UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

REDES DE COMPUTADORAS

MODELO IPv6: PROPUESTA DE SU INTEGRACION AL PROTOCOLO TCP/IP.

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE:
LICENCIADA EN INFORMATICA
P R E S E N T A :

ANGELICA ESPINOZA GODINEZ

ASESOR: LIC. CARLOS PINEDA MUÑOZ

CUAUTITLAN IZCALLI, EDO. DE MEX. 1997

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

UNIVERSIDAD NACIONAL AVPNMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS SUPERIORES-CUAUTITLAN

DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JAIME KELLER TORRES
DIRECTOR DE LA FES-CUAUTITLAN
P R E S E N T E .

AT'N. ING. RAFAEL RODRIGUEZ CEBALLOS
Jefe del Departamento de Exámenes
Profesionales de la FES-C.

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Redes de Computadoras.
IPv6: Propuesta de su integración al protocolo TCP/IP.

que presenta la **pasante:** Angélica Espinoza Godínez.
con número de cuenta: 9001293-8 **para obtener el Título de:**
Licenciada en Informática.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E .
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Edo. de México, a 15 **de** octubre **de 19** 97.

MODULO:	PROFESOR:	FIRMA:
Módulo I	Lic. Carlos Pineda Muñoz	
Módulo II	Ing. Miguel Alvarez Pasaye	
Módulo III	M. en I. Gloria Ponce Vanegas	

DEP/VOBOSE/I

AGRADECIMIENTOS

Ante la culminación de una de mis metas doy gracias a ...

- *Dios por darme sabiduría y paciencia,*
- *Mi familia por brindarme su apoyo,*
- *La UNAM por forjar en mi una actidud de responsabilidad y servicio,*
- *Mis profesores por compartir su conocimiento conmigo,*
- *José Luis por darme su amor y cariño y*
- *Todas aquellas personas que me han apoyado en mi formación profesional y personal*

INDICE

INTRODUCCION

Hoy en día, es común el uso de Internet como un valioso sistema de información; tanto para los ámbitos económicos, financieros y sociales, además en actividades culturales y de esparcimiento. No obstante, el crecimiento desmedido del número de los nodos conectados a Internet ha ocasionado ineficiencia en el control del direccionamiento de sitios.

El área de informática como muchas otras especialidades, necesita una actualización continua del software y hardware para lograr una coherencia entre éstos y la tecnología en auge, siempre con la intención de atender las necesidades que imperan tanto en los usuarios finales como en los programadores de sistemas de cómputo.

Un conjunto de necesidades apremiantes de comunicación mundial integral crece junto con los complejos sistemas de redes. La heterogeneidad de las arquitecturas de red es, por ejemplo, uno de los obstáculos que aún en nuestros días los fabricantes de software y hardware siguen considerando para la creación de sus productos, tratando de lograr la mayor satisfacción de las necesidades de comunicación : representadas en compatibilidad, transportabilidad, bajos costos, eficiencia-eficacia en la transmisión-recepción de datos, imagen y sonido.

Las organizaciones, instituciones y grupos de trabajo de Internet están preocupadas por prever la eficiencia en la operación de Internet, y manifiestan gamas de normas y sugerencias para este fin. Por consiguiente, crearon el nuevo modelo de direccionamiento de datos, llamado IPv6, con la intención de sustituir el actual IPv4 del protocolo TCP/IP y obtener mejores servicios en Internet.

Entre las razones principales, por la cual el protocolo de comunicación TCP/IP se modificará en la parte del Protocolo Internet (IP), esta la referente a la capacidad de direccionamiento de nodos Internet, cuya longitud ha sido considerada ineficiente para responder a la inmensa demanda de localidades de red.

Por lo anterior, el presente trabajo de investigación tiene, como objetivo general, describir el nuevo modelo de direccionamiento de datos IPv6 y las limitaciones del IPv4 ; para la integración del primero, en el protocolo TCP/IP. Por otra parte, la hipótesis sobre la cual se fundamenta asume que la integración de IPv6 al protocolo TCP/IP ; contribuirá a un direccionamiento eficiente de los nodos conectados a Internet en pro de su crecimiento.

Con el propósito de comprender los fundamentos funcionales del protocolo TCP/IP y en consecuencia los del IPv4 e IPv6, el primer capítulo conceptualiza la terminología utilizada en el área de protocolos y en desarrollo de TCP/IP e Internet. El segundo capítulo, se encargará de abordar los principios de la estructura del modelo de referencia OSI y los del protocolo TCP/IP, para luego detallar la parte IP de éste último.

El tercer capítulo, esta abocado a describir el funcionamiento del nuevo modelo IPv6 considerando, esencialmente ; las características que se conservan y las adicionales con respecto al modelo actual IPv4.

Finalmente, el capítulo cuarto desarrolla el caso práctico de la investigación, el cual propone la integración del nuevo modelo IPv6 al protocolo TCP/IP.

OBJETIVO GENERAL

DESCRIBIR EL NUEVO MODELO DE DIRECCIONAMIENTO DE DATOS IPv6 Y LAS LIMITACIONES DEL IPv4; PARA LA INTEGRACIÓN DEL PRIMERO, EN EL PROTOCOLO TCP/IP.

OBJETIVOS ESPECIFICOS

ANALIZAR EL FUNCIONAMIENTO DE LOS MODELOS IPv4 E IPv6 PARA LA IDENTIFICACION DE SUS SIMILITUDES Y DIFERENCIAS.

EVALUAR LAS PROPUESTAS DEL NUEVO MODELO IPv6 PARA SU INTEGRACION EN EL PROTOCOLO TCP/IP.

CAPITULO 1.
PROTOCOLOS

CAPITULO 1. PROTOCOLOS

1.1. GENERALIDADES

Al inicio de la computación, las computadoras sólo intercambiaban información con los dispositivos conectados a ellas, como las lectoras de tarjetas perforadas y las impresoras. La transición de la comunicación de datos a través de redes, como la conocemos ahora, surgió por el cambio en las necesidades de transferencia de información y la disposición de recursos distantes. Al principio, se requirió de enlaces locales y luego de enlaces remotos para accesar o intercambiar datos, disponiendo de recursos de cómputo lejanos.

La comunicación entre computadoras fue generando redes de comunicación cada vez más grandes, complejas y heterogéneas, a la par de su tecnología; lo cual ha traído consigo la competencia por perfeccionar los servicios de comunicación, así como su costo.

El desarrollo de las comunicaciones se fue dando conforme las organizaciones fueron adquiriendo más computadoras. La organizaciones buscaron la forma de transferir datos entre sus computadoras y permitir el acceso a una computadora desde otra dentro de un área pequeña o local.

Fue así como se les encomendó a los fabricantes de cómputo el desarrollo de hardware y software para facilitar los servicios de comunicación entre computadoras. Sin embargo, los productos ofrecidos por los fabricantes resultaron limitados, ya que eran implementados en cierto equipo; soportados en un número limitado de redes de área local y de área amplia; el software era complejo porque utilizaba diferentes lenguajes para cada dispositivo y cada aplicación y, no contaban con flexibilidad de prever la conexión de redes independientes, sencilla y económicamente.

A través de los años la conectividad de redes de cómputo ha llegado a ser necesaria y urgente. Hoy en día, las organizaciones necesitan combinar estaciones de trabajo, servidores y terminales en localidades de Red de Area Local (*Local Area Network LAN*); conectar una LAN a otras LANs y/o a una Red de Area Amplia (*Wide Area Network WAN*); desean habilitar cualquier par de sistemas en cualquier momento,

sin importar donde estén ubicados en la red y, buscan obtener el costo-beneficio de la tecnología de punta lo más pronto posible.

Como consecuencia de las necesidades anteriores y ante los resultados del hardware y software dispuesto por los fabricantes de cómputo, fue necesario diseñar reglas que lograran el entendimiento entre aplicaciones de cómputo y coordinaran el intercambio de mensajes entre ellas; a estas reglas se les denominó ***protocolo***.

1.2. OBJETIVOS

Los objetivos de los protocolos deben buscar la satisfacción de las necesidades de red y en función de eso, se regirán.

Algunas de las necesidades de red son las siguientes:

I. Comunicación entre los diferentes elementos de cómputo: estaciones de trabajo, servidores, terminales, impresoras, etc.
II. Acceso e intercambio de datos entre diferentes tipos de red: *LAN*, *WAN* o Red de Area Metropolitana (*Metropolitan Area Network MAN*).
III. Servicios de red disponibles para el usuario desde cualquier punto de una red.
IV. Adaptación de nuevas tecnologías de comunicación dentro de las organizaciones.

Determinadas las necesidades de red, podemos enunciar los objetivos principales de los protocolos:

1. Acceder a cualquier *host* desde una terminal.
2. Permitir el copiado de archivos de un *host* a otro.
3. Establecer correo electrónico entre usuarios.
4. Mostrar acceso transparente para archivos remotos como si fueran locales.
5. Disponer de recursos remotos de un host a otro.
6. Proporcionar el servicio de administración de red para hosts, ruteadores y otros dispositivos.

1.3. TERMINOLOGIA

La comunicación de datos requiere del uso de términos propios para la correcta comprensión de sus funciones y procesos; los siguientes son algunos de éstos términos:

BYTES Y OCTETOS

Un ***Byte*** u ***Octeto*** representa 8 bits y equivale a un caracter. Los dos términos significan lo mismo y pueden ser usados indistintamente, según lo convenga el usuario.

HOSTS

Host es una computadora con uno o más usuarios. Por ejemplo, una PC, una estación de trabajo, una minicomputadora y un mainframe puede ser un host.

PROTOCOLOS, STACKS Y SUITES

Un ***protocolo*** es un conjunto de reglas que rigen la operación de las funciones de comunicación. Por ejemplo, el Protocolo Internet (*Internet Protocol IP)* consiste en un grupo de reglas para rutear datos, y el Protocolo para el Control de Transmisión (*Transmission Control Protocol TCP*) incluye reglas para asegurar el envío secuencial de datos.

Protocolo ***stack*** es un grupo de protocolos enlazados que trabajan juntos para proveer la comunicación entre aplicaciones. Por ejemplo, *TCP*, *IP* y *Ethernet* forman un protocolo stack.

El protocolo ***suite*** es un grupo de protocolos que trabajan juntos en forma coordinada. La Suite de Protocolos Internet TCP/IP (*Transmission Control Protocol/Internet Protocol*) es un ejemplo de esta clasificación.

GATEWAYS, PUENTES Y RUTEADORES

Ruteador es el dispositivo conectado a dos o más redes, encargado de dirigir *datagramas* entre ellas, mediante la dirección IP del destino. Un ruteador esta definido también, como un nodo que envía *datagramas* a las capas bajas, sin realizar cambios de protocolos. La capa de red (capa IP) es el nivel de operación de los ruteadores para el protocolo TCP/IP.

Los ruteadores de Internet son capaces de tomar decisiones de ruteo basados en la información de la cabecera del protocolo IP y en sus tablas de ruteo.

Puente es un dispositivo que conecta dos o más LANs usando los mismos protocolos de Control de Acceso al Medio (*Media Access Control MAC*). Un puente opera absorbiendo todo el tráfico de una LAN y examinando la dirección física del origen y del destino en la cabecera del MAC. El puente, se encarga de acarrear tramas de datos de una LAN origen conectada a una interface de puente hacia una LAN destino con otra interface.

Un puente esta definido también, como un nodo que enlaza dos segmentos de red. La capa física es el nivel de operación de los puentes.

Los puentes pueden operar en la red como ruteadores (*brouters*); es decir, para unos protocolos servirá como puente y para otros como ruteador.

Una de las diferencias entre un ruteador y un puente es que el primero opera en la capa de red usando direcciones IP, mientras que el segundo opera en la capa de enlace y física mediante direcciones físicas.

Gateway es el dispositivo que enlaza dos protocolos diferentes y ejecuta una traducción para lograr la comunicación entre ambos.

En la literatura original de TCP/IP se utiliza la palabra gateway para referirse a un ruteador. Actualmente, cada término se usa para especificar fines distintos.

NODO, ENLACE, NODO VECINO E INTERFACE

Nodo o elemento de red es el usado para referirse a una entidad de comunicación en la red sin especificar si se trata de un host, un ruteador; o cualquier otro dispositivo de red, como un puente.

Enlace es la comunicación establecida entre nodos; o bien, el medio por el cual los nodos pueden comunicarse en la capa de enlace y física.

Nodo Vecino son los nodos conectados en un mismo enlace.

Interface es la conexión de un nodo a un enlace.

NOMBRE, DIRECCIÓN, RUTA Y UNIDAD DE DATO

Nombre son palabras seleccionadas para identificar a un host.

Dirección es un identificador de nodo que sirve para determinar el lugar donde se encuentra y para relacionarlo a su red.

Ruta indica la secuencia de direcciones necesarias para llegar a un host destino.

Unidad de dato es un bloque de datos enviado de una capa a otra en una arquitectura de red; o bien un bloque de datos transmitido a lo largo de una red. Su longitud varia de acuerdo al tipo de unidad y al medio de transmisión de la red (Ver Figura 1.1). Las unidades de dato del TCP/IP empleadas en esta investigación serán:

- ***Mensajes*** o ***Flujos*** se refiere a la secuencia de mensajes individuales o un flujo continuo de octetos enviados o recibidos entre la capa de aplicación y la capa de transporte.

- ***Segmento*** es la unidad de datos utilizada por el Protocolo para el Control de Transmisión (*Transmission Control Protocol TCP*) para realizar la transmisión y recepción de datos entre la capa de transporte y la capa de Internet.

- ***Datagrama de usuario o paquete*** [1] es la unidad empleada por el Protocolo de Datagramas de Usuario (*User Datagram Protocol UDP*) en la transmisión y recepción de datos entre la capa de transporte y la capa Internet.

---

[1] Algunos autores identifican el término ***"paquete"*** como la unidad de transmisión o recepción entre el protocolo UDP y la capa Internet. Sin embargo, en esta investigación el término "paquete" se utilizará para generalizar el tráfico de información a través de la red, sin hacer mención de alguna capa en específico y cuando se aborde el Modelo OSI se empleará para referirse a la unidad de datos empleada en cualquiera de sus capas.

- ***Datagrama*** es la unidad de datos usada por IP para transmitir o recibir datos. Esta unidad es empleada entre la capa de Internet y la capa de enlace y física.

- ***Trama*** es la unidad empleada entre la capa de enlace y física de un nodo emisor y la del receptor.

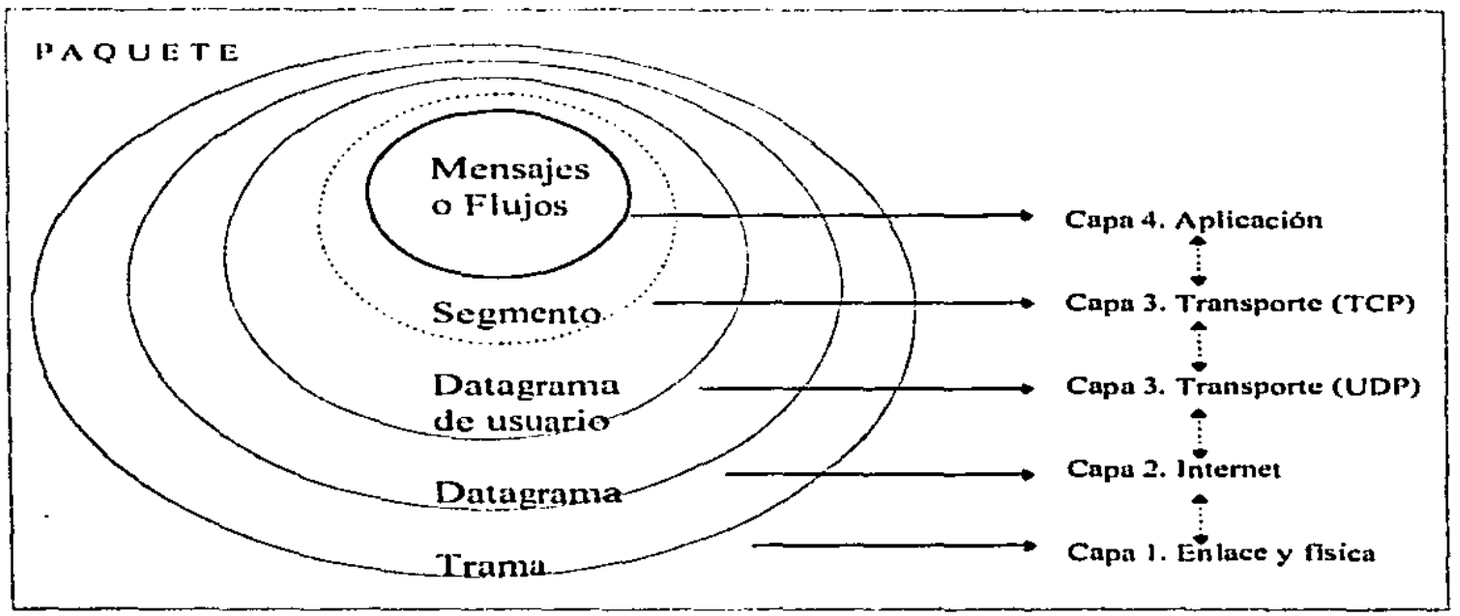


Figura 1.1 Unidades de datos empleadas en el protocolo TCP/IP

MTU DE ENLACE Y MTU DE RUTA

MTU de enlace es la Unidad Máxima de Transmisión (*Maximum Transfer Unit*) o el tamaño máximo de la trama que puede ser transferido en grupos de octetos, sobre un enlace.

MTU de ruta es la unidad mínima de MTU de enlace a lo largo de la ruta de un nodo origen a un nodo destino. Antes de que el nodo origen de IPv6 envíe tráfico de información, debe realizar una técnica para Descubrir la MTU de Ruta (*Path MTU Discovery*) y así identificar la MTU mínima a lo largo de la trayectoria hasta el destino.

1.4. TCP/IP E INTERNET

Al final de la década de 1960, hubo una gran demanda de universidades y centros de investigación de Estados Unidos por una red que permitiera la disposición nacional de sus recursos de cómputo y el intercambio de datos entre computadoras distantes.

Paralelamente a lo anterior, existía el interés por el diseño, implementación y uso de tecnologías de red en general, así como la creación de una red que permitiera el intercambio de paquetes de información. Para este fin, la Agencia de Proyectos de Investigaciones Avanzadas *(Advanced Research Projects Agency ARPA)* del Departamento de Defensa de los Estados Unidos, (mas tarde renombrada *DARPA Defense Advanced Research Projects Agency*), invirtió (desde 1972) en proyectos de interés militar creando *ARPANET* (Red de ARPA), la cual daría lugar al diseño del protocolo TCP/IP de Internet.

Nacimiento del protocolo TCP/IP de Internet

En 1957 es formada *ARPA*, con el fin de desarrollar la ciencia y la tecnología en apoyo a las estrategias militares. Los colaboradores iniciales de ARPA fueron universidades y organizaciones de investigación de los Estados Unidos dedicadas a la investigación de nuevas tecnologías de comunicación de datos.

ARPA y sus colaboradores diseñaron la primera red de intercambio de paquetes denominada ARPANET, la cual inició su operación con cuatro nodos en el año de 1969. La primera propuesta de ARPANET con cuatro Procesadores de Mensajes Internet (*Internet Message Processors IMP)*, fue inicialmente para la Universidad de California en los Angeles (UCLA), la Universidad de California en Santa Barbara (UCSB), el Instituto de Investigación de Stanford (SRI) y la Universidad de Utah en el verano de 1968. No obstante, el contrato de IMPs fue ganado por la compañía *Bolt, Beranek & Neuman Inc. (BBN)* en diciembre de 1968.

Inicialmente, ARPANET era una red de líneas telefónicas rentadas punto-a-punto; conectada por nodos de intercambio especial, denominados *IMPs*. Un host accesaba ARPANET conectándose a un IMP usando el protocolo 1822. En aquel tiempo, el protocolo fue expuesto en la Nota de Ingeniería Internet (*Internet Engineering Note IEN*) número 1822, parecida o los documentos de ahora llamados Requisición para Comentarios (*Request For Comments RFC)*.

La BBN tuvo desde entonces, fuerte influencia sobre el desarrollo de la arquitectura del TCP/IP. El diseño de protocolos individuales y las nociones específicas

de lo que ARPANET debería realizar fueron desarrollados gradualmente al principio. En 1970, las demandas existentes para accesos remotos y transferencia de archivos fueron satisfechas a través del Protocolo de Control de Red *(Net Control Protocol NCP)*, el predecesor de la actual Suite de Protocolos Internet TCP/IP (*Transmission Control Protocol/Internet Protocol).*

En 1972 *Robert E. Kahn* organiza la Conferencia Internacional de Comunicaciones entre Computadoras con la demostración de ARPANET entre 40 equipos. El moderador de dicha conferencia fue *Vinton G. Cerf.* Robert y Vinton más tarde propusieron una nueva suite de protocolos. En ese mismo año, *Ray Tomlinson* de BBN inventa un programa de correo electrónico para enviar mensajes a través de una red distribuida.

