento que aumenta su tamaño de 32 bits a 128 bits. Este aumento es consecuencia del gran aumento que ha sufrido INTERNET en los últimos años, agotando el número de direcciones existentes y colapsando las tablas de encaminamiento de los Routers.
2. Campos de longitud fija. Con el objetivo de minimizar el tiempo necesario para procesar y encaminar los datagramas por INTERNET, se adopta un formato fijo. De esta forma se agiliza el tráfico de datagramas y se suprimen opciones poco utilizadas. No obstante se mantiene la posibilidad de especificar opciones, pero ya sin formar parte de la cabecera IP como ocurría anteriormente.

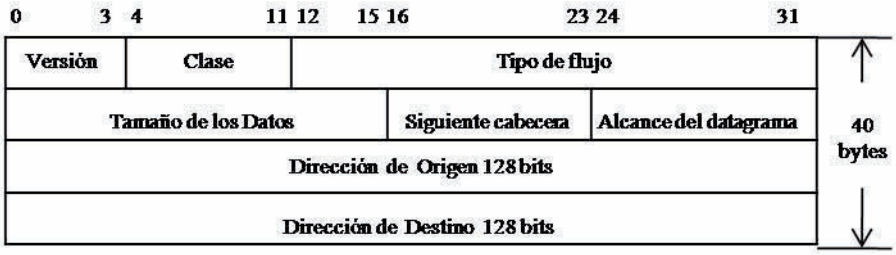

Figura 4- 1 Estructura de un datagrama IPv6.

El protocolo IP versión 6 sigue siendo al igual que las versiones anteriores, un protocolo no fiable y sin conexión. Esto continua siendo así debido a que la experiencia ha enseñado que este sistema funciona y da flexibilidad a la comunicación. Además permite

que sean los protocolos de las capas superiores los encargados de mantener un estado de conexión o fiabilidad según crean necesario, manteniendo la estructura en capas del modelo TCP/IP.

El único campo que se mantiene en la misma posición y con el mismo significado que en formatos anteriores es el de versión, debido a que durante el tiempo de implantación de la nueva versión convivirán simultáneamente la versión 4 y 6. De esta forma, los Routers podrán saber rápidamente si el datagrama que reciben es de una versión u otra.

Se han suprimido seis campos (tamaño de cabecera, tipo de servicio, número de identificación del datagrama, banderas, número de byte del datagrama fragmentado y el checksum. Además se han redefinido los campos de longitud del datagrama, tiempo de vida y de tipo del protocolo.

4.2.1 Campos de un Datagrama IPv6

La **versión** (4 bits) se sigue manteniendo como el primer campo del datagrama. Esto es así para mantener la compatibilidad con formatos anteriores y porque permite de una forma sencilla y rápida que versión de datagrama se recibe, facilitando a los Routers el proceso de diferenciar entre versión 4 y versión 6.

La **clase** (Class) es un número de 8 bits que hace referencia a la prioridad del datagrama. Este campo es una de las nuevas aportaciones para conseguir algunos tipos de aplicaciones (videoconferencia, telefonía...) puedan realizarse en **tiempo real**.

El **tipo de flujo** (Flow Label) se compone de 16 bits, que permiten especificar que una serie de datagramas deben recibir el mismo trato. Esto es aplicable por ejemplo a una serie de datagramas que van del mismo origen al mismo destino y con las mismas opciones. Junto con el campo de clase (Class) permiten aplicaciones en tiempo real.

El **tamaño de los datos** (Payload Length) al igual que en la versión 4, es un número de 16 bits, lo que permite un tamaño máximo en principio de 2^16 = 65536 bytes (64K).

No obstante, a diferencia de la versión 4, este número hace referencia sólo al tamaño de los datos que transporta, sin incluir la cabecera (Si en *IPv4* enviamos 100 bytes de datos utilizando TCP, tendríamos que el valor seria 100 bytes + 20 bytes de cabecera TCP + 20 bytes de cabecera IP versión 4 = 140. En *IPv6* suponiendo los mismos valores nos darían un valor de 120. No se contaría el tamaño de la cabecera IP).

La **siguiente cabecera** (Next Header) es un valor de 8 bits que indica al Router si tras el datagrama viene algún tipo de extensión u opción. Este campo substituye al campo de banderas (flags) de la versión 4. De esta manera, en lugar de complicar la cabecera IP con la interpretación de los diferentes bits de opciones, se sitúan fuera del datagrama básico (ver Fig. 3.2). En la versión 6 del protocolo IP se definen una serie de cabeceras de extensión (ver Fig. 3.3) que se colocan justo después de los datos en forma de cadena (*daisy chain*) y que permiten al usuario personalizar el tipo de datagrama. De tal forma que podemos tener varias extensiones de cabecera tan solo indicando en el campo de siguiente cabecera de cada una de ellas el tipo de la cabecera que vendrá a continuación.

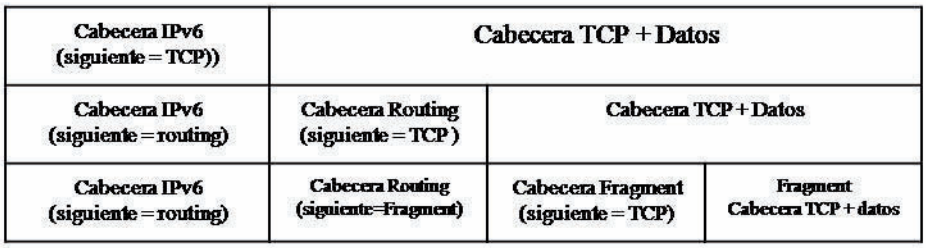

Figura 4- 2 Cadena de cabeceras en IP versión 6.

El **alcance del datagrama** (Hop Limit) es un número de 8 bits que indica el número máximo de Routers que puede atravesar un datagrama hasta llegar a su destino. Este campo es el equivalente al tiempo de vida (*TTL*) de la versión 4. Cuando un datagrama llega a un Router y es encaminado hacia otro ordenador, este campo es decrementado en una unidad. Este campo es necesario para evitar que los datagramas circulen infinitamente por la red, eliminándose al llegar a 0 (su valor máximo es de 2^8 = 256).

Tabla 4- 1 Muestra de algunos valores para los tipos de cabecera en IP versión 6.

VALOR DECIMAL	ABREVIATURA	DESCRIPCION
0	HBH	OPCIONES ENTRE SALTOS
4	IP	IP EN IP ENCAPSULACION IPV4
5	ST	STREAM
6	TCP	TRANSMISION CONTROL PROTOCOL
17	UDP	USER DATAGRAM PROTOCOL
51	AH	AUTENTICATION HEADER
52	ESP	ENCRYTED SECURITY PAYLOAD
59	NULL	NO NEXT HEADER
60	DO	DESTINATION OPTIONS HEADER
194	JBGR	JUMBOGRAM

4.3 Direccionamiento (Addressing)

Características:

- No existen direcciones Broadcast.
- Se divide el campo de 128 bits en interfaz y prefijo.
- El prefijo permite conocer donde está conectada la interfaz, o sea permite conocer la ruta.
- Cualquier campo puede tener solo ceros a solo unos
- Una única interfaz pude tener varias direcciones IP.
- Las direcciones se organizan de forma jerárquica.

La distinción más obvia son las características de IPv6 es el uso de de direcciones muy largas, el tamaño de direcciones es de 128 bits, una pequeña secuencia que es cuatro veces más largo que la direcciones de 32 bits (IPv4). Ya que la direcciones de 32 bits de espacio permiten direcciones de 2x32 o lo que es 4, 294, 967,296 posibles direcciones. Las direcciones de 128 bits permiten 2x128 o lo que es 340, 282, 366, 920, 938, 463, 463,374, 607, 431, 768, 211,456 de posibles direcciones.

4.3.1 Sintaxis IPv6

La sintaxis de IPv4 es representada por el formato de punto decimal, donde los 32bit direcciones es dividido a lo largo de 8-bit de limite, cada sistemas lo conforma 8 bits es convertido a equivalente decimal y separado por periodos. Y para IPv6 los 128 bits

de direcciones es dividido a lo largo de 16 bit de limite y cada bloque de 16 bit es convertido a 4 dígitos de números hexadecimales y separados por 2 puntos así resultando la representación llamada punto hexadecimal.

A continuación se muestra las direcciones de IPv6 en su forma binaria.
0010000000000001000011011011100000000000000000000010111100111011
0000001010101010000000001111111111111110001010001001110001011010

Las direcciones de 128 bits es divido en 16bits de limite.
0010000000000001 0000110110111000 **0000000000000000** 0010111100111011
0000001010101010 0000000011111111 **1111111000101000** 1001110001011010

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

La representación de la dirección IPv6 es simplificada más a fondo suprimiendo los ceros principales dentro de cada bloque de 16 bits. Sin embargo, cada bloque debe tener por lo menos un solo dígito. Con la supresión cero principal, el resultado es el siguiente:
2001:DB8:0:2F3B:2AA: FF: FE28:9C5A

Algunos tipos de las direcciones IPv6 contienen secuencias largas de ceros. Para simplificar más la representación de las direcciones IPv6, una sola secuencia contigua de bloques de 16 bits fijados a 0 en el formato hexadecimal de los dos puntos se puede comprimir: conocido como dos puntos dobles. Por ejemplo, la dirección enlace local de FE80: 0: 0: 0: 2AA: FF: FE9A: 4CA2 se puede comprimir a FE80::2AA:FF:FE9A:4CA2. La dirección Multicast FF02:0:0:0:0:0:0:2 puede ser comprimida a FF02:2.

4.3.2 Prefijos IPv6

El prefijo es la parte de la dirección donde los bits tienen valores fijos o los bits son los que definen una ruta o una subnet. Los prefijos para las subnets IPv6 y sus rutas y las rutas resumidas se expresan de la misma forma que el encaminamiento del inter-dominio (CIDR) para IPv6. Un prefijo IPv6 se escribe la notación de la dirección del prefijo longitud. Es decir 2001: DB8: 2A0: 2F3B: /64 es un prefijo del subnet y 2001: DB8: 3F:

/48 es un prefijo resumido de la ruta el prefijo 64 bit se utiliza para los subnets individuales a los cuales se atan los nodos.

Un prefijo IPv6 es relevante solamente para las rutas o las gamas de dirección, no para las direcciones individuales del Unicast. En IPv4, es común expresar una dirección IPv4 con su longitud del prefijo. Por ejemplo, 192.168.29.7 /24 (equivalente a 192.168.29.7 con el subnet mask 255.255.255.0) denota IPv4 la dirección 192.168.29.7 con 24 subnet mask del bit. La longitud del prefijo es incluida de modo que usted pueda determinar qué bits identifican el subnet y qué bits identifican el Host en el subnet. Porque el número de bits usados para identificar el subnet en IPv4 es variable, la longitud del prefijo es necesaria separar el prefijo del subnet de la identificación del Host.

4.4 Tipos de direccionamiento IPv6

4.4.1 Unicast

Una dirección del Unicast identifica un solo interfaz dentro del alcance del tipo de dirección. El alcance de una dirección es la región de la red IPv6 sobre la cual la dirección es única. Con la topología apropiada del encaminamiento del Unicast, los paquetes tratados a una dirección del Unicast se entregan a un solo interfaz.

Direcciones globales de Unicast

Las direcciones globales IPv6 son equivalentes a las direcciones del público IPv4. Son ruteo global y accesibles en el Internet IPv6. Las direcciones globales del Unicast se diseñan para ser agregadas o para ser resumidas para una infraestructura eficiente del encaminamiento. Semejante del Internet actual de IPv4, que es una mezcla de plano y de ruteo jerárquico, el Internet de IPv6 se ha diseñado de su fundación para apoyar la dirección y el encaminamiento eficientes, jerárquicos. El alcance de una dirección global es el Internet entero IPv6. El RFC 4291[12] define direcciones globales como todas las direcciones que no estén sin especificar, Loopback, Unicast enlace local, o direcciones del Multicast Sin embargo, La figura 3.3 demuestra la estructura del Unicast global.

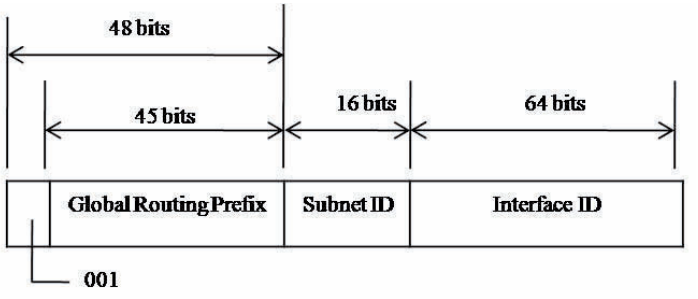

Figura 4- 3 La estructura de las direcciones globales del Unicast definidas en RFC 3587 [3]

Los campos en la dirección global del Unicast se describen en la lista siguiente:

- El sistema de porción fija a 001 los tres bits de categoría alta se fija a 001.
- Indica el prefijo global del encaminamiento para una organización específica sitio. La combinación de los tres bits fijados y del prefijo global de la encaminamiento de 45 bits se utiliza a crear un prefijo del sitio de 48 bits, que se asigna a un sitio individual de una organización. Un sitio es una red IP basada autónoma en el funcionamiento que está conectada con el Internet IPv6.
- La ID del Subnet se utiliza dentro del sitio de una organización para identificar subnets dentro de su sitio. El tamaño de este campo es 16 bits. El sitio de la organización puede utilizar estos 16 bits dentro de su sitio para crear 65,536 subnets o niveles múltiples de tratar jerarquía e infraestructura eficiente del encaminamiento. Con 16 bits de flexibilidad subnetting, un prefijo global del Unicast se asigna a un sitio de la organización equivalente a un prefijo de la dirección de la clase A del público IPv4.
- Indica el interfaz en un subnet específico dentro del sitio. El tamaño de esto el campo es 64 bits. La identificación del interfaz en IPv6 es equivalente a la identificación del nodo o a la identificación del Host en IPv4.

Topologías dentro de direcciones globales

Los campos dentro de la dirección global crean una estructura topológica de tres niveles.

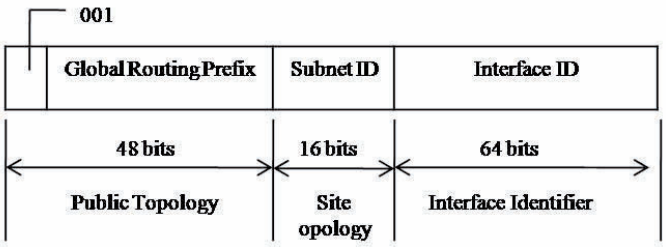

Figura 4- 4 La estructura topológica de la dirección global

La topología pública es la colección de ISPs más grandes y más pequeñas que proporcionan el acceso al Internet IPv6. La topología del sitio es la colección de subnets dentro del sitio de una organización. El identificador del interfaz especifica un interfaz único en un subnet dentro del sitio de una organización.

Uso local de direcciones Unicast

Uso local de direcciones del Unicast no tienen un alcance global y pueden ser reutilizados. Hay dos tipos de uso local de direcciones del Unicast:

1. Las direcciones enlace locales se utilizan entre los vecinos del en enlace y para descubrir los procesos vecinos.
2. Las direcciones Sitio locales se utilizan entre los nodos que comunican con otros nodos en la misma organización.

Direcciones enlace Locales

Las direcciones enlace locales IPv6, identificadas por los 10 bits de la inicial que son fijados a 1111 1110 10 y los 54 bits siguientes fijados a 0, son utilizadas por nodos al comunicar con nodos vecinos en el mismo enlace. Por ejemplo, en una red de un solo enlace IPv6 sin el Router, las direcciones enlace locales se utilizan para comunicar entre los anfitriones en el enlace. Las direcciones enlace locales IPv6 son similares a las direcciones enlace locales IPv4 definidas en RFC 3927 que utilizan 169.254.0.0 /16 prefijo. El uso de las direcciones enlace locales IPv4 se conoce como IP privado automático que trata (APIPA) en Windows Vista, el servidor 2008 de Windows, el servidor 2003 de Windows, y Windows Xp.

Demuestra la estructura de la dirección enlace local.

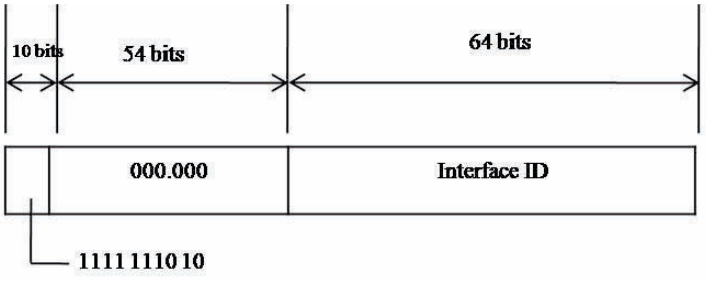

Figura 4- 5 Estructura de direcciones enlace local

A diferencia de direcciones enlace locales, las direcciones sitio locales no se configuran automáticamente, las direcciones enlace local es usado en el proceso de descubrimiento del vecino.

Los primeros 10 bits son siempre fijos para las direcciones sitio local, comenzando con FEC0:: /10. Después de que los 10 bits fijados sean un campo de la identificación del Subnet de 54 bits que proporciona 54 bits con los cuales usted pueda crear subnets dentro de su organización.

Las direcciones Sitio locales se han desaprobado formalmente en RFC 3879 para las puestas en práctica futuras IPv6. Sin embargo, las puestas en práctica existentes de IPv6 pueden continuar utilizando direcciones sitio local.

La zona de IDs para uso local de direcciones

A diferencia de la direcciones globales, el uso de de direcciones locales ya sea direcciones de enlace local y de sitio local, pueden ser reutilizadas, las direcciones de enlace local se reutilizan en cada enlace, las direcciones de sitio local se pueden reutilizar dentro de cada sitio de una organización. Para especificar el enlace en el cual está situado es destino o el sitio dentro del destino se encuentra, se usa un identificador adicional necesario. Este identificador adicional es un identificador de la zona que se encarga del (ID) y es conocido como identificación de alcance, que se encarga de de identificar una parte conectada de una red que tenga un alcance bien especificado.

Para los Host basados en IPv6, la zona de IDs para direcciones enlace locales y de sitio local se describe así:

Las direcciones de enlace local, la zona de identificación es el índice de la interfaz que se le asignó una dirección típica o puede ser utilizada como interfaz de envió para un destino de enlace local. Este índice de la interfaz es un número entero que comienza en 1 que se asigna a las interfaces IPv6 y que incluye el dispositivo de red Loopback e interfaces múltiples de la LAN o del túnel. Estas interfaces múltiples pueden tener el mismo identificador de zona enlace local si están al mismo enlace.

Las direcciones sitio local, el identificador de la zona es el mismo de del sitio. Las organizaciones que no reutilizan el prefijo sitio local de la dirección, el identificador del sitio se fija a 1 por abandono y no necesita ser especificada. Esto se puede ver en Windows donde se puede ver, modificar, administrar y diagnosticar la configuración de la red por medio del comando netsh.

Direcciones locales únicas

Las direcciones de sitio local proveen un direccionamiento privada ya que es una alternativa al direccionamiento global para el tráfico de una intranet. Sin embargo el prefijo de direccionamiento de sitio local puede ser rehusado para el direccionamiento de múltiples sitios dentro de una organización, ya que el prefijo de direccionamiento de sitio local puede ser duplicado. La ambigüedad de del direccionamiento sitio local en una organización adquiere complejidad y dificultad para las aplicaciones, Routers y administradores de la red.

Para substituir direcciones sitio local por un nuevo tipo de dirección que sea privada a una organización única a través de todos los sitios de la organización.

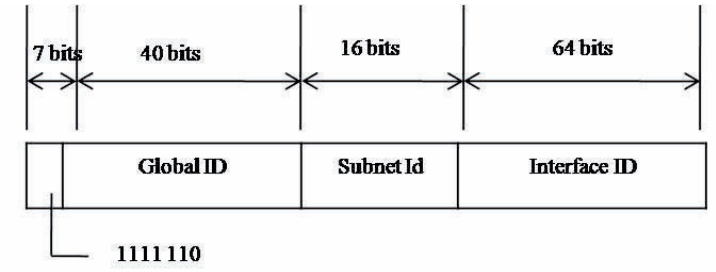

Figura 4- 6 Estructura de la dirección local única

Los 7 bits primero contienen un valor binario fijo de 1111110. Todas a las direcciones locales tienen el prefijo FC00::/7. La Local (L) es una bandera local que su valor se fija en 1 para indicar que el prefijo está localmente asignado. Y si la bandera L es asignada a 0 esta no está definida.Por lo tanto, las direcciones locales únicas dentro de una organización con L bandera a 1 tienen el prefijo de la dirección de FD00: /8.