ARPANET se expandió cada vez más teniendo gran aceptación, pero los protocolos empleados hasta ese momento eran lentos y problemáticos. En 1974, fue propuesto un nuevo grupo de protocolos por *Vinton* y *Robert*, quienes publicaron el documento "Un Protocolo para Interconectar Redes de Paquetes" (*A Protocol for Paccket Network Information*), el cual especificaba en detalle el diseño del Protocolo para el Control de Transmisión *(Transmission Control Protocol TCP)* y proporcionaba las bases para el desarrollo del Protocolo Internet (*Internet Protocol IP*).

Aunque tomó tres años incorporar la nueva suite de protocolos a los más de cien hosts de ARPANET, desde 1980 a 1983, la transición de los protocolos de TCP/IP hacia la tecnología Internet se completó en enero de 1983, cuando la Oficina del Secretario de Defensa ordenó que todas las computadoras (más de trescientas) conectadas a redes de área amplia utilizaran el TCP/IP. Es por este tiempo, cuando surge la primera definición de *Internet* como el conjunto de redes interconectadas a través del protocolo TCP/IP, empleando los términos Internet TCP/IP como uno solo, o simplemente Internet.

Al mismo tiempo, la Agencia de Comunicación de la Defensa (*Defense Communicatios Agency DCA)* a cargo de ARPANET desde 1975, divide ARPANET en dos redes, una conservando el nombre de ARPANET cuya función sería la investigación y el desarrollo futuros; y la otra, llamada *MILNET* (Red Militar) para propósitos militares. Finalmente en 1990, ARPANET fue disuelta.

Internet red de redes

El contar con la posibilidad de conectar dos o más redes TCP/IP, adherirlas a la red ARPANET para expandirla, y lograr que todas las redes operen como una sola se le

denominó *Internet*. Durante la década de 1980, ARPANET fue mantenida como la columna vertebral (*backbone*) de Internet.

A causa de las características ofrecidas por los protocolos TCP/IP, Internet creció súbitamente, llegando a ser la red más grande del mundo, conectando redes del gobierno, militares, académicas y comerciales, cada cual con cientos de subredes. Al final de la década de 1980 la Red de la Fundación Nacional de Ciencia (*Net Science Fundation NETwork NSFNET*), fue incorporada como columna vertebral para proporcionar mayor velocidad en las búsquedas de sitios.

Aunque Internet era más grande que el núcleo de la red de investigación militar, el Departamento de Defensa de los Estados Unidos siguió coordinando Internet a través de la Agencia de Sistemas de Información de la Defensa (*Defense Information Systems Agency DISA* antes *DCA*), la cual es responsable de determinar los protocolos, arquitectura, políticas, estrategias de administración y procedimientos de operación oficiales de la Red de Datos de la Defensa (*Defense Data Network DDN*). Además, el Centro de Información de la Red Internet (INTERnet Network Information Center *InterNIC* antes *Network Information Center NIC*) provee servicios de información de Internet y proporciona documentación acerca de protocolos a usuarios, administradores de hosts, coordinadores de sitios y administradores de red; y tiene a cargo el registro de direcciones IP y los nombres de los dominios.

Internet sigue implementando la nueva tecnología; sus servicios de correo electrónico, noticias y mesa de boletines disponen foros públicos en los cuales las ideas son debatidas y refinadas. Los investigadores, programadores de sistemas y administradores de redes intercambian correcciones a software, soluciones a problemas de interconexión y sugerencias para el mejoramiento de ejecuciones.

Organizaciones Internet

En 1979, ARPA formó un comité para establecer el diseño de los protocolos y la arquitectura de Internet. Dicho comité se nombró Junta de Control y Configuración de Internet (*Internet Control and configutation Board ICCB*) y estaba integrado por investigadores que compartían ideas y discutían los resultados de los experimentos en ARPANET. En 1983, cuando ARPANET fue dividida en ARPANET y MILNET, el ICCB también fue reorganizado para convertirse en la Junta de Arquitectura de Internet (*Internet Architecture Board IAB*).

Durante 6 años (1983-1989), la IAB pasó de ser un organismo de ARPANET a una organización autónoma. Su organización original consistía en que cada miembro tenía a su cargo una *Fuerza de Tarea de Internet*, para investigar y resolver algún

aspecto importante de Internet. La IAB tenia aproximadamente diez fuerzas de tarea y la representaba un presidente, quien era denominado *Arquitecto de Internet* y era responsable de informar de las conclusiones del desarrollo de Internet y TCP/IP a los representantes de las agencias patrocinadoras, como ARPA y la Fundación Nacional de Ciencias (*National Sciene Fundation NSF*).

El desarrollo de la operación de TCP/IP e Internet fueron creciendo tanto que, el mercado comenzó a dominar la evolución tecnológica como se venía ofreciendo por los investigadores y organismos a cargo. Los investigadores se encontraron agobiados ante la aplastante y urgente demanda de los servicios de Internet, que representaba una valiosa herramienta de producción para todos los ámbitos productivos. Ante esta evolución las organizaciones a cargo de Internet tuvieron la necesidad de reorganizarse en el año de 1989, para reflejar la realidad política y comercial de TCP/IP e Internet. Ver Figura 1.2

Figura 1.2 Estructura de la *IAB* después de la reorganización de 1989.[2]

[2] Comer, Douglas E. Redes Globales de Información con Internet y TCP/IP, p. 10

La *IAB* es un grupo de personas que establecen la políticas y directivas para el TCP/IP y la red Internet, esta organización fue originalmente conocida como Junta de Actividades Internet (*Internet Activities Board IAB*).

La IAB supervisa dos organismos:

1. La Fuerza de Tareas de Investigación Internet (*Internet Research Task Force IRTF)* establece grupos de trabajo para investigaciones de largo plazo, dichas nvestigaciones están relacionadas con los protocolos TCP/IP y con Internet en general.

2. La Fuerza de Tareas de Ingeniería Internet (*Internet Engineering Task Force IETF*) administra las necesidades y problemas de ingeniería a corto y mediano plazo.

La IRTF coordina las investigaciones relacionadas al desarrollo de TCP/IP y la arquitectura de Internet, se integra de un grupo llamado Grupo de Control de Investigaciones de Internet (*Internet Research Steering Group IRSG*), el cual tiene encomendadas las actividades relacionadas a los proyectos de investigación. Cada miembro de la IRSG tiene a su cargo un Grupo de Investigación de Internet voluntario.

Por su parte, la IETF esta dividida en doce áreas, cada una con un gerente al mando. El presidente de la IETF junto con los gerentes de cada área forman el Grupo de Control de Ingeniería de Internet (*Internet Engineering Steering Group IESG*), siendo las personas encargadas de coordinar a los grupos de trabajo de la IETF.

Otros organismos se han reunido con el fin de apoyar a la IAB, tal es el caso de la Sociedad Internet *(Internet SOCiety ISOC)*, siendo una organización interna surgida de la Sociedad Nacional de Geografía (*National Geographic Society)*, su propósito es fomentar el uso de Internet alrededor del mundo.

El Centro de Información de la Red Internet (*Internet Network Information Center InterNIC*), tiene la función de mantener y distribuir la documentación sobre TCP/IP e Internet; además, maneja el registro de las direcciones IP y los nombres de dominio, ésta últimas provenientes de su antecesor *NIC*. InterNIC es un grupo de AT&T que recibe fondos de la Fundación Nacional de Ciencia (*NFS)*.

Toda la documentación relacionada al desarrollo de TCP/IP e Internet, así como las propuestas de nuevos protocolos y sus revisiones, son compiladas en reportes técnicos llamados Requisición para Comentarios (*Request For Comments RFC)*. Además de los RFC existieron otros reportes llamados Nota de Ingeniería Internet (*Internet Engineering Note IEN*), los cuales ya no están activos.

Actualmente, están disponibles un derivado de los RFC llamados Para Tu Información (For Your Information *FYI*) y contienen comunicados relacionados al protocolo TCP/IP e Internet.

Los números asignados a las constantes del protocolo TCP/IP de Internet son administrados por la Autoridad de Números Asignados de Internet (Internet Assigned Numbers Authority *IANA*), estos números se refieren a parámetros de red, direcciones de redes especiales, nombres de servicios e identificadores para terminales y sistemas de cómputo.

CAPITULO 2. TCP/IP Y EL MODELO DE REFERENCIA OSI

CAPITULO 2. TCP/IP Y EL MODELO DE REFERENCIA OSI

2.1. GENERALIDADES

El Modelo de Referencia para la Interconexión de Sistemas Abiertos (*Reference Model of Open Systems Interconnection OSI*), integra funciones estándar a cada capa de su esquema para que cualquier tipo de arquitectura de red las integre, considerándolas como los principios uniformes para el diseño y ejecución de una suite de protocolos.

La *suite* de protocolos TCP/IP influenció sobre los estándares del Modelo de Referencia OSI, precisamente cuando la arquitectura del TCP/IP estaba siendo organizada. Aprovechando los fundamentos de TCP/IP, la Organización Internacional de Estándares (*International Organization for Standarization OSI*) agregó nuevas características a los protocolos de comunicación y acrecentó la funcionalidad de las aplicaciones de red.

Para lograr la normatividad de protocolos estándar, el gobierno de los Estados Unidos ordenó la migración al modelo OSI, y con ello, proporcionó una especificación del Perfil de Interconexión de Sistemas Abiertos del Gobierno (*Government Open Systems Interconnection Profile GOSIP*), la cual detalla los protocolos OSI que pueden ser solicitados por las instituciones gubernamentales señaladas.

Agosto de 1990, fue la fecha propuesta para que las agencias del gobierno de los Estados Unidos empezarían a integrar el modelo OSI en sus redes. La migración se espera tome algún tiempo, debido a que:

- Los protocolos OSI son más complejos que los del TCP/IP.
- Los documentos de los protocolos OSI son difíciles de obtener.
- El flujo libre de información que caracteriza el desarrollo del protocolo TCP/IP no existe en el entorno del OSI.

Mas aún, los proveedores de cómputo han descubierto que la implementación OSI y la ejecución de pruebas que son necesarias para asegurar la interconexión mediante proveedores, es un compromiso costoso y de pérdida de tiempo. Sin embargo, un interesante acercamiento a la migración del OSI es proporcionada por el software Ambiente Desarrollado para ISO (*ISO Development Environment ISODE*). ISODE es un software que habilita aplicaciones ISO para ejecutarse por encima de las

comunicaciones de TCP/IP y fue diseñado para experimentar los protocolos OSI de alto nivel sin requerir una red de redes que soporte los niveles inferiores del modelo OSI. Haciendo uso del espíritu de Internet, el software ISODE se puede obtener a través de una transferencia de archivos.

2.2. ARQUITECTURA DE REDES

Los sistemas de comunicación ejercen sus funciones a través de una ***arquitectura de red***, la cual esta definida como un conjunto de capas y protocolos. Cada capa deberá cumplir con metas definidas y de acuerdo a ellas, se colocará en cierto nivel. El número, nombre, contenido y función de las capas varia de una red a otra. No obstante, el objetivo de cada red es proporcionar servicios entre las capas, sin importar como la capa superior o inferior realiza esta labor.

La jerarquía de una arquitectura de red, tiene relación con la jerarquía de protocolos. En la agrupación más general tenemos al grupo de capas, las cuales definen su propósito principal de acuerdo a un protocolo *suite*. Cada capa integra uno o varios protocolos formando un *stack* para alcanzar sus planes; mientras que cada operación concreta de una capa esta a cargo de un protocolo simple.

El diseño de una arquitectura de red se establece con el fin de representar una jerarquía de protocolos que pueda identificar funciones independientes y específicas para cada una de sus capas; de esta manera, si se acordara sustituir alguno de los protocolos, se sabría con mayor exactitud en que capa se realizarán las modificaciones; o bien, en caso de fallas, se podría aislar el problema de acuerdo a sus características y a las de las capas del protocolo.

Asimismo, es importante establecer una arquitectura de red para lograr que las capas análogas de una máquina a otra se entiendan, utilizando los mismos procesos de ensamble y desensamble de paquetes y el mismo flujo de procesos entre las dos maquinas conectadas.

2.3 ARQUITECTURA DEL MODELO DE REFERENCIA OSI

En 1984, la Organización Internacional de Estándares (*International Organization for Standarization ISO*), en colaboración con Day y Zimmermann; diseñaron un modelo de comunicación para formalizar internacionalmente varios

protocolos. Dicho modelo, fue llamado Modelo de Referencia para la Interconexión de Sistemas Abiertos, o bien Modelo OSI[3] (*Reference Model of Open Systems Interconnection OSI)*, cuyo propósito adicional es establecer comunicación entre redes heterogéneas, fundamentando en ello los términos "sistemas abiertos".

Básicamente el Modelo de Referencia OSI establece los lineamientos para que le software y los dipositivos de diferentes fabricantes funcionen juntos.

El Modelo de Referencia OSI aplica los siguientes principios para determinar su arquitectura:

1. Se creará una capa cada vez que se detecte un propósito general diferente.
2. Cada capa tendrá asignada una función concreta.
3. La función de cada capa se seleccionará buscando definir protocolos normalizados internacionalmente.
4. Los límites de las capas deberán determinarse de acuerdo al mínimo de flujo de información requerida en las interfaces.
5. El número de capas beberá ser tan grande que cada una represente una sola función y, tan pequeño que su arquitectura sea sencilla de manejar.

El modelo en cuestión, esta sustentado en el principio de que cualquier capa puede usar los servicios de la capa inferior, sin conocer como lo capa inferior realiza esta disposición.

La arquitectura del Modelo de Referencia OSI se muestra en la Figura 2. 1

Capa	Nombre
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de Datos
1	Física

Figura 2. 1 Arquitectura del Modelo de Referencia OSI

[3] También es conocido como Modelo ISO tomando las siglas de su organización creadora *International Organization for Standarization (ISO)*

Capa 7. Aplicación

En esta capa se llevan a cabo funciones entre aplicaciones de usuario y aplicaciones del administrador de la red. La capa de aplicación proporciona servicios como la transferencia de archivos a través del Protocolo de Transferencia de Archivos *(File Transfer Protocol FTP)*.

Capa 6. Presentación

Los sistemas de cómputo ocasionalmente usan métodos variados para codificar texto y números. En esta capa se determina como los tipos de datos son codificados para poder ser intercambiados entre diferentes sistemas. La Notación de Sintáxis Resumida 1 *(Abstract Syntax Notation.1 ASN.1)* y la Representación de Datos Externa (*eXternal Data Representation XDR)* son estándares para representar mensajes codificados.

Capa 5. Sesión

Crear, mantener y terminar la conexión de red son funciones de la capa de sesión, la cual esta íntimamente relacionada con la capa de transporte. En el ejercicio de sus funciones, dicha capa controla el intercambio de mensajes durante la conexión establecida en el transporte de paquetes. El cambio en la dirección de transferencia, el reinicio de sesión después de una conexión interrumpida, etc. son algunos ejemplos de las tareas de esta capa. El protocolo de Llamada a Procedimiento Remoto *(Remote Procedure Call RPC)* esta considerado para operar en la capa de sesión.

Capa 4. Transporte

Esta capa es responsable de transportar mensajes entre dos hosts; controla el flujo de los paquetes y asegura que no contengan errores. El Protocolo para el Control de Transmisión *(Transmission Control Protocol TCP)* y el Protocolo de Datagrama de Usuario (*User Datagram Protocol UDP)* son protocolos de esta capa.

Capa 3. Red

La principal tarea de esta capa es establecer rutas virtuales entre estaciones de red, por ejemplo, cuando se transmiten paquetes [4] por una vía de nodos conmutados. El protocolo *IP* es operado en esta capa.

Capa 2. Enlace de Datos

La tarea de esta capa es asegurar la transmisión confiable de los paquetes y direccionar estaciones conectadas a un medio de transmisión. El método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (*Carrier Sense Multiple Access with Collision Detection CSMA/CD)* y el Control de Enlace de Datos de Alto Nivel *(High-level Data Link Control HDLC)* son ejemplos de operación para esta capa.

Capa 1. Física

Esta capa controla el intercambio de información en bits a lo largo de un medio de transmisión (o cable); por ejemplo, la cantidad de bits a transmitir, la unidad de voltaje y su intensidad. El estándar de interconexión *RS232* especifica características para la capa física.

2.4. ARQUITECTURA DE TCP/IP

En 1973, se concluyó que los protocolos usados eran funcionalmente inadecuados. Por lo anterior, *Vinton G. Cerf* y *Robert E. Kahn* en 1974, publicaron un documento para establecer las bases de los nuevos protocolos. Los objetivos de la arquitectura propuesta fueron:

1. Independencia entre las tecnologías subyacentes de red y la arquitectura del host

[4] En el Modelo de Referencia OSI se utiliza el término ***"paquete"*** como la unidad de datos empleada para la transmisión o recepción de datos entre sus capas.

2. Conexión universal a través de toda la red
3. Reconocimiento de paquetes de extremo-a-extremo
4. Protocolos de aplicación estandarizados

Los objetivos anteriores, dieron lugar a las siguientes características de la arquitectura de TCP/IP:

- Protocolos sin conexión en la capa de red
- Nodos como computadoras conmutadoras de paquetes
- Un grupo común de programas de aplicación
- Ruteo dinámico

Determinados los objetivos y las características de lo que debería reunir la *suite* TCP/IP, se diseño su arquitectura. La arquitectura del TCP/IP consta de cuatro capas; aunque algunos autores contemplan cinco capas, tomando a la parte de enlace de datos y la parte física como la capa 4 y la capa 5, respectivamente. Ver Figura 2. 2

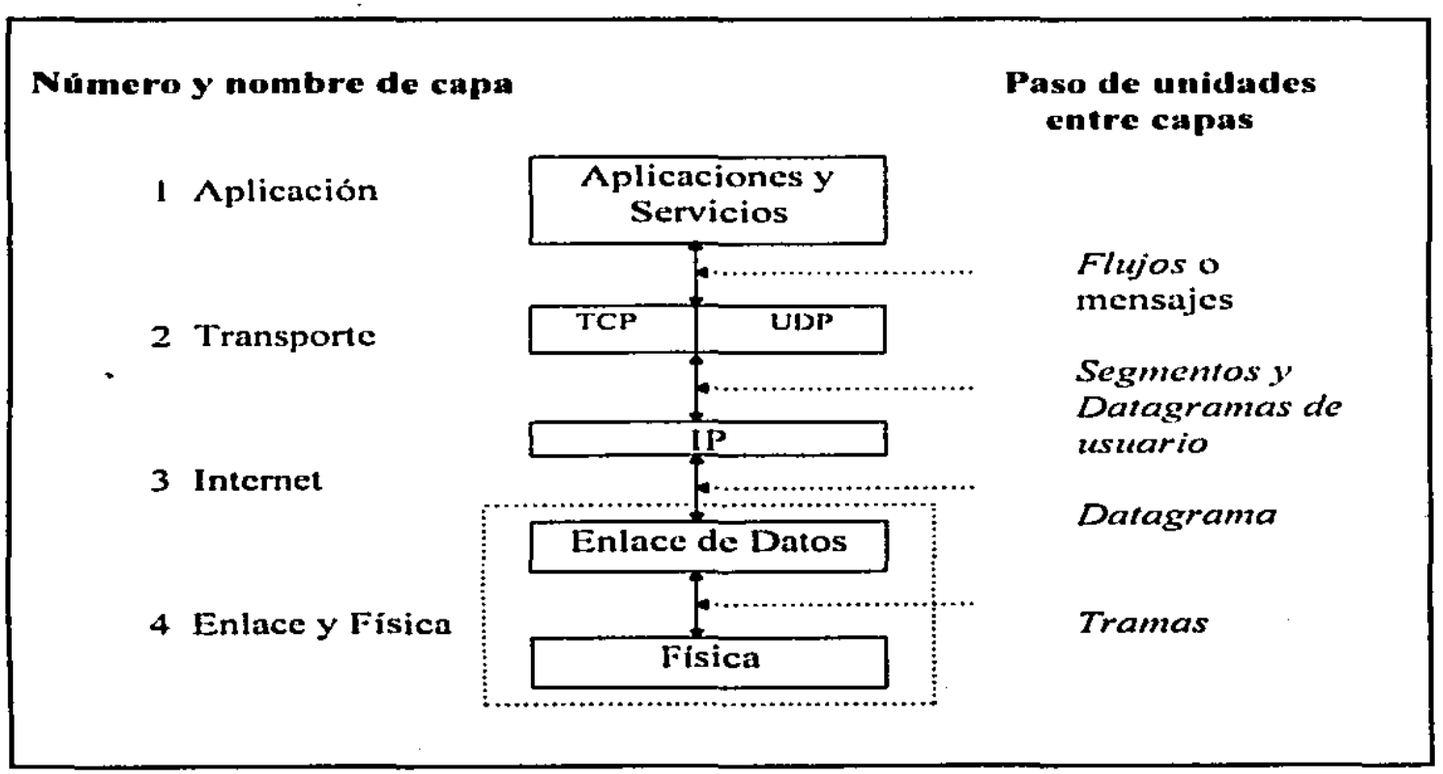


Figura 2.2 Arquitectura del TCP/IP de Internet

Capa 4. Aplicación

Mediante esta capa los usuarios disponen de un grupo de aplicaciones estándar que accesan servicios disponibles de TCP/IP, tales como el Protocolo de Transferencia de Archivos *(File Transfer Protocol FTP)*, el Protocolo de Transferencia de Correo Simple *(Simple Mail Transfer Protocol SMTP)*, el protocolo de acceso a una terminal de Red Remota (*TELNET*) y el Sistema de Nombres de Dominio (*Domain Name System DNS*).

La mayoría de aplicaciones TCP/IP soporta servidores de archivos y clientes de archivos en el Sistema de Archivos de Red *(Network File System NFS)*.

Las aplicaciones también incluyen librerías de comunicación programables, que pueden ser usadas por diseñadores de software. Una de esas librerías comprende la Interface de Programación de Socket, la cual incluye llamadas que habilitan aplicaciones para interactuar con TCP, UDP o IP. Adicionalmente, es proporcionada una librería para usarse en aplicaciones escritas en sistemas de red cliente/servidor, conocida como Llamada a Procedimiento Remoto *(Remote Procedure Call RPC)*.

Capa 3. Transporte

El Protocolo para el Control de Transmisión (*Transmission Control Protocol TCP*) envía unidades llamadas *segmentos* al IP, el cual se encarga de rutearlos al destino. TCP acepta los segmentos que llegan de IP, determina cual aplicación es la receptora, y pasa los segmentos, a esa aplicación, en el orden en que fueron enviados.

TCP proporciona, a las aplicaciones, servicios de conexión de datos confiables. TCP contiene los mecanismos empleados para garantizar que el segmento este sin errores, completo y en la secuencia correcta.

Las aplicaciones pueden invocar al otro protocolo disponible en la capa de transporte, el Protocolo de Datagramas de Usuario (*User Datagram Protocol UDP*), para enviarse recíprocamente mensajes o flujos de datos, ya sea un envío o una recepción. UDP ensambla datos en unidades llamadas *Datagramas de Usuario* o *paquetes* y se los pasa al IP para rutearlos a un destino. UDP es un servicio de comunicación sin conexión que a menudo es usado para búsquedas de bases de datos simples, es decir es un servicio que no verifica si el dato es el correcto, si está íntegro y si tien una secuencia coherente.

Capa 2. Internet

La capa Internet contiene al Protocolo Internet (*IP*), razón por la cual es también conocida como capa IP; su objetivo consiste en rutear datos entre hosts mediante direcciones IP. A través de las funciones de esta capa, los datos pueden atravesar una red o pueden ser retransmitidos a través de varias redes como si se tratara de una sola, dichos datos son transportados en unidades llamadas *Datagramas IP*.

La característica de transmisión sin conexión es asignada a la capa IP, porque todos los datagramas son enrutados independientemente e IP no garantiza la confiabilidad o la secuencia al momento de recibirlos.

Capas 1. Física y de Enlace de Datos

Estas capas, denominadas capas inferiores, interactuan con los controladores de dispositivos, ejecutan los métodos de control de acceso al medio, establecen las conexiones y señales físicas.

Las capas inferiores se encargan de recibir el datagrama IP, empaquetarlo en unidades llamadas *trama* y enviarlo hacia una red específica, desde una interface del sistema local (por ejemplo una tarjeta *Ethernet*, una tarjeta *Token-Ring* o un dispositivo de línea serial), hacia una interface destino conectada a la misma red, a través de un medio de transmisión (cable).

La capa de enlace de datos o interfaz de red, puede consistir en un dispositivo controlador para máquinas conectadas directamente, o un subsistema que utilice un protocolo propio de enlace de datos.

Las funciones de las capas inferiores son proporcionadas tanto por LANs como por WANs.

2.5. PROTOCOLO INTERNET VERSION 4

El protocolo Internet es el núcleo de la arquitectura de TCP/IP. Todas las computadoras en Internet entienden y usan IP. Las principales tareas de IP son el direccionamiento de hosts y la fragmentación de datagramas. IP no contiene alguna

función para asegurar mensajes de extremo-a-extremo o para el control de flujo; IP "hace el mejor esfuerzo" para transmitir datagramas al destino siguiente, aunque esta transmisión no esté garantizada. La cabecera de un datagrama contiene 5 o más bloques de 32 bits cada uno [5], su tamaño máximo es de 15 bloques (60 octetos), pero el tamaño más común de un datagrama es por lo menos de 5 bloques (20 octetos).

Las principales características de IP son:

- Protocolo sin conexión
- Fragmenta o divide datagramas si es necesario
- Identifica hosts a través de direcciones Internet de 32 bits
- Trabajo en conjunto con el protocolo de transporte
- Tamaño máximo del datagrama es de 65 535 bytes
- Contiene un campo llamado Suma Verificadora de la Cabecera IPv4 (*Checksum Header*)
- Campos opcionales en la cabecera
- Tiempo de vida finito del datagrama
- Tipo de envío no confiable con el "mejor esfuerzo"

Los campos en la cabecera del protocolo se muestran a continuación en la Figura 2. 3

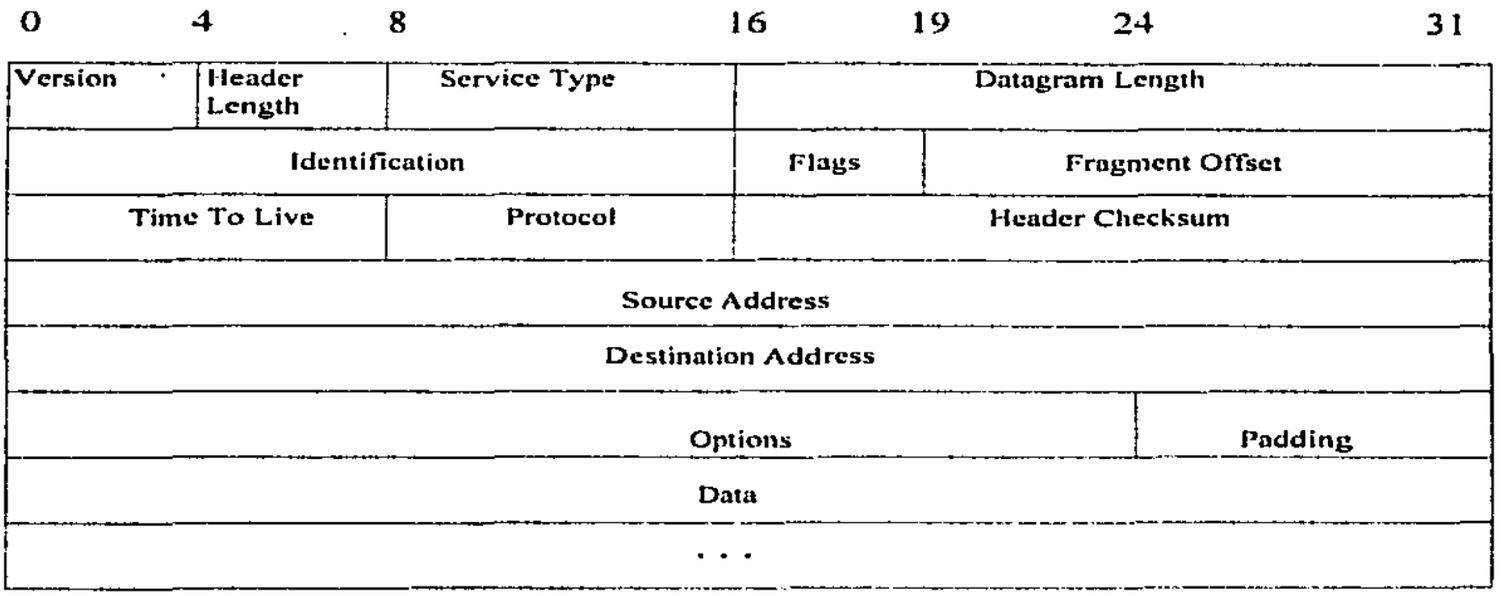


Figura 2. 3 Formato de la cabecera IPv4

[5] Un bloque de 32 bits recibe el nombre de palabra (32-bit word)

La cabecera base de un datagrama esta comprendida desde el campo *Version* hasta el campo *Header Checksum*, el espacio restante es empleado por las opciones, las direcciones IP y los datos que vienen de las otras capas de TCP/IP.

Version (4 bits): contiene el número de la versión del IP, 4 es el valor de la versión actual de IP.

Header Length (4 bits): especifica la longitud de la cabecera del protocolo en bloques de 32 bits. La cabecera más pequeña es de 5 bloques normalmente. La longitud de la cabecera de IPv4 puede ser incrementada añadiendo campos opcionales, indicados en el campo *Options*. Si ninguna opción es incluida la cabecera tiene una longitud de 5 bloques de 32 bits (20 octetos) y si alguna de las opciones es integrada la cabecera podría necesitar un relleno con ceros para completar un bloque.

Service Type (8 bits): contiene disposiciones para solicitar calidad de servicio especial para que los datagramas sean manipulados de acuerdo al criterio fijado. La Tabla 2. 4 contiene la estructura detallada de este campo:

Bits	Significado	Valores
0 - 2	Prioridad	Niveles del 0 - 7 0 = prioridad normal 7 = la más alta prioridad.
3	Indicador de tiempo de espera	0 = normal 1 = retardo
4	Conexión	0 = normal 1 = rápida
5	Indicador de seguridad	0 = normal 1 = alta
6 - 7	Reservado	

Tabla 2. 4 Valores del campo Service Type

Otra manera de representar este campo es:

0	1	2	3	4	5	6	7
Prioridad			D	T	R	SIN USO	

Los bits D, T y R especifican el tipo de transporte y si están activados:

D	Solicita procesamiento con retardos cortos
T	Solicita un alto desempeño
R	Solicita alta confiabilidad

Datagram Length (16 bits): contiene el valor de la longitud del datagrama desde la cabecera base hasta la parte de datos. Este valor es usado para calcular la longitud de los datos cuando se transfieren al protocolo de transporte. Un datagrama puede tener una longitud máxima de 65 535 octetos ($2^{16} - 1$), aunque; actualmente no existe una MTU que considere esta longitud, ni tampoco los buffers de memoria utilizados en la conmutación de datagramas la considera adecuada para su tráfico de información.

Las especificaciones de IP afirman que cualquier host debe tener la capacidad de recibir y reensamblar un datagrama mayor que 576 octetos (4 608 bits), el cual corresponde a 512 bytes de datos más las cabeceras adicionales de los protocolos. Como regla, las computadoras son capaces de procesar paquetes de mayor tamaño, por lo menos arriba del tamaño máximo que manejan las redes en las que están conectadas (por ejemplo, un paquete Ethernet).

Identification (16 bits): el identificador es un número único para un datagrama creado por el host emisor. Este campo es usado para reensamblar los fragmentos de un datagrama mediante la identificación de todas sus piezas fragmentadas.

Flags (3 bits): el primer bit esta reservado y siempre debe ser 0, el segundo bit está determinado como DF (Don't Fragment) y el tercer como MF (More Fragments). Este campo controla el manejo de los datagramas cuando se necesita fragmentación. Si el DF es 1, el datagrama IP no es fragmentado bajo ninguna circunstancia, si se deseara fragmentarlo cuando su longitud sea mayor a la MTU, el valor 1 del DF no lo permitirá y el datagrama será eliminado enviando un mensaje de regreso al host origen. El bit MF es 1, significa la existencia de varios fragmentos y si MF es 0 quiere decir que el fragmento es el último o el único del datagrama.

Fragment Offset (13 bits): Si el bit MF del campo *Flags* es 1, este campo contiene la posición de inicio del fragmento en el datagrama completo. El host receptor puede usar el valor de este campo para reconstruir el datagrama original correctamente. Este campo debe contar las posiciones de un datagrama en octetos y la máxima longitud de un datagrama será $(8*2^{13}) - 1 = 65\ 535$. El proceso de fragmentación se describe más adelante.

Time To Live (8 bits): en este campo el host emisor especifica cuanto tiempo puede permanecer el datagrama en la red antes de ser eliminado (4.25 equivale a 11111111). El tiempo de vida (TTL) es usualmente igual al máximo número de nodos que el datagrama puede visitar. Si este campo es igual a 0, el datagrama debe ser eliminado por el proceso actual, evitando la circulación infinita de un datagrama dentro de la red. En este caso, el emisor del datagrama recibe un mensaje del Protocolo de Control de Mensajes Internet (*Internet Control Message Protocol ICMP*) informando de tal situación.

Las máquinas UNIX colocan un valor entre 15 y 30 en este campo. Algunos sistemas antigüos decrementan este campo de 5 en 5, mientras que las nuevas versiones lo reducen en 1. También se recomienda especificar en este campo, el doble del número de hosts por recorrer en la ruta más larga del trayecto de transmisión, a esta ruta se le llama algunas veces *diámetro de internet*.

Protocol (8 bits): contiene el identificador del protocolo de transporte asignado para manipular el datagrama en la capa de transporte del TCP/IP. Por ejemplo, para TCP el identificador es 6, para UDP es 17 y para ICMP es 1. Estas constantes numéricas son determinadas por IANA. En la Tabla 2. 5 se listan algunos ejemplos de constantes numéricas de protocolos de transporte que se asignan actualmente.

CONSTANTE NUMÉRICA	ABREVIATURA	NOMBRE
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Managment
6	TCP	Transmission Control
17	UDP	User Datagram
27	RDP	Reliable Data

Tabla 2. 5 Constantes numéricas para el campo *Protocol*

Header Checksum (16 bits): contiene una suma verificadora de todos los campos de la cabecera IPv4. Este control de chequeo previene a los nodos de trabajar con valores falsos de los campos de la cabecera IPv4. Por eficiencia, el campo *Data* contenido en el datagrama no es verificado; esto lo realiza el receptor dentro del protocolo de transporte TCP. Desde luego el datagrama es alterado al momento de decrementar el campo de TTL, por tal razón es importante que el campo checksum tenga un diseño eficiente. El valor del campo *Header Checksum*, se determina considerando el encabezado IPv4 como una secuencia de enteros de 16 bits, sumándolos mediante el complemento

aritmético a uno, y después tomando el complemento a uno del resultado. Antes de los cálculos este campo es inicializado a 0.

Source Address y Destination Address (32 bits): la dirección Internet, tanto del emisor como del receptor son colocadas en éstos dos campos. Mas adelante se explica la manera en que son creadas y representadas las direcciones.

Data (longitud variable): muestra el comienzo del área de datos de un datagrama.

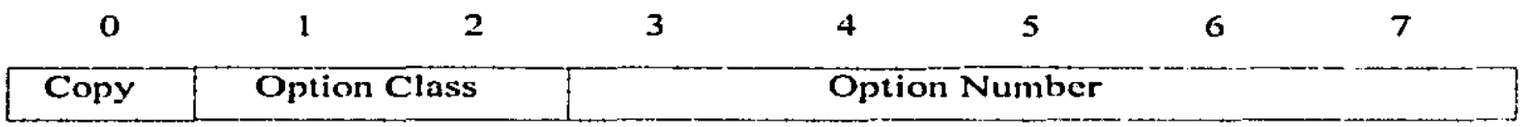
Options y Padding (longitud variable): el campo *Options* es usado para especificar tareas especiales y representa una extensión de la cabecera base. La cabecera IPv4 es expandida para incluir éstas opciones.

El campo *Padding* es un conjunto de ceros utilizados como relleno del campo *Options*, con el objeto de asegurar que la extensión de la cabecera sea un múltiplo exacto de 32 bits; su longitud varía según la longitud total de las opciones seleccionadas.

OPCIONES IPv4

En los datagramas IPv4, las opciones son colocadas como suplemento o extensión de la cabecera base de IPv4 con el propósito de que en la cabecera no sea reservado más espacio del necesario; de esta manera, la cabecera se mantiene tan pequeña como es posible.

La longitud del campo de opciones de IPv4 varía de acuerdo a la opción seleccionada. Cuando se decide incluir una o más opciones en un datagrama, aparecen contiguas una de otra. Cada opción debe llevar un código de un octeto que la identifique, dividido de la forma siguiente:



Copy (1 bit): controla la forma en que los ruteadores manipulan las opciones durante la fragmentación:

COPY	SIGNIFICADO
1	La opción se debe copiar en todos los fragmentos

0	La opción sólo se debe de copiar en el primer fragmento

Option Class y Option Number (2 bits y 5 bits, respectivamente): especifican la clase general de opción y establecen una opción específica en esta clase.

OPTION CLASS	SIGNIFICADO
0	Control de red o datagrama
1	Reservado para uso futuro
2	Depuración y medición
3	Reservado para uso futuro

La Tabla 2. 6 muestra las opciones posibles para un datagrama IP, de acuerdo a los valores de los campos *Option Class y Option Number*.

OPTION CLASS	OPTION NUMBER	LONGITUD	OPCIONES IPv4
0	0	-	Fin de la lista de opciones (*End Option List*). Se utiliza como un indicador para la lista de opciones que no terminan al final.
0	1	-	Alinear octetos en una lista de opciones (*No operation o Padding*).
0	2	11	Seguridad (*Security*)
0	3	variable	Ruta de Origen no Estricto (*Loose Source Route*)
0	7	variable	Registro de Ruta (*Record Route*)
0	8	4	Identificador de flujo (obsoleto)
0	9	variable	Ruta de Origen Estricto (*Strict Source Route*)
2	4	variable	Sello de Tiempo Internet (*Timestamp*)

Tabla 2. 6 Valores del posibles del campo *Options* sin considerar el subcampo *Copy*

El código de opción puede representarse en valores decimales de acuerdo a su tipo:

CODIGO BINARIO	CODIGO DECIMAL	OPCION
10001001	137	*Strict Source Route*
10000011	131	*Loose Source Route*
00000111	7	*Record Route*
01000100	68	*Timestamp*
10000010	130	*Basic Security*
10000101	133	*Extended Security*

Cada una de las opciones tiene una longitud variable y tiene una estructura propia. Las opciones disponibles en IPv4 son las siguientes:

Source Route

Mediante esta opción, la cabecera IP es seguida por una lista de direcciones Internet a través de las cuales el datagrama debe pasar, prescribiendo un ruta exacta. Las rutas pueden ser de dos tipos: Ruta de Origen Estricto (*Strict Source Route*) y Ruta de Origen no Estricta (*Loose Source Route*).

La opción *Strict Source Route* es una secuencia de direcciones IP de los ruteadores que van a ser recorridos desde el origen hasta el destino. Este servicio puede ser usado como parte de un programa de seguridad, o podría ser invocado por un programa de administración de red que prueba si una ruta esta disponible. La siguiente figura muestra el formato de la opción *Strict Source Route*:

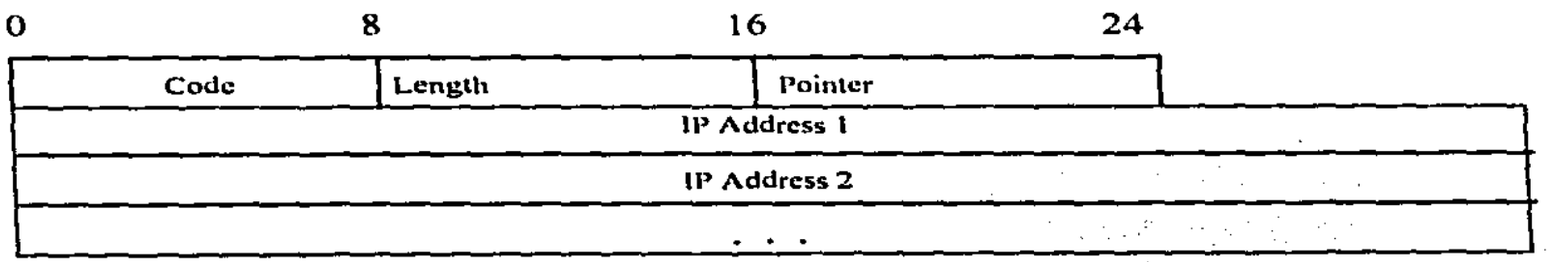


Figura 2. 7 Formato de la opción *Strict Source Route*

Por otra parte, la opción *Loose Source Route* es una lista de direcciones IP de los ruteadores que van a ser recorridos desde el origen hasta el destino. La diferencia con la opción *Strict Source Route*, es que en la actual las direcciones de los ruteadores son

contempladas como un grupo de señales o marcas que ayudarán a encontrar el camino para llegar al host destino. El datagrama visitará las direcciones de la lista, pero también visitará nodos intermedios que estén sobre el camino de los señalados. Esta opción puede ser útil cuando se trata de rutear datos hacia lugares remotos de una red.