El ID global identifica un sitio específico dentro de una organización y se fija a un valor de bit aleatoriamente derivado 40. Derivando un valor al azar para la identificación global, una organización puede tener estadístico 48 bits únicos asignados a sus sitios. Una ventaja es que dos organizaciones que utilizan el único local en sus direcciones tienen una baja probabilidad de duplicar su prefijo de 48 bits, reduciendo tener que volver reunmeramiento de sitios. Muy diferente a lo que se presenta con direcciones globales, ya que los IDs globales son prefijos únicos de la dirección local y no están diseñados para ser resumidos.

Las direcciones locales únicas tienen un alcance global, pero su alcance es definido encaminando topología y filtrando políticas en los límites del Internet. Las organizaciones no harán publicidad de sus prefijos únicos de la dirección local fuera de sus organizaciones

ni crearán entradas del DNS con direcciones locales únicas en el Internet DNS. Las organizaciones pueden crear fácilmente políticas de filtración en sus límites del Internet para evitar que todo el tráfico local tratado único sea remitido. Porque tienen un alcance global, las direcciones locales únicas no necesitan una identificación de la zona.

Por ejemplo, un subnet específico de su organización se puede asignar ambos casos, el prefijo global 2001: DB8: 4D1C: 221A:: /64 y el prefijo local FD0E: 2.o: BA9: 221A:: /64, donde el subnet es identificado para ambos tipos de prefijos por el valor de la identificación del Subnet de 221A. Aunque el identificador del subnet sea igual para ambos prefijos, las rutas para ambos prefijos se deben todavía propagar a través de la infraestructura del encaminamiento de modo que las direcciones basadas en ambos prefijos sean accesibles.

4.4.2 Multicast

Una dirección del Multicast identifica cero o más interfaz en el mismo o los diversos anfitriones. Con la topología apropiada del encaminamiento del Multicast, los paquetes tratados a una dirección del Multicast se entregan a todos los interfaces identificados por la dirección. [13]

Direcciones Multicast IPv6

En IPv6, el tráfico del Multicast funciona de la misma manera que hace en IPv4. Los nodos arbitrariamente localizados IPv6 pueden estar atentos al tráfico del Multicast en una dirección arbitraria del Multicast IPv6. Los nodos IPv6 pueden escuchar las direcciones múltiples al mismo tiempo. Los nodos pueden ensamblar o dejar a un grupo en cualquier momento.

Las direcciones del Multicast IPv6 tienen los primeros 8 bits fijados a 1111 1111. Por lo tanto, una dirección del Multicast IPv6 comienza siempre con el FF. Las direcciones del Multicast no se pueden utilizar como direcciones de fuente o como destinaciones intermedias en un jefe de la extensión del encaminamiento. Más allá de los primeros 8 bits, las direcciones incluyen la estructura adicional para identificar banderas, su alcance y al grupo. [14]

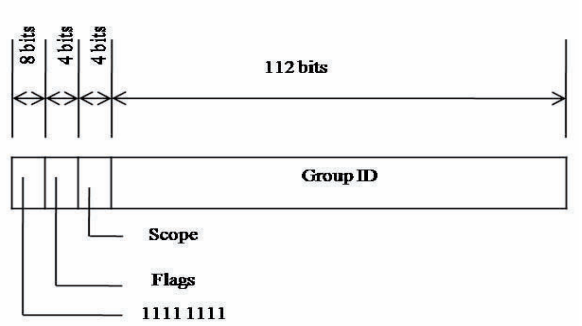

Figura 4- 7 Estructura de direccionamiento Multicast IPv6

Flags

Indica las banderas fijadas en la dirección del Multicast. El tamaño de este campo es 4 bits consistiendo en tres banderas en los bits de peso inferior. El primer bit de bajo nivel es (T) la bandera transitoria. Cuando el sistema es colocado a 0, la bandera de T indica que la dirección del Multicast es una dirección permanentemente asignada por el Internet Assigned Numbers Authority (IANA). Cuando la bandera es colocada a 1 indica que la dirección del Multicast es una dirección (que no es permanente). El segundo bit de nivel inferior está para la bandera del prefijo (P), que indica si la dirección del Multicast está basada en un prefijo de la dirección del Unicast.

Scope

Indica el alcance de la red IPv6 para la cual el tráfico del Multicast se prepuso ser entregado. El tamaño de este campo es 4 bits. Además de usar la información proporcionó por los protocolos del encaminamiento del Multicast, los Routers utilizan el alcance para determinar si el tráfico puede ser remitido.

Enumera los valores para el campo del alcance asignado en RFC 4291. El resto de los valores son no asignados.

Tabla 4- 2 Valores definidos para el campo del alcance

Scope Field Value	Scope
0	Reserver
1	Interface-local scope
2	Link-local scope
3	Reserved
4	Admin-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved

Por ejemplo, tráfico con la dirección del Multicast de FF02:: 2 tiene un alcance enlace local. Un Router IPv6 nunca remite este tráfico más allá del acoplamiento local.

Identificador de Grupo

Identifica al grupo del Multicast y es único dentro del alcance. El tamaño de este campo es 112 bits. Las identificaciones del grupo permanentemente asignadas son independientes del alcance. Direcciones del Multicast de FF01:: con FF0F:: son las direcciones reservadas.

Para identificar todos los nodos para los alcances interfaz local y enlace locales, las direcciones siguientes se definen:

FF01:: 1 (dirección interfaz local del Multicast de todos los nodos del alcance).
FF02:: 1 (dirección enlace local del Multicast de todo los nodos del alcance).

Para identificar todos los Routers para el interfaz local, los alcances enlace locales, y sitio locales, las direcciones siguientes se definen:

FF01:2 (Alcance de todos los Routers direccionamiento Multicast interfaz local)
FF02:2 (Alcance de todos Routers de la dirección acoplamiento local del Multicast)
FF05:2 (Alcance de todos los Routers direccionamiento Multicast sitio local)

Dirección solicitada del nodo

La dirección del nodo solicitada hace fácil y eficiente la consulta de los nodos de la red durante la capa de enlace la resolución de la dirección resuelve la dirección de capa de

enlace también conocida como IPv6. En IPv4, el marco de la petición del Address Resolution Protocol (ARP) se envía el marco de petición a nivel Mac, distorsionando todos los nodos en los segmentos de la red, incluyendo los que no estén funcionando en IPv4. Sin embargo IPv6 utiliza el método de solicitud de mensaje vecino para realizar la resolución de direcciones de la capa de enlace, La dirección del Multicast del nodo solicitado se construye del prefijo FF02:: 1: FF00: 0/104 y los 24 bits pasados de una dirección del Unicast IPv6.

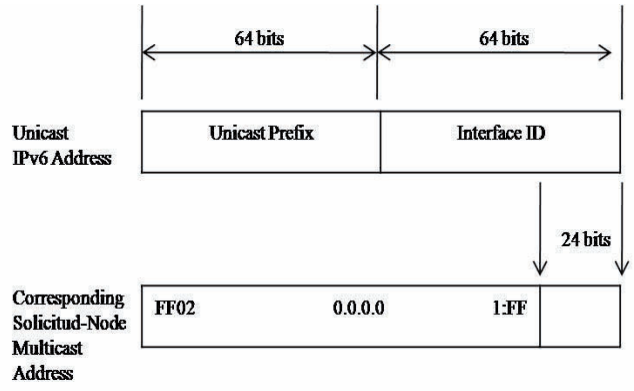

Figura 4- 8 Mapping de direcciones Unicast y el nodo solicitado de direcciones Multicast

Usando la dirección del nodo solicitado, muy pocos nodos se disturban durante la resolución de direcciones. En la práctica, debido a la relación entre la identificación del interfaz IPv6 y la dirección del nodo solicitado, la dirección del nodo solicitado actúa como seudo Unicast dirección para la resolución de direcciones muy eficiente.

Trazado de direcciones del Multicast IPv6 a las direcciones de Ethernet

Al enviar los paquetes del Multicast IPv6 en enlace Ethernet, el MAC Address correspondiente de la destinación es 0x33-33-mm-mm-mm-mm, donde mm-mm-mm-mm es un trazado directos de los últimos 32 bits (8 dígitos hexadecimales) de la dirección del Multicast IPv6. El trazado de una dirección del Multicast IPv6 a una dirección del Multicast de Ethernet.

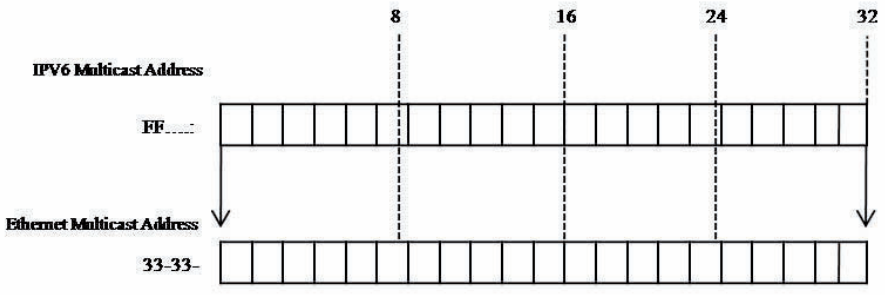

Figura 4- 9 Trazado de una dirección Multicast IPv6 para una dirección Multicast Ethernet

Los adaptadores de la red de Ethernet mantienen una tabla de direcciones interesantes del MAC de la destinación. Si un marco de Ethernet con un MAC Address interesante de la destinación se recibe, se pasa a las capas superiores para el proceso adicional. Ya viene predeterminada la tabla que contiene la dirección de la difusión del Mac-nivel (0xFF-FF-FF-FF-FF-FF) y el MAC Address del Unicast asignado al adaptador. Para facilitar la entrega eficiente del tráfico del Multicast, las direcciones de destinación adicionales del Multicast se pueden agregar o quitar de la tabla. Para cada dirección del Multicast que es escuchada por el Host, hay una entrada de correspondencia en la tabla de direcciones interesantes del MAC.

Por ejemplo, una Cabecera IPv6 con el MAC Address de Ethernet de 00-AA-00-3F-2A-1C (dirección enlace-local de FE80:: 2AA: FF: FE3F: 2A1C) agrega las direcciones siguientes del MAC del Multicast a la tabla de direcciones interesantes del MAC de la destinación en el adaptador de Ethernet:

- La dirección de 33-33-00-00-00-01, corresponde a el enlace local alcance todo los nodos de direcciones Multicast FF02:: 1 (expresado completamente como FF02: 0000: 0000: 0000: 0000: 0000: 0000: 0001).
- La dirección de 33-33-FF-3F-2A-1C, que corresponde a la dirección del nodo solicitado de FF02:: 1: FF3F: 2A1C. ay que recordar que la dirección del nodo solicitado es el prefijo FF02:: 1: FF00: 0/104 y los 24 bits pasados de la dirección del Unicast IPv6.

4.4.3 Anycast

Una de las nuevas características presentes en la versión 6 de IP es la incorporación de un nuevo tipo de direcciones denominado Anycast .Este tipo de direcciones aún en fase experimental se diferencia de las direcciones Multicast en que el datagrama no es entregado a todos los miembros del grupo, sino que se entrega al integrante del grupo más cercano del origen del datagrama.

Una dirección Anycast identifica múltiples interfaces. Con una topología de encaminadores adecuada, los paquetes destinados a una dirección Anycast se entregarán a una sola interfaz (la que este más “cerca”, dentro del grupo de direcciones Anycast). Si una dirección Multicast define una comunicación “uno” a “muchos”, una dirección Anycast se define como “uno” a “uno-entre-muchos”.

Para que los paquetes se entreguen a la dirección Anycast más "cercana", el "Routing" de la red debe conocer qué interfaz tienen asignada una dirección Anycast y sus distancias.

Las direcciones Anycast no tienen un espacio propio dentro del direccionamiento IPv6, utilizan el mismo espacio que las direcciones Unicast (es decir, no podemos diferenciar entre direcciones Unicast y Anycast). El ámbito de las direcciones Anycast se equipara con el Unicast, así pues pueden existir direcciones Anycast de ámbito de sitio, de enlace o global. También cabe remarcar que este tipo de direcciones solo pueden usarse como dirección de destino, jamás como fuente.

Existe una dirección Anycast, requerida para cada subred, que se denomina "dirección Anycast del Router de la subred"6 (subnet Router Anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección Unicast, siendo el indicador de interfaz igual a cero:

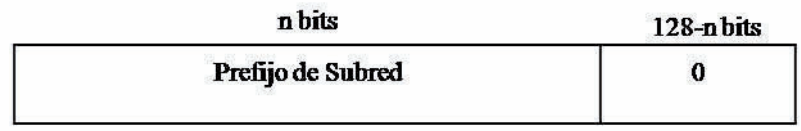

Figura 4- 10 Dirección Anycast del Router de la subred

Todos los Routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección Anycast del Router de la subred", serán enviados a un Router de la subred.

La utilidad de estas direcciones es para implementar los siguientes mecanismos:

- Comunicación con el servidor más "cercano": Estas direcciones permiten que un cliente pueda comunicarse con un servidor de entre un grupo, y que la red le seleccione el que sea más cercano.
- Descubrimiento de Servicios: Al configurar un nodo con IPv6, no haría falta especificarle la dirección del servidor DNS, Proxy etc... Podría existir una dirección Anycast que identificara a esos servicios.
- Movilidad: Nodos que tienen que comunicarse con un Router, del conjunto disponible en su red.

4.4.4 Direcciones especiales IPv6

Dirección sin especificar

La dirección sin especificar (0: 0: 0: 0: 0: 0: 0: 0 o ::) se utiliza para indicar solamente la ausencia de una dirección. Es equivalente a la dirección sin especificar IPv4 de 0.0.0.0. La dirección sin especificar se utiliza típicamente como dirección de fuente cuando una dirección única todavía no se ha determinado. La dirección sin especificar nunca se asigna a un interfaz o se utiliza como dirección de destinación.

Dirección del Loopback

La dirección del Loopback (0: 0: 0: 0: 0: 0: 0: 1 o :: 1) se asigna a un interfaz del Loopback, permitir a un nodo enviar los paquetes a sí mismo. Es equivalente a la dirección del Loopback IPv4 de 127.0.0.1. Los paquetes tratados a la dirección del Loopback, nunca se deben enviar en un acoplamiento o remitir por un Router IPv6.

Direcciones para un HOST IPv6

Un Host de IPV4 con un adaptador de red típicamente tiene una dirección de IPV4 asignada a aquel adaptador. Un Host de IPV6, sin embargo por lo general tiene múltiples direcciones de IPV6 asignadas a cada adaptador. Las interfaces sobre un Host de IPV6 típico son asignadas las direcciones de Unicast siguientes:

- Una dirección local de enlace para cada interfaz
- Unicast Adicional se dirige para cada interfaz (que podría ser uno o múltiples direcciones únicas locales o globales)
- La dirección de Loopback (:: 1) para el interfaz Loopback

Hosts de IPV6 típicos son siempre lógicamente para múltiples lugares porque ellos siempre tienen al menos dos direcciones con las cuales ellos pueden recibir paquetes a la dirección local de enlace para el tráfico de enlace local y una dirección ruteable única local o global.

Además, cada interfaz sobre un Host de IPV6 escucha para el tráfico sobre las direcciones de Multicast siguientes:

- La dirección de interfaz local alcanza todo los nodos del Multicast con esta dirección (FF01:: 1)

- La dirección enlace local alcanza todos los nodos del Multicast con esta dirección (FF02:: 1)
- La dirección de nodo solicitado para cada dirección de Unicast se le asignó.
- Las direcciones de Multicast de grupos unidos.

Direcciones para un Router IPv6

Las interfaces sobre un Router IPV6 son asignadas las direcciones de Unicast siguientes:

- Una dirección local de enlace para cada interfaz
- Unicast Adicional se dirige para cada interfaz (que podría ser un o múltiples direcciones únicas locales o globales)

La dirección de Loopback (:: 1) para el interfaz Loopback Además, las interfaces de un Router IPV6 son asignadas las direcciones de Anycast siguientes:

- Una Subnet Router de Anycast dirigen para cada subred.
- Direcciones de Anycast Adicionales (opcionales).

Además, los interfaces de un Router IPV6 escuchan para el tráfico sobre las direcciones de Multicast siguientes:

- La dirección de interfaz local alcanza todo los nodos del Multicast con esta dirección (FF01:: 1)
- La dirección de interfaz local alcanza todo los Routers del Multicast con esta dirección (FF01:: 2)
- La dirección de enlace local alcanza todo los nodos del Multicast con esta dirección (FF02:: 1)
- La dirección de enlace local alcanza todo los Routers del Multicast con esta dirección (FF02:: 2)
- La dirección de sitio local alcanza todo los nodos del Multicast con esta dirección (FF05:: 2)
- Para la dirección del nodo solicitado para cada dirección Unicast asignada.
- Las direcciones de Multicast de grupos unidos

Subredes del Espacio de Dirección de IPV6

Tal como en IPv4, el espacio de dirección IPv6 puede ser dividido usando los bits de categoría alta que no tienen ya valores fijos para crear prefijos subnetted de la dirección. Éstos se utilizan para resumir un nivel en el encaminamiento o jerarquía de la dirección (con una longitud del prefijo menos de 64), o para definir un segmento específico del subnet o de la red (con una longitud del prefijo de 64). IPv4 subnetting diferencia de IPv6 subnetting en la definición de la porción de la identificación del Host de la dirección. En IPv4, la identificación del Host puede estar de longitud diversa, dependiendo del esquema subnetting. Para las direcciones actualmente definidas del Unicast IPv6, la identificación del Host es la porción de la identificación del interfaz de la dirección del Unicast IPv6 y es siempre una de tamaño fijo de 64 bits.

Para la mayoría de los administradores de red dentro de una organización, subnetting el espacio de dirección IPv6 consiste en el usar de técnicas subnetting para dividir la porción de la identificación del subnet de un prefijo global o único de la dirección local de una forma que permita la recapitulación de la ruta y la delegación del espacio de dirección restante a diversas porciones de un intranet IPv6. Para las direcciones locales globales y únicas, los primeros 48 bits de la dirección son fijos. Para la dirección global, los primeros 48 bits son fijos y asignados por una ISP. Para la dirección local única, los primeros 48 bits son fijos en FD00:: /8 y la identificación global al azar de 40 bits asignada a un sitio de una organización.

Subnetting la porción ID del subnet de un espacio de dirección local global o único requiere un procedimiento de dos etapas:

1. Determine el número de bits que se utilizarán para subnetting.
2. Enumere los nuevos prefijos subnetted de la dirección. La técnica subnetting descrita aquí asume eso subnetting.

La técnica subnetting descrita aquí asume que el subnetting es hecho dividiendo el espacio de dirección de 16 bits de la ID del subnet usando los bits de categoría alta en la ID del subnet. Aunque este método promueva la dirección jerárquica y el encaminamiento, no se requiere.

Paso 1: Determinación del número de bits de Subnetting

El número de bits que son utilizados para subnetting determina el número posible de nuevos prefijos subnetted de la dirección que se puedan asignar a las porciones de su red basada en las divisiones geográficas o departamentales. En una infraestructura jerárquica del routing, se necesita determinar cuántos prefijos de la dirección, y por lo tanto cuántos bits, es necesario en cada nivel en la jerarquía. Cuantos más bits que se eligen para los varios niveles de la jerarquía, poco los bits se tendrán disponibles para enumerar subnets individuales en el nivel pasado de la jerarquía.

En algunos casos, el bit-nivel subnetting se requiere. Por ejemplo, un administrador de red decide ejecutar una jerarquía de dos niveles que refleja una estructura geográfica/departamental y utiliza 4 bits para el llano geográfico y 6 bits para el nivel departamental. Esto significa que cada departamento en cada localización geográfica tiene solamente 6 bits de espacio subnetting dejados (16-4-6), o solamente 64 (de = subnets 26) por el departamento.

En cualquier nivel dado en la jerarquía, usted tendrá un número de bits que sean fijados ya por el nivel siguiente para arriba en la jerarquía (f), un número de bits usados para subnetting en el nivel actual en la jerarquía (s), y un número de bits que siguen habiendo para el nivel siguiente abajo en la jerarquía (r). Siempre f + s + r = 16.

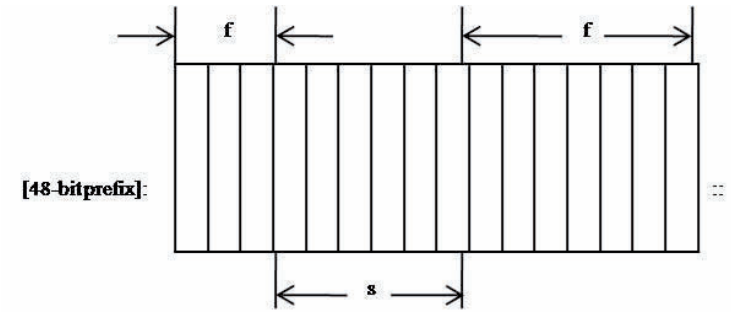

Figura 4- 11 El subnetting de una Subred ID

Pasó 2: Enumeración de prefijos de la dirección de Subredes

De acuerdo con el número de bits usados para subnetting, usted debe determinar los nuevos prefijos subnetted de la dirección. Hay tres acercamientos principales:

El binario enumera nuevos prefijos subnetted de la dirección usando representaciones binarias de la identificación del subnet y el convertir al hexadecimal para los prefijos subnetted de la dirección.