Record Route

El campo de Registro de Ruta (*Record Route*) contiene una lista de direcciones IP de los ruteadores visitados por un datagrama. Cada ruteador a lo largo del camino del datagrama agrega su dirección IP de salida a la lista recibida.

La longitud del campo es fijada por el emisor y es posible que todo el espacio sea agotado antes de que el datagrama llegue a su destino, en este caso; el ruteador actual simplemente envía el datagrama sin añadir su dirección.

Timestamp

El campo opcional Sello de Hora (*Timestamp*) contiene una lista inicial vacía y cada ruteador, a lo largo del camino, desde el origen hasta el destino coloca sus datos en él. Cada entrada a la lista contiene 2 datos de 32 bits: la dirección IP del ruteador que proporciona la entrada y un entero de sello de hora de 32 bits.

Existen tres formatos para el campo sello de hora, los cuales establecen como los ruteadores deben suministrar el sello de hora. Los formatos son representados de acuerdo a los tres criterios siguientes:

- Registrar de sello de hora solamente; omitiendo direcciones IP
- Anteponer a cada sello de hora una dirección IP
- Las direcciones IP se especificarán por el emisor; un ruteador sólo registra un sello de hora si la próxima dirección IP en la lista concuerda con la dirección del ruteador actual

El espacio puede agotarse si el primero o segundo formato es usado. Hay un campo de flujo desbordado (*overflow*) es utilizado para contar el número de nodos que pudieron no registrar su sello de hora.

Las opciones de Registro de Ruta y Sello de Hora son útiles para la administración de red.

Security

La opción de seguridad fue definida para satisfacer las necesidades de los usuarios militares y del gobierno, y el contenido del campo de seguridad fue colocado por el Departamento de Defensa de los Estados Unidos. Esta opción es frecuentemente omitida en implementaciones comerciales.

DIRECCIONAMIENTO IPv4

La comunicación entre las cuatro capas de la arquitectura de TCP/IP, necesita de de cuatro tipos de direcciones distintas:

1. Una dirección de interface física (por ejemplo una dirección Ethernet)
2. Una dirección Internet
3. Una dirección del protocolo de transporte
4. Un número de puerto

Dos de las direcciones anteriores; la dirección Internet y la dirección del protocolo de transporte, son empleadas en campos dentro de la cabecera del protocolo IP (*Protocolo, Source Address y Destination Address*). La más importante de estas dos direcciones es la dirección IP, la cual tiene un campo de 32 bits (4 octetos) en valores binarios y sirve para asignar direcciones Internet a todos los hosts.

Existen cinco clases de direcciones IP que cuentan con un identificador de red y un identificador de host de diferentes longitudes. El identificador de red (*netid*) define la red en la cual un host esta situado y es proporcionado por la InterNIC, por su parte, el identificador de host (*hostid*), señala un host específico dentro de la red y es determinado por la organización que representa a la red [6]. La Figura 2. 8 muestra el esquema de las cinco clases de direciones:

[6] Los identificadores de hosts con todos los bits puestos en 0 ó 1 están reservados para funciones especiales.

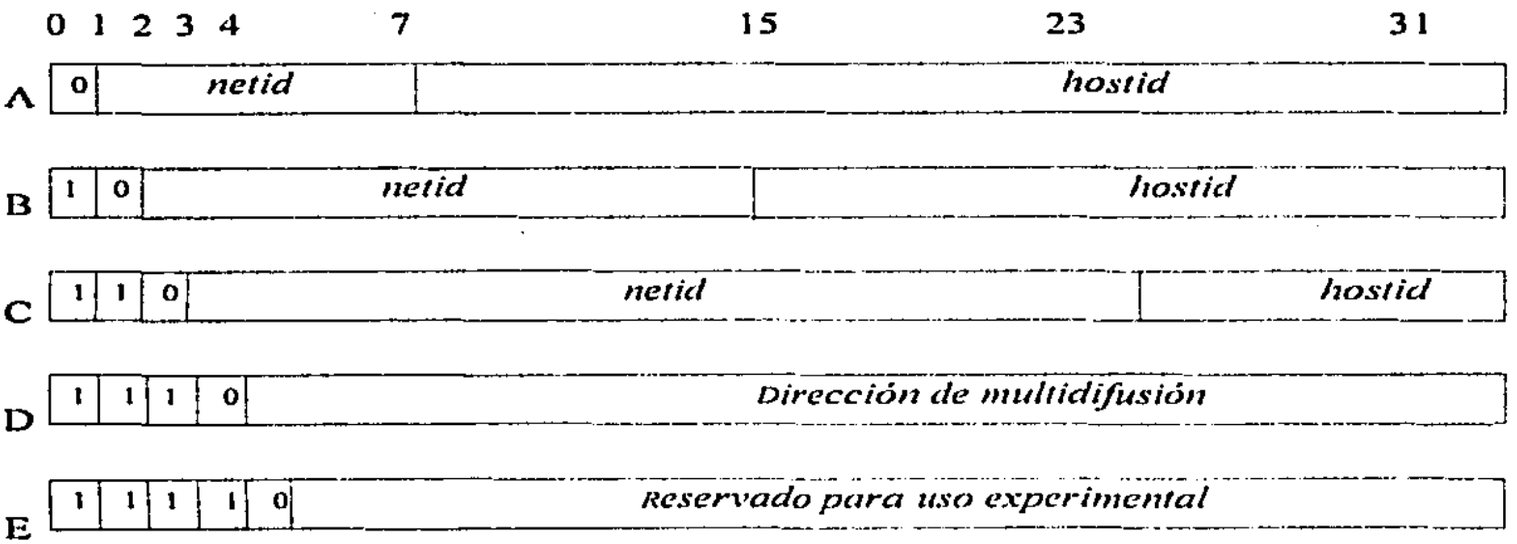


Figura 2. 8 Esquema de las clases de red en IPv4

Cada dirección IP con disponibilidad pública debe tener una de las tres clases A, B o C de acuerdo a la magnitud de la red.

Clase A para redes grandes
Clase B para redes medianas
Clase C para redes pequeñas

La clase D es usada para efectuar procesos de multidifusión, se asigna a grupos de sistemas distribuidos por toda Internet. La clase E, esta reservada para uso experimental.

Los primero cuatro bits identifican la clase de dirección:

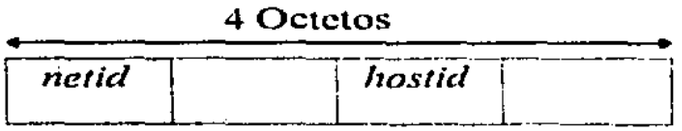
BITS DE INICIO	CLASE	RANGO DECIMAL
0XXX	A	0-127
10XX	B	128-191
110X	C	192-223
1110	D	224-239
1111	E	240-255

Las organizaciones con redes privadas se apegan a los convencionalismos de TCP/IP y utilizan direcciones de la clase A, B y C.

La asignación de direcciones IP la efectua InterNIC con el proposito de asegurar que cada una de ellas sea única en Internet. InterNIC registra todas las direcciones IP, de acuerdo al tamaño de la red que solicita el servicio, cada clase de dirección se relaciona con el tamaño de la red e InterNIC asigna uno, dos o tres octetos con valores constantes para la clase A, B y C respectivamente. Partiendo del hecho de que una direccion IP consta de 32 bits (4 octetos), tenemos la siguiente representación:

Direcciones de la clase A

32.10.5.81
32.45.4.7
32.87.19.4



Direcciones de la clase B

128.247.5.95
128.247.5.15
128.247.4.131
128.247.4.84

Direcciones de la clase C

223.247.102.95
223.247.102.96
223.247.102.97

ASIGNACIÓN DE NOMBRES A LAS DIRECCIONES IP

Las direcciones IP son identificadores numéricos fáciles de procesar en cualquier equipo eléctrico; sin embargo, para el usuario es más sencillo recordar un nombre que un número al hacer referencia a un host. Por tal razón, una dirección IP es dividida en jerarquías, llamadas dominio y subdominios, los cuales reciben un nombre en particular.

La responsabilidad para asignar nombres de dominio es delegada a un administrador de dominios, quien a su vez, puede crear subdominios y delegar la autoridad a alguien más en cada subdominio. Los subdominios pueden ser particionados tantas veces como se desee y el límite lo permita.

El dominio y los subdominios tienen una estructura jerárquica, de lo general a lo particular y son separados por un punto.

Existen nombres definidos por InterNIC para nombres de dominio y son los siguientes:

com	Para organizaciones comerciales
edu	Para instituciones educativas
gov	Para organismos gubernamentales
mil	Para organizaciones militares
net	Para sistemas de ejeccución de servicios de red
org	Para organizaciones diferentes a las comerciales
int	Para las organizaciones de grupos internacionales
nato	Para la Organización del Tratado del Atántico del Norte

De esta manera si se pretende conectar una red a Internet tendríamos que:

- Determinar el número de hosts que tendrán el servicio,
- Identificar la clase de red correspondiente al número de hosts
- Solicitar un número en *netid*
- Determinar los números y/o jerarquías para *hostid*
- Obtener los nombres de dominio y subdominio para relacionarlos al *netid* y al *hostid*

Ejemplo de una dirección IP usando nombres de dominios:

servidor.unam.mx 132.248.10.1

Observe que el número correspondiente al dominio es el primero en una dirección IP de forma numérica, mientras que en la dirección por nombre el dominio es lo que aparece al final.

PROCESO DE FRAGMENTACION EN IPv4

El proceso de fragmentación se lleva a cabo a través de los campos: *Identification, Flags y Fragment Offset*. Cuando un ruteador fragmenta un datagrama, cada parte debe ser separada en múltiplos de ocho octetos, llamados bloques de fragmentos o simplemente fragmentos. El campo *Fragment Offset* toma la posición

inicial de cada fragmento, donde cada posición tiene un valor de 0, 8, 16, etc. Dicho campo tiene la capacidad de identificar de 0 a 8192 fragmentos (2^{13} gracias a su longitud de 13 bits).

Los fragmentos son enviados uno a uno hasta su destino, el cual esta encargado de reensamblarlos. El campo *Identification*, permite asociar un fragmento con otros concluyendo que, fragmentos con un mismo identificador pertenecen al mismo datagrama. El valor del campo *Fragment Offset* ayuda a conservar el orden de los fragmentos al momento de su reensamble; ya que éstos pueden llegar al nodo receptor en un orden distinto al que fueron enviados. De acuerdo al valor que guarde el campo *Flags* es posible saber si el datagrama esta fragmentado y si el fragmento actual es único, el último de todo el datagrama o si existen más fragmentos consecutivos.

Cada fragmento que llega es comparado de acuerdo a los valores de los campos *Identification, Source, Destination y Protocol*, los que coinciden se van ensamblando en un datagrama como van llegando. Existe un inconveniente dentro del protocolo IP al omitir la longitud del datagrama, puesto que el campo *Total Lenght* en un fragmento revela sólo la longitud del datagrama y no la del fragmento en sí; con lo cual el nodo receptor tiene dificultades para asignar el espacio necesario de memoria y disponerla para un datagrama en el proceso de reensamble.

La omisión anterior de IP significa que el receptor tiene que calcular un espacio en memoria para reservarlo al siguiente fragmento del cual ignora su tamaño. Los fabricantes de hardware manejan este problema en diferentes sentidos. Algunos destinan pequeños espacios de memoria incrementales para esperar y alojar a los fragmentos venideros y cuentan con memoria fija para recibir datagramas completos.

Una de las características del proceso de fragmentación del IPv4 consiste en que un datagrama puede ser fragmentado en cada ruteador que visita si su MTU no permite transmitir un datagrama completo.

CAPITULO 3.
PROTOCOLO INTERNET VERSION 6.

CAPITULO 3. PROTOCOLO INTERNET VERSION 6

3.1. GENERALIDADES

El Protocolo Internet versión 6 (*IPv6*) o Protocolo Internet de la Próxima Generación (*Internet Protocol Next Generation IPng*) es el resultado de los esfuerzos de la IETF durante tres años (1993-1996). Este protocolo fue recomendado por la IETF en la reunión de Toronto el 25 de julio de 1994, y documentado en el RFC 1752 titulado "Recomendación para el Protocolo IP de la Siguiente Generación" (*The Recommendation for the IP Next Generation Protocol*).

La idea de cambiar la versión actual de IP (*IPv4*), surgió originalmente de la premisa de que las direcciones de 32 bits son ineficientes, cuando se trata de representar lógicamente a los hosts y la estructura jerárquica de las redes y subredes de Internet.

Para encontrar solución a la ineficiencia de las direcciones de 32 bits, se determinaron dos vías de análisis. La primera, consistió en corregir el sistema de direcciones, el cual era demasiado rígido, ya que por cada clase de red, A, B, C, D o E disponían de un número limitado de direcciones asignadas casi en su totalidad. La segunda vía de análisis se orientó a la creación de un nuevo IP que permitiera incrementar la capacidad de direccionamiento del nivel de red y dispusiera de nuevos servicios de Internet.

La IETF, convocó a toda la comunidad a participar en el proceso de estandarización, por lo cual investigadores, fabricantes de computadoras, vendedores de hardware y software de red, programadores, administradores, usuarios, compañías telefónicas y televisoras por cable presentaron sus requerimientos y propuestas para el diseño de un nuevo IP.

Varios grupos de trabajo elaboraron propuestas para un nuevo IP; algunos de los modelos fueron los siguiente:

1. TCP y UDP sobre Direcciones más Grandes (*TCP and UDP over Bigger Addresses TUBA*).
2. IP sobre IP (*IP over IP*)
3. Encapsulación de Direcciones IP (*IP Address Encapsulation IPAE*)
4. Protocolo Internet Simple (*Simple IP SIP*)

5. Protocolo Internet P (*"P" Internet Protocol PIP*)
6. Plus del Protocolo Internet Simple (*Simple IP Plus SIPP*)
7. Arquitectura Común para el Internet (*Common Architecture for the Internet CATNIP*)

Después de varios consensos, la IEFT seleccionó la propuesta SIPP y la depuró, tomando en cuenta las cualidades de las versiones en competencia y suprimiendo sus deficiencias; hasta conceptualizar lo que después se llamaría IPv6. La evolución del protocolo IPng se llevó a cabo según se muestra en la Figura 3. 1

Julio 1994	Informe de Ipng en Toronto
Agosto 1994	Primeras implementaciones de prueba
Septiembre 1994	Publicación de las primeras especificaciones como recomendaciones Internet
Diciembre 1994	Unión de documentos en una proposición estándar
Julio 1995	Primeras versiones beta del protocolo
Febrero 1996	Fin de las pruebas a gran escala y salidas de los protocolos de producción

Figura 3. 1 Evolución de IPng

El nombre asignado al nuevo IP, causó conflictos, cuando la IAB publicó el nuevo IP como IP versión 7, la gente se confundió preguntándose por las versiones 5 y 6. El problema se originó porque el *Protocolo ST* experimental (*Internet STream Protocol* [7]) estaba asignado con la versión 5 y uno de los documentos de la IAB reportó a la versión actual (IPv4) como la versión 6; y por lo tanto, la siguiente versión sería la 7.

Ante la confusión anterior, la IETF asignó el nombre de "IP la Próxima Generación", basado en una serie popular de televisión, y a partir de esto, el desarrollo del nuevo IP estaría denominado como IP Next Generation (*IPng*).

Cabe señalar que el nombre del nuevo IP, ha sido empleado indistintamente como IPv6 o IPng, pero en realidad el nombre oficial del protocolo Internet es IPv6. La denominación IPng fue usada durante las discusiones y propuestas en torno a la nueva versión IP.

[7] El Protocolo ST es un protocolo experimental desarrollado como adjunto a IP para soportar transportes en tiempo real de datos multimedia.

3.2. CARACTERISTICAS

El nuevo protocolo Internet de TCP/IP (IPv6) conserva las características funcionales del IPv4, optimiza aquellas que eran poco o nada empleadas a través de opciones. Además, incluye ocho características adicionales. Ver Figura 3. 2

NUEVAS CARACTERÍSTICAS DE IPv6	IMPLEMENTACIÓN
1. Direcciones más largas	* La dirección IP aumenta de 32 a 128 bits.
2. Formato de cabecera simplificado	* Campos suprimidos, sustituidos por otros o convertidos en cabecera suplementaria.
3. Opciones mejoradas a través de cabeceras suplementarias.	* Las opciones IPv6 estan contenidas en cabeceras suplementarias de longitud variable.
4 Cabeceras de autenticidad y de confidencialidad	* Herramientas de criptografía para autenticidad de usuarios e integridad de datos.
5. Posibilidades de autoconfiguración	* Configuración "Plug and Play" de direcciones.
6. Posibilidades para la opción "Ruta de Origen" (Source Route)	* Difusión de vías de ruteo en redes y subredes mediante el Protocolo de Ruteo Demandado por el Origen *(SDRP)* [8].
7. Una transición de IPv4 a IPv6 sencilla y flexible.	* Compatibilidad entre nodos IPv4 y nodos IPv6. * Hosts y ruteadores de IPv4 pueden ser instalados en cualquier momento sin requisistos previos. * Los hosts y ruteadores de IPv4 no necesitan redireccionamiento. * Costo bajo de la puesta en marcha, porque se requiere poco o nada de trabajo preparativo.
8. Posibilidades de calidad de servicio.	* Flujos etiquetados (con prioridad) * Servicio de "tiempo real".

Figura 3. 2 Ocho nuevas características de IPv6 sobre IPv4

[8] Source Demand Routing Protocol SDRP

3.3. CRITERIOS TECNICOS

Los criterios técnicos sobre los cuales esta sustentado IPv6, tienen origen en los requerimientos, presentes y futuros, solicitados por fabricantes de computadoras, vendedores de hardware y software de red, programadores, administradores, usuarios, compañías telefónicas y televisoras por cable.

Los criterios técnicos han sido clasificados por temas. IPv6 considera:

* **Especificación completa**. Descripción completa de IPv6 en documentos específicos disponibles al público. Las especificaciones referentes a la transición y autoconfiguración de direcciones son requeridos para lograr completar este criterio técnico.

* **Simplicidad Arquitectónica**. Funciones simples y bien definidas dentro del contexto de las demás capas de protocolo TCP/IP.

* **Escala**. Identifica y direcciona por lo menos mil millones de redes y 2^{128} direcciones de hosts.

* **Flexibilidad topológica**. La arquitectura de ruteo y los protocolos IPv6 permiten diferentes topologías de red. El diseño de IPv6 no restringe la ejecución de las topologías de red, excepto para limitar el número de saltos a 255 en la ruta de un paquete desde su origen hasta su destino.

* **Ejecución**. La simplicidad de procesos, el formato de la cabecera y la eliminación de algunos campos, permite a IPv6 una eficiente ejecución en el manejo de los datos.

* **Servicio robusto**. El servicio de red, su ruteo y los protocolos de control son confiables y robustos.

* **Transición**. Métodos de transición claros y realistas.

* **Independencia del medio**. Independencia con la red física, ya sea LAN, MAN y WAN, con una de velocidad de hasta de cientos de gigabits por segundo (100Gbps).

* **Servicio de datagramas**. Es conservado el servicio de envío de datagrama sin conexión.

* **Facilidad de configuración**. Configuración y puesta en marcha sencillas; ofrece configuración automática de hosts y ruteadores.

* **Seguridad**. Capa de red segura, disponiendo de operaciones para la autenticidad o la criptografía de usuarios y datos.

* **Nombres únicos**. Asignación de nombres únicos, permitiendo el direccionamiento global y único de cada equipo.

* **Acceso a estándares**. El protocolo que define IPv6, sus protocolos asociados y RFCs relacionados estan disponibles al público como el IPv4 y no hay cuotas de licencia para la implementación o la venta del software relacionado a especificaciones de IPv6.

* **Soporte Multicast**. Difusión de grupo (*multicast*)

* **Clases de servicio**. El protocolo IPv6 permite a los controladores de red asociar paquetes con clases de servicio particulares, mediante el campo *Flow Label* de su cabecera.

* **Movilidad**. Soporte de hosts móviles en redes o subredes.

* **Protocolo de control**. Incluye soporte básico de prueba y rastreo de redes, como los presentes en IPv4 Ping y Traceroute.

* **Soporte de redes privadas**. Permite a los usuarios la construcción de redes privadas sobre la infraestructura básica de Internet. Ambas, las redes basadas en IP privado y las redes basadas en IP no privado deben ser soportadas.

* **Soporte de encapsulado**. La encapsulación de otros protocolos en su propia cabecera, es una de las capacidades de IPv6.

3.4. DIRECCIONAMIENTO EN IPv6

En el IPv6, cada dirección ocupa 16 octetos, lo cual indica que se pueden soportar un amplio número de identificadores de direcciones IP. La inmensa cantidad de cifras direccionables del IPv6 no nos permite comprender su magnitud, necesitamos relacionarla con alguna otra cantidad cotidiana.

Una forma de entender el tamaño de espacio de direcciones IPv6, es relacionando la magnitud con el tamaño de la población: el espacio de direcciones es

tan grande que cada persona en el planeta puede tener direcciones suficientes como para poseer una red de redes tan grande como la Internet actual. Otra manera de comprender el tamaño es relacionarlo con el agotamiento de direcciones. Por ejemplo, consideremos qué se necesitaría para asignar todas las posibles direcciones. Un entero de 128 bits puede manejar 2^{128} valores. Si las direcciones se asignaran a razón de un millón de direcciones por milisegundo, tomaría alrededor de 20 años asignar todas las direcciones posibles [9]

REPRESENTACIÓN DE DIRECCIONES IPv6

Las direcciones IPv6 se representan en ocho bloques de dos octetos cada uno en valor hexadecimal. Por ejemplo:

1) Dirección decimal de 128 bits expresada en dieciséis bloques de octetos

250.36.145.230.255.255.255.255.0.0.17.128.150.10.255.255

es equivalente a la siguiente dirección de ocho bloques de dos octetos en valor hexadecimal

FA24:91E6:FFFF:FFFF:0:1180:96A:FFFF

Hay tres formas convencionales de representar las direcciones IPv6 :

I. Siguiendo el esquema **x:x:x:x:x:x:x:x**, donde las x representan los valores hexadecimales de los ocho bloques de dos octetos cada uno.

Por ejemplo:

1) ABCD:98BA:1234:7865:FEDC:98BA:5432:0123

2) 1156:800:41AF:0:0:0:9D6B

No es necesario indicar todos los ceros que hay por delante de un nombre hexadecimal, basta con colocar por lo menos una cifra en cada campo.

II. El método para alojar direcciones IPv6 muestra la comodidad de colocar bits a 0 en medio de las direcciones. Sin embargo, para una escritura fácil y una sintáxis adecuada es sugerido se supriman éstos ceros. La escritura de dos "::" indica uno o varios grupos

[9] Ob. Cit. Comer, Douglas E., p. 510, 511

de 16 bits iguales a 0. Los "::" sólo pueden aparecer una vez en la dirección. Por ejemplo:

1) La dirección multicast FF03:0:0:0:0:0:98 se representaría FF03::98.
2) La dirección de enlace local FE80:543D:1234:9876:0:0:0:15 se representaría FE80:543D:1234:9876::15

III. Otra forma alternativa, cuando deseamos referirnos a un entorno mixto de nodos IPv6 e IPv4, es **x:x:x:x:x:x:d.d.d.d**, donde los 'x' son valores hexadecimales y los 'd' son valores decimales. Ejemplos :

1) 0:0:0:0:0:0:102.95.13.40

2) 0:0:0:0:0:129:245.144.79.6

o bien; con el formato comprimido:

1a) ::102.95.13.40

2a) ::129.245.144.79.6

Jerarquía de direcciones IPv6

Para dividir la dirección IPv6 se consideran dos puntos importantes:

- Cómo administrar la asignación de direcciones
- Cómo transformar una dirección en una ruta

El primer punto, se refiere al diseño de la jerarquía de autoridad de la cual se desprenden otros niveles. En IPv4 se utilizan dos niveles de prefijos de red asignados por la autoridad Internet y sufijos de host determinados por la organización que representa a la red. Por su parte, IPv6 permite la existencia de una jerarquía de multiniveles o jerarquías múltiples, gracias a su amplio espacio de direcciones.

Con respecto al segundo punto, éste se enfoca a la eficiencia computacional: verificación de datagramas por cada ruteador y elección de una ruta hacia su destino. Asi para mantener bajo el costo de los ruteadores de alta velocidad, el tiempo de procesamiento requerido para elegir una ruta debe ser bajo.

Por lo anterior, los diseñadores de IPv6 proponen asignar clases de direcciones de manera similar que IPv4, distinguiendo cada tipo de dirección de acuerdo a su prefijo.

El tipo de direcciones IPv6 se determina con los primeros ocho bits de la dirección. El campo de longitud variable que identifica al tipo de dirección es llamado Prefijo del Formato (*Format Prefix FP*). La asignación de éstos prefijos se muestra en la Tabla 3. 3:

TIPO DE DIRECCION (Allocation)	**PREFIJO BINARIO** (Binary Prefix)	**PARTE DEL ESPACIO DE DIRECCION** (Fraction of Address Space)
Reservado para direcciones de compatibilidad con IPv4	0000 0000	1/256
No asignado	0000 0001	1/256
Reservado para direcciones NSAP	0000 001	1/128
Reservado para direcciones 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
Globales de unidifusión mediante proveedor	010	1/8
No asignado	011	1/8
Reservado para direcciones de unidifusión geográficas	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
Unidifusión de enlace local	1111 1110 10	1/1024
Unidifusión de sitio local	1111 1110 11	1/1024
Multidifusión	1111 1111	1/256

Tabla 3. 3 Prefijos de los tipos de direcciones de IPv6

TIPOS DE DIRECCIONES IPv6

Las direcciones IPv6 son de 128 bits de longitud, y pueden identificar a interfaces individuales o a un conjunto de ellas. Existen tres tipos de direcciones IPv6:

1. **Dirección de unidifusión** (*unicast*): identifica a una interface. Cuando un paquete es enviado a una dirección unidifusión, es conducido directamente a la interface identificada con esa dirección.

2. **Dirección de grupo** (*anycast*): identifica a un grupo de interfaces que pertenecen generalmente a nodos diferentes. Cuando un paquete es enviado a una dirección de grupo, es conducido a una de las interfaces identificadas con esa dirección. La interface que reciba el paquete será la más cercana de acuerdo al cálculo de distancia de los protocolos de ruteo.

3. **Dirección Multidifusión** (*multicast*): identifica a un grupo de interfaces que pertenecen generalmente a nodos diferentes. Cuando un paquete es enviado a una dirección de grupo, es conducido a todos las interfaces identificadas con esa dirección.

IPv6 no contiene direcciones de difusión (*broadcast*), las funciones de éstas se concedieron a las direcciones multicast.

DIRECCION DE UNIDIFUSION (UNICAST) EN IPv6

Existen varios tipos de direcciones para unidifusión y se podrán definir tipos adicionales en el futuro. Los tipos de direcciones "unicast" actuales son las siguientes:

1. Direcciones de compatibilidad con IPv4
2. Direcciones Punto de Acceso al Servicio de Red (*Network Service Access Point NSAP*)
3. Direcciones del Protocolo de Intercambio de Paquetes en Red Novell (Netware's *Internetwork Packetl eXchange IPX*)
4. Direcciones para enlace de uso local
5. Direcciones para sitios de uso local

Un nodo IPv6 puede tener mucho o poco conocimiento de la estructura interna de la dirección IPv6, dependiendo si se trata de un host o de un ruteador.

Un nodo podría tener una dirección unidifusión sin estructura interna; es decir sin jerarquías, como se ve en la Figura 3. 4

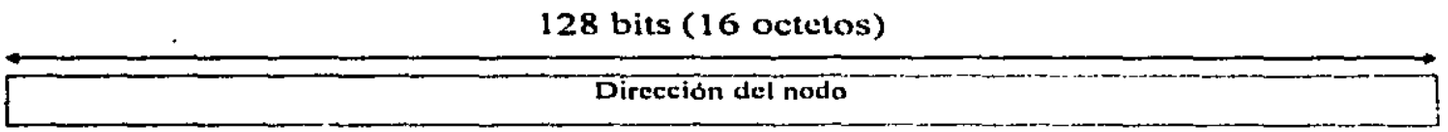


Figura 3. 4 Dirección unidifusión sin jerarquías

Algunos hosts o ruteadores pueden contar con límites jerárquicos dentro de su dirección unidifusión. Los límites conocidos diferirán de nodo a nodo, dependiendo de su alcance y su posición en la jerarquía estructurada:

Un ejemplo del formato de una dirección unidifusión, de uso común en LANs y otros ambientes; donde las direcciones del estándar *IEEE 802 MAC* están disponibles, es mostrado en la Figura 3. 5

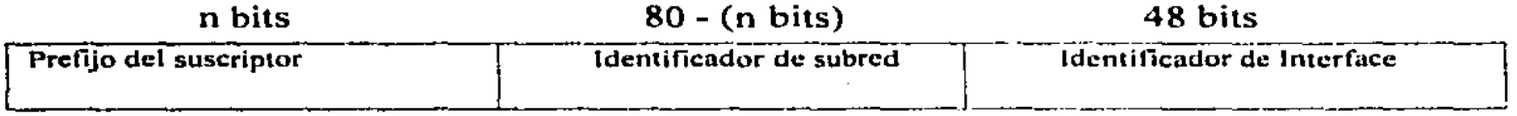


Figura 3. 5 Dirección de unidifusión con jerarquías para IEEE 802 MAC

Donde el identificador de la interface es una dirección IEEE 802 MAC de 48 bits. El uso de direcciones IEEE 802 MAC es muy esperado en topologías de red de este tipo. En otro ambientes, donde IEEE 802 MAC no esta disponible, se usan otros tipos de direcciones de enlace.

La inclusión de un identificador global único para la interface, como el IEEE 802 MAC, hace posible la autoconfiguración de direcciones, un nodo puede descubrir un identificador de subred por escuchar los mensajes de aviso de un ruteao mediante un ruteador conectado al mismo enlace, y esto ayuda a la fabricación de una dirección IPv6 por sí misma usando su propia dirección IEEE 802 MAC como un identificador de interface sobre una subred.

Otro ejemplo de dirección de unidifusión es donde una localidad u organización necesita capas o niveles adicionales en la jerarquía interna. En la Figura 3. 6 se muestra un el formato de una dirección unidifusión multinivel, donde el identificador de la subred esta dividido en un identificador de de área y un identificador de subred.

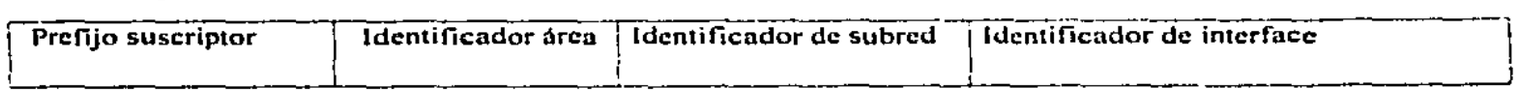


Figura 3. 6 Dirección unidifusión con varias capas de jerarquía interna

Esta técnica puede ser aplicada una vez más para permitirle a un sitio o a una organización agregar niveles a la jerarquía interna, o se puede convenir en usar un identificador más pequeño que las direcciones de 48 bits para disponer mayor espacio para niveles adicionales del estructura jerárquica. Esto podrían ser identificadores de interfaces los cuales son administrativamente creados por el sitio o la organización que lo desea.

Dirección indefinida

Las dirección 0:0:0:0:0:0:0:0 es conocida como dirección indefinida, nunca debe ser asignada a algún nodo, indica la ausencia de dirección. Un ejemplo de su uso esta en el campo Source Address de un datagrama IPv6 enviado; inicializando el host antes de que conozca su propia dirección.

Dirección de autoreconocimiento

La dirección unidifusión 0:0:0:0:0:0:0:1 es nombrada la dirección de autorreconocimiento (*loopback*), puede ser usada por un nodo que envía un datagrama IPv6 a si mismo; nunca debe ser asignada a una interface y no debe ser usada como una dirección emisora de datagramas IPv6.

Direcciones de compatibilidad con IPv4

Los mecanismos de transición incluyen una técnica para hosts y ruteadores para el encapsulado dinámico de paquetes IPv6 sobre la infraestructura de ruteo de IPv4. Los nodos IPv6 que utilizan esta técnica son asignados a una dirección unidifusión IPv6 que permite ubicar a una dirección IPv4 dentro de los 32 bits menos significantes. Este tipo de direccion es nombrada "Dirección IPv6 compatible con IPv4" como se muestra en la Figura 3. 7

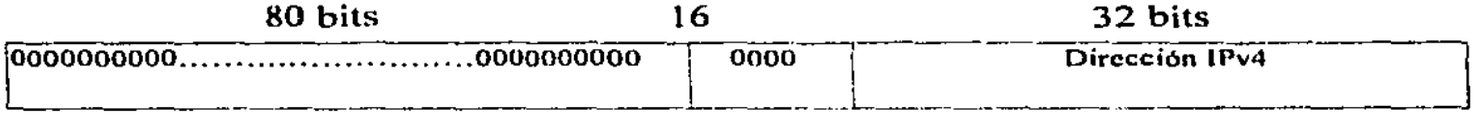


Figura 3. 7 Formato de dirección IPv6 compatible con IPv4

Un segundo tipo de dirección IPv6 que mantiene encapsulada a una dirección IPv4 esta definida para representar los nodos IPv4. Este tipo de dirección es llamada "

Dirección IPv6 con mapeo de IPv4", la cual consta del formato mostrado en la Figura 3. 8

80 bits	16	32 bits
0000000000.....0000000000	FFFF	Dirección IPv4

Figura 3. 8 Formato de dirección IPv6 con mapeo de IPv4

Direcciones NSAP

El mapeo de direcciones NSAP dentro de las direcciones IPv6 es como sigue:

7 bits	121 bits
0000001	En proceso de definición

Direcciones IPX

El mapeo de direcciones *IPX* dentro de las direcciones IPv6 es como sigue:

7 bits	121 bits
0000010	En proceso de definición

Direcciones globales de unidifusión mediante proveedor

Las direcciones de unidifusión mediante proveedor son usadas para la comunicación global, su formato es mostrado en la Figura 3. 9

3 bits	n bits	m bits	o bits	125-n-m-o bits
010	Identificador de Registro	Identificador del proveedor	Identificador del suscriptor	Identificador del intersuscriptor

Figura 3. 9 Dirección global de unidifusión mediante proveedor

Los primeros tres bits identifican la dirección de una dirección de este tipo, los siguientes campos son asignados respectivamente por autoridades, quienes asignan porciones de espacio de dirección a proveedores de servicios, los cuales a su vez, asignan porciones de espacio de dirección para los suscriptores. La parte de la dirección para el intersuscriptor es organizada de acuerdo a la topologia de red local del suscriptor.

Direcciones unidifusión de uso local

Una dirección de uso local es una dirección de unidifusión que tiene el objeto de ruteo local. Existen dos tipos de direcciones de uso local: la de enlace local y la de sitio local. Las *direcciones de enlace de uso local* tienen el siguiente formato:

10 bits	n bits	118 -n bits
1111111010	0	Identificador de Interface

Las direcciones para enlace de uso local son diseñadas para ser usadas en direccionamientos de un enlace simple, para propósitos como una autoconfiguración de dirección, descubrimiento del nodo vecino o cuando ningún ruteador esta presente.

10 bits	n bits	m bits	118 -n-m bits
1111111011	0		Identificador de Interface

Por otro lado tenemos, *las direcciones para sitios de uso local* que pueden ser utilizadas para localidades u organizaciones que no están (aún) conectadas a Internet. Las cuales pueden obtener un prefijo del espacio global de direcciones Internet. Cuando la organización se conecte a Internet entonces podrá intercambiar el prefijo de sitio de uso local por el de un prefijo de suscriptor.

Los ruteadores no deben enviar paquetes fuera de su sitio, especificando una dirección emisora con una direccion de sitio de uso local.

La parte del orden inferior de los dos tipos de direcciones de uso local contienen un campo Identificador, el cual debe ser único en el dominio en el que esta siendo usado. En la mayoría de los casos, este campo contendrá la dirección de 48 bits del estándar *IEEE 802.*

DIRECCION DE GRUPO (ANYCAST) EN IPv6

Una dirección de grupo es una dirección que esta asignada a más de una interface, generalmente pertenecientes a nodos diferentes. Un envío de paquete a una dirección de grupo es ruteado hacia la interface más cercana que posee esa dirección; según el ruteo de los protocolos usados para medir la distancia.

Es de esperarse que el uso de la dirección de grupo sirve para identificar el conjunto de ruteadores que pertenecen a los proveedores de servicios Internet. Algún otro uso es identificar el conjunto de ruteadores conectados a una subred en particular, o para el conjunto de ruteadores que proporcinan la entrada a un dominio de ruteo particular.

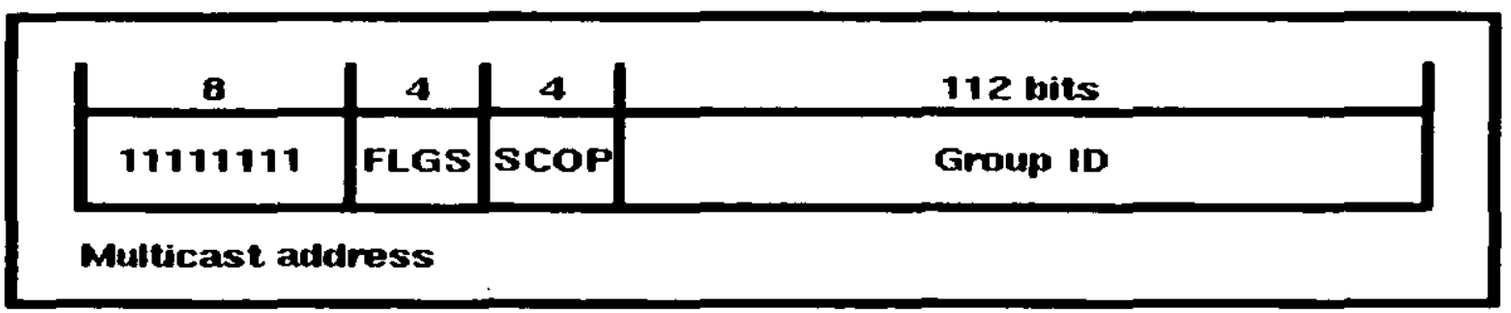
Las direcciones de grupo están especificadas dentro del espacio de direcciónes unidifusión usando cualquiera de los formatos definidos para las ellas. Por lo tanto, una dirección de grupo es sintácticamente indistinguible de una de unidifusión. Cuando una dirección unidifusión es asignada a más de una interface, se convierte en una dirección de grupo, los nodos a los cuales la dirección es asignada deben estar explícitamente configurados para saber que se trata de una dirección de grupo.

Las direcciones de grupo deben acatar dos restricciones:

1. Una dirección de grupo no debe usarse como dirección emisora de un paquete IPv6.
2. Una dirección de grupo no debe asignarse a un host IPv6, esto es, debe asignanrse a un ruteador IPv6 solamente.

DIRECCION DE MULTIDIFUSION (MULTICAST) EN IPv6

Una dirección de multidifusión o "multicast" es un identificador para un grupo de nodos. Un nodo puede pertenecer a cualquier grupo de multidifusión.



11111111 es el inicio de la dirección que identifica a una dirección multidifusión.

FLGS: especifica el valor 000T, donde 000 está reservado y si:

T = 0 indica que se trata de direcciones asignadas permanentemente o conocidas.

T = 1 indica que la dirección es una dirección transitoria.

SCOP: es usado para limitar el alcance del grupo de multidifusión. Los valores disponibles son:

VALOR	OBJETIVO
1	Reservado
2	Alcance nodo-local
3, 4	Alcance enlace-local
5	Indefinido
6, 7	Alcance Sitio-local
8	Indefinido
9 - D	Alcance Organización-local
E	Indefinido
F	Alcance global

Group ID: identifica el grupo multidifusión.

Las direcciones multidifusión no deben ser usadas como direcciones de emisor en datagramas de IPv6 o aparecer en la cabecera de ruteo.