El Hexadecimal enumera nuevos prefijos subnetted de la dirección usando las representaciones hexadecimales de la ID del subnet y de un incremento calculado entre sucesivo subnetted prefijos de la dirección.

El decimal enumera nuevos prefijos subnetted de la dirección usando las representaciones decimales de la identificación del subnet y del incremento.

4.5 SIMPLIFICACION DE LAS DIRECCIONES IPv6

Las direcciones IP de la versión 6 están compuestas por 128 bits. Los diseñadores del protocolo optaron por representarlas en 8 agrupaciones de 16 bits. De esta forma se puede utilizar la notación hexadecimal, que permite una representación más compacta que una serie de 128 unos y ceros. Esta simplificación continua siendo bastante complicada de manipular y recordar (es posible recordar que www.uvaq.edu.mx.es tiene la dirección 158.109.0.4, pero es imposible recordar que le corresponde la dirección IP versión 6 3FFE:3326:FFFF:FFFF:FFFF:FFFF:FFFF:1). Por lo cual se opto por esta cualidad para impulsar el uso de los nombres (www.uvaq.edu.mx.) por los usuarios.

Para compactar estas direcciones tan voluminosas, se aceptaron una serie de simplificaciones:

- Supresión de los ceros redundantes situados a la izquierda.
- Simplificación de los ceros consecutivos mediante el uso del prefijo '::'. Este prefijo tan sólo puede ser utilizado una vez en una misma dirección.
- Para las direcciones IP versión 6 obtenidas añadiendo 6 ceros a la dirección IP versión 4 (10.0.0.1 -> 0:0:0:0:0:0:A00:1) se permitirá el uso de la notación decimal (::10.0.0.1).
- La especificación de un prefijo de direccionamiento en la versión 6 se realizará mediante la forma dirección ipv6/prefijo (Si tenemos el prefijo de 40 bits FEDC:BA98:76 en la dirección FEDC:BA98:7600::1 se especificará como FEDC:BA98:7600::1/40). Se debe tener mucho cuidado con las simplificaciones siempre que se indican prefijos, ya que puede pasar que con el prefijo de 64 bits FEDC:BA98:0: y la dirección FEDC:BA98:0

Tabla 4- 3 Simplificaciones en el direccionamiento IP versión 6.

1080:0000:0000:0000:0008:0800:200C:417C 1080:0:0:0:8:800:200C:417C	Simplificación	1080:0:0:0:8:800:200C:417C 1080::8:800:200C:417C
0:0:0:BC98:6564:0:0:0	Simplificación	::BC98:6564:0:0:0 :BC98:6564:: (ambiguo) ::BC98:6564::
0:0:0:0:0:0:0A00:001 ::A001	Notación Decimal	::A00:1 ::10.0.0.1
FEDC:BA98:7600::1/40	Uso de prefijos	Prefijo: FEDC:BA98:76 Dirección: FEDC:BA98:7600:1

Después de observar cómo se van agotando con los años las direcciones IP versión 4 sin poder ampliar o reestructurar el direccionamiento de una forma no traumática, los diseñadores de la versión 6 optaron por no consumir todo el espacio direccionable de los 128 bits, realizando una partición en subgrupos independientes (ver Tabla 4-3) para facilitar en un futuro la ampliación de tipos de direcciones o incluso un nuevo tipo de direccionamiento.

Y así, se han reservado algunos prefijos de direcciones para aquellos grupos específicos de direcciones (como direcciones compatibles NSAP o direcciones compatibles IPX) que se prevé que en un futuro pueden necesitar un rango de direcciones separado del resto de direcciones IP, incluso se ha reservado un rango de direcciones para un posible direccionamiento geográfico. Todo y esta partición del espacio de direcciones, aún queda más de un 70% del espacio total de direcciones sin asignar.

Tabla 4- 4 Distribución inicial del espacio de direcciones en la versión 6 de IP

GRUPO ASIGNADO	PREFIJO	FRACCION DE ESPACIO OCUPADO
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Dirección NSAP	0000 001	1/128
Direccion IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
No Asignado	001	1/8
Direcciones globales unicast	010	1/8
No Asignado	011	1/8
Direcciones geográficas Unicast	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 locales (link local)	1111 1110 10	1/1024
Direcciones locales (site local)	1111 1110 11	1/1024
Direcciones Multicast	1111 1111	1/256

4.6 Identificadores de interfaz de IPv6

Los últimos 64 bits de una dirección IPv6 corresponden al identificador de la interfaz, que es único para el prefijo de 64 bits de la dirección IPv6. Las formas de determinar un identificador de interfaz son las siguientes:

En el documento RFC 2373 [15] se indica que todas las direcciones de unidifusión que utilicen los prefijos del 001 al 111 deben utilizar también un identificador de interfaz de 64 bits derivado de la dirección EUI-64 (Extended Unique Identifier o Identificador único extendido).

En el documento RFC 3041 [16] se describe un identificador de interfaz generado aleatoriamente que cambia al cabo del tiempo para proporcionar un nivel de anonimato.

Un identificador de interfaz que se asigna durante la configuración automática de direcciones con estado (por ejemplo, mediante DHCPv6). Los estándares DHCPv6 se están definiendo actualmente. En la familia de Windows Server 2003 y en Windows XP, el protocolo IPv6 no admite la configuración de direcciones con estado ni DHCPv6.

Un identificador de Interfaz configurado manualmente.

Identificadores de interfaz basados en direcciones EUI-64

El Institute of Electrical and Electronic Engineers (IEEE) define la dirección EUI-64 de 64 bits. Las direcciones EUI-64 se asignan a un adaptador de red o se derivan de las direcciones IEEE 802.

Direcciones IEEE 802

Los identificadores de interfaz tradicionales para los adaptadores de red utilizan una dirección de 48 bits que se llama dirección IEEE 802. Esta dirección consta de un Id. Que viene por marcado por la compañía de 24 bits y un Id. De extensión (también llamado Id. de tarjeta) de 24 bits. La combinación del Id. De compañía, que se asigna de forma única a cada fabricante de adaptadores de red, y el Id. De tarjeta, que se asigna de forma única a cada adaptador de red en el momento del ensamblaje, genera una dirección única global de

48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, Media Access Control).

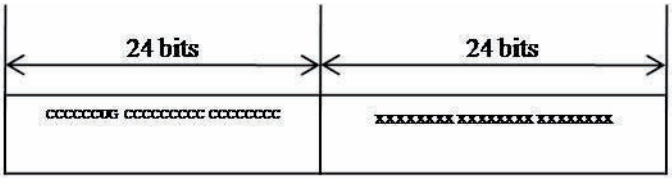

Figura 4- 12 Dirección IEEE 802.

Los bits definidos en la dirección IEEE 802 son los siguientes:

- **Universal o local (U/L)**

El bit U/L es el séptimo bit del primer byte y se utiliza para determinar si la dirección se administra de forma universal o local. Si el bit U/L está establecido en 0, la administración de la dirección corresponde a IEEE, mediante la designación de un Id de compañía único. Si el bit U/L está establecido en 1, la dirección se administra de forma local. El administrador de la red ha suplantado la dirección de fábrica y ha especificado una dirección distinta.

- **Individual o grupo (I/G)**

El bit I/G es el bit de orden inferior del primer byte y se utiliza para determinar si la dirección es individual (unidifusión) o de grupo (multidifusión). Si está establecido en 0 la dirección es de unidifusión. Si está establecido en 1 la dirección es de multidifusión.

En una dirección típica de adaptador de red 802.x, los bits U/L e I/G están establecidos en 0, lo que corresponde a una dirección MAC de unidifusión administrada de forma universal.

Direcciones IEEE EUI-64

La dirección IEEE EUI-64 representa un nuevo estándar para el direccionamiento de interfaces de red. El Id de compañía sigue teniendo 24 bits de longitud, pero el Id de extensión tiene 40 bits, por lo que se crea un espacio de direcciones mucho mayor para los

fabricantes de adaptadores de red. La dirección EUI-64 utiliza los bits U/L e I/G de la misma forma que la dirección IEEE 802.

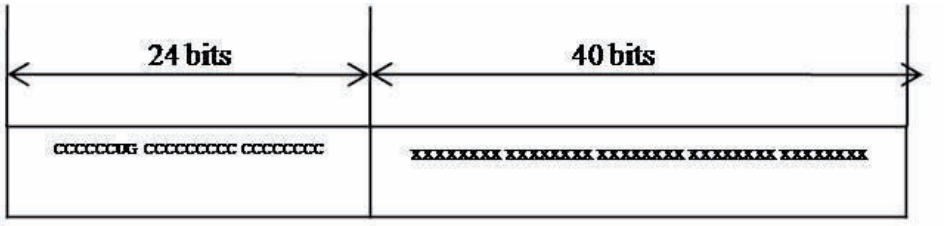

Figura 4- 13 Direcciones IEEE EUI-64

Asignación de direcciones IEEE 802 a direcciones EUI-64

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id de compañía y el Id de extensión. En la siguiente ilustración se muestra la conversión de una dirección IEEE 802 en una dirección EUI-64.

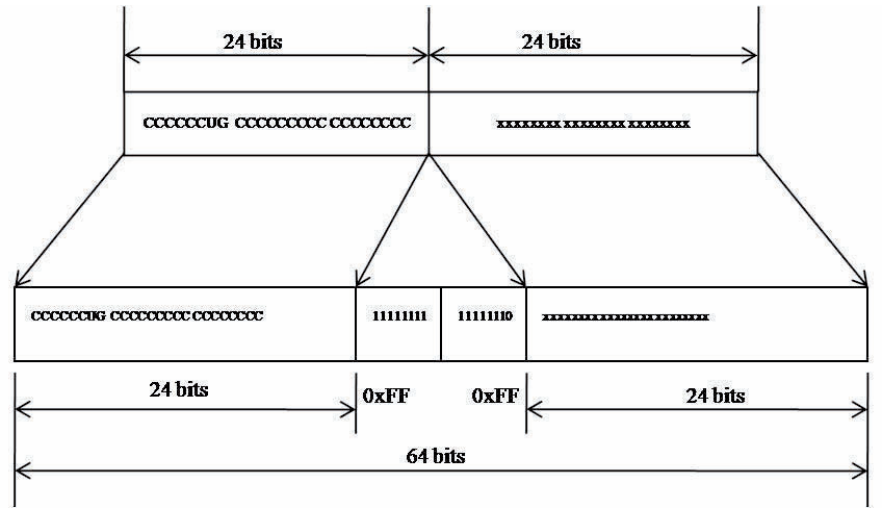

Figura 4- 14 Asignación de direcciones IEEE 802 a direcciones EUI-64

Asignación de direcciones EUI-64 a identificadores de interfaz IPv6

Para obtener el identificador de interfaz de 64 bits para las direcciones IPv6 de unidifusión, se complementa el bit U/L de la dirección EUI-64 (si es 1, se establece en 0; y si es 0, se establece en 1). En la ilustración siguiente se muestra la conversión de una dirección EUI-64 de unidifusión administrada de forma universal.

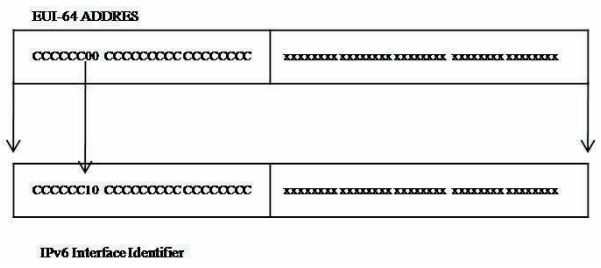

Figura 4- 15 Asignación de direcciones EUI-64 a identificadores de interfaz IPv6

Para obtener un identificador de interfaz IPv6 a partir de una dirección IEEE 802, primero se debe asignar la dirección IEEE 802 a una dirección EUI-64 y, después complementar el bit U/L. En la ilustración siguiente se muestra el proceso de conversión de una dirección IEEE 802 de unidifusión administrada de forma universal

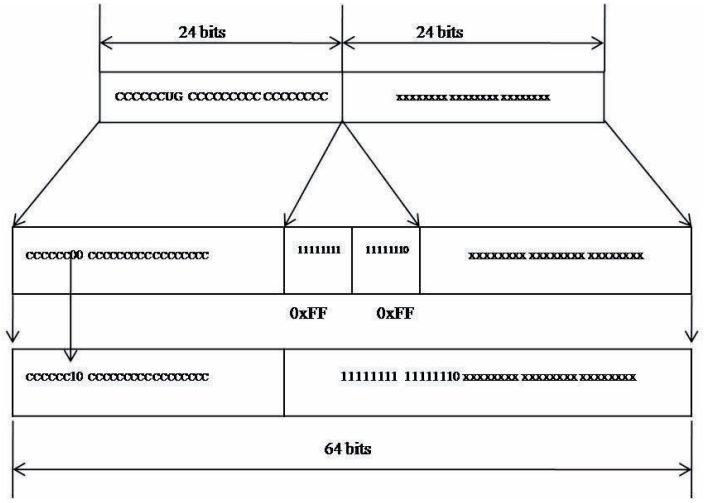

Figura 4- 16 IEEE 802, EUI-64 E Identificador de interface IPv6

Ejemplo de conversión de una dirección IEEE 802

El Host A tiene la dirección MAC de Ethernet de 00-AA-00-3F-2A-1C. Primero, se convierte al formato EUI-64 insertando FF-FE entre el tercer y cuarto bytes, con el resultado de 00-AA-00-FF-FE-3F-2A-1C. Después, se complementa el bit U/L, que es el séptimo bit del primer byte. El primer byte en formato binario es 00000000. Al complementar el séptimo bit, se convierte en 00000010 (0x02). El resultado final es 02-AA-00-FF-FE-3F-2A-1C que, cuando se convierte a notación hexadecimal con dos puntos, da como resultado el identificador de interfaz 2AA:FF:FE3F:2A1C. En consecuencia, la dirección local del vínculo correspondiente al adaptador de red que tiene la dirección MAC de 00-AA-00-3F-2A-1C es FE80::2AA:FF:FE3F:2A1C. [17]

Identificadores de interfaz de direcciones temporales

En la actual red Internet basada en IPv4, un usuario típico de Internet conecta con un proveedor de servicios Internet (ISP) y obtiene una dirección IPv4 mediante el Protocolo punto a punto (PPP) y el Protocolo de control de protocolo Internet (IPCP). Cada vez que el usuario se conecta, obtiene una dirección IPv4 distinta. Debido a esto, es difícil hacer un seguimiento del tráfico de un usuario en Internet sobre la base de la dirección IP.

En las conexiones de acceso telefónico basadas en IPv6, se asigna al usuario un prefijo de 64 bits después de realizar la conexión mediante descubrimiento de enrutadores y configuración automática de direcciones sin estado. Si el identificador de interfaz siempre se basa en la dirección EUI-64 (derivada de la dirección IEEE 802 estática), es posible identificar el tráfico de un nodo específico independientemente del prefijo, por lo que resulta fácil hacer un seguimiento de un usuario específico y del uso que hace de Internet. Para solucionar este problema y proporcionar un nivel de anonimato, en el documento RFC 3041[18] se describe un identificador de interfaz IPv6 alternativo que se genera aleatoriamente y cambia al cabo del tiempo.

El identificador de interfaz inicial se genera mediante números aleatorios. En los sistemas IPv6 que no pueden almacenar información de historial para la generación de futuros valores de identificador de interfaz, se genera un nuevo identificador de interfaz aleatorio cada vez que se inicializa el protocolo IPv6. En los sistemas IPv6 que tienen capacidades de almacenamiento, se almacena un valor de historial y, al inicializar el protocolo IPv6, se crea un nuevo identificador de interfaz mediante el proceso siguiente:

1. Se recupera el valor de historial almacenado y se anexa el identificador de interfaz basado en la dirección EUI-64 del adaptador.
2. Se calcula el algoritmo Hash de cifrado unidireccional de Síntesis del mensaje 5 (MD5) con la cantidad del paso 1.
3. Se guardan los últimos 64 bits del algoritmo Hash MD5 calculado en el paso 2 como valor de historial para el siguiente cálculo de identificador de interfaz.
4. Se toman los primeros 64 bits del algoritmo Hash MD5 calculado en el paso 2 y el séptimo bit se establece en cero. El séptimo bit corresponde al bit U/L que cuando

está establecido en 0, indica un identificador de interfaz administrado de forma local. El resultado es el identificador de interfaz.

La dirección IPv6 resultante, basada en este identificador de interfaz aleatorio, se conoce como dirección temporal. Las direcciones temporales se generan para prefijos de direcciones públicas que utilizan configuración automática de direcciones sin estado. Las direcciones temporales se utilizan para el menor de los siguientes valores de duración válida y duración preferida:

- Las duraciones incluidas en la opción Información de prefijo del mensaje de anuncio de enrutador recibido.
- Valores locales predeterminados de 1 semana para la duración válida y 1 día para la duración preferida.

Capítulo 5 La Cabecera IPv6

Describiremos la estructura del paquete de la cabecera de IPv6, denotando cada campo de cabecera de IPv6 y así como sus cabeceras de extensión que son de gran ayuda porque aportan gran eficacia y flexibilidad ya que se pueden definir en cualquier momento a medida que se vayan necesitando entre la cabecera fija y la carga útil. Existen 8 tipos de cabeceras de extensión, donde la cabecera fija y las de extensiones opcionales incluyen el campo de cabecera siguiente que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior.

Unidad máxima de transferencia de datos el cual expresa el tamaño en bytes, la unidad de datos más grande que puede ser enviado usando un protocolo de Internet. Así como el propósito de los mensajes de errores y de los mensajes informativos, definiendo las estructura de los mensajes así como los diferentes tipos de de mensajes que existen y como reconocerlos.

Para que son usados los mensajes informativos, como para diagnostico. Describir los mensajes más comunes de ICMPv4 y sus equivalentes de ICMPv6.

5.0 La estructura de un Paquete IPV6

Un paquete de la versión 6 (IPv6) de Protocolo de Internet consiste en una cabecera IPV6, cabeceras de Extensión y una unidad de datos de protocolo de capa superior.

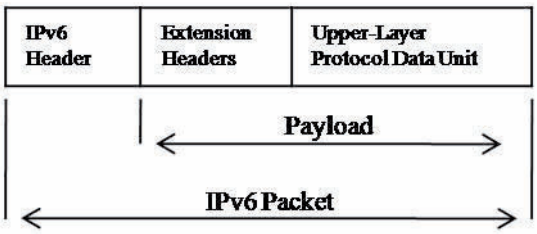

Figura 5- 1 Estructura de un paquete IPv6

Algunos componentes de un paquete IPv6:

Cabecera IPv6: La cabecera IPv6 está siempre presente y es un de tamaño fijo de 40 bytes.

Cabecera de extensión: Cero o más cabeceras de la extensión pueden ser presentes y está de la variación longitudes. Si las cabeceras de la extensión están presentes, un campo de la siguiente cabecera en la cabecera IPv6 indica la primera cabecera. Dentro de cada extensión la cabecera es otra cabecera del siguiente campo, indicando la cabecera siguiente de la extensión.

Upper-Layer Protocol Data Unit: La unidad de datos upper-layer de protocolo (PDU) típicamente consiste en una cabecera de protocolo y su carga útil, La carga útil del paquete IPv6 es la combinación de las cabeceras de la extensión IPv6 y de la PDU upper-layer. Normalmente, puede ser hasta 65.535 bytes de largo. Los paquetes IPv6 más grandes de las cargas útiles de 65.535 bytes en la longitud, conocida como jumbograms, pueden también ser enviados. [19]

5.1 Cabeceras del protocolo IP versión 6

Como ya se vio anteriormente la cabecera IPv6 no tiene opciones muy diferentes a las que ya contiene el protocolo que actualmente está en uso (versión 4), sin embargo es necesario resaltar algunas de las características especiales que son incorporadas a los Routers para que puedan así tratar el datagrama de una forma adecuada, ya que no todos los datagramas son datos que andan circulando en Internet de un usuario a otros sino como mensajes entre los diferentes Routers (un ejemplo seria cuando los Routers no pueden lograr la conexión y así recibir o envira los datagramas por causa de que están fuera de servicio).

5.1.1 La cabecera de encaminamiento

En IPv6 consiste en la misma ocupación que en la versión 4. Son 4 bytes (su valor máximo de cada opción 2^8 = 256) de cabecera a los que se añade una serie de direcciones de 128 bits que corresponden a los Routers por los que debe pasar el datagrama hasta llegar a su destino. En el primer campo le corresponde a el de la siguiente cabecera (Next Header), en esta versión 6 se utiliza un sistema de cadena margarita (daisy chain) dónde se

pueden especificar múltiples cabeceras. Después le toca al tamaño de la cabecera (Header Extensión Length) que es el tamaño total de la cabecera en palabras de 64 bits. El tipo de encaminamiento (Routing Type) es la política que se debe seguir en el encaminamiento, actualmente sólo existe el tipo 0 (si el Router aparece en la lista de direcciones especificadas, se quita de la lista, decrementa el campo de segmentos restantes y busca cual de la lista está más cerca para enviar el datagrama. Si no aparece en la lista, se limita a encaminarlo ignorando esta opción). El número de segmentos restantes (Segments Left) es un valor que indica el número de direcciones de encaminamiento que aún restan. De esta forma, al llegar a 0 significa que el datagrama ha alcanzado su destino.