Algunas de las direcciones multidifusión han sido predefinidas y son las mostradas en la Figura 3. 10

DIRECCIÓN	FUNCIÓN
FF00:0:0:0:0:0:0	Reservada
FF01:0:0:0:0:0:0	Reservada
FF02:0:0:0:0:0:0	Reservada
FF03:0:0:0:0:0:0	Reservada
FF04:0:0:0:0:0:0	Reservada
FF05:0:0:0:0:0:0	Reservada
FF06:0:0:0:0:0:0	Reservada
FF07:0:0:0:0:0:0	Reservada

FF08:0:0:0:0:0:0	Reservada
FF09:0:0:0:0:0:0	Reservada
FF0A:0:0:0:0:0:0	Reservada
FF0B:0:0:0:0:0:0	Reservada
FF0C:0:0:0:0:0:0	Reservada
FF0D:0:0:0:0:0:0	Reservada
FF0E:0:0:0:0:0:0	Reservada
FF0F:0:0:0:0:0:0	Reservada
FF01:0:0:0:0:0:1	Todos los nodos (Alcance nodo-local)
FF02:0:0:0:0:0:1	Todos los nodos (Alcance enlace-loca)
FF01:0:0:0:0:0:2	Todos los ruteadores (Alcance nodo-local)
FF02:0:0:0:0:0:2	Todos los ruteadores (Alcance enlace-local)

Figura 3. 10 Algunas de las direcciones multidifusión predefinidas

3.5. CABECERAS SUPLEMENTARIAS DE IPv6

La cabecera IPv6, aunque lo doble de grande que la de IPv4, está simplificada. Algunas funciones de la cabecera de IPv4 han sido reubicadas en cabeceras suplementarias, y otras han sido eliminadas. Ver Figura 3. 11

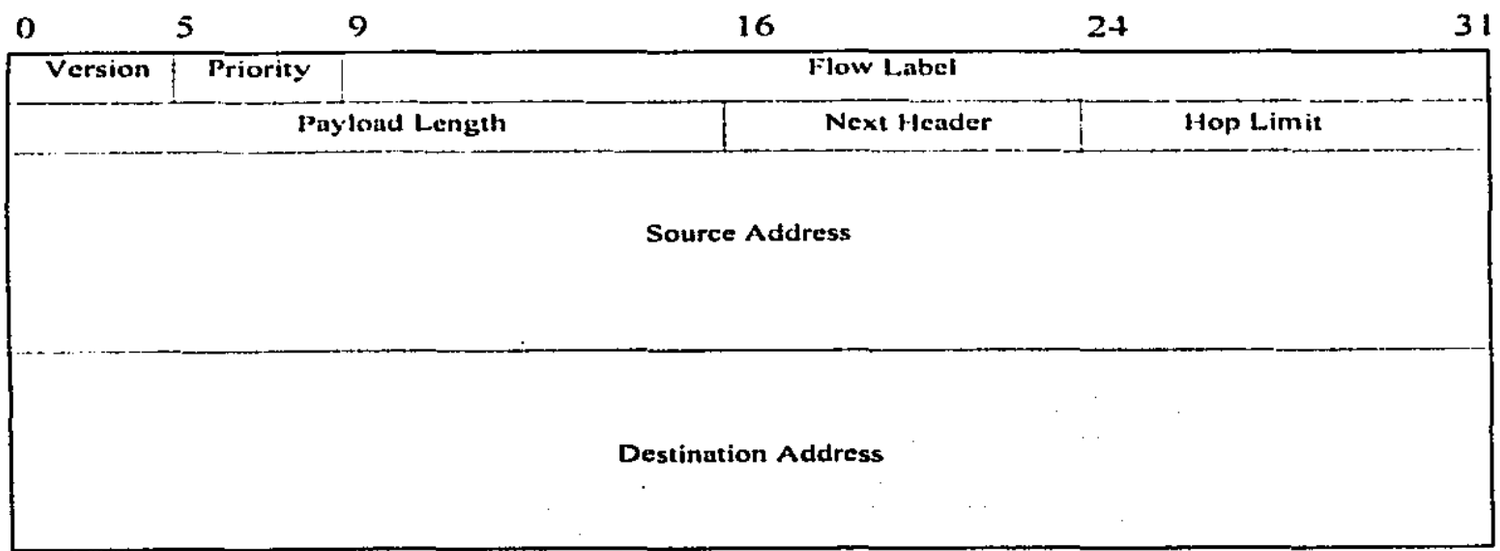


Figura 3. 11 Cabecera base IPv6

Versión (4 bits): número de versión del IP.

Priority (4 bits): identifica la prioridad deseada del datagrama. El rango de 0 a 7 es utilizado para datagramas que pueden ser regresados en respuesta a la congestion de la red. El resto de valores del 8 al 15 se emplean para tráfico que no debe regresar, por ejemplo cuando se trata de un envío de datagramas de tiempo real en fracciones de tiempo constante, una retransmisión de dicho datagrama originaria un retraso de comunicación.

Flow Label (24 bits): contiene un identificador de flujo seleccionado por el host origen. Este campo puede ser usado por un host origen para etiquetar aquellos paquetes para los cuales es solicitado un manejo especial por los ruteadores de la red, como una calidad de servicio diferente a la predeterminada o un servicio de "tiempo real". Los hosts o ruteadores que no soportan los servicios de este campo necesitan asignar el valor cero cuando se crea un datagrama; considerarlo como inalterable cuando se envía e ignorarlo cuando se recibe.

Las funciones de este campo son útiles para soportar aplicaciones que requieren la determinación de cierta calidad de servicio, como aplicaciones multimedia o comunicación en tiempo real, necesitan una conexión garantizada y con retardos de extremo a extremo.

Este campo maneja el concepto "flujo" como la trayectoria que sigue un datagrama desde su origen hasta su destino, donde cada ruteador implicado se compromete a garantizar una calidad de servicio específica; en otra palabras, se trata de en un tipo de conumutación de paquetes sin conexión de circuito virtual porque los datagramas con la misma etiqueta de flujo son tratados similarmente y la red los verifica asociándolos a entidades.

La naturaleza especial de *Flow Label* puede ser transportada a los ruteadores de la red mediante un protocolo de control, como el Protocolo de Reservación de Recursos (*ReSource reserVation Protocol RSVP*) o mediante la información de flujo de los mismos datagramas.

Payload Length (Número entero sin signo de 16 bits): Longitud (en bytes) del remanente del paquete después de la cabecera IPv6. Si el paquete (*Payload*) es mayor de 64Kbytes (65,536 octetos), se especifica el valor 0 en este campo y la longitud del paquete actual se expresa en la opción Nodo-por-Nodo.

Next Header (Campo selector de 8 bits): Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6 base. El campo *Next Header* usa los mismos valores que el campo *Protocol* de la cabecera IPv4 [10].

Hop Limit (128 bits): Usado para limitar el impacto de los ciclos de ruteo. El campo *Hop Limit* es decrementado en uno por cada nodo al que envía el paquete. El paquete es eliminado cuando el valor del campo llega a 0.

Source Address (128 bits): La dirección del emisor inicial del paquete.

Destination Address (128 bits): La dirección del receptor del paquete, posiblemente no sea la del último receptor, si la cabecera de ruteo suplementaria (*Routing Header*) esta presente.

CABECERAS SUPLEMENTARIAS IPv6

En IPv6, la información opcional de la capa internet es codificada en cabeceras suplementarias que pueden estar colocadas en el paquete entre la cabecera IPv6 y la cabecera de la capa de transporte (Ver Figura 3. 12). Hay un número pequeño de extensiones de cabeceras, cada una identificada por un valor distinto en el campo *Next Header*. Las cabeceras suplementarias son las siguientes:

1. Cabecera de opciones Nodo-por-Nodo
2. Cabecera de opciones Extremo-a-Extremo
3. Cabecera de ruteo o encaminamiento
4. Cabecera de fragmentación
5. Cabecera de autenticidad
6. Cabecera de confidencialidad

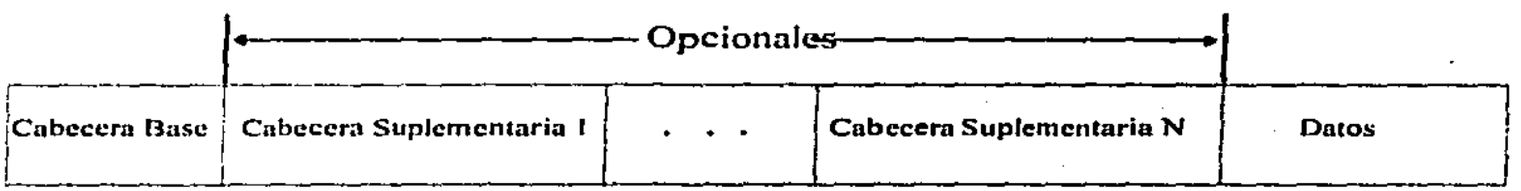


Figura 3. 12 Cabecera base de IPv6 y la posición de sus cabeceras suplementarias

[10] Postel, Jon y Reynolds, Joyce., "Assigned numbers", RFC 1700, USC/Information Sciences Institute, Octubre 1994.

1. CABECERA DE OPCIONES NODO-POR-NODO IPv6[11]

La cabecera de opciones *Nodo-por-Nodo* es usada para transportar información adicional que debe de ser examinada por cada nodo a lo largo del trayecto de la ruta. Esta cabecera es identificada por el valor 0 en el campo *Next Header* de la cabecera IPv6 base y tiene el formato de la Figura 3. 13

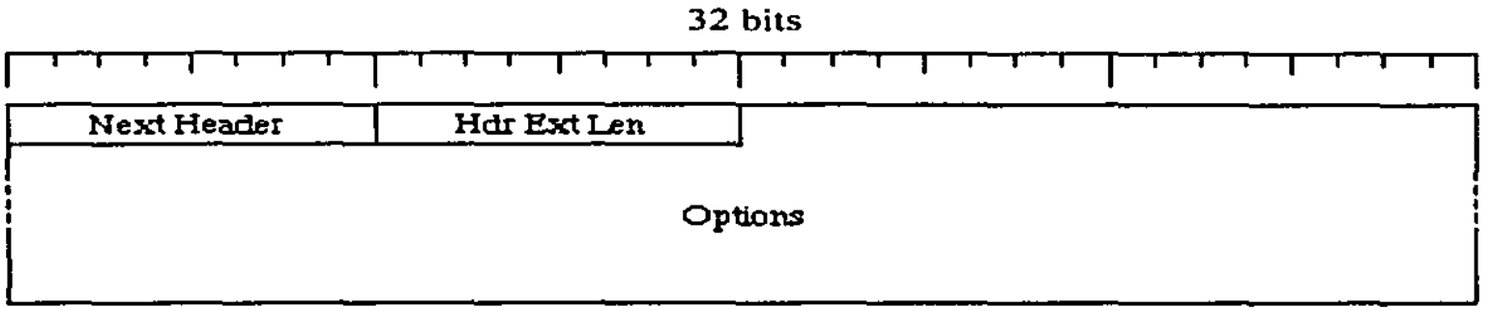
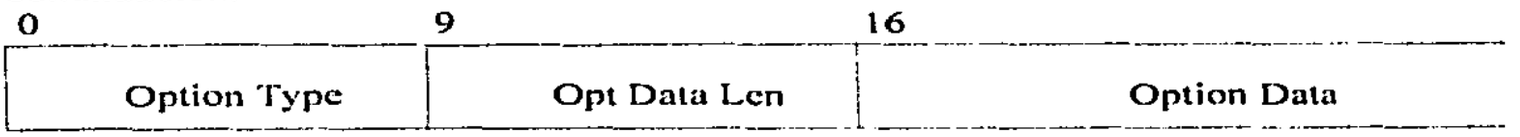


Figura 3. 13 Formato de la cabecera suplementaria *Nodo-por-Nodo* de IPv6

Next Header (Campo selector de 8 bits): Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de opciones *Nodo-por-Nodo*, usa los mismos valores que el campo *Protocol* de IPv4.

Hdr Ext Len (Número entero sin signo de 8 bits): Longitud en octetos de la cabecera de opciones *Nodo-por-Nodo*, sin contar los primeros 8 octetos.

Options (Campo de longitud variable, usando múltiplos de 8 octetos de longitud): Este campo contiene una o varias opciones codificadas por un subcampo *Tipo, Longitud y Valor* (*Type-Length-Value TLV*). La estructura de este subcampo se muestra a continuación:



Option Type (Campo de 8 bits): Identificador de un tipo de opción.

Opt Data Len (Número entero sin signo de 8 bits): Longitud del campo Option Data.

[11] Su nombre en inglés es Hop-by-Hop Option Header o Host-by-Host Option Header

Option Data (Campo de longitud variable): Dato específico según el tipo de opción.

Los identificadores del campo *Option Type* están codificados internamente, de tal manera que los dos primeros bits más significativos especifican la acción que debe ser tomada si el procesamiento del nodo IPv6 no reconoce el valor del campo Option Type:

00 Brincar esta opción y continuar el procesamiento de la cabecera
01 Destruir el datagrama; no enviar mensaje al Protocolo de Control de Mensajes Internet (*Internet Control Message Protocol ICMP*)
10 Destruir el paquete y enviar un mensaje desconocido al ICMP hacia la dirección emisora del paquete, indicando al campo *Option Type* desconocido.
11 Destruir datagrama y no enviar mensaje ICMP para multidifusión

Si el tercer bit de *Option Type* es 1, indica que el campo *Option Data* puede cambiar el tipo de ruteo para llegar al destinatario final del datagrama.

2. CABECERA DE OPCIONES EXTREMO-A-EXTREMO IPv6 [12]

La cabecera de opciones *Extremo-a-Extremo* proporciona información opcional que necesita ser examinada por el (los) nodo(s) destinatario(s) del paquete; está identificada por el valor del campo *Next Header* que sigue inmediatamente a la cabecera previa, y tiene el mismo formato que la cabecera de opciones *Nodo-por-Nodo*, a excepción de la capacidad de excluir una opción de cálculo de integridad o autenticidad.

3. CABECERA DE RUTEO O ENCAMINAMIENTO IPv6

La cabecera de ruteo o encaminamiento es usada por un emisor IPv6 para listar uno o más nodos intemediarios (o un conjunto de grupos) que deben ser visitados en la ruta del paquete a su destino. Esta forma particular de la cabecera de ruteo (Ver Figura 3. 14) esta diseñada para soportar el Protocolo de Ruteo Demandado por el Origen (*Source Demand Routing Protocol SDRP*)

[12] Su nombre en inglés es End-to-End Option Header o Destination Options Header

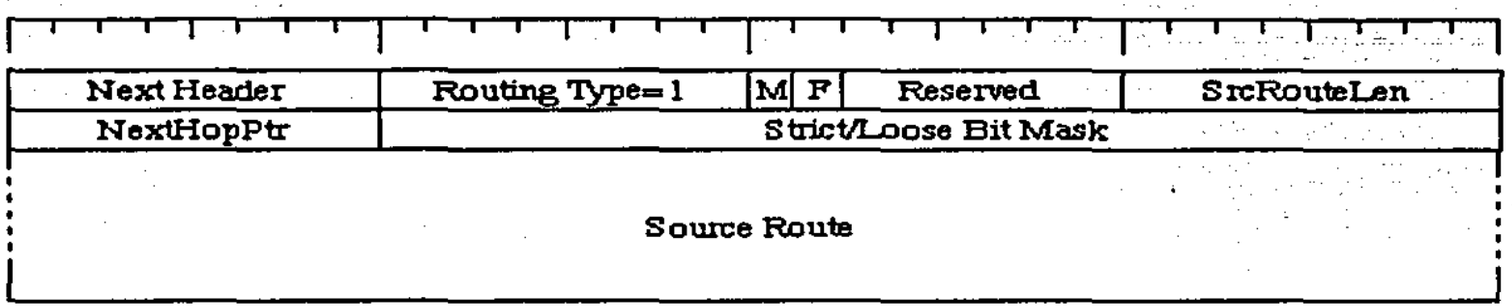


Figura 3. 14 Formato de la cabecera suplementaria de ruteo de IPv6

Next Header (Campo selector de 8 bits): Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de ruteo, usa los mismos valores que el campo *Protocol* de IPv4.

Routing Type (El valor debe ser el número 1): Indica el tipo de ruteo soportado por esta cabecera.

MRE (Must Report Errors flag, 1 bit): Si este bit es un 1 y un ruteador no puede emitir un paquete correctamente como se especifica en la lista de la opción Ruta de Origen (*Source Route*), el ruteador genera un mensaje de error ICMP. En el caso en que el bit MRE esté a 0, el ruteador no generará este mensaje aunque no pueda emitir el paquete correctamente como se especifica en la lista de la Ruta de Origen.

F (*Failure of Source Route Behavior Flag*, 1 bit): Si este bit está en 1 indica que si un ruteador no puede transmitir más allá un datagrama, como se especifica en la lista de Ruta de Origen, coloca el valor del campo *Next Hop Pointer* con el valor del campo *Source Route Length*. De esta forma, el destino siguiente del paquete estará basado únicamente en la dirección del campo *Destination Address*. De la misma manera, si el bit F está a 0, en las mismas condiciones, el ruteador destruirá el paquete.

Reserved (6 bits): Inicializado a 0 por el emisor, es ignorado por el receptor.

SrcRouteLen (*Source Route Length*, número entero sin signo de 8 bits): Es el número de elementos o nodos que hay en una cabecera de ruteo SDRP. La longitud de la cabecera SDRP puede calcularse a partiendo de este valor (longitud = SrcRouteLen * 16 + 8). Este campo no debe exceder el valor 24.

NextHopPtr (*Next Hop Pointer*, número entero sin signo de 8 bits): Apunta a los elementos o nodos que hay que recorrer. Es inicializado a 0 para apuntar al primer elemento o nodo del *Source Route*. Cuando *Next Hop Pointer* es igual al campo Source Route Length, significa que la Ruta del Emisor está terminada.

Strict/Loose Bit Mask (24 bits): Esta máscara se utiliza para que un nodo se decida por una ruta. Si el valor de *Next Hop Pointer* es N, significa que el N-ésimo bit del *Strict/Loose Bit Mask* está a 1; esto indica que el siguiente nodo es un nodo *Strict Source Route Hop*, mientras que si está a 0, el siguiente nodo es un *Loose Route Hop*.

Source Route (múltiplo de 128 bits): Es una lista de direcciones IPv6 que indica el camino que debe seguir el paquete. La lista de la Ruta de Origen (*Source Route*) puede contener un conjunto de direcciones de tipo "*unicast y anycast*".

4. CABECERA DE FRAGMENTACIÓN IPv6

La cabecera de fragmentación es utilizada por el emisor IPv6 para enviar paquetes más grandes que lo permitido, los cuales se ajustan a una MTU de ruta hacia sus destinatarios. A diferencia de IPv4, en IPv6 la fragmentación es ejecutada únicamente por los nodos origen, y no por los ruteadores que intervengan a lo largo de la ruta (Ver Figura 3. 15). La cabecera de fragmentación se distingue por un valor 44 en el campo *Next Header*, el cual se encuentra justo después de la cabecera de ruteo El formato es el siguiente:

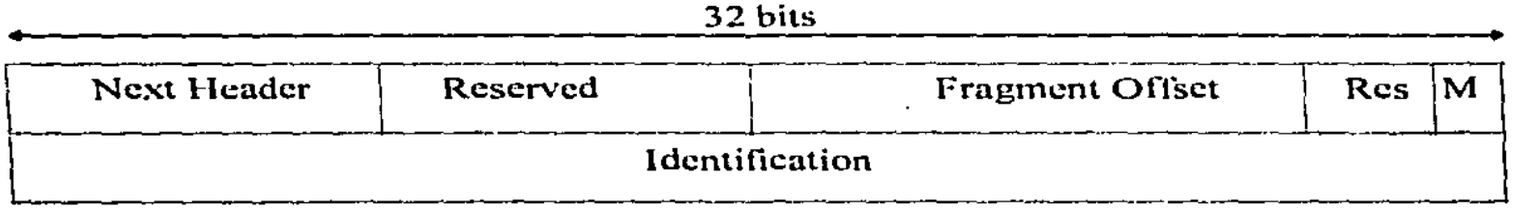


Figura 3. 15 Formato de la cabecera suplementaria de fragmentación de IPv6

Next Header (Campo selector de 8 bits): Identifica el tipo de la cebecera que sigue inmediatamente a la cabecera de fragmentación, usa los mismos valores que el campo *Protocol* de IPv4.

Reserved y Res (8 bits y 2 bits, respectivamente): Son inicializados ambos a 0 por el emisor al principio de la transmisión e ignorados en la recepción.

Fragmentation Offset (Número entero sin signo de 13 bits): Indica la posición del siguiente fragmento del paquete, tomando en cuenta las posiciones del paquete original sin fragmentar. El primer fragmento estará en el lugar número 0. El valor de este campo es un múltiplo de 8 octetos.