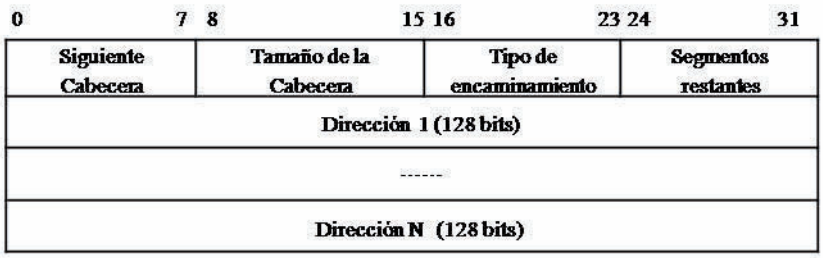

Figura 5- 2 Cabecera de Routing (tipo 0)

5.1.2 La cabecera de fragmentación

En esta nueva versión tiene diferencias con respecto a la de la versión 4 en la que no existe un bit de fragmentación, ya que no se fragmentan los datagramas. La gran versatilidad de la fragmentación implementada en la versión anterior, si un Router recibe un datagrama de tamaño superior al que puede enviar, lo fragmentaba en varios datagramas de menor tamaño. Estos datagramas se encaminaban independientemente y por lo tanto si uno sólo de ellos no llegaba a su destino o llegaba incorrecto, todo el datagrama original se desechaba y debía ser retransmitido. Esto causaba mucha problemática más que ser algo beneficioso debido a la gran variedad de redes conectadas a Internet y se tendría que llevar a cabo la retransmisión de todo el datagrama.

Así que si llegaba a un Router un datagrama que superara el tamaño del que se podía transmitir, este era descartado y se tenía que enviar al origen del datagrama un mensaje de error ICMP. Así que existe una cabecera de fragmentación para que desde el origen se pueda fragmentar un tamaño de datos de datos que no sea superior al soportado por la red (MTU) y este sea fragmentado para que sean soportados y que sean

independientes entre sí y así puedan ser enviados y reenviados por separados si es necesario.

El primer campo es la cabecera siguiente que nos indica el siguiente tipo de cabecera que puede ser encontrado (si es el caso).
El segundo campo es un byte que hasta ahora está reservado así que debe ser puesto a 0. En el campo de desplazamiento de fragmento que es el que indica los 13 bits más significativos del desplazamiento, ya que se asume que la fragmentación son múltiplos de 64. En la anterior versión (versión 4) se usaban 13 bits como ahora, pero eran los menos significativos y estos tenían que ser multiplicados por 8 para que se pudiera obtener el desplazamiento total del byte y en esta nueva versión no es necesario. Y los 2 bits siguientes están reservados para que sean usados en el futuro. Y el último bit que se llama el bit de más fragmentos (more) y este es colocado a 1 en los fragmentos y a 0 en el ultimo.

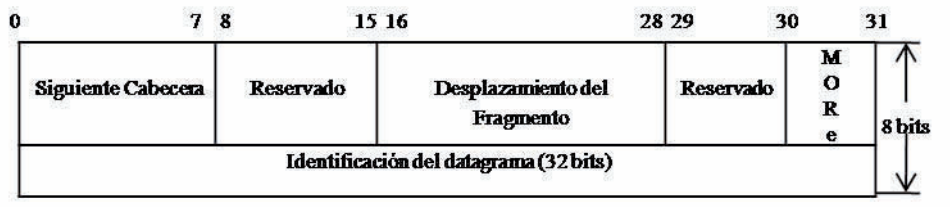

Figura 5- 3 Cabecera de fragmentación de datagramas.

5.1.3 La cabecera de opciones de destino

Nos permite añadir opciones extras a los datagramas para que solo puedan ser manipuladas y procesadas únicamente por el destinatario. Así este formato permite que los Routers intermedios no necesitan interpretar y estas puedan ser enviadas sin perder tiempo en el proceso. En el primer campo es la siguiente cabecera, que nos indica la presencia de más cabeceras, después tenemos el campo de tamaño de la cabecera que en sus 8 bits especifica el tamaño de la cabecera en palabras de 64 bits y ahí no se incluyen los primeros 64 bits, esto permite tener un valor de 0 en este campo así evita que cada Router examine este campo para asegurase que no es 0. Y las opciones son procesadas por el destinatario del datagrama y el formato mismo obliga que sean múltiplos de 64 bits para que se especifiquen en el tamaño de la cabecera.

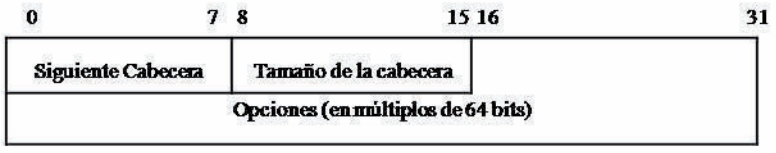

Figura 5- 4 Cabecera de opciones de destino.

5.1.4 La cabecera de opciones entre saltos

En esta cabecera se nos permite especificar las opciones que serán procesadas por los todos Routers intermedios. En el formato es el mismo utilizado para la cabecera de opciones de destino, una diferencia entres estas dos cabeceras es que esta solo puede ser interpretado por el destinatario del datagrama, así cuando un datagrama llega a una cabecera extra, en el datagrama esta especificado el tipo de cabecera y con un código numérico.

5.1.5 La cabecera de autentificación

Es una de las nuevas mejoras y de las más importantes en IPv6. Donde se coloca una cabecera de autentificación la cual no modifica el comportamiento de los otros protocolos del nivel superior como TCP O UDP, en esta su función es la de mantener la seguridad contenida del origen del datagrama. Por consecuente los protocolos superiores no deben aceptar a los paquetes que no hayan sido autentificados. El primer campo indica como en todas las cabeceras siguientes que se encuentra tras esta. Seguido el tamaño de datos que se representan por palabras de 32 bits y otro campo de 16 bits que están reservados que tiene que estar inicializado a 0. El siguiente es el índice de parámetros de seguridad y el campo de numero de secuencia que están representan 32 bits cada uno, por ultimo viene lo que son los datos de autentificación y que este campo puede ser variable.

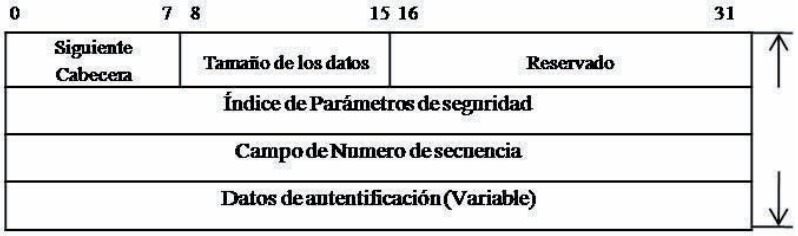

Figura 5- 5 Cabecera de autentificación de la versión 6.

Figura 5- 6 Situación de la cabecera de autentificación.

Ya que un datagrama puede tener más de una cabecera y esto no debería suponer ningún problema para los Routers intermedios que son los encargados de realizar el encaminamiento hasta su destino, así que las cabeceras son procesadas por los Routers conforme están van llegando. A este método se le ha comparado con las capas de una cebolla donde cada cabecera es como capa. Algunas cabeceras cuentas con mayor importancia que otras, como lo es el caso de de la cabecera de autentificación que la que analiza que el datagrama se descartado si este es incorrecto o la cabecera de fragmentación que es el que obliga al unir a los datagramas. Ya que es importante mas no está como un formato bien establecido y solo puede recomendar un orden de estas cabeceras:

1. Cabecera IP versión 6 (IPv6 Header).
2. Cabecera de opciones entre saltos (Hop-by-hop Options Header).
3. Primera cabecera de opciones de destino (Destination Options Header).
4. Cabecera de encaminamiento (Routing Header).
5. Cabecera de fragmentación (Fragment Header).
6. Cabecera de autentificación (Authentication Header).
7. Segunda cabecera de opciones de destino (Destination Options Header).
8. Cabecera de protocolo de nivel superior (TCP, UDP...).

5.2 ICMP y los Mensajes de Error

5.2.1 Tipos de mensajes ICMPV6

5.2.1.1 Mensajes de Error

Estos mensajes son los encargados de la entrega de los datagramas al nodo de destino o se lo entrega a un Router intermedio y el bit más significativo tiene la capacidad de 8 bits, este campo se usa para todos los mensajes de error el cual se fija a 0 y los valores

que este puede tomar son desde 0 hasta 127. Dentro de este rango se incluye el destino inalcanzable, el paquete demasiado grande, tiempo excedido y el problema de parámetro.

Ya que este es un protocolo que se encuentra por encima de nivel superior al de IP se ha colocado en IPv6, pero a este se le han quitado servicios que solían ser redundantes o que en si no eran utilizados, se le ha impuesto un formato fijo para que sea más fácil su tratamiento por los Routers y nuevas características como la extensión de la direcciones a 128 bits. Ya esta nueva característica de ICMP para la versión 6 del IP hace que esta nueva versión de ICMP sea incompatible con la que se usaba para la versión 4.

Encontramos en su primer campo de tipo que es el cual especifica la versión del protocolo ICMP y es aquí donde se coloca 1 si se encuentra compatible con la versión 4 y se encuentra compatible con la versión 6 se coloca a 2.El siguiente campo es el de campo de código que es el que muestra la naturaleza del mensaje que acarrea. Luego encontramos el checksum que es la suma que se lleva del control de los datos que se envían y así de esta forma se puede revisar que sean correctos y ya por último el mensaje contiene la longitud variable y contiene los datos también conocido como Body Message. [20]

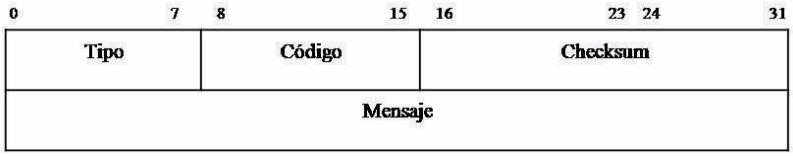

Figura 5- 7 Formato del ICMP versión 2 compatible con la versión 6 de IP

Codigo	Significado
1	Destino inalcanzable (Destination Unrechable)
2	Datagrama demasiado grande (Packet too big)
3	Tiempo de respuesta agotado (Time Exceeded)
4	Parametros incorrectos (Parameter Problem)
128	Solicitud de ECHO (ECHO Request)
129	Respuesta a ECHO (ECHO Reply)
133	Solicitud de router (Router Solicitation)
135	Solicitud de vecino (Neighbor Solicitation)

Tabla 5- 1 Tabla con los códigos más relevantes del ICMP versión 2

Cuando un Router no acepta o descarta algún datagrama es enviado un mensaje de error ICMP al dueño del datagrama avisando la causa del error. Así con códigos como lo

muestra la Tabla 4.1 los códigos 1, 2, 3 y 4 nos indican los motivos por los cuales un Router no acepta y descarta un datagrama. Esto hace actualmente los Routers no envíen mensajes ICMP hacia los datagramas que va dirigidos a más de un usuario simultáneamente (haciendo Multicast) así evitando que sean recibidas demasiadas respuestas. Y por lo tanto no sean respondidos a datagramas de con tipo ICMP y así sean evitados bucles infinitos de las respuestas de error.

El código de mensaje 2, datagrama demasiado grande es método usado para el cálculo del tamaño máximo de datos que se pueden transferir (MTU) que son los que el Router puede soportar. Mediante este código hace saber al emisor cual es tamaño del datagrama máximo que se puede enviar al destino sin peligro de que sea rechazado o descartado por algún Router intermedio y esto hace más eficaz la comunicación entre 2 computadoras en Internet. Esto optimiza la comunicación dinámicamente ya que este depende del camino que tenga el datagrama y los hace de una forma más fácil y rápida.
A continuación explicaremos como funcionan:

5.2.1.2 Destino Inalcanzable

Un Router o Host de destino se encarga de enviar un mensaje ICMP de destino inalcanzable cuando ocurre que el paquete no se puede enviar al nodo de destino o al protocolo que lo requiere.

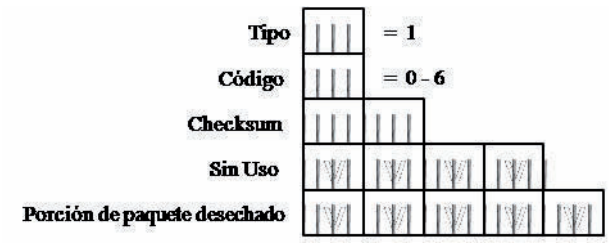

Figura 5- 8 La estructura del mensaje de Destino inalcanzable

El mensaje de destino inalcanzable su primer campo (type) es puesto a 1 y segundo campo (code) tiene una rango de 0 a 6. Después de la suma de comprobación, el campo que no se usa de 32 bits y la porción principal del paquete desechado, clasificados de modo que el paquete entero IPv6 contiene el mensaje ICMPv6 sea no más grande de 1280 octetos (el MTU del mínimo IPv6). El número de bytes del paquete que son descartados es incluido en el mensaje, este varía dependiendo la cabecera de extensión Ipv6 presente. Para un mensaje de error ICMPv6 sin cabecera de extensión, hasta 1232 bytes se incluye el

paquete que es descartado así que 1232 menos 40 byte de IPv6 y 8 bytes de ICMPv6 es el paquete de error de destino inalcanzable.

Tabla 5- 2 Mensajes inalcanzables de Destino ICMPv6

Valor del campo Código	Descripción
0 – ninguna ruta al destino	No se encontró ninguna ruta que emparejaba la destinación en la tabla de encaminamiento.
1 - Comunicación con Destinación administrativo prohibida	La comunicación con la destinación se prohíbe por política administrativa. Esto se envía típicamente cuando el paquete es desechado por un cortafuego.
2 - Más allá del alcance de la dirección de fuente	Un Router envía esto cuando el paquete se debe remitir usando un interfaz que no esté dentro de la zona scoped de la dirección de fuente
3 - Dirección inalcanzable	Esto es enviado típicamente por un Router debido a una inhabilidad de resolver la dirección de la capa de enlace de la destino.
4 - Puerto Inalcanzable	En este puerto el destino es inalcanzable ya que se envía cuando un paquete Ipv6 contiene un mensaje UDP que llego a ese destino pero no tiene ningún uso cuando usaba el puerto UDP.
5 - Ingreso fallido de la dirección fuente / Política de la salida	El paquete con esta dirección de fuente no es permitida ya que no pasa las políticas de salida o ingreso.
6 – Rechazo de la ruta de Destino	El paquete emparejó una ruta que lo rechazo y fue desechado. Un rechazo de la ruta es un prefijo de la dirección configurado en un Router para el tráfico que el Router debe desechar inmediatamente.

5.2.1.3 Paquete demasiado grande

Esto ocurre cuando un Router envía un mensaje demasiado grande del paquete de error ICMPv6 y este no puede ser enviado ya que excede los límites del MTU ya que el mínimo que se puede transmitir es más pequeño que el paquete permitido por IPv6.

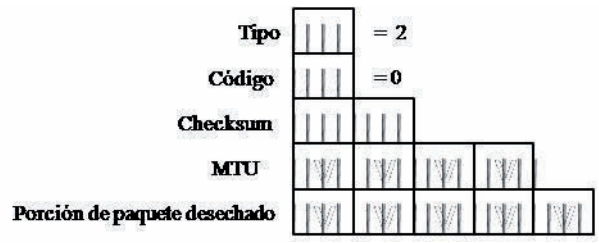

Figura 5- 9 La estructura del mensaje demasiado grande del paquete

En este mensaje su primer campo es fijado a 2 y el segundo campo es puesto a 0, el checksum contiene 32 bits del MTU que almacena el enlace del MTU de la interfaz del paquete enviado. Está después la porción principal del paquete desechado, clasificado de modo que el paquete entero IPv6 que contiene el mensaje ICMPv6 sea no más grande de

1280 bytes. El mensaje demasiado grande del paquete se utiliza para el proceso de descubrimiento del MTU de la trayectoria IPv6.

5.2.1.4 Tiempo Excedido

Aquí el Router envía el mensaje de tiempo excedido cuan el campo tiene el límite del salto en la cabecera IPv6 y esta llega hasta cero y después tiene un decremento en su valor durante el proceso de expedición.

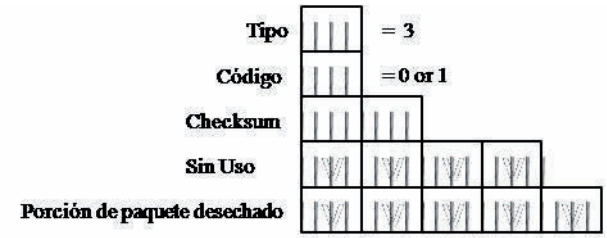

Figura 5- 10 Estructura del mensaje de Tiempo Excedido

En este mensaje el campo de tipo se fija a 3 y el campo del código se puede fijar de la siguiente forma:

A 0 cuando un Router en el campo del salto limite en la cabecera IPv6 se decrementa a 0 o cuando este mismo campo la cabecera IPv6 en el paquete llega hasta 0.

A 1 cuando un Host se pasa el tiempo de fragmentación. Esto en un tiempo de enlace de 60 segundos.

Ya que el checksum contiene 32 bits y es la porción principal desechada, entonces el paquete entero de IPv6 que contiene el mensaje de error no sea más grande de 1280 bytes.

5.2.1.5 Problema del parámetro

Cuando un Router envía un mensaje del problema de parámetro es porque hay un error en la cabecera IPv6 o en la cabecera de extensión y que provoca que evite que IPv6 realice algún proceso adicional.

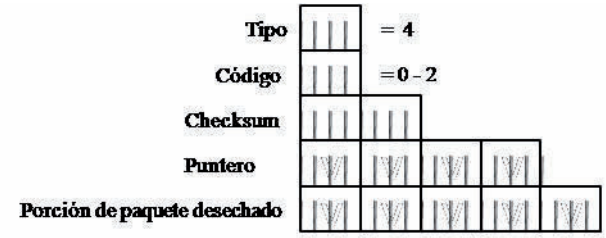

Figura 5- 11 La estructura del mensaje del problema del parámetro

Su primer campo se coloca a 4 y segundo campo debe contener un valor de 0 a 2. Después se muestra el checksum que es un campo de 32 bits del identificador el cual nos indica el Bit compensado comenzando desde 0 para el paquete IPv6 donde el error fue encontrado. Después del indicador el campo es la porción principal del paquete desechado, clasificada de modo que el mensaje entero ICMPv6 no sea más grande de 1280 bytes. El valor del campo del indicador se fija a la compensación correcta incluso cuando la localización del error no está dentro de la porción del paquete desechado.

Tabla 5- 3 Valores para Mensajes de Error

Valor del campo Código	Descripción
0 - Error en cabecera encontrado	Un error en un campo dentro de la cabecera IPv6 o de una cabecera de extensión fue encontrado.
1 - Tipo desconocido en la siguiente cabecera fue encontrado	Un valor desconocido del campo de siguiente cabecera fue encontrado. Esto es equivalente al mensaje inalcanzable del Inalcanzable-Protocolo de la destinación ICMPv4.
2 - Opción desconocida IPv6 encontrada	Una opción desconocida IPv6 fue encontrada.

Mensajes del problema del parámetro ICMPv6

Este tipo de mensajes de Problema de Parámetro desconocido se usa cuando ambos valore son validos:

- Una opción es cuando la cabecera Salto por Salto o una cabecera de destino no se reconocen.
- Dentro del campo de tipo las opciones, los bits de categoría más alta se fijan a 10 o 11 binario.

5.2.2 Mensajes informativos

Estos mensajes conocidos como informativos son los que nos proporcionan las funciones que nos ayudaran al diagnostico y funcionalidad adicional de los Host como lo son MLD Y ND. Al igual que el mensaje de error este campo contiene 8 bits para los mensajes y se coloca a 1. Así que el valor para este campo es de 128 a 255.

Mensajes informativos ICMPv6

Los mensajes informativos ICMPv6 definidos en RFC 4443 [21] proporcionan una capacidad de diagnóstico simple para ayudar en la localización de daños y la cual consiste en los siguientes mensajes:

- Echo Request
- Echo Reply

5.2.2.1 Echo Request

El Echo Request en el protocolo ICMP es un mensaje que se envía a un Host para que éste le responda con un Echo Reply. Todo Host debe responder a un Echo Request con un Echo Reply que contenga exactamente los mismos datos que el primero.

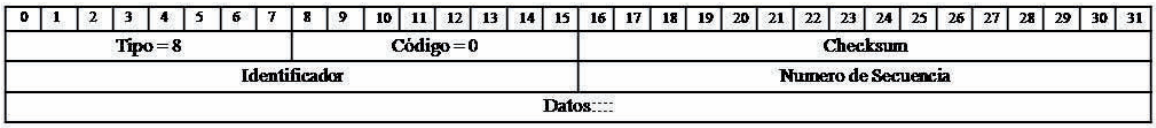

Figura 5- 12 Formato mensaje Echo Request

El tipo debe ser 8, El código debe ser 0. El identificador y el número de secuencia pueden ser usados por el cliente para asociar cada Echo Request a cada Echo Reply. Los datos incluidos en el Echo Request deben estar siempre en los datos del Echo Reply.

5.2.2.2 Echo Reply

Un Echo Reply en el protocolo ICMP es un mensaje generado como contestación a un mensaje Echo Request.

Figura 5- 13 Formato mensaje Echo Reply

El tipo y el código deben ser 0, El identificador y el número de secuencia pueden ser usados por el cliente para asociar cada Echo Request a cada Echo Reply. Los datos incluidos en el Echo Request deben estar siempre en los datos del Echo Reply. [22]

Descubrimiento de la Trayectoria de la Unidad Máxima de Transferencia (MTU).

El envió de paquetes lo más grande posible ayuda a maximizar y utilizar al máximo la capacidad de la red, cuando se llevan a cabo la transferencia de datos a granel. Por lo que en los Routers que soportan IPv6 se le da más apoyo a la fragmentación, donde el Host al realizar el envió debe fragmentar su carga útil o bien descubrir el paquete de transferencia máxima que puede ser enviado a la destinación y enviar los paquetes desfragmentados de su tamaño.

PMTU es Unidad Máxima de transmisión de la Trayectoria es como el MTU pero más pequeño apoyado por la unión en la trayectoria entre la fuente y el destino. El MTU es la carga útil máximo clasificado y este se puede enviar a la capa de enlace. En este se incluye la cabecera de acoplamiento. Por ejemplo es que en Ethernet se encapsula con Ethernet II donde el MTU es de 1500 octetos y con marco máximo de 1526 octetos donde ya se incluye el Ethernet, la fuente y el destino de las direcciones, el tipo de Ethernet y el campo donde se lleva a cabo la secuencia. “apéndice A”.

Los paquetes con tamaño máximo en PMTU no requiere la fragmentación en el Host de envió por que estos son remitidos con éxito por los Routers sobre la misma trayectoria. Donde el nodo de envió confía en los mensaje demasiado grandes del paquete ICMIPv6.

Este trabaja de la siguiente manera:

1. El nodo de envío asume que la destinación PMTU es el MTU del interfaz en el cual se está remitiendo el tráfico.

2. El nodo de envío envía los paquetes IPv6 en el tamaño supuesto de PMTU.

3. Si un Router en la trayectoria no puede remitir el paquete porque el interfaz de la expedición tiene un MTU del acoplamiento que sea más pequeño que el tamaño del

paquete, envía un mensaje demasiado grande del paquete ICMPv6 de nuevo al nodo de envío y desecha el paquete IPv6. El mensaje demasiado grande del paquete ICMPv6 contiene el MTU del acoplamiento del interfaz en el cual la expedición falló.

4. El nodo de envío fija el nuevo PMTU presunto para los paquetes que son enviados a la destinación al valor del campo del MTU en el mensaje demasiado grande del paquete ICMPv6.

5.3 Neighbor Discovery (ND)

Este protocolo de Internet conocido como "ND" Neighbor Discovery o lo que es descubridor del vecino, es un sistema de mensajes y de los procesos que determinan la relación entre nodos vecinos, y este substituye a protocolo usado en IPv4 ARP (Address Resolution Protocol) es una combinación de ARP, ICMP Router Discovery e ICMP redirect, y a su vez se han incorporado nuevas funciones.

Los paquetes del anuncio del Router contienen el prefijo para un acoplamiento (información del subnet). No hay necesidad de configurar más mascaras del subnet.

El descubrimiento vecino proporciona mecanismos para volver a numerar redes fácilmente. Nuevos prefijos y las direcciones pueden ser introducidos y las viejas pueden ser desaprobadas y ser quitadas.

Los anuncios del Router permiten la autoconfiguración de estado de la dirección y pueden notificar a los Host cuándo utilizar la configuración stateful de la dirección.

Los Routers pueden anunciar de un MTU que se utilizará en un enlace.

Los prefijos múltiples se pueden asignar a un enlace. Por abandono, los Hosts aprenden todos los prefijos del Router, pero el Router se puede configurar para no hacer anuncio de alguno o de todos los prefijos.

Los anuncios del Router y el ICMP vuelven a dirigir direcciones enlace local del uso para identificar los Routers. Esto permite que los Host mantengan sus asociaciones del Router incluso en el caso de volverse a enumerar o del uso de nuevos prefijos globales.

Los mensajes del Neighbor Discovery tienen un valor límite del salto de 255 y las peticiones con un límite más bajo del salto no se contestan. Esto hace al Neighbor

Discovery inmune a los Host alejados que intentan hacer de manera oculta en su enlace porque sus paquetes decrementan el límite del salto y se no hacen caso así.

El protocolo vecino del descubrimiento se utiliza para detectar IP Address duplicados en un acoplamiento. Los mecanismos estándar de la autentificación y de seguridad del IP se pueden aplicar al Neighbor Discovery. [23]

El ND para los Nodos es también utilizado para lo siguiente:

- Para que resuelva la dirección de la capa de enlace de un nodo vecino a el cual se le está remitiendo un paquete IPv6.
- Que determine cuando la dirección de la capa de enlace de un nodo vecino ha cambiado.
- Determinar si un vecino se encuentra todavía accesible.

El ND para los Host es también utilizado para lo siguiente:

- Descubrir Routers vecinos.
- Auto configurar las direcciones, tratar los prefijos, las rutas y demás parámetros de la configuración.

El ND para los Routers es también utilizado para lo siguiente:

- Advertir su presencia, recibir los parámetros de la configuración, las rutas y los prefijos de estado en enlace.
- Informar a los Host una mejor dirección del siguiente salto para remitir los paquetes para un destino específico.

En el ND de IPv6 incluye nuevos procesos que pueden ser utilizados que se enlistan a continuación:

Descubrimiento de Router: Comunica al Host y a otros Routers, la existencia de un nuevo Router, permanencia o eliminación de los actuales.

Descubridor de Prefijo: Este es el proceso por el cual los Hosts descubren los prefijos de red para los destinos de enlace local. Comunica al nodo el prefijo de la red, que tiene la dirección IPv6 de su subred.

Descubrimiento del parámetro: da información a los nodos de una red sobre el MTU, también el límite de salto para los paquetes salientes que viene por de default así como el mayor para poder llegar a su destino.

Autoconfiguración de dirección: Durante el proceso de autoconfiguración de dirección, el direccionamiento IP es configurado para la interfaces, presente o ausente el servidor, como lo es el DHCPv6.

Resolución de Dirección: Se encarga de establecer la correspondencia entre la dirección IP y la de su capa de enlace (Dirección MAC de una Ethernet).

Determinación del Siguiente Salto: Durante el proceso del siguiente salto, un nodo determina la dirección IPv6, este lo realiza basado en una dirección de destino. Comunica el nodo más cercano. Este valor puede ser usado para determinar la ruta más corta por la cual se encaminaran los paquetes.

Detección del vecino Inalcanzable: Durante este proceso por el cual un nodo determina que la capa de del vecino que no está recibiendo los paquetes o que la dirección Ipv6 se ha cambiado o movido a una interfaz física.

Dirección duplicada: durante este proceso, un nodo determina que una dirección está o no en uso o funcionando por lo nodos vecinos. Puede ser usado antes de dar de alta un nuevo nodo.

Redireccionamiento: en este proceso de lo que se encarga es de informar a él Host la mejor dirección o la más corta del primer salto para alcanzar un destino y así direccionar el mensaje.

Formato del Mensaje Neighbor Discovery

Básicamente el mensaje de ND utiliza la estructura del mensaje de ICMPv6 y sus tipos desde 133 hasta 137. Estos mensajes tienen una cabecera de mensaje del ND, integrado por una cabecera ICMPv6 y los datos específicos del ND y cero o más opciones.

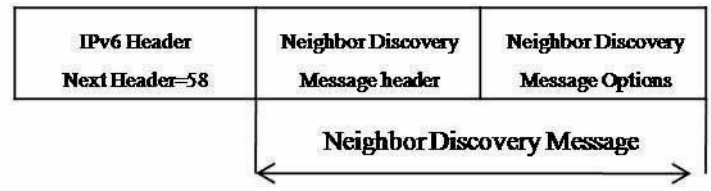

Figura 5- 14 Formato Neighbor Discovery

5.3.1 Formato Mensaje Descubridor de Vecino

Hay 5 diferentes tipos de mensaje:

- Router Solicitation (ICMPv6 type 133)
- Router Advertisement (ICMPv6 type 134)
- Neighbor Solicitation (ICMPv6 type 135)
- Neighbor Advertisement (ICMPv6 type 136)
- Redirect (ICMPv6 type 137)

5.3.1.1 Router Solicitation

Este mensaje es enviado por los Hosts de IPv6 para detectar la presencia de Routers en los enlaces y estos Hosts envían un mensaje Multicast avisando a los Routers que respondan inmediatamente.

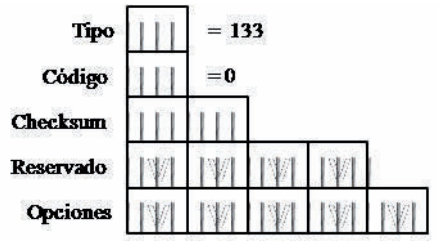

Figura 5- 15 Estructura del Router Solicitation Message

Options:

- Source link-layer Address: cuando está presente contiene la dirección de la capa de enlace del origen del mensaje, para los nodos Ethernet esta opción contiene la dirección MAC del Host de envió.

5.3.1.2 Router Advertisement

En este mensaje los Routers de IPv6 envían mensajes de anuncios no solicitados supuestamente periódicamente, esto es decir en intervalos que son tomados a el azar para reducir la sincronización de ediciones cuando hay múltiples anuncios de Routers en un enlace.

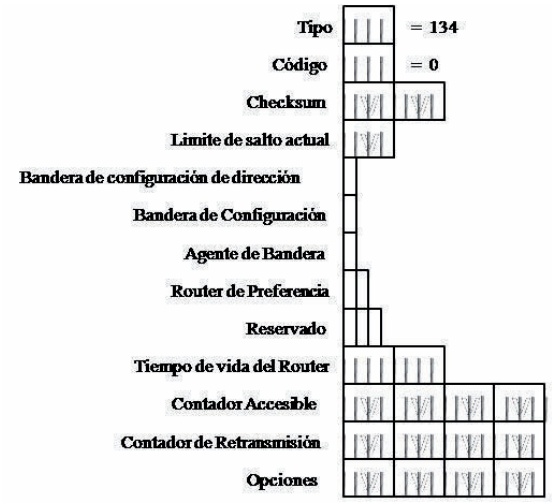

Figura 5- 16 Estructura del Router Advertisement Message

Current Hop Limit: Valor actual que debe tomar el campo de IP que indica el numero de saltos por defecto, especificado en 8 bytes. Un valor de 0, no especifica nada.

Managed adress configuration flag: Flag de 1 bit sirve para obtener direcciones además de direcciones que se pudieron derivar de la autoconfiguración apátrida de la dirección.

Other stateful configuration: Flag de 1 bit, para no obtener la dirección de la información de la configuración.

Home Agent Flag: es usado para la movilidad de IPv6.

Default Router Preference: El campo de la preferencia del Router del defecto indica el nivel de preferencia por este Router como el Router del defecto.

Router Lifetime: Valor de 16 bits. El tiempo de vida del Router por defecto es de 65 535 segundos que serian más o menos 18 hrs. Si el valor es 0 este puede ser considerado como Router de Default.

Reachable Time: Tiempo medido en 32 bits, que indica, en milisegundos, el tiempo desde que un nodo, ha recibido una confirmación de alcance, por parte de sus vecinos. Un valor de 0, no especifica nada.

Retrans Timer: Tiempo en milisegundos, trascurrido entre 2 mensajes de solicitud de vecindad. Un valor de 0, inhabilita este campo.

Options:

- Source link-layer Address: Dirección de la capa de enlace del origen del mensaje.
- MTU: Debe ser enviada en redes con la MTU variable.
- Prefix Information: Los prefijos de las redes que alcanza el Router excepto la local.

5.3.1.3 Neighbor Solicitation

Los nodos IPv6 envían el mensaje vecino de la solicitación para descubrir la dirección de la capa de enlace de un nodo del enlace IPv6 para confirmar una dirección que fue anteriormente determinada, en esta se incluye la dirección de la capa de enlace del remitente.

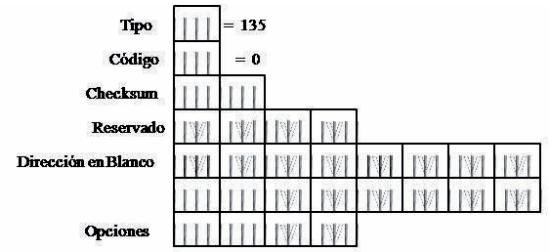

Figura 5- 17 Estructura del Neighbor Solicitation Message

Target Address: Dirección IP hacia la cual se envía la solicitud. Este campo tiene un tamaño de 128 bits.

Options:

- Source link-layer Address: Dirección de la capa de enlace del origen del mensaje. No debe incluirse si es una dirección de arranque.

5.3.1.4 Neighbor Advertisement

Un nodo IPv6 también envía los anuncios vecinos no solicitados para informar a nodos vecinos cambios en direcciones de la capa de enlace o el rol del nodo, El anuncio del vecino contiene la información requerida por los nodos para determinar el tipo de mensaje vecino, el rol del remitente en la red y la dirección de la capa de enlace del remitente.

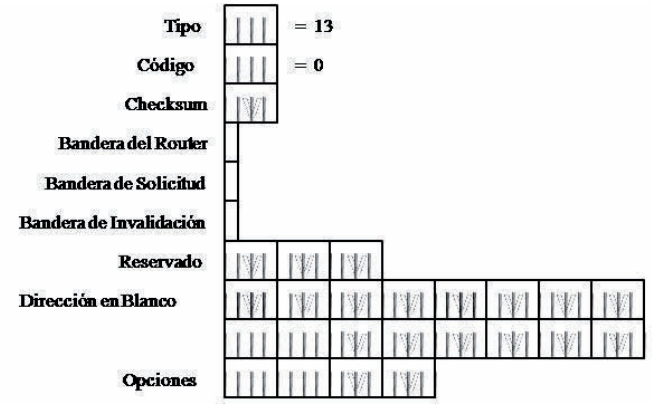

Figura 5- 18 Estructura Neighbor Advertisement Message

Router Flag: Indica que el nodo de envió es un Router. Es usado por el Neighbor Unreachability Detection, para ver si un Router cambia a Host, se coloca a 1 si es un Router y a 0 cuando no lo es.

Solicited Flag: Toma valor 1, si el mensaje es en respuesta a una solicitud de vecindad.

Override Flag: Con valor 1, indica que la cache de destino debe ser actualizada. Si el valor es 0, la cache de destino no debe ser actualizada menos para los nodos implicados.

Reserved: 29 bits sin uso, destinados a futuras implementaciones. Debe ser inicializado a 0. Otro valor,

Target Address: Dirección de destino, que debe ser la del nodo que solicito este mensaje.

Options:

- Target link-layer Address: Dirección de la capa de enlace del destino. Puede ser incluida, respondiendo a una solicitud de Multicast y debe ser incluida si es una respuesta a una solicitud de Anycast.

5.3.1.5 Redirect

Este mensaje es enviado por el Router para informarle al Host, para originar una mejor dirección del primer salto para un destino específico. Estos mensajes solo son enviados por Routers para trafico Unicast, solo son originados por un Host Unicast y solo son procesados por los Hosts.

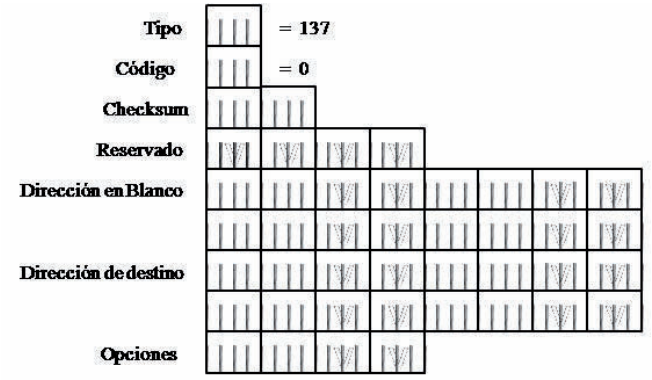

Figura 5- 19 Estructura de Redirect Message

Target Address: Informa al Host de que hay un camino mejor por donde encaminar su tráfico hacia su destino, indicándolo en este campo.

Destination Address: Aquí informa el Router al Host, el destino del tráfico al cual se refiere.

Options:

- Target link-layer Address: Dirección de la capa de enlace del destino. Debe incluirse si es posible. En enlaces del tipo NBMA (nobroadcast multi access), los Host podría requerir la dirección de la capa de enlace del destino.
- Redirected Header: Incluir tanto como sea posible de la cabecera IP del paquete que ha provocado el envió del mensaje.

5.3.2 Opciones del ND.

Estas opciones del mensaje de ND proporcionan la información adicional e indicaciones de las direcciones MAC, los prefijos de la red de acoplamiento, también la información del MTU, los datos de cambio de dirección así como la información de la movilidad y las rutas específicas.

Para asegurarse de que los mensajes del ND sean recibidos, se hayan originado en un nodo en el enlace local (enlace físico o un túnel) todos los mensajes del ND se envían con un límite de salto de 255. Cuando es recibido el mensaje el campo del límite del salto en la cabecera IPv6 se comprueba. Si no es fijado a 255 y este se desecha.

Verifica que el mensaje tenga un límite de salto de 255 y proporciona la protección contra los ataques ND que son basado en la red que ponen en marcha nodos de apagado,

con un límite de salto de 255, un Router no podría remitir el mensaje del ND de un nodo apagado.

Las opciones del ND se dan formato en formato del tipo-longitud-valor (TLV).

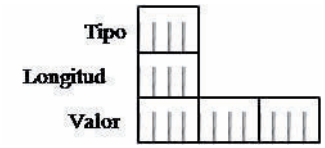

Figura 5- 20 Formato TLV para Opciones ND

El tipo de 8 bits campo indica el tipo de opción del ND. Los tipos de la opción del ND definidos en RFC 4861, RFC 3775, y RFC 4191.

5.3.2.1 Tipo de Opciones ND

El campo de longitud tiene un valor de 8 bits y nos indica lo largo de la opción entera en los 8 bloques del octeto. Esta es para todas las opciones del ND que tener su límite en 8 bits del octeto. El campo de valor variable contiene los datos necesarios para se lleve a cabo la opción.

5.3.2.2 Source and Target Link-Layer Address Options

Esta opción indica la dirección de la capa de enlace del remitente del mensaje y esta opción la contienen los mensajes Neighbor Solicitation, Router Solicitation y Neighbor Adversitisement, esta no está incluida en los mensajes cuando no se especifica la dirección (::).

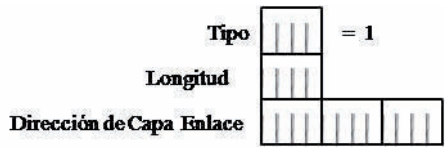

Figura 5- 21 Estructura del la opción Source link-layer Address

Esta indica la dirección de la capa de enlace del nodo a la cual deben ser dirigidos los paquetes.

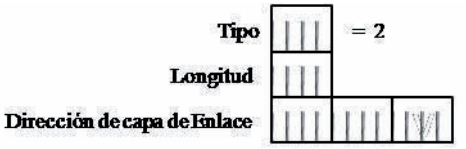

Figura 5- 22 La estructura de la opción Target Link-Layer Address

Los 2 tipos de opciones tienen el mismo formato y sus especificaciones son:

Type: 1 Para el Source Link-Layer Address, 2 Para el Target Link-Layer Address
Length: el campo Type y Length medida en valores de 8 bytes.

5.3.2.3 MTU

La opción del MTU se envía en mensajes de la advertencia del Router para indicar el MTU IPv6 del enlace. Esta opción se utiliza típicamente cuando el MTU IPv6 para un enlace que no es bien conocido, ni necesita ser fijado debido a una de translación o los que hacen puente sobre la configuración. La opción del MTU elimina el MTU IPv6 divulgado por el hardware del interfaz.

La opción del MTU se utiliza para indicar el MTU más alto IPv6 apoyado por todas las tecnologías de la capa de enlace.