M flag (1 bit): Si éste bit es igual a 1, significa que queda uno o más fragmentos. En caso contrario, indica que el fragmento que hay es el último o el único.

Identification (32 bits): Es un valor asignado al paquete original, diferente al de cualquier otro datagrama enviado recientemente con la misma dirección origen IPv6, la misma dirección destino IPv6 y el mismo valor del campo *Next Header* de la cabecera de fragmentación. Si la cabecera de ruteo esta presente, la dirección de destino IPv6 es la del destinatario final. El valor de identificación esta contenido en la cabecera de fragmentación de todos los fragmentos del paquete original, y es usado por el receptor para identificar todos los fragmentos que pertenecen al mismo datagrama.

5. CABECERA DE AUTENTICIDAD IPv6

La cabecera de autenticidad es utilizada para acreditar y asegurar la integridad de los datagramas IPv6. La aceptación de los datagramas es proporcionada por un algoritmo de autenticidad ejecutado sobre esta cabecera, pero no es proporcionada por todos los algoritmos de autenticación. La cabecera de autenticidad esta identificada por el valor 51 del campo *Next Header* y tiene el formato de la Figura 3. 16

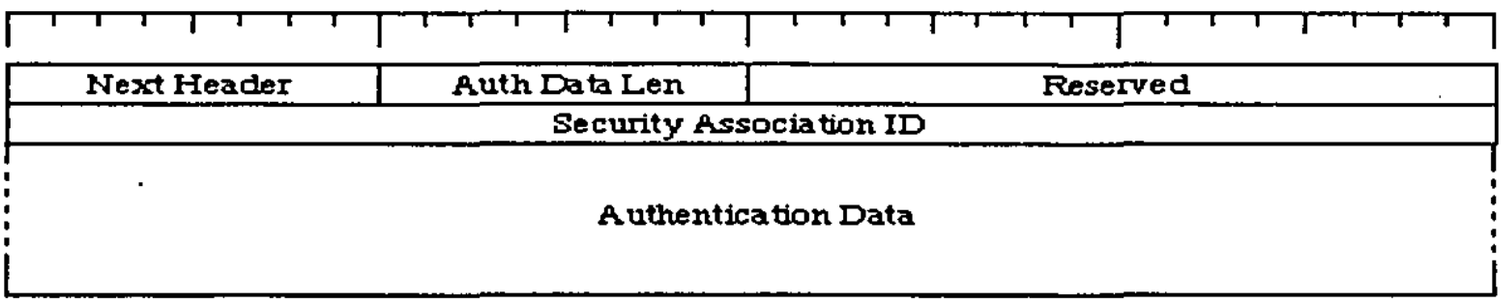


Figura 3. 16 Formato de la cabecera suplementaria de autenticidad de IPv6

Next Header (Campo selector de 8 bits): Identifica el tipo de cabecera que sigue inmediatamente la cabecera de autenticidad, usa los mismos valores que el campo *Protocol* de IPv4.

Auth Data Len (*Authentication Data Length*, número entero sin signo de 8 bits): Es la longitud del campo Authentication Data, en múltiplos de 8 octetos.

Reserved (16 bits): Inicializado a 0 por el emisor al principio de la transmisión e ignorado en la recepción.

Security Association ID (*SAID*, 32 bits): Combinado con la dirección del emisor, identifica tanto al (los) destinatario(s) de acuerdo al tipo de seguridad preestablecida, como al receptor al que pertenece el datagrama.

Authentication Data (Número entero, múltiplo de 8 octetos y de longitud variable): Información sobre el algoritmo específico requerido para autenticar el origen del datagrama y para asegurar su integridad como se especifico en el tipo de seguridad preestablecida.

6. CABECERA DE CONFIDENCIALIDAD IPv6 [13]

La cabecera de confidencialidad busca proporcionar confidencialidad e integridad de los datos a través de su encriptamiento. Una vez encriptados los datos a proteger, se colocan en una de las partes de la cabecera de confidencialidad. Tanto los segmentos de TCP (o los datagramas de usuario de UDP), así como el datagrama IPv6 completo; pueden ser encriptados dependiendo de los requerimientos de seguridad del usuario. Este enfoque de encapsulación es necesario para asegurar la confidencialidad completa del datagrama original. Si esta presente, la cabecera de confidencialidad es siempre el último campo no encriptado de un paquete.

La cabecera de confidencialidad opera entre hosts, entre un host y un *gateway* de seguridad o entre dos gateways de seguridad. El soporte para gateways de seguridad permite redes confiables, sin representar costos financieros elevados en seguridad ni en ejecución, mientras se transmite un tráfico de información seguro sobre partes de la red que no lo son. (Ver Figura 3. 17)

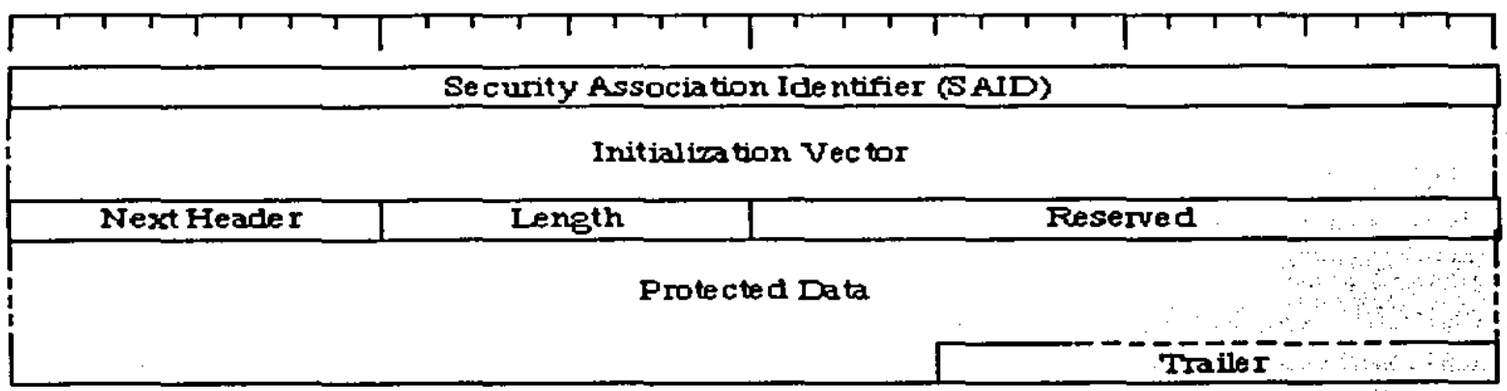


Figura 3. 17 Formato de la cabecera suplementaria de confidencialidad de IPv6

[13] Su nombre en inglés es Encapsulating Security Payload Header

Security Association Identifier (*SAID*, 32 bits): Identifica el tipo de seguridad del datagrama. Si no se ha establecido algún tipo de seguridad, el valor de este campo será 0x0000. El tipo de seguridad es normalmente unilateral. Una sesión de comunicación confidencial entre dos hosts debe tener normalmente dos SAID (uno para la dirección de cada host). El host receptor utiliza una combinación del valor del SAID y de la dirección del emisor para distinguir la asociación correcta, del tipo de seguridad.

Initialization Vector (Presencia y longitud dependientes del SAID): Este campo es opcional, y su valor depende del SAID utilizado. Por ejemplo, el campo puede contener datos con sincronización de criptográfica para cierto algoritmo de encriptación y puede alojar un vector de inicialización criptográfica. La implementación de una cabecera de confidencialidad emplea el valor del SAID para determinar si este campo tiene valores, de ser así; evalúa su longitud y lo utiliza.

Next Header (Encriptado, campo selector de 8 bits): Identifica el tipo de la cabecera que sigue inmediatamente a la cabecera de confidencialidad, usa los mismos valores que el campo *Protocol* de IPv4.

Reserved (Encriptado, 17 bits): Ignorado por el receptor.

Length (Encriptado, 8 bits): Longitud de la cabecera de confidencialidad en múltiplos de 8 octetos, sin contar los primeros 8.

Protected Data (Encriptado, longitud variable): Este campo puede contener encapsulado un datagrama IPv6 completo, una secuencia de cero o más cabeceras suplementarias IPv6, y el segmento o datagrama de usuario de la capa de transporte, o bien; solo una secuencia de cero a más cabeceras suplementarias seguidas por la unidad de dato de la capa de transporte.

Trailer (Encriptado, presencia y longitud variable dependientes del SAID): Este campo es utilizado para rellenar (necesario en algunos algoritmos) o para almacenar datos de autenticidad empleados en un algoritmo de criptografía que proporcione confidencialidad sin autenticidad. Este campo está presente únicamente si el algoritmo en ejecución requiere un campo así. (El campo *Trailer* es usado para la longitud total de un bloque encriptado por algoritmos de encriptación).

Cuando hay más de una cabecera suplementaria en un mismo paquete, se recomienda que aparezcan en el orden siguiente:

- Cabecera IPv6 base
- Cabecera de opciones Nodo-por-Nodo
- Cabecera de opciones de Extremo-a-Extremo **(Nota 1)**
- Cabecera de ruteo o encaminamiento
- Cabecera de fragmentación
- Cabecera de autenticidad
- Cabecera de confidencialidad
- Cabecera de opciones de Extremo-a-Extremo **(Nota 2)**
- Cabecera de la capa superior

Nota 1. Para opciones que son procesadas por el primer destino que aparece en el campo Destination address de IPv6 y por los que aparecen listados en la cabecera de ruteo o encaminamiento.

Nota 2. Para opciones que son procesadas solamente por el destinatario final al recibir el datagrama.

Cada tipo debe aparecer una sola vez, excepto en el caso de la cabecera de opciones *Extremo-a-Extremo* que es presentada antes de la cabecera de ruteo y antes de la cabecera de la capa superior.

El valor 59 en el campo *Next Header* de la cabecera IPv6 base o de cualquier cabecera suplementaria, indica que no hay más cabeceras adelante.

RESOLUCIÓN DE DIRECCIONES IPv4 E IPv6

El Sistema de Nombres de Dominio (*Domain Name System DNS*) es usado para "mapear" nombres de hosts en ambas direcciones IPv4 e IPv6. Las direcciones de IPv4 (32 bits) estan listadas en un registro de recursos "A". Un nuevo registro de recursos llamado "AAAA" ha sido definido para registrar las direcciones IPv6 de hosts (128 bits). Un hosts que tiene más de una dirección IPv6 debe estar poseer más de un registro, uno para cada una.

Los nodos IPv6/IPv4 deben estar habilitados para interoperar directamente con ambos nodos IPv4 e IPv6 y deberán proporcionar librerias de resolución capaces de operar con los registros "A" de IPv4 tan bien como con aquellos de IPv6.

REGISTRO Y CONTROL DE DIRECCIONES

La Autoridad de Números Asignados de Internet (*Internet Assigned Numbers Authority IANA*) tiene la rsponsabilidad para la administración del espacio de direcciones IPv6, con la supervisión y coordinación de la Junta de Arquitectura Internet (*Internet Architecture Board IAB*) y el Grupo de Control de Ingeniería de Internet (*Internet Engineering Steering Group IESG*).

La administración de las localidades de las direcciones estará a cargo de un elemento pequeño de autoridad central sobre la delegación de registros regionales. Estos registros regionales crearán localidades de direcciones específicas para proveedores de servicio de red y otros registros subregionales.

IANA desarrollará un plan para las localidades de las direcciones IPv6 iniciales, incluyendo una provisión para localización automática de direcciones IPv6 para quien mantenga en uso las direcciones IPv4.

CAPITULO 4.
PROTOCOLOS IPv4 E IPv6.

CAPITULO 4. PROTOCOLOS IPv4 E IPv6

El resultado final de la búsqueda de una mejor administración de los recursos de Internet ante su devastador crecimiento, está convertido en la propuesta de integración de la versión 6 del Protocolo Internet al TCP/IP, que junto con el objetivo original de su creación ha coordinado e integrado una mejor funcionalidad y ejecución para satisfacer necesidades actuales y venideras.

Aunque, la renovación del protocolo IP implique mejoras, no esta libre de contrariedades que pueden parecer desventajas. Para la integración de IPv6 se requiere del esfuerzo de los administradores de red para cambiar el software del protocolo stack en cada dispositivo conectado a la red, es decir se requieren cambios en los hosts y ruteadores a nivel de sistema operativo de red, para configurarlos adecuadamente.

La necesidad de desarrollo de una nueva versión del protocolo Internet esta sustentada en varios factores: el crecimiento de hosts conectados a Internet y el consecuente agotamiento de direcciones IP, el surgimiento de nuevos mercados (computadoras personales móviles para accesos remoto desde sitios diversos, "ludored" o entrenimiento por red, control de dispositivos generales), nuevas aplicaciones (software multimedia que requiere servicio de tiempo real), calidad de servicio y seguridad.

Todos los factores anteriores son solicitudes reales de usuarios que a diario conviven con recursos de Internet. Los cambios y mejoras del nuevo modelo IPv6 intentan satisfacer necesidades fundamentales de investigadores, administradores de red, fabricantes de hardware, diseñadores de software y organizaciones relacionadas a la conmutación de paquetes a través medios de telecomunicación.

4.1 FUNCIONALIDAD DE IPv4 E IPv6

La ineficiencia de la ejecución de funciones de la estructura de IPv4, necesita eliminarse, debido a que las tareas encomendadas a cada campo son insuficientes para las demandas de transmisión y recepción de paquetes y algunas de las opciones son subutilizadas.

La cabecera IPv6 propuesta representa una gran simplicidad con respecto a la cabecera IPv4, con el propósito de crear mayor funcionalidad a los procesos de direccionamiento y fragmentación de datagramas a través de una red.

El cambio más significativo en IPv6 con respecto a IPv4, consiste en la asignación de funciones del campo Options, a una lista de cabeceras suplementarias de IPv6; así como la longitud de la dirección IP, la cual para IPv4 es de 32 bits y para IPv6 de 128 bits.

Las diferencias y semejanzas entre la cabecera de IPv4 e IPv6 se describen a continuación:

- Los campos *Version, Source address y Destination Address* se conservan. El tamaño de los campos de las direcciones de origen y destino se incrementó de 32 bits (4 octetos) a 128 bits (16 octetos) cada uno. Más adelante se realiza un análisis de este incremento.

- El campo *Header Length* se ha eliminado. La cabecera de IPv6 propone un tamaño fijo de 40 octetos, no un tamaño variable (20 a 60 octetos) como lo utiliza IPv4; con lo cual ya no es necesario asignar el tamaño de la longitud de la cabecera al campo *Header length*.

- El campo *Service Type* (8 bits) se ha reemplazado por los campos *Priority* (4 bits) y *Flow label* (24 bits). En IPv4 este campo no es utilizado completamente por todos los hosts y ruteadores, sólo algunos lo utilizan para decisiones de ruteo o en decisiones que prevengan por ejemplo, la eliminación de datagramas cuando la memoria proporcionada por el receptor es escasa; determinando tiempos de espera. En IPv6, se ofrecen funciones similares a las de la versión IPv4, y otras adicionales en fase de prueba, como el servicio de "tiempo real", útil para la transmisión de video.

  Service Type es poco utilizado ya que para efectuar servicios de transporte especiales es necesario que los algoritmos de ruteo sean eficaces y garanticen una entrega rápida; tomando en consideración la tecnología de red del trayecto para determinar las características de retardo, desempeño y confiabilidad, las cuales pueden no coincidir con las especificadas en los subcampos de *Service Type*.

- El campo *Datagram Length* ha sido reemplazado por el campo *Payload Length*, con la diferencia de que el último especifica el número de octetos transportados por un datagrama sin incluir los octetos de la cabecera IP base (40 octetos), mientras que el campo Datagram length considera la longitud de la cabecera y de todos sus campos.

De esta manera el campo de las dos versiones, puede expresar un máximo de 65 535 ($2^{16} - 1$) valores, pero en IPv4 representará un datagrama completo, mientras que en IPv6 sólo serán las cabeceras suplementarias y los datos que vienen de las otras capas del protocolo TCP/IP.

- La información de los campos *Identification, Flags y Fragment Offset* se han cambiado a la cabecera suplementaria de fragmentación. Más adelante se explican una diferencia importante entre el proceso de fragmentación y reensamblaje de datagramas según cada versión.

- El campo *Time To Live* ha sido sustituido por el campo *Hop Limit*. Aunque se cambio el nombre del campo, en la práctica, la tarea es la misma para los dos. La modificación se realizó tomando en cuenta que el campo *Time To Live* del IPv4 no representa el valor con el cual fue diseñado, es decir su longitud de 8 bits debería identificar el tiempo máximo (4.25 minutos = 11111111) para que un datagrama llegue a su destino antes de ser eliminado, en cambio; se emplea frecuentemente para determinar el número de nodos que un datagrama debe visitar antes de ser deshechado. Por su parte, *Hop Limit* interpreta su valor como el límite estricto de saltos para cada nodo visitado a lo largo de su ruta y no el tiempo máximo para lograr alcanzar su destino.

- El campo *Protocol* se cambió por el campo *Next Header*. Los valores asignados a uno y otro campo son los mimos, la diferencia es que *Next header*, generalmente tiene un valor que apunta hacia la cabecera siguiente.

- El campo *Options* de IPv4, es sustituido por varias cabeceras suplementarias en IPv6. Para IPv4 se necesita un formato fijo del datagrama, una *cabecera base* de longitud variable (20 a 60 octetos), donde el campo *Options* es opcional y su longitud varía de acuerdo al tipo. En IPv6 la cabecera base consta de una longitud fija (40 octetos), con un formato dinámico de campos, ya que pueden incluirse o no las cabeceras suplementarias, colocándose entre la cabecera base y el campo *Data*. La longitud fija de la cabecera base simplifica el formato, eliminando el campo *Header Length* de IPv4.

  Una de las ventajas de la cabecera base fija es que ayuda al proceso de fragmentación a distinguir la parte del datagrama que tiene que copiar para colocarla en cada fragmento y lo mismo ayuda para reensamblar el datagrama original.

  En cuanto al formato dinámico del datagrama IPv6, se facilitará la adaptación de nuevos protocolos que necesiten cambiar el hardware de red o las aplicaciones;

porque se podrán añadir nuevas cabeceras para servicios especiales futuros o se podrán eliminar sin afectar la cabecera IPv6 base.

Las cabeceras suplementarias ofrecen algunas funciones no disponibles en las opciones de IPv4. La cabecera de autenticidad y la cabecera de confidencialidad de IPv6 proporcionan servicios para filtrar usuarios no autorizados y garantizar la integridad-confidencialidad de los datos, tales servicios no encuentran analogía en IPv4.

Proceso de fragmentación de IPv4 e IPv6

La fragmentación de IPv4 e IPv6 difiere en algunos puntos importantes.

IPv4 establece el valor 1 en el primer bit del campo *Flags*, llamado *no fragmentación*; para impedir la fragmentación y el valor 0 para realizarla. Esta especificación está disponible para cualquier ruteador que funcione como intermediario para la transmisión de una cantidad de bits superiores a la MTU de la red. Tal disposición, aumenta el riesgo de que el datagrama sea corrupto, ya que si alguno de los fragmentos se pierde, el nodo receptor no podrá reensamblar totalmente el datagrama y mandará un mensaje al emisor para que nuevamente, se envíe el datagrama completo, lo que significa tiempo de retraso y carga de tráfico en la red.

Debido a que la capa IP realiza una transmisión sin a conexión, el error en el datagrama es detectado hasta que la capa de transporte reciba y verifique su integridad, lo cual también implica demora e ineficiencia de procesos.

En cambio, IPv6 establece un proceso de fragmentación diferente. Un nodo origen IPv6 antes de transmitir un datagrama, utiliza una técnica para Descubrir la MTU de Ruta (*Path MTU Discovery*) y así identificar la MTU mínima a lo largo de la trayectoria hasta el destino. La MTU descubierta, es la que se toma como base para fragmentar el datagrama desde el nodo emisor y no se necesita ruteadores intermediarios que realicen este proceso. Este método de fragmentación, decide sacrificar ancho de banda del medio de transmisión, a cambio de no correr el riesgo de retransmitir todo el datagrama a través de fragmentos y congestionar el trafico en la red.

4.2 IPv6 ANTE EL CRECIMIENTO DE INTERNET

La longitud de la dirección IPv4 se ha tornado limitada al asignar direcciones a todas las redes y hosts del futuro. El problema de raíz para que la capacidad de IPv4 se prevea agotada es el esquema de jerarquías usado para determinar los tipos de red. Como se sabe, las direcciones IPv4 se asignan de acuerdo a una clase: A, B, C, D y E, de las cuales las tres primeras son de uso público general. A causa de la estructura anterior de clases, el número de direcciones disponibles se han otorgado a organizaciones que no agotan la cantidad disponible de ellas; sin embargo, sería difícil que éstas direcciones se reasignarán a otro propietario.