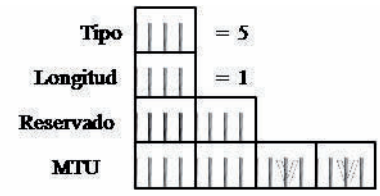

Figura 5- 23 MTU

Type: 5
Length: 1
Reserved: Campo reservado para futuros usos. Debe ser inicializado a 0.
MTU: 32 Bits indica el MTU recomendado. El valor debe ser aplicado a todos los segmentos.

Capítulo 6 Movilidad, Seguridad.

6.0 Movilidad

La movilidad nos permite que los nodos en IPv6 puedan ser dinámicos y para cambiar arbitrariamente su localización en una red IPv6 y todavía mantener sus conexiones existentes. Cuando un nodo IPv6 cambia su localización, puede ser que también cambie su enlace. Cuando un nodo cambia su enlace, su dirección puede que cambie para mantener su conectividad, hay varias consideraciones cuando hay cambios en las direcciones que se mueven a un enlace diferente y se coloca la autoconfiguración *stateful* y *stateless* de direcciones. Pero cuando la dirección cambia, sus conexiones existentes del nodo móvil que está utilizando la dirección que se le asigno anteriormente del enlace no se puede mantener y termina.

Una de las ventajas de la movilidad que nos ofrece IPv6, es que cuando un nodo cambie su localización de direcciones, sus conexiones existentes por las cuales este se está comunicando no se vienen abajo y se retienen activas. Para que sea posible esto, las conexiones a los nodos tienen la dirección específica que se asigna siempre al nodo móvil y con la cual siempre se encuentra accesible por el nodo móvil.

Los nodos móviles tienen componentes que ayudan a su operación:

Para llevar a cabo la movilidad en IPv6 debe existir un nodo móvil y este debe contar con una dirección de casa (home address) y esta será la dirección en su red de origen, esta dirección se mantiene en ese nodo aunque cambiemos de red y sus paquetes son encaminados de forma normal como si no hubiese existido movilidad.

Cuando el nodo cambie a una red que no sea la de origen, se le asigna una nueva dirección de invitado (care of address) y este podrá ser contactado por esta nueva dirección, después se conecta un Router a sus dirección de origen y le es comunicado cual es su dirección actual de invitado, así cuando un paquete sea enviado a la dirección de casa u origen (home address), el Router sabrá que tiene que interceptarlo y reenviarlo con destino de la dirección de invitado del nodo móvil.

Lo que hace el nodo móvil al moverse es mandar un mensaje de actualización para así mantener actualizada la dirección de invitado, así asocia la dirección de invitado con la dirección de casa durante un periodo de tiempo. A los nodos que se comuniquen con el nodo móvil ya sea fijo o móvil se le conoce como nodo correspondiente.

Cuando un nodo móvil se comunica con un nodo correspondiente, el nodo móvil envía los paquetes utilizando la dirección de invitado que ha obtenido en la red en la que encuentra actualmente. Pero el nodo correspondiente envía los paquetes a la dirección de origen del nodo móvil que serán interceptados y serán reenviados a la dirección de invitado del nodo móvil.

Esto hace que sea trace una ruta triangular, que no afecta a nada pero es ineficiente. Por esto la movilidad de IPv6 tiene una ruta de optimización y por medio de este mecanismo permite al nodo móvil avisarle al nodo correspondiente de que puede enviar los paquetes directamente a su dirección de invitado para ello utilizando los mensajes de actualización (Binding Update).[24]

6.1 Mobility Header

Para que las funciones anteriores que fueron añadidas a esta movilidad funcionen se hace uso de la extensión de la cabecera de movilidad. Ya que este permite enviar información de señalización en el mismo paquete de datos. Las opciones son:

6.1.1 Home Address Option: Indica cual es la dirección de origen del nodo móvil cuando éste se encuentra fuera de su red origen.

6.1.2 Binding Update Option: Que sirve para crear, actualizar y eliminar entrada de las asociaciones que se mantienen entre el nodo móvil y la dirección de invitado. Un paquete con esta opción hará que se produzca una asociación en el nodo correspondiente o en el Home Agent entre la dirección origen del paquete y la dirección contenida en el campo de Home Address Option.

6.1.3 Binding Acknowledgement (BA) Option: Es enviada por el Home Agent y por el Nodo correspondiente como respuesta a la actualización de direcciones enviadas por el nodo móvil.[25]

6.1.4 Binding Request (BR) Option: Enviada por el nodo correspondiente para solicitar al nodo móvil refrescar su entrada en la lista de asociaciones actual del nodo móvil.

6.2 Seguridad Sobre IPv6

Los paquetes IP en una red tan grande como lo es Internet no cuentan con seguridad por sí mismos y serian un blanco muy fácil para poder ver sus contenidos, modificarlos y reenviarlos por la red, así que al recibir un paquete no hay garantía de que el que envía el paquete sea quien dice ser, que sus datos sean los originalmente enviados y no hayan sido modificados.

Para eso en IPv6 ha colocado un protocolo ahí basando la seguridad de IPv6 (IPSec), por el cual 2 encabezados de extensión que pueden ser utilizadas juntas o de manera separada para brindar servicios de seguridad en la capa de red.

- Confidencialidad de Datos: el nodo de donde es enviado el paquete puede cifrar los paquetes antes de transmitirlos atreves de la red.
- Integridad de Datos: el nodo que recibe puede llevar a cabo una prueba de autentificación para los paquetes enviados por el nodo emisor para asegurar que los datos no han sido alterados durante la transmisión en la red.
- Autentificar Datos de Origen: el nodo que recibe puede autentificar de donde proviene los paquetes enviados para asegurar que estos paquetes fueron enviados por quien dice ser el nodo emisor.
- Anti-reenvió: aquí se detecta los paquetes que han sido reenviados y así detectarlos y rechazarlos.
- Cifrado: Un mecanismo para transformar los datos desde una forma inteligente (plaintext) a una forma no inteligente (ciphertext), así proveyendo confidencialidad.
- Índice de Parámetros de Seguridad (SPI): Un valor de 32 bits que es usado para distinguir entre diferentes Asociaciones de Seguridad (SAs) terminando en el mismo destino y usando el mismo protocolo IPSec.

- Asociación de Seguridad (SA): Es una conexión lógica simple que va en una sola dirección, que es usada para brindar seguridad. Esta es usada por AH y ESP así que les provee servicios de seguridad, atendiendo uno por uno no a ambos. La SA puede incluir: el algoritmo de autentificación, el modo del algoritmo y claves; el algoritmo de cifrado, el modo del algoritmo y claves; tiempo de vida de la clave, o tiempo en que la clave debe ser cambiada. Dos tipos de SA son definidos: modo de transporte y modo túnel.
- Gateway de Seguridad: Un sistema que actúa como un sistema intermediario entre 2 redes. Los Hosts o redes en el lado externo del Gateway de seguridad son vistos como sistemas no confiables, mientras que los Hosts o redes en el lado interno son vistos como sistemas confiables.
- Análisis de Tráfico: El análisis del flujo de tráfico en la red para el propósito de deducir información que es útil para un adversario.
- Asociación de Seguridad en Modo de Transporte: Una SA entre 2 Hosts, primariamente proveyendo seguridad para los protocolos de capa más alta.
- Asociación de Seguridad en Modo de Túnel: Una SA aplicada a un túnel de IP, primariamente proveyendo seguridad para un paquete en el túnel.

6.2.1 Asociaciones de Seguridad

La Asociación de Seguridad (SA) es una conexión lógica simple de una sola vía, que da servicios de seguridad al tráfico que está siendo enviado o cargado en esa conexión. Y proporciona servicios de seguridad a AH y ESP pero solo puede ser a uno si es necesario dar servicio a ambos, se requieren dos SA.

Hay dos tipos de SA los cuales son los siguientes:

Modo transporte: Donde hay 2 Host y su encabezado de protocolo de seguridad (AH o ESP) va después del encabezado IP y los demás encabezados de extensión opcionales, pero puede aparecer antes o después del encabezado de destino y antes de cualquier protocolo UDP o TCP. Y cuando es usada para AH en este modo, esta proporciona seguridad a partes del encabezado IP y protocolos de la capa más alta y cuando es usado para ESP le proporciona seguridad solo a los protocolos de la capa más alta.

En modo de túnel: Donde la seguridad es aplicada a el túnel, donde un extremo del túnel es un Gateway de seguridad, por otro lado sus dos extremos del túnel son Hosts se puede

usar el modo de túnel o transporte. Para el modo túnel hay 2 tipos de encabezado IP: un encabezado externo que especifica el destino para el proceso de IPsec y un encabezado interno que especifica el destino del paquete. Para AH la seguridad es proporcionada del encabezado externo IP más el paquete del túnel interno. Y para el ESP la seguridad es proporcionada solo para el paquete del túnel interno.

6.2.2 La cabecera de autentificación (AH)

La cabecera de Autentificación (AH) proporciona integridad sin conexión, así como autentifica el origen de los datos y un servicio anti reenvió. Esta cabecera puede ser implementada en dos formas: modo transporte que se da en entre los Host y modo túnel que puede ser entre Hosts y Gateway de seguridad. AH es un protocolo apropiado para implementar cuando la confidencialidad no es requerida, o no es permitida.

Tanto en ESP como AH puede proporcionar autentificación, solo que hay una diferencia entre los servicio de autentificación proporcionados y que es grado de cobertura que ofrecen. Ya que ESP no da protección a ningún campo de encabezado IPv6 a menos que esos campos sean encapsulados por ESP. Al contrario AH puede cubrir más rango de cobertura.

En modo de transporte, AH está considerado una carga útil de extremo a extremo, así que debe ser colocado después de los encabezado hop-by-hop, routing y fragmentation. El encabezado Destination Options puede ser colocado antes o después de AH, como lo requiera la implementación específica.

El modo de túnel contiene tanto un paquete interno IPv6 (para el destino) como un paquete externo IPv6, que puede ser enviado a un Gateway de seguridad intermedio. En modo de túnel, AH protege el paquete interno IP completo, incluyendo el encabezado del paquete interno IPv6.

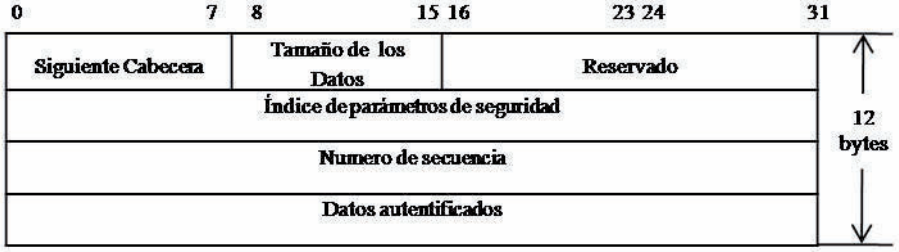

Figura 6- 1 Cabecera de Autentificación

El **tamaño de los datos** (Payload Length) especifica la longitud de los datos en palabras de 32 bits (4 bytes).

El **índice de parámetros de seguridad** (SPI) es un número de 32 bits, lo que nos permite tener hasta 2^32 conexiones de IPSec activas en un mismo ordenador.

El **número de secuencia** (Sequence Number) identifica en número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas.

Los **datos autenticados** (Authentication Data) se obtienen realizando operaciones entre algunos campos de la cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados.

6.2.3 La cabecera de cifrado de seguridad (ESP)

Encapsulated Security Payload (ESP) proporciona confidencialidad (cifrado o encriptado) autentificación del origen de los datos, servicio de antireplay y la confidencialidad de flujo de tráfico. También puede ser usado para el control de acceso, basado en los flujos de tráfico y la distribución de claves que actualmente están en uso.

En modo transporte ESP es muy útil de extremo a extremo, por lo cual va después del encabezado de hop-by-hop, routing y fragmentation. El encabezado de opción de destino puede colocarse antes o después de ESP, pero a su vez como solo protege los encabezados que van colocados después del él, lo mejor es colocar el encabezado de opción de destino.

En modo túnel tiene un paquete interno IPv6 para el destino y un paquete externo IPv6, que puede ser enviado a un Gateway de seguridad intermedio. ESP protege el paquete interno IP completo incluyendo en el encabezado del paquete interno IPv6.

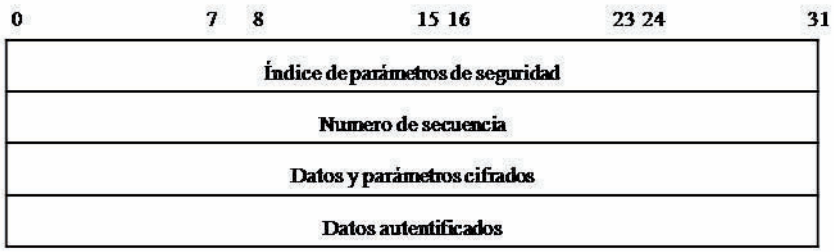

Figura 6- 2 Cabeceras de Cifrado.

A lo contario de la cabecera de Autentificación, en ESP no es necesario especificar el tamaño de los datos cifrados, porque desde el principio hasta el final de la cabecera de cifrado todo se encuentra cifrado todo el datagrama.

El **índice de parámetros de seguridad** (SPI) es un número de 32 bits, lo que nos permite tener hasta 2^32 conexiones de IPSec activas en un mismo ordenador.

El **número de secuencia** (Sequence Number) identifica el número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas.

Los **datos autentificados** (Authentication Data) se asegura de que el texto cifrado no ha sido modificado, para es utiliza un algoritmo llamado Hash (esto depende del algoritmo que sea a elegido).

Ya que en la cabecera de Autentificación como en la de cifrado de seguridad, se pueden utilizar independientemente, es muy recomendable en casos necesarios que se necesite la autentificación así como la seguridad de los datos sean incluidos en la cabecera de cifrado tras la de autentificación. Así se autentifican los datos cifrados.

Capítulo 7 TRANSICION A IPv6 Y CONFIGURACÓN

7.0 Transición a IPv6

Para llevar a cabo la transición de IPv4 a IPv6, esto toma su tiempo el migrar totalmente de un versión a otra, se crearon métodos para ayudar a la convivencia de protocolos en el transcurso de la migración a su nueva versión, estos métodos desarrollados para la convivencia y comunicación entre nodos, permitiendo sea cual sea su versión. Estos métodos desarrollados, cuenta con sus ventajas y desventajas pero permitiendo un principio de convivencia durante la migración.

Desde el principio de su creación se vio que no se podría la migración inmediata de de IPv4 a IPv6, ya que la mayoría de Router y Hosts vendidos son manufacturados por diferentes compañías, por lo cual es necesario crear métodos para la coexistencia de IPv4 y IPv6 hasta que sea totalmente preferido el protocolo IPv6.

Se deben tomar en cuenta los siguientes términos que son relacionados con los nodos y serán usados en la arquitectura para llevar a cabo la transición como se define en el RFC1933. [26]

Nodo IPv4-only: Un Host ó Router que implemente solamente IPv4.
Nodo IPv6/IPv4: Es un Host ó Router que implemente tanto IPv4 como IPv6.
Nodo IPv6-only: Es un Host ó Router que implemente solamente IPv6.
Nodo IPv6: Cualquier Host o Router que implemente IPv6. IPv6/IPv4 y IPv6-only.
Nodo IPv4: Cualquier Host o Router que implemente IPv4. IPv6/IPv4 y IPv4-only
Direcciones IPv6 Nativo: Un Host ó Router que implemente IPv6 sin necesidad de usar métodos de túneles. Esta direcciones no llevan el prefijo 0:0:0:0:0:0.

Técnicas de transición y coexistencia

Al diseñar la esta versión (IPv6) se pensó en la forma de lograr la transición y coexistencia de direcciones, por cual se han ido creando técnicas y métodos para poder llevar a cabo la transición.

Para esto se han agrupado algunos métodos por categorías, las cuales hay 3 actualmente:

1) Doble-pila, para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y las mismas redes.
2) Técnicas de túneles, encapsulando los paquetes IPv6 dentro de paquetes IPv4. Es la más común.
3) Técnicas de traducción, para permitir la comunicación entre dispositivos que son sólo IPv6 soporta y aquellos que son sólo IPv4. Debe ser la última opción ya que tiene problemas.

Estos métodos pueden ser usados en combinación para llevar a cabo una buena coexistencia y transición entre protocolos.

7.1 Doble pila

En este método el modelo de nodos que se encuentran en la red, todos los nodos poseen doble pila, así de esa forma se puede comunicar con los nodos IPv4, ya que para poder comunicar utiliza las aplicaciones en la pila IPv4 y para el IPv6 utiliza la pila de IPv6.

Un inconveniente de este método es que todos los nodos en la red tienen que tener doble pila, esto hace que en una red de gran tamaño puede llegar a ser un problema al hacer la migración.

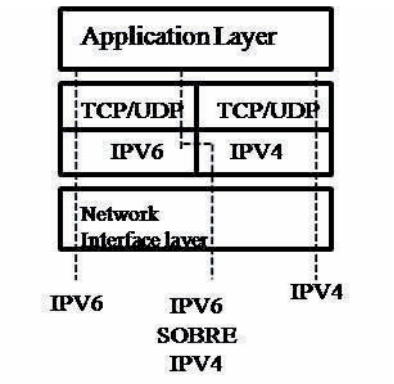

Figura 6- 3 Paquetes de doble Pila

Se muestra cómo funciona la doble pila, que soporta el IPv6, el IPv4 o ambos. El protocolo IPv6 para el servidor 2003 de Windows y para XP, no contiene una capa dual de IP pero funciona de la misma manera que una capa dual IP normal, así proporciona la transición a IPv6.

7.2 Túneles

El método de crear túneles para la transición de IPv6 a IPv4, es la encapsulación de los paquetes IPv6 en una cabecera IPv4, para poder ser enviados los paquetes IPv6 sobre una infraestructura de solo IPv4. Dentro de la cabecera IPv4. Este método es muy conocido actualmente ya que es usado para crear redes privadas virtuales.

Túneles Estáticos

Es una de las mejores soluciones o métodos para poder tener acceso a IPv6 como IPv4 ya que es sencilla. Esto se da cuando en un Host que todavía maneja IPv4 y quiere tener acceso a una red de IPv6, deberá crear un túnel con un Router que tengo acceso a IPv6 y a IPv4. Por ahora se han creado un servidor de túneles que permite conectarte a cualquier usuario que le sea necesario, estas son interfaces web.

Algunos de los métodos usan los túneles automáticos, ya que estos no requieren la configuración manual, porque los puntos finales del túnel son determinados para el uso de rutas, interfaces del túnel y las direcciones del siguiente salto, para las direcciones del destino en IPv6.

Algunos de los métodos son:

7. 3 6to4

Por medio de este método se puede comunicar redes IPv6 por medio de la red IPv4, y se usa para asignar direcciones Router a Router y Router a Host. Se crea un túnel en el extremo de IPv6 de la red sobre IPv4 para poder alcanzar la otra red IPv6.

Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IPv4. De esta forma, los sitios pueden empezar a utilizar IPv6 sin solicitar nuevo espacio de direccionamiento.

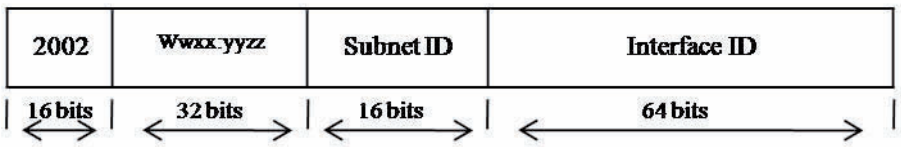

Figura 6- 4 2002::/16 : es el espacio reservado para el túnel 6to4.

WWXX:*YYZZ:* es la representación hexadecimal de las direcciones públicas de IPv4 asignadas a un sitio o un Host y que son totalmente accesibles en internet IPv4.

Subnet ID: se utiliza dentro del sitio de una organización para enumerar subnets individuales.

Interface ID: identifica un nodo en un subnet dentro de una organización.

6to4 Host : es un Host nativo de IPv6 que se configura con los menos una dirección de 6to4 (que es una dirección global con prefijo 2002:: /16). Los Hosts 6to4 nos necesitan soporte adicional o configuración manual y pueden crearse direcciones 6to4 usando los mecanismos estándar de autoconfiguración, los Hosts 6to4 no tienen interface de túnel, porque no realizan el túneles.

6to4 Router: un Router IPv6/IPv4 que utiliza una interfaz al hacer un túnel 6to4 para enviar el trafico de direcciones entre Host 6to4 dentro de un sitio o de otros Routers 6to4, para procesar la información atreves de Internet IPv4. Los Routers 6to4 pueden o no requerir configuración manual.

6to4 Host/Router: un Host que soporta IPv6/IPv4 y que utiliza una interfaz de túnel 6to4 para intercambiar direcciones con otros Host y Routers, Routers 6to4 y así pasar la información atreves de Internet sobre IPv4. Pero no es igual un Router 6to4 y un 6to4 Host/Router por que no reenvía el trafico de direcciones a otros Host. Un ejemplo es una computadora que está funcionando con Windows vista, está conectada directamente a Internet y se le ha asignado una dirección pública IPv4.

6to4 Relay: Un Router 6to4 que es configurado para apoyar el encaminamiento del tránsito de direcciones entre 6to4 y las direcciones nativas de IPv6.

7.4 Taredo

Consiste en la asignación de dirección en una tecnología automática para realizar un túnel, que proporciona conectividad del Unicast atreves del Internet IPv4.

Es un método transversal mediante el NAT para llevar a cabo el trafico IPv6, este tráfico se realiza mediante un túnel, así usando Taredo este puede cruzar uno o múltiples NAT's permitiendo la comunicación y acceso a otros clientes cuando estén usando Taredo sobre Internet IPv4 y los Host sobre Internet IPv6 (este tiene que ser ayudado por un Relay Taredo). La capacidad que tiene para conectar con otros clientes del Taredo que están

conectados sobre el Internet IPv4 permitiendo la comunicación entre aplicaciones, de otra manera tendría problemas al comunicarse sobre un NAT.

La infraestructura del Teredo consiste en los componentes siguientes:

- Teredo clients
- Teredo servers
- Teredo relays
- Teredo Host-specific relays

Taredo Client

El cliente Taredo es un nodo IPv6/IPv4 que apoya a la interfaz para realizar el túnel, por el cual atreves de él, los paquetes se harán un túnel a otros clientes o a nodos en el Internet IPv6.

Un cliente del Taredo se comunica con un servidor del Taredo para obtener un prefijo de la dirección basada en IPv6 para ayudar a la comunicación con otros Taredos o Host en el Internet IPv6.

Teredo Server

Este es un nodo IPv6/IPv4 que está conectado a él Internet sobre IPv4 y Internet IPv6, dándole soporte a hacer túnel a la interfaz del Taredo cuando este está recibiendo paquetes. Su función principal del servidor del Taredo es la ayudar a la configuración de la dirección de los clientes del Taredo y así facilitar la comunicación entre ellos y otros Hosts. El servidor del Teredo escucha en el puerto 3544 del UDP tráfico del Teredo.

Teredo Relay

Es un Router IPv6/IPv4 que puede reenviar los paquetes entre los clientes sobre Internet IPv4 mediantes la interfaz usando túnel Taredo. En algunos casos interactúa con el server Taredo para ayudarle a facilitar la comunicación inicial entre los clientes del Taredo y los Host de IPv6.

Teredo Host-Specific Relay

La comunicación entre los clientes del Taredo y los Host IPv6 que se configuran con una dirección global, debe pasar atreves de un relay del Taredo. Esto se requiere para los Host IPv6 que están conectados a la Internet sobre IPv6. Pero cuando el Host IPv6 e IPv4 se encuentra conectado sobre Internet IPv4 e IPv6 la comunicación debe ocurrir entre el cliente del Taredo y el Host IPv6 de Internet sobre IPv4. Por lo cual debe pasar por un relay del Taredo.

Teredo Host-specific relay es un nodo IPv6/IPv4 que tiene una interfaz y una conectividad a la Internet IPv4 y a la Internet IPv6 y se puede conectar directamente con el Cliente Taredo sobre Internet Ipv4, sin la necesidad de hacer un relay intermedio. La conectividad al Internet IPv4 puede llevarse acabo con una dirección pública o privada IPv4 y con una NAT vecina.

Figura 6- 5 Formato del Paquete de Taredo

IPv4 Header : contiene la fuente y el destino de la direccion conrrespondoente para el tunel automatico y los puntos finales que puedes ser transladados por el NAT.

UDP Header: contiene la fuente y el destino de los puertos UDP para el tráfico del Taredo y el traslado por una NAT.

IPv6 Header: contiene fuente y las direcciones del destino IPv6, por lo menos una es una dirección del Teredo.

The IPv6 payload: es la que contiene los paquetes encapsulados.

7.5 ISATAP

Es una dirección asignada de Host a Host, Host a Router, Router a Host usando la tecnología automática de túnel, que proporciona la conectividad del Unicast IPv6 entre los Host IPv6/IPv4 atreves de una Intranet IPv4. Los Host de ISATAP usan el mecanismo estándar de autoconfiguración de dirección IPv6.

Las direcciones de ISATAP tienen uno de los dos formatos siguientes:

*64-bitUnicastPrefix:0:5EFE:*w.x.y.z
*64-bitUnicastPrefix:200:5EFE:*w.x.y.z

La dirección de ISATAP consiste en el siguiente:

- 64-bitUnicastPrefix: es cualquier prefijo 64bits de la dirección del Unicast, incluyendo prefijos locales, enlaces locales, globales, y únicos.

- :: 0: 5EFE: w.x.y.z y:: 200: 5EFE: w.x.y.z son los identificadores localmente administrados del interfaz. Para:: 0: 5EFE: w.x.y.z, w.x.y.z es una dirección privada del Unicast IPv4. Para:: 200: 5EFE: w.x.y.z, w.x.y.z es una dirección pública del Unicast IPv4. El identificador de la interface (ID) contiene un porción de la dirección ISATAP encajada en IPv4 que determina la dirección de destino IPv4 en la cabecera del encapsulado IPv4 del trafico de ISATAP.

ISATAP permite que coloque en fase el IPv6 nativo, direcciona y encamina la capacidad en su intranet:

Fase 1: la intranet de Solo IPv4, la intranet puede ser una subnet lógica de ISATAP.

Fase 2: la intranet tiene una porción de solo IPv4 (el subnet lógico de ISATAP) y una porción de IPv6. La porción de IPv6 de su intranet se ha puesto al día para apoyar IPv6 nativo que direcciona y que encaminaba.

Fase 3: En esta fase, su intranet entera apoya IPv4 e IPv6 nativo que direcciona y que encamina el ISATAP.

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

- Reenvía los paquetes entre Host de ISATAP en la Subnets de ISATAP y los Host IPv6.
- Muestra los prefijos de la dirección a los Host de ISATAP en la subnet de ISATAP.Los Host ISATAP utilizan los prefijos de divulgación de la dirección para configurar las direcciones globales o únicas locales en ISATAP.

- Actúa como un Router por defecto para los Host ISATAP. Cuando un Host recibe un anuncio del Router que está haciendo publicidad de si mismo del Router como Router por defecto, el Host de ISATAP agrega por default la ruta (::/0) usando la interfaz del túnel con la dirección del siguiente salto. Cuando anfitriones de ISATAP envíe los paquetes destinados a las localizaciones más allá de su subnet de ISATAP, los paquetes se hacen un túnel a la dirección IPv4 del Router de ISATAP. El Router de ISATAP entonces remite el paquete IPv6 al siguiente salto apropiado en la porción de IPv6 del intranet.

7.6 Configuración de IPv6

Aquí se explica de una forma sencilla como instalar y configurar el protocolo de Internet Versión 6, este protocolo se puede instalar y configurar su funcionamiento desde el sistema operativo Windows XP, Windows Server 2003,2008 y Windows Vista.

Veremos algunos comandos que pueden ser usados para configurar de manera automática o manual las funciones del protocolo.

Las plataformas de Microsoft cuentan con un buen soporte para el protocolo IPv6. A partir de algunas versiones de Windows XP viene preinstalado y su configuración es muy sencilla.

Para instalar IPv6

1. Abrir Conexiones de red.
2. Hacer clic con el botón derecho del ratón en alguna conexión de área local y después hacer clic en **Propiedades**.
3. Hacer clic en **Instalar**.
4. En el cuadro de diálogo **Seleccionar tipo de componente de red**, haga clic en **Protocolo** y a continuación en **Agregar**.
5. En el cuadro de diálogo **Seleccionar el protocolo de red**, haga clic en **Microsoft TCP/IP versión 6** y a continuación hacer clic en **Aceptar**.
6. Haga clic en **Cerrar** para guardar los cambios en la conexión de red.

Para quitar IPv6

1. Abrir Conexiones de red.
2. Hacer clic con el botón secundario del ratón en cualquier conexión de área local y a después haga clic en **Propiedades**.
3. Hacer clic en **Microsoft TCP/IP versión 6** en la lista de componentes instalados y después clic en **Desinstalar**.
4. En el cuadro de diálogo **Desinstalar Microsoft TCP/IP versión 6** se da clic en **Sí**.
5. Haga clic en **Cerrar** para guardar los cambios en la conexión de red.

Para poder instalar o desinstalar el protocolo es necesario hacer clic en ***Inicio***, elegimos ***panel de Control*** y con un doble clic en ***Conexiones de Red.***

7.6.1 Instalando IPv6 en Windows XP

Como habilitar IPv6 desde una consola. Para ello es necesario ejecutar con privilegios de administrador, el siguiente comando (Menú de Inicio – Ejecutar – CMD – Enter).

C:\>ipv6 install

Aparecerá un mensaje indicando que se ha configurado correctamente.

Para comprobar que ha sido correctamente instalado usaremos:

C:\>ipv6 if

```
Interfaz 6: Pseudo-interfaz de protocolo de túnel Teredo
  GUID {8180B71D-89B3-4274-BC8B-92E4AC9600FD}
  zonas: link 6 site 3
  cable desconectado
  usa descubrimiento de vecinos
  usa descubrimiento de enrutador
  preferencia de enrutamiento 2
  dirección de capa de enlace: 0.0.0.0:0
    preferred link-local fe80::ffff:ffff:fffd, duración infinite
    multidifusión interface-local ff01::1, 1 referencias , no reportable
    multidifusión link-local ff02::1, 1 referencias , no reportable
  enlace MTU 1280 (enlace MTU 1280)
  límite de saltos actual128
  tiempo alcanzable 21500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 0
  longitud de prefijo de sitio predeterminada 48

Interfaz 5: Ethernet: Conexiones de red inalámbricas
```

```
  GUID {B27C6009-F343-46CF-92C6-ED3E7DAA6E2F}
  usa descubrimiento de vecinos
  usa descubrimiento de enrutador
  dirección de capa de enlace: 00-0e-35-b4-9b-16
    preferred link-local fe80::20e:35ff:feb4:9b16, duración infinite
    multidifusión interface-local ff01::1, 1 referencias , no reportable
    multidifusión link-local ff02::1, 1 referencias , no reportable
    multidifusión link-local ff02::1:ffb4:9b16, 1 referencias , último informado
r
  enlace MTU 1500 (enlace MTU 1500)
  límite de saltos actual128
  tiempo alcanzable 16000ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 1
  longitud de prefijo de sitio predeterminada 48

Interfaz 4: Ethernet: Conexión de área local
  GUID {38F35A5A-C388-465D-872F-BF2B1F6630F7}
  zonas: link 4 site 2
  cable desconectado
  usa descubrimiento de vecinos
  usa descubrimiento de enrutador
  dirección de capa de enlace: 00-c0-9f-70-80-3c
    tentative link-local fe80::2c0:9fff:fe70:803c, duración infinite
    multidifusión interface-local ff01::1, 1 referencias , no reportable
    multidifusión link-local ff02::1, 1 referencias , no reportable
    multidifusión link-local ff02::1:ff70:803c, 1 referencias , último informado
r
  enlace MTU 1500 (enlace MTU 1500)
  límite de saltos actual128
  tiempo alcanzable 29500ms (base 30000ms)
  intervalo de retransmisión 1000ms
  transmisiones DAD 1
  longitud de prefijo de sitio predeterminada 48
```

Se muestran las configuraciones que se han hecho de modo automático para cada interfaz ya sea Inalámbrica o de Ethernet y el puente que fue usado ya que está siendo configurado en WINDOWS XP y es necesario usar método automático de transición, y las direcciones IPv6han sido asignadas automáticamente

C:\>ipv6 help

```
uso:   ipv6 [-p] [-v] if [ifindex]
       ipv6 [-p] ifcr v6v4 v4src v4dst [nd] [pmld]
       ipv6 [-p] ifcr 6over4 v4src
       ipv6 [-p] ifc ifindex [forwards] [-forwards] [advertises] [-advertises]
           [mtu #bytes] [site id_sitio] [preference P]
       ipv6 rlu ifindex v4dst
       ipv6 [-p] ifd ifindex
       ipv6 [-p] adu ifindex/address [life validlifetime[/preflifetime]]
           [anycast] [unicast]
       ipv6 nc [ifindex [dirección]]
       ipv6 ncf [ifindex [dirección]]
       ipv6 rc [ifindex dirección]
       ipv6 rcf [ifindex [dirección]]
```

```
ipv6 bc
ipv6 [-p] [-v] rt
ipv6 [-p] rtu prefix ifindex[/dirección] [life valid[/pref]]
    [preference P] [publish] [age] [spl longitud_predet_sitio]
ipv6 spt
ipv6 spu prefix ifindex [life L]
ipv6 [-p] gp
ipv6 [-p] gpu [valor parámetro] ... (try -?)
ipv6 renew [ifindex]
ipv6 [-p] ppt
ipv6 [-p] ppu prefix precedence P srclabel SL [dstlabel DL]
ipv6 [-p] ppd prefix
ipv6 [-p] reset
ipv6 install
ipv6 uninstall
```

Son algunos de los comandos con los cuales se puede configurar de manera manual las direcciones Ipv6.

Para comprobar el funcionamiento de Ipv6 se usa el comando de Ping.

C:\>ping6 ::1

```
Haciendo ping ::1
de ::1 con 32 bytes de datos:

Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m
Respuesta desde ::1: bytes=32 tiempo<1m

Estadísticas de ping para ::1:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

::1 es la dirección de Loopback en IPv6, al igual que 127.0.0.1 en IPv4. Windows XP incorpora la versión 6 del Internet Explorer, adaptada para navegar en las webs IPv6 (e IPv4).

C:\>ping6 fe80::20e:35ff:feb4:9b16

```
Haciendo ping fe80::20e:35ff:feb4:9b16
de fe80::20e:35ff:feb4:9b16%5 con 32 bytes de datos:

Respuesta desde fe80::20e:35ff:feb4:9b16%5: bytes=32 tiempo<1m
Respuesta desde fe80::20e:35ff:feb4:9b16%5: bytes=32 tiempo<1m
Respuesta desde fe80::20e:35ff:feb4:9b16%5: bytes=32 tiempo<1m
Respuesta desde fe80::20e:35ff:feb4:9b16%5: bytes=32 tiempo<1m

Estadísticas de ping para fe80::20e:35ff:feb4:9b16:
```

```
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Se hizo ping a la dirección ***fe80::20e:35ff:feb4:9b16*** la cual es una dirección propia.

C:\>tracert www.kame.net

```
Traza a la dirección www.kame.net [203.178.141.194] sobre un máximo de 30 saltos:
  1    4 ms     1 ms     1 ms  home [192.168.1.254]
  2   15 ms    11 ms    13 ms  dsl-servicio-l200.uninet.net.mx [200.38.193.226]
  3   54 ms    54 ms    55 ms  bb-dallas-stemmons-4-pos0-15-2-0.uninet.net.mx [201.125.6.37]
  4   75 ms    74 ms    76 ms  xe-8-3.r02.dllstx09.us.bb.gin.ntt.net [157.238.224.29]
  5   75 ms    74 ms    74 ms  ae-2.r20.dllstx09.us.bb.gin.ntt.net [129.250.2.153]
  6   74 ms    73 ms    96 ms  as-2.r20.lsanca03.us.bb.gin.ntt.net [129.250.2.168]
  7  190 ms   186 ms   186 ms  as-2.r20.osakjp01.jp.bb.gin.ntt.net [129.250.3.202]
  8  184 ms   181 ms   178 ms  ae-4.r20.tokyjp01.jp.bb.gin.ntt.net [129.250.4.209]
  9  330 ms   317 ms   234 ms  po-1.a15.tokyjp01.jp.ra.gin.ntt.net [203.105.72.154]
 10  188 ms   183 ms   182 ms  203.105.72.18
 11  190 ms   189 ms   188 ms  ve-51.foundry6.otemachi.wide.ad.jp [203.178.141.141]
 12  186 ms   186 ms   181 ms  ve-42.foundry4.nezu.wide.ad.jp [203.178.136.66]
 13  191 ms   196 ms   198 ms  ve-45.foundry2.yagami.wide.ad.jp [203.178.136.74]
 14  185 ms   391 ms   187 ms  ve-190.nec1.k2.wide.ad.jp [203.178.136.90]
 15  197 ms   192 ms   190 ms  orange.kame.net [203.178.141.194]

Traza completa.
```

El comando ***tracert*** se utiliza para comprobar la ruta de acceso a la dirección IP de destino que desea alcanzar y registrar los resultados, cuando en estos existen problemas de conectividad. El comando ***tracert*** muestra el conjunto de enrutadores IP que se usan para entregar paquetes desde el equipo al destino y la duración de cada salto. En caso de que no sea posible entregar los paquetes en el destino, el comando ***tracert*** muestra el último enrutador que reenvió los paquetes correctamente.

C:\>tracert -h 3 www.kame.net

```
Traza a la dirección www.kame.net [203.178.141.194] sobre un máximo de 3 saltos:

  1    2 ms     2 ms     1 ms  home [192.168.1.254]
  2    *       19 ms    15 ms  dsl-servicio-l200.uninet.net.mx [200.38.193.226]
  3  184 ms    54 ms    56 ms  bb-dallas-stemmons-4-pos0-15-2-0.uninet.net.mx [201.125.6.37]

Traza completa.
```

También se puede delimitar hasta q numero de saltos te muestre con este caso que solo fueron requeridos 3.

7.6.2 Windows Vista

En esta versión de Windows Vista como es de esperarse el protocolo de internet IPv6 es una función nativa, que viene instalado por defecto y solo tenemos que verificar si está funcionando correctamente por cual usaremos el siguiente comando para ver que este funciona de manera correcta.

Con el comando **ping** se comprueba que IPv6 está funcionando.

Se abre una ventana de consola y se escribe **ping –n 5 ::1**

C:\>ping -n 3 ::1

Haciendo ping a ::1 desde ::1 con 32 bytes de datos:
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m

Estadísticas de ping para ::1:
Paquetes: enviados = 3, recibidos = 3, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms

Si sale esto significa que IPv6 esta instalado y que funcionamiento es correcto, y este es capaz de de ver " 3 paquetes recibidos".

Habilitar IPv6

En Windows Vista, el protocolo IPv6 ya está configurado y habilitado por defecto de manera que no hace falta hacer nada. A pesar de esto se pueden configurar algunas características de IPv6.

Configuración automática de la dirección

Se puede configurar automáticamente la dirección de un nodo IPv6 que no es un encaminador (es decir, un ordenador IPv6) de la siguiente manera:

1. Usando “Stateless address autoconfiguration” con el descubrimiento de un encaminador IPv6

El PC IPv6 construye su dirección IPv6 basándose en el paquete “Router Advertisement” que envía el encaminador IPv6 conectado al mismo segmento de red donde está conectado el PC. Este es el método habilitado por defecto en un PC Windows Vista.

2. Usando “Stateful address autoconfiguration” con DHCPv6

Con DHCPv6 un PC IPv6 puede recibir un prefijo de subred además de otros parámetros de configuración. Un uso común de DHCPv6 para PCs basados en Windows es recibir y configurar automáticamente la dirección IPv6 de los servidores DNS, los cuales no se reciben a través del paquete “Router Advertisement” que envían los encaminadores IPv6 de la red. El paquete “Router Advertisement” que recibe un PC durante la fase del descubrimiento de encaminadores contiene un campo que indica si se va a utilizar también DHCPv6 para configurar la dirección IPv6.

Ipconfig

C:\>ipconfig

Configuración IP de Windows

Adaptador LAN inalámbrico Conexión de red inalámbrica:

Sufijo DNS específico para la conexión. . : gateway.2wire.net
Dirección IPv6 . . . . . : 2001:db8:3c4d:1::76
Vínculo: dirección IPv6 local. . . : fe80::f0af:6e53:72ad:98fa%13
Dirección IPv4. . . . . : 192.168.1.149
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 2001:db8:3c4d:1::75
192.168.1.254

Los adaptadores que estén desconectados no muestran las direcciones solo que sean habilitados.

Adaptador de Ethernet Conexión de red Bluetooth:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Conexión de área local:

```
   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
```

Este comando nos muestra todos los valores de la configuración de TCP/IP y también puede ser utilizado para dar mantenimiento, como la restauración de valores del DHCO.

Route

Este comando nos muestra las entradas en la tabla de enrutamiento local de IPv4 como IPv6 y nos permites realizar cambios.

```
C:\>route print
===========================================================================
ILista de interfaces
 13 ...00 21 00 4b 95 3a ...... WLAN Broadcom 802.11b/g
 12 ...00 21 86 7d 1c eb ...... Dispositivo Bluetooth (Red de ßrea personal)
 10 ...00 1e 68 c1 a9 bc ...... Realtek RTL8101E Family PCI-E Fast Ethernet NIC
(NDIS 6.0)
  1 ........................... Software Loopback Interface 1
 15 ...00 00 00 00 00 00 00 e0  isatap.gateway.2wire.net
 17 ...00 00 00 00 00 00 00 e0  isatap.{4C66CD01-70AC-4786-9B84-5131529D2449}
 16 ...00 00 00 00 00 00 00 e0  isatap.{82A40E6C-F6B8-4C49-8691-E49C89F249D8}
 14 ...02 00 54 55 4e 01 ...... Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0    192.168.1.254    192.168.1.149     30
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    306
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    306
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
      192.168.1.0    255.255.255.0      En vínculo     192.168.1.149    286
    192.168.1.149  255.255.255.255      En vínculo     192.168.1.149    286
    192.168.1.255  255.255.255.255      En vínculo     192.168.1.149    286
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    306
        224.0.0.0        240.0.0.0      En vínculo     192.168.1.149    286
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    306
  255.255.255.255  255.255.255.255      En vínculo     192.168.1.149    286
===========================================================================
Rutas persistentes:
  Ninguno

IPv6 Tabla de enrutamiento
===========================================================================
Rutas activas:
 Cuando destino de red métrica      Puerta de enlace
 13    286 ::/0                      2001:db8:3c4d:1::75
  1    306 ::1/128                   En vínculo
 13    286 2001:db8:3c4d:1::/64     En vínculo
 13    286 2001:db8:3c4d:1::76/128  En vínculo
 13    286 fe80::/64                En vínculo
```

```
 13    286 fe80::f0af:6e53:72ad:98fa/128
                                    En vínculo
  1    306 ff00::/8                 En vínculo
 13    286 ff00::/8                 En vínculo
===========================================================================
Rutas persistentes:
 Cuando destino de red métrica      Puerta de enlace
  0 4294967295 ::/0                 2001:db8:3c4d:6::78
  0 4294967295 ::/0                 2001:db8:3c4d:1::75
===========================================================================
```

Ping

Este comando nos sirve para verificar la conectividad de una computadora a otra y que está funcionando correctamente con el protocolo, este puede recibir mensajes de contestación que le fueron enviados.

```
C:\>ping -n 5 www.kame.net

Haciendo ping a www.kame.net [203.178.141.194] con 32 bytes de datos:
Respuesta desde 203.178.141.194: bytes=32 tiempo=185ms TTL=52
Respuesta desde 203.178.141.194: bytes=32 tiempo=233ms TTL=52
Respuesta desde 203.178.141.194: bytes=32 tiempo=184ms TTL=52
Respuesta desde 203.178.141.194: bytes=32 tiempo=183ms TTL=52
Respuesta desde 203.178.141.194: bytes=32 tiempo=183ms TTL=52

Estadísticas de ping para 203.178.141.194:
    Paquetes: enviados = 5, recibidos = 5, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 183ms, Máximo = 233ms, Media = 193ms
```

Tracert

```
C:\>tracert  fe80::2c0:9fff:fe70:803c

Traza a fe80::2c0:9fff:fe70:803c sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  fe80::2c0:9fff:fe70:803c

Traza completa.
```

El comando ***tracert*** se utiliza para comprobar la ruta de acceso a la dirección IP de destino que desea alcanzar y registrar los resultados, cuando en estos existen problemas de conectividad. El comando ***tracert*** muestra el conjunto de enrutadores IP que se usan para

entregar paquetes desde el equipo al destino y la duración de cada salto. En caso de que no sea posible entregar los paquetes en el destino, el comando ***tracert*** muestra el último enrutador que reenvió los paquetes correctamente

Netstat

Nos muestra la conexiones activas del TCP , escucha los puertos de la computadora, estadísticas de Ethernet , la tabla de enrutamiento y las estadísticas para IPv6,ICMPv6,TCP y UDP sobre los protocolos IPv6.

C:\>netstat -s

Estadísticas de IPv6

Paquetes recibidos	= 29
Errores de encabezado recibidos	= 0
Errores de dirección recibidos	= 0
Datagramas reenviados	= 0
Protocolos desconocidos recibidos	= 0
Paquetes recibidos descartados	= 0
Paquetes recibidos procesados	= 910
Solicitudes de salida	= 1410
Descartes de enrutamiento	= 0
Paquetes de salida descartados	= 10
Paquetes de salida sin ruta	= 0
Reensamblados requeridos	= 0
Reensamblados correctos	= 0
Reensamblados erróneos	= 0
Datagramas correctamente fragmentados	= 0
Datagramas mal fragmentados	= 0
Fragmentos creados	= 0

Estadísticas de ICMPv6

	Recibidos	Enviados
Mensajes	90	501
Errores	0	0
Destino inaccesible	5	5
Paquete demasiado grande	0	0
Tiempo agotado	0	0
Problemas de parámetros	0	0
Echos	28	52
Respuestas de eco	47	28
Consultas MLD	0	0
Informes MLD	0	0
Ejecuciones MLD	0	0
Solicitudes de enrutador	0	6
Anuncios de enrutador	0	0
Solicitudes de vecino	5	405
Anuncios de vecino	5	5
Redirecciones	0	0
Renumeraciones de enrutador	0	0

Estadísticas de TCP para IPv6

Activos abiertos	= 0
Pasivos abiertos	= 0
Intentos de conexión erróneos	= 0
Conexiones restablecidas	= 0
Conexiones actuales	= 0
Segmentos recibidos	= 0
Segmentos enviados	= 0
Segmentos retransmitidos	= 0

Estadísticas UDP para IPv6

Datagramas recibidos	= 152
Sin puerto	= 0
Errores de recepción	= 0
Datagramas enviados	= 820

Capítulo 8 Proyectos sobre IPv6

8.0 IPv6 UNAM MEXICO

Se conformo un grupo de trabajo de personas para poder fomentar el conocimiento de esta tecnología que se espera sea usada en un futuro no muy lejano ya que las direcciones o espacios se están agotando rápidamente, así se pueden aprovechar las oportunidades que nos brinda esta tecnología para que sean usadas adecuadamente y poder apoyar su despliegue realizando experimentos sobre ella, así crear una comunidad en la cual participen personas que aporten su conocimiento y lograr que instituciones se adhieran a el proyecto aportando sus ideas y conocimientos para poder impulsar esta tecnología y poner en práctica en el campo de IPv6 en México. [27]

Objetivos

- Investigar, probar e instalar IPv6 en redes de telecomunicaciones en México.
- Participar en el desarrollo de proyectos de IPv6 nacionales e internacionales.
- Participar en el fortalecimiento y difusión de IPv6 y sus aplicaciones.
- Proveer servicios de IPv6 en México y Latinoamérica.
-

Historia del protocolo IPv6 en México

IPv6 en México

La UNAM inició investigaciones en la materia desde el mes de diciembre de 1998, fecha en la que se constituye el proyecto IPv6 en nuestra Máxima Casa de Estudios, y durante el segundo semestre del año 1999 es notable el liderazgo de la UNAM en el ámbito nacional. Dentro del Proyecto IPv6 de la UNAM se estableció un amplio programa de pruebas y trabajos con temas como: implementaciones, stacks IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y DNS, autoconfiguración, calidad de servicio, IPv6 sobre ATM, conexión con redes internacionales de IPv6 (6Bone, 6REN), IPv6 en Internet2, etc.

Dentro de las primeras pruebas realizadas, destaca la de conexión a 6Bone , la cual fue una red mundial experimental utilizada para probar los conceptos y la puesta en

operación de IPv6. Al final en 6Bone participaron en el ámbito mundial 47 países, entre ellos México, donde la UNAM fue el primer nodo en el país, registrándose en junio de 1999.

Posteriormente en septiembre de 1999 la UNAM fue aceptada como uno de los 68 nodos de Backbone que en esa fecha operaban en 6Bone, obteniendo un rango de direcciones tipo pTLA: 3ffe:8070::/28. Cabe destacar que con este hecho la UNAM fue el primer nodo, y hasta ese momento el único, de este tipo en México, y el tercero en Latinoamérica. Adicionalmente, la UNAM ha podido delegar direcciones y configurar túneles a instituciones en México y en el mundo interesadas en realizar pruebas con IPv6.

En octubre del 2000 se obtuvo un bloque del tipo sTLA (2001:0448::/35) que se ha utilizado por ejemplo en la RedCUDI de Internet2 en México

Para contar con una red de pruebas en una primera etapa, y posteriormente con una red de producción, se instaló la Red IPv6 de la UNAM, la primera red IPv6 instalada en México y que inició operaciones en agosto de 1999. Esta red contó con varios túneles hacia otros nodos de Backbone de 6Bone:

SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que tiene la UNAM corriendo con sistemas operativos como Win 2003, Win 2000, Win XP, Solaris, Linux y BSD.

Actualmente se sigue trabajando con instituciones mexicanas y de América Latina para realizar su conexión IPv6 hacia la UNAM. Entre las instituciones mexicanas han destacado: Instituto Politécnico Nacional, Universidad Autónoma Metropolitana, Instituto Tecnológico de Estudios Superiores de Monterrey, Universidad Autónoma de Chiapas, Universidad Autónoma de Guerrero, Universidad Autónoma del Estado de Hidalgo, Universidad Autónoma de Nuevo León, Instituto Tecnológico de Oaxaca, Instituto Tecnológico de Mérida, Instituto Tecnológico Autónomo de México, PEMEX, STYX, ASTER, etc.

Entre las instituciones latinoamericanas han estado: Instituto de Informática de la Universidad Austral de Chile y las universidades UBio-Bio, UFRO y UDLA; ex-RETINA ahora InnovaRed, y las universidades LINTI-UNLP, UBA, de Argentina; EAFIT y las universidades UdeA, UniCauca y UniPamplona de Colombia; INICTEL, NITCOM, y la UNI de Perú, etc. [28]

8.1 Proyecto CUDI

Corporación Universitaria para el Desarrollo de Internet

Desde sus inicios la red de Internet2 de México ha funcionado con IPv4 sin embargo, actualmente ya se tiene soporte, en el Backbone, de la nueva versión denominada IPv6; por lo que paulatinamente se ha empezado a utilizar IPv6 desde los equipos centrales hasta los equipos terminales de los integrantes de esta red, siendo necesario desarrollar y utilizar aplicaciones con soporte para IPv6 e IPv4, mientras dura el proceso de transición de la versión 4 a la 6.

Objetivos

- Instalar IPv6 en la red avanzada de México (RedCUDI)).
- Realizar pruebas de desempeño con IPv6.
- Utilizar y desarrollar aplicaciones con soporte para IPv6.
- Realizar pruebas en colaboración con otros Grupos de Trabajo y Comités.
- Trabajar estrechamente con grupos de otros países.

Proyectos

- Multicast IPv6 en OSTN. En colaboración con otros Grupos de Trabajo de CUDI.
- Multicast IPv6 en Opera Oberta. En colaboración con otros Grupos de Trabajo de CUDI.
- Remuneración de IPv6 en CUDI. (Concluido) En colaboración con otros Grupos de Trabajo de CUDI.
- Red nativa de IPv6 en las NRENs de Latinoamérica.(En Proceso) En colaboración con el Grupo de Trabajo de IPv6 de CLARA
- Desarrollo y programación de aplicaciones con soporte IPv6.
- Soporte de Multicast con IPv6 en el Backbone.(En Proceso) En colaboración con el Grupo de Trabajo de Multicast.
- Uso de aplicaciones de videoconferencia con soporte IPv6 en eventos de CUDI. En colaboración con el NOC de Videoconferencia. [28]

CONCLUSIÓN

IPv6 que es la nueva generación de protocolos de Internet y que en la actualidad es integrado para brindar soporte IP a la mayoría de sistemas operativos de todo tipo de dispositivo que cuente con un sistema que requiera y que tenga la capacidad de conectarse a Internet, este nuevo protocolo fue creado gracias a la IETF que es la encargada de mantener el la tecnología y la seguridad como su funcionalidad y hacernos mejor las experiencia del Internet.

Como vimos anteriormente las mejoras que se van haciendo progresivamente a partir de la vieja versión IPv4 que en algún momento será poco a poco sustituida por la versión más reciente IPv6 por sus grandes ventajas que esta nos ofrece. Esta actualización se hará de forma independiente ya que cada proveedor de servicio de Internet y el usuario tienen la decisión de cuando migrar ya que actualmente hay métodos que hacen posible la convivencia entre ambas tecnologías o versiones. Pero paulatinamente tendrá que migrar ya que las direcciones de IPv4 como ya vimos solo cuenta con 32 Bits de direcciones lo que hace que algún día se tiene que agotar por el crecimiento de la demanda de direcciones lo que nos lleva a la solución que es IPv6 ya que nos permite 128 Bits lo que nos da billones de posibles direcciones.

Este nuevo protocolo nos presenta la optimización de su encabezado, lo que nos permite realizar la comunicación de una forma más eficiente y así llevar a cabo en todo el sistema de comunicaciones. A su vez integra extensiones de cabeceras que permiten que un paquete establezca un mecanismo para autentificar su origen para así asegurar la integridad de los datos y que no ha sido modificado por nadie.

Este protocolo fue estructurado y basado en IPv4 integrándole mejoras y quitándole bloques innecesarios que solo hacían que su función no fuera la adecuada, colocándole nuevas formas de ir con el tiempo modificando o agregando funciones haciendo posible la actualización y no la migración a otro protocolo.

BIBLIOGRAFÍA

[1] http://lacnic.net/en/anuncios/2007_agotamiento_ipv4.html visitado en septiembre, octubre 2009.
[2] http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html#wp1020627 visitado en octubre, noviembre y diciembre 2008.
[3] http://www.ietf.org/rfc/rfc0791.txt?number=791 visitada en septiembre y noviembre 2008.
[4] http://www.ietf.org/rfc/rfc0791.txt?number=791 visitada en septiembre y octubre 2008.
[5] http://www.ietf.org/rfc/rfc1550.txt?number=1550 Visitada en septiembre 2008.
[6] http://www.ietf.org/rfc/rfc1726.txt?number=1726 visitada en septiembre 2008.
[7] http://www.ietf.org/rfc.html visitada de enero 2009 hasta diciembre 2009.
[8] http://www.ipv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf visitado en noviembre y diciembre 2008.
[9] http://town.hall.org/trendy/sipp/sipp-doc/sipp-whitepaper.TXT visitado en diciembre 2008.
[10] http://tools.ietf.org/html/rfc1347 visitada en diciembre 2008.
[11] http://www.ipv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf visitado en diciembre 2008.
[12] HandBook of IPv4 to IPv6 Translation, John J. Amoss, Daniel Minoli Auerbach Publications Boca Raton New York
[13] HandBook of IPv4 to IPv6 Translation, John J. Amoss, Daniel Minoli Auerbach Publications Boca Raton New York
[14] Understanding IPv6 (Second edition), Joseph Davis Microsoft Press. Segunda Edición, 2008 Redmond, Washington pp: 53 -64
[15] http://www.ietf.org/rfc/rfc2373.txt?number=2373 visitado junio 2009.
[16] http://www.ietf.org/rfc/rfc3041.txt?number=3041 visitada junio 2009.
[17] Understanding IPv6 (Second edition), Joseph Davis Microsoft Press. Segunda Edición, 2008 Redmond, Washington pp: 73-77
[18] http://www.ietf.org/rfc/rfc3041.txt?number=3041 visitada junio 2009.
[19] Understanding IPv6 (Second edition), Joseph Davis Microsoft Press. Segunda Edición, 2008 Redmond, Washington pp: 83-85
[20] IPv6 Essentials Second Edition, Silvia Hagen , O'ReillySecond edition, 2006 Sebastopol, CA
[21] http://www.ietf.org/rfc/rfc4443.txt?number=4443 visitada en agosto 2009.
[22] IPv6 Essentials Second Edition, Silvia Hagen , O'ReillySecond edition, 2006 Sebastopol, CA
[23] Understanding IPv6 (Second edition), Joseph Davis Microsoft Press. Segunda Edición, 2008 Redmond, Washington
[24] Understanding IPv6 (Second edition), Joseph Davis Microsoft Press. Segunda Edición, 2008 Redmond, Washington pp: 453
[25] Understanding IPv6 (Second edition), Joseph Davis Microsoft Press. Segunda Edición, 2008 Redmond, Washington pp 455
[26] http://www.ietf.org/rfc/rfc1933.txt?number=1933 visitada en agosto 2009
[27] http://www.ipv6.unam.mx/ visitado en septiembre 2009.
[28] http://www.cudi.edu.mx/ visitado en octubre 2009.

INDICE DE FIGURAS

Capítulo 2

Capítulo 3

Capítulo 4

Capítulo 5

Capítulo 6

INDICE DE TABLAS

Capítulo 2

Capítulo 3

Capítulo 4

Capítulo 5

GLOSARIO

ACKNOWLEDGEMENT (ACK) (en español **acuse de recibo**), en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

ARPANET (*Advanced Research Projects Agency Network*) fue creada por encargo del Departamento de Defensa de los Estados Unidos ("DoD" por sus siglas en inglés) como medio de comunicación para los diferentes organismos del país.

Backbone: se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de Routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo.

Bridge o puente de red es un dispositivo para interconexión de redes locales.

Cabecera (Header): Información que suele situarse delante de los datos (por ejemplo en una transmisión) y que hace referencia a diferentes aspectos de estos (longitud...).

Capa (Layer): Cada una de los elementos que conforman una estructura jerarquica.

Comercio electrónico (E-comerce): Actividad que consiste en la compra o venta de artículos por INTERNET. Caracterizado por ser gobernado por el propio sistema operativo de forma autónoma.

CLNP Protocolo de red no orientado a la conexión. Protocolo de capa de red OSI que no requiere un circuito para establecerse antes de que se transmitan los datos.

Daisy Chain (Cadena de Margarita): Sistema de enlace de objetos dónde cada objeto contiene un apuntador al siguiente formado una lista.

DARPA: Defense Advanced Research Projects Agency.

Datagrama: Conjunto de estructurado de bytes que forma la unidad básica de comunicación del protocolo IP (en todas sus versiones).

Encaminamiento (Routing): Procedimiento que consiste en conducir un datagrama hacia su destino a través de INTERNET.

Encapsulamiento: Sistema basado en colocar una estructura dentro de otra formando capas.

IETF (***I**nternet **E**ngineering **T**ask **F**orce*, en castellano Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986.

Encapsulating Security Payload (ESP): El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro.

FTP (sigla en inglés de **F**ile **T**ransfer **P**rotocol - **Protocolo de Transferencia de Archivos**) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

Firewall (Cortafuegos): Máquina encargada del filtrado del tráfico de INTENET (tanto de entrada como de salida) basado en reglas de comportamiento, que se sitúa entre INTERNET y una Intranet.

HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un URL.

Half-close: Sistema de finalización de una comunicación establecida con el protocolo TCP.

PNP: plug and play.

ICMP (INTERNET Control Message Protocol): Protocolo encargado de la comunicación de mensajes entre nodos conectados a INTERNET.

IP (INTERNET PROTOCOL): Protocolo no fiable y sin conexión en el que se basa la comunicación por INTERNET. Su unidad es el datagrama.

IPng (IP Next Generation): Abreviatura escogida en IETF con la que también se denomina la versión 6 del protocolo IP.

IPv6 (IP versión 6): Abreviatura escogida en IETF con la que se denomina la versión 6 del protocolo IP.

Kernel: Conjunto de servicios básicos que debe ofrecer un sistema operativo para poder funcionar.

LAN (Local Area Network): Red local. Es la encargada de conectar ordenadores en distancias inferiores a 1Km.

MAC Address: Dirección única que llevan las tarjetas de red grabadas en una ROM para identificarse y diferenciarse de las demás.

MTU (Maximun Transfer Unit): Siglas que denominan el tamaño máximo en unidades de transmisión que se permite en un canal de comunicación.

OSI (Modelo): Modelo teórico propuesto por IEEE que describe cómo deberían conectarse distintos modelos de ordenadores a diferentes tipos de red para poder comunicarse entre sí.

Overhead: Pérdida de rendimiento.

Pipelining: Sistema consistente en la solapación de tareas (una tras otra) de forma que se mejore el rendimiento.

Periféricos: Cualquier tipo de dispositivo que pueda ser conectado a un ordenador.

Protocolos: Conjunto de reglas que establece cómo debe realizarse una comunicación.

Red: Dispositivo físico que conecta dos o más ordenadores.

RFC (Request For Comments): Documento de especificaciones que se expone públicamente para su discusión.

Router: Dispositivo físico u ordenador que conecta dos o más redes encargado de direccionar los distintos datagramas que le lleguen hacia su destino.

Seteados : establecer la configuración correcta de un programa o hardware

Socket: Secuencia compuesta por una dirección IP y un número de port.

Socket pair: Pareja sockets que permiten definir una comunicación (origen y destino).

SSL (Secure Socket Layer): Protocolo que proporciona seguridad en INTERNET a partir del protocolo TCP.

Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SYN es un byte de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases (*3 way handshake*) Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

TIC: son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno.

TCP (Transmission Control Protocol): Protocolo de nivel superior que permite una conexión fiable y orientada a conexión mediante el protocolo IP.

Telnet (**TELecommunication NETwork**) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a

la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Three Way Handshake: Protocolo de tres pasos en el que se basa el establecimiento de conexión en el protocolo TCP.

UDP (User Datagram Protocol): Protocolo no fiable y sin conexión basado en el protocolo IP.

User Datagram Protocol (**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.

WAN (Wide Area Network): Red de gran alcance. Este tipo de red suele utilizarse en la unión de redes locales (LAN).