Para comprobar que el esquema de administración de direcciones IP, no cuenta con el diseño apropiado para permitir, a los millones de hosts futuros, accesar a Internet; se realiza un cálculo de la capacidad de direccionamiento de IPv4 y posteriormente se tabulan el número de redes y hosts en cada clase.

Porqué IPv6 tiene una longitud de 128 bits ?

Uno de los principales puntos por discutir y el más trascendental es la longitud en bits de la dirección IPv6. A continuación se dan algunas razones por las cuales IPv6 es de 128 bits de longitud, y no de 64, 120 o variable:

- Con 64 bits (8 octetos) se desperdiciaría ancho de banda y causaría ineficiencia en la asignación de direcciones como sucede en IPv4.

- Con 160 bits (20 0ctetos) se intentaba establecer un estándar al incluir el formato de direcciones NSAP, el cual utiliza la longitud de 160 bits. Sin embargo, se considera que una dirección de esta magnitud podría implicar problemas en la representación de direcciones, no empero; la idea de las direcciones NSAP es considerada en la tabla de localidades de direcciones IPv6, se le ha asignado un prefijo y una estructura que aún está en desarrollo.

- Una longitud variable es inadecuada para un sistema en que intervienen procesos de ensamble y desensamble de datos, para luego ser verificados. Una longitud variable complicaría el manejo de DNSs, sus registros tendrían también que variar, las máscaras de direcciones que permiten a un ruteador la capacidad de limitar búsquedas, se convertiría en un proceso complejo.

Por lo tanto, la longitud de 128 bits es considerada la más adecuada para la ejecución eficiente de dispositivos tales como ruteadores y DNS, así como la magnitud más adecuada para aprovechar los recursos de nuevas tecnologías que están

relacionadas con la capacidad de unidades de transmisión y recepción de datos; además de proporcionar la flexibilidad de interoperar con sistemas diferentes a través de otros formatos de dirección y permitir el uso de las actuales direcciones basadas en IPv4.

4.3 CAPACIDAD DE DIRECCIONAMIENTO DE IPV4

La capacidad de direccionamiento total de IPv4 esta considerada en 2^{32} combinaciones posibles en el sistema numérico posicional binario. Cada dirección esta clasificada por cinco clases de red: A, B, C, D y E.

Cada clase de red esta dividida en dos partes, una para identificar a la red (*netid*) y la otra para identificar al host (*hostid*). Los primeros cuatro bits del netid, llamados prefijo, son asignados para clasificar las cinco clases de red. Las clases dependen de las características del prefijo:

Para la clase A, el primer bit siempre es 0
Para la clase B, los dos primeros bits son siempre 10
Para la clase C, los tres primeros bits son siempre 110
Para la clase D, los cuatro bits son siempre 1110
Para la clase E, los cuatro bits son siempre 1111

Si deseamos conocer el rango de valores correspondiente a cada clase de red, estos deben encontrarse dentro de los primeros 8 bits y restarles la cantidad de bits constantes del prefijo (porque ya no deben modificar su valor). Hecho lo anterior tenemos:

Rango de la clase A 2^{7} = 128
Rango de la clase B 2^{6} = 64
Rango de la clase C 2^{5} = 32
Rango de la clase D 2^{4} = 16
Rango de la clase E 2^{4} = 16

Ahora bien, si lo que necesitamos es conocer el número de redes de cada clase, primero debemos considerar la cantidad de bits que se toman para asignar al *netid*. Para esto hay que recordar que la clase A toma 8 bits (octeto) para el *netid*, la B toma 16, C 24, D 23 y E 24. La fórmula para obtener el número de redes en cada clase es la siguiente:

Redes de la clase X = (Rango) ($2^{\text{netid} - 8}$)

ESTA TESIS NO DEBE
...OTECA

donde; Rango = valores permitidos para cada clase
netid = cantidad de bits asignados a cada clase para identificar la red
8 = indicador de que el primer octeto no debe tomarse en cuenta; ya que esta destinado para determinar el prefijo de la clase y el rango.

Redes de la clase A = (128) (2^{8-8}) = (128) (2^{0}) = (128) (1) = 128
Redes de la clase B = (64) (2^{16-8}) = (64) (2^{8}) = (64)(256) = 16 384
Redes de la clase C = (32) (2^{24-8}) = (32) (2^{16}) = (32)(65 536) = 2 097 152
Redes de la clase D [14] = (16) (2^{8-8}) = (16) (2^{0}) = (16)(1) = 16
Redes de la clase E = (16) (2^{8-8}) = (16) (2^{0}) = (16)(1) = 16

Una vez que conocemos la cantidad de redes de cada clase, es conveniente conocer cuantos hosts es posible direccionar en cada una de las redes según su clase; para lograrlo, es suficiente tomar el valor en bits del *hostid* como exponente de 2 y resolver.

Hosts en cada red de la clase A = (2^{24}) = 16 777 216
Hosts en cada red de la clase B = (2^{16}) = 65 536
Hosts en cada red de la clase C = (2^{8}) = 256
Hosts en cada red de la clase D = (2^{24}) = 16 777 216
Hosts en cada red de la clase E = (2^{24}) = 16 777 216

Por ultimo, para obtener el total de hosts direccionables para cada clase, se multiplican el número de redes en cada clase por el número de hosts de cada red según su clase.

Total de hosts de la clase A = (128) (16 777 216) = 2 147 483 648
Total de hosts de la clase B = (16 384) (65 536) = 1 073 741 824
Total de hosts de la clase C = (2 097 152) (256) = 536 870 912
Total de hosts de la clase D = (16) (16 777 216) = 268 435 456
Total de hosts de la clase E = (16) (16 777 216) = 268 435 456

Como se mencionó al principio, una dirección IPv4 direcciona la cantidad de 2^{32} números, que son considerados como identificadores de red y de hosts. Por lo anterior, antes obtener la capacidad de direccionamiento de IPv4 en Internet, se comprobará que no se ha rebasado esta cantidad.

[14] Para las clases D y E fue considerado un *netid* de 8 bits y un *hostid* de 24, sin restringir ninguna el uso de alguna de sus direcciones.

Para diseñar un modelo de comprobación, se considerará que la suma de todos los direccionamientos posibles por cada clase de red deben conducir al total de direccionamiento Internet. A la vez, cada uno de estos direccionamientos estará constituido por una longitud de 8 bits que determina la clase y la cantidad de redes (Rango) y dejará disponibles 24 para realizar combinaciones de bits que generen diferentes valores. Luego, si se toma los bits del rango y los disponibles como dos unidades, se podrá hacer que el producto de las dos unidades represente la cantidad de direcciones disponible en cada clase; y por ultimo, se procederá a sumar el producto de estas unidades para obtener la capacidad de direcciones IP de la versión 4.

Se formula:

Capacidad direccionamiento IPv4 = [(Rango de la clase A) (Disponible) +
(Rango de la clase B) (Disponible) +
(Rango de la clase C) (Disponible) +
(Rango de la clase D) (Disponible) +
(Rango de la clase E) (Disponible)]

Se sustituyen valores:

$$\text{Capacidad IPv4} = [\ (128)(2^{24}) + (64)(2^{24}) + (32)(2^{24}) + (16)(2^{24}) + (16)(2^{24})\ ]$$

Se factoriza:

$$\text{Capacidad IPv4} = (128 + 64 + 32 + 16 + 16)(2^{24})$$
$$= (256)(2^{24})$$
$$= (2^{8})(2^{24})$$
$$= (2^{8+24})$$

$$= \mathbf{2^{32}}$$ **Capacidad de direccionameinto IPv4 con una dirección de 32 bits**

$$\mathbf{2^{32} = 4\ 294\ 967\ 296}$$ **direcciones IPv4**

Tomando en consideración que existen algunas direcciones de uso especial como todas las que inician con el valor 127, las de la clase D y las de la clase E se deben excluir de la cantidad total de direccionamiento. También deben quedar fuera de consideración los octetos en 0 y en 255.

Cada dirección puede ser representada en 4 octetos con un valor decimal de 0 a 255 combinaciones de valores:

(1er. Octeto) (2do. Octeto) (3er. Octeto) (4°. Octeto) = 32 bits
$(2^8)(2^8)(2^8)(2^8) = (2^{24})$
$(256)(256)(256)(256) = (256^4)$

Clase A (considerar del 1 - 126)

Eliminamos el número 0 del primer octeto quedando 127 posibilidades de combinaciones. En cada octeto subsecuente se elimina el 0 y el 255, quedando con un valor máximo de 254.

$$(127)(254)(254)(254) = (126)(254^3)$$

Clase B (considerar del 128 - 191)

Se conserva el valor máximo de 64 del rango en el primer octeto. En cada octeto subsecuente se elimina el 0 y el 255, quedando con un valor máximo de 254.

$$(64)(254)(254)(254) = (64)(254^3)$$

Clase C (considerar del 192 - 223)

Se conserva el valor máximo de 32 del rango en el primer octeto. En cada octeto subsecuente se elimina el 0 y el 255, quedando con un valor máximo de 254.

$$(32)(254)(254)(254) = (32)(254^3)$$

Clase D (considerar del 224 - 239)

Se conserva el valor máximo de 16 del rango en el primer octeto. En cada octeto subsecuente se elimina el 0 y el 255, quedando con un valor máximo de 254.

$$(16)(254)(254)(254) = (16)(254^3)$$

Clase D (considerar del 224 - 239)

Eliminamos el número 255 del primer octeto quedando 15 posibilidades de combinaciones en el primer octeto. En cada octeto subsecuente se elimina el 0 y el 255, quedando con un valor máximo de 254.

$$(15)\,(254)\,(254)\,(254) = (15)\,(254^{3})$$

Aclarando los valores anteriores, reducimos las direcciones no válidas de la cantidad total de la siguiente manera:

Capacidad IPv4 real = [Clase A + Clase B + Clase C + Clase D + Clase E]

Se sustituyen los valores:

$$\begin{aligned}\text{Capacidad IPv4 real} = {} & [\,(127)\,(254^{3}) + (64)\,(254^{3}) + (32)\,(254^{3}) + \\ & (16)\,(254^{3}) + (15)\,(254^{3})\,] \\ = {} & (127 + 64 + 32 + 16 + 15)\,(254^{3}) \\ = {} & (254)\,(254^{3}) \\ = {} & (254^{4}) \\ = {} & 4\,162\,314\,256\end{aligned}$$

Se eliminan el valor 127 de la clase A, la clase D y la clase E

$$\begin{aligned}\text{Capacidad IPv4 real} = {} & (254^{4}) - [\,(1)\,(254^{3}) + (16)\,(254^{3}) + (15)\,(254^{3})\,] \\ = {} & (254^{4}) - [\,1 + 16 + 15\,(254^{3})\,] \\ = {} & (254^{4}) - [\,32\,(254^{3})\,] \\ = {} & (254)\,(254^{3}) - (32)\,(254^{3}) \\ = {} & 254 - 32\,(254^{3}) \\ = {} & 222\,(254^{3})\end{aligned}$$

Capacidad IPv4 real = 3 637 928 208

La capacidad de direccionamiento de IPv4, sin considerar la clase D, la clase E, los valores 127.X.X.X, los valores de 0 y 255 en los octetos es igual a 3 637 928 208 direcciones de hosts.

Interpretación de los resultados

Para efectos prácticos, se han tabulado las cifras de las direcciones IPv4 correspondientes a los datos que arrojan los cálculos sin restricciones del uso del 0, del 127.X.X.X y del 255, las cuales aparecen en la Tabla 4. 1

Clase de red	Redes	Direcciones IP por cada red	Total de direcciones IP en cada clase
A	128	16,777,216	2,147,483,648
B	16,384	65,536	1,073,741,824
C	2,097,152	256	536,870,912
D	16	16,777,216	268,435,456
E	16	16,777,216	268,435,456
Total	**2,113,696**	**50,397,440**	**4,294,967,296**

Tabla 4. 1 Capacidad de direccionamiento de IPv4

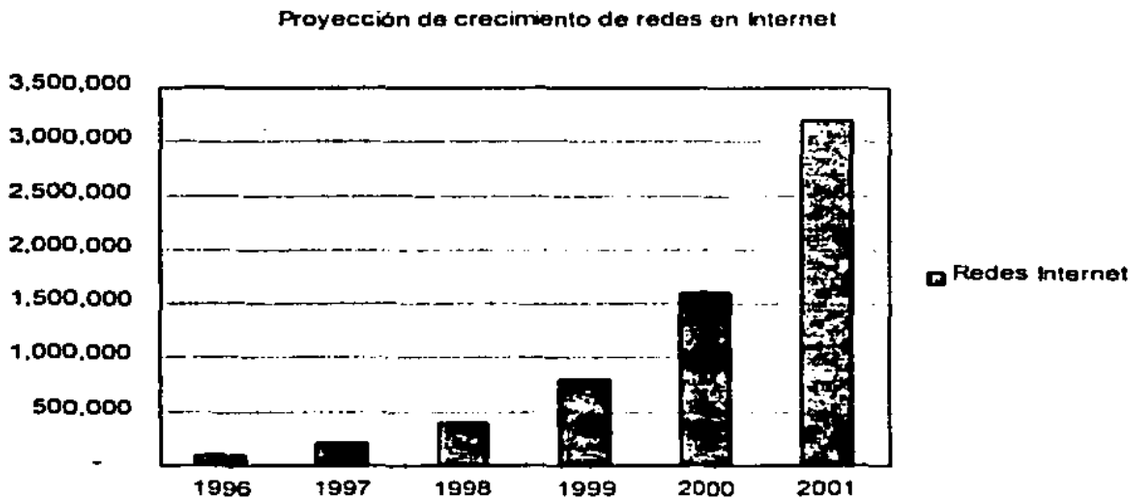
Como se puede observar, una red de la clase A necesita contar con 16,777,216 nodos para realmente agotar su capacidad. No obstante, es difícil que una red tenga una magnitud a esta escala. Además 128 es un número de redes que pueden ser fácilmente demandadas por empresas de gran tamaño alrededor del mundo. Cabe recordar, que el criterio principal para alinear las compañías que solicitan conexión a Internet es su tamaño, se considera que el número de redes para esta clase es pequeño y es razón suficiente para extinguirlo.

Por lo que respecta a B, es la clase con mayor problema de disponibilidad, debido a que las organizaciones medianas no encuentran suficiente el número de nodos proporcionados por la clase C, y la clase A es demasiado amplia para sus necesidades. Por ende, las solicitudes de direcciones IP se enfatiza sobre la clase B.

En la clase C, encontramos que el número de direcciones por red es chico. Por ejemplo: si una organización quisiera integrar su red de 320 nodos a Internet, tendría forzozamente que optar por solicitar un número de la clase B, o bien; dividir su red en dos de la clase C, con lo cual sobrecargaría sus tablas de ruteo.

Partiendo de lo anterior, se considera que el problema con el actual IP no es tanto la longitud de sus direcciones, sino más bien la asignación de valores para cada clase de red.

Se sabe que el tamaño de la dirección IP actual, permite identificar aproximadamente mas de 2 millones redes y 4 mil millones de hosts (de acuerdo al cálculo previo), de los cuales 13 millones de hosts Internet incluyendo PCs hasta supercomputadoras en más de 100,000 redes alrededor del mundo ya cuentan con una dirección IP, según una estimación de septiembre de 1996. Con los datos anteriores, se prevé el consumo total de direcciones IP entre los años 2000 y 2001, porque la cantidad de redes en Internet se está duplicando aproximadamente cada 10 a 12 meses. (Ver Gráfica 4. 2).



Grafica 4. 2 Proyección de la estimación del crecimiento de Internet

Como se muestra en la gráfica, para año 2001 la demanda de más de 3 millones de redes habría superado la capacidad de Internet, con una diferencia de un millón de redes justificando éste problema la integración de un nuevo protocolo IP que le de solución.

Antes de que suceda lo anterior fue pensado diseñar el nuevo formato de 128 bits, a través de IPv6, el cual podrá identificar a cada protón de la Tierra (con 340 282 366 920 938 463 374 607 431 768 211 456 direcciones igual a 2^{128}). Se espera para el año 2000 haya cerca del 40 % de redes integradas con el nuevo modelo IPv6, la transición total se estima en cuatro años.

Con la nueva estructura de direcciones IP, se busca optimizar la asignación de éstas para asegurar una mejor administración y disminuir el desuso de direcciones IP. Con lo anterior se deduce que el problema de agotamiento de direcciones no se debe tanto al crecimiento de Internet, sino más bien, a la incorrecta asignación clases de dirección y rangos amplios.

4.4 ESQUEMA DE JERAQUÍAS DE LAS DIRECCIONES IPv6

Una vez determinada la longitud de la dirección IPv6 y calculada su capacidad de direccionamiento, es permisible analizar el interior de los tipos de direcciones IPv6 definidos hasta el momento de elaboración de este trabajo de investigación.

Los tipos y las jerarquías del espacio de direcciones de IPv6, no estan completamente asignados ni definidos, por lo tanto no se realizará un análisis tan a fondo como se hizo con IPv4. Sin embargo, lo que debe ser considerado importante para proponer a IPv6 en lugar de IPv4, es evaluar el criterio de jerarquías que se usan en las direcciónes ya diseñadas.

Lo más relevante y que proporciona la base para obtener un direccionamiento eficiente en IPv6, es precisamente su filosofía de jerarquías multinivel, donde cada parte podrá administrar y diseñar la estructura que más se adecue a sus necesidades.

Los prefijos de IPv6 han contemplado varias alternativas interesantes, que permitirán controlar todos aquellos nodos que tengan planeado conectarse a Internet y que en su momento han considerado permanecer aislado, pero IPv6 les brinda la flexibilidad de cambiar de criterio. La consideración de nodos no conectados a Internet, bajo el control del mismo; ha sido una medida que evita los conflictos de direcciones únicas.

La estructura multinivel adaptará a la cantidad de nodos que necesite cada entidad y facilitará la asignación de direcciones de una manera más real que como se ha venido haciendo con IPv4; tal es el caso de las redes clase A, donde es difícil que una organización cuente con 16 777 216 nodos a los cuales pueda asignar todas y cada una de las direcciones proporcionadas.

4.5 TRANSICIÓN DE IPv4 A IPv6

A momento de que se eliminan las imperfecciones de IPv4 y se da lugar a futuras características, IPv6 proporciona la flexibilidad de un cambio paulatino y discrecional.

Algunos de los puntos principales de la estrategia de cambio son:

1. IPv6 se puede instalar como cualquier otro software en los dispositivos de la red.
2. Los hosts, ruteadores y DNS pueden ser actualizados uno por uno.

3. Los prerequisitos son mínimos, para que un host en particular pueda ser actualizado, de inicio solo se requiere que su servidor DNS ya esté actualizado a IPv6.
4. No hay que redireccionar los dispositivos actuales.
5. Los dispositivos actuales con conectividad limitada, como es el caso de las impresoras, no necesitan ser actualizados.

La flexibilidad de la tansición de IPv4 a IPv6 otorga una ventaja frente a otras propuestas de la industria, puesto que permitirá a las redes del futuro no depender de protocolos que sean propios de una marca comercial.

Cabe señalar que la representación de direcciones IPv6 no serán problema para el usuario final, usuarios a nivel de administración tendrán que pasar por un proceso de ajuste en la configuración de los elementos de red, como los ruteadores. La confusión de la representación de direcciones de 128 parece demasiado larga, pero el usuario común solo le interesa usar el nombre de éstas y en pocas ocasiones tendrá que recordar la dirección en formato numérico hexadecimal.

4.6 LA TECNOLOGÍA EN DESARROLLO E IPv6

La tecnología actual y la del futuro demandan un IPv4 reformado, para permitir la comunicación punto a punto vía satélite, en estaciones de trabajo múltiples de satélites sincronizados; la conmutación de paquetes de radio y el Modo de Transmisión Asíncrona (*Asynchronous Transfer Mode ATM*).

Además, en este rubro se espera que algunos dispositivos como los teléfonos celulares y los localizadores, sean reemplazados con dispositivos que puedan comunicarse a través de redes con conexión por cable, redes con conexión infrarroja o redes inalámbricas desde cualquier sitio en el mundo.

También se ha pensado que cuando se reemplacen a los actuales teléfonos celulares y radios, surgirán aplicaciones para instalar dispositivos de control como: máquinas expendedoras automáticas, anuncios, motores y ventiladores. Dichos dispositivos de control proporcionarán útiles ventajas de operación y mercadeo si se conectan directamente a las redes. Así por ejemplo, se podrán revisar inmediatamente los reportes de ventas.

Se ha previsto que la integración de IPv6 a TCP/IP, y por consiguiente a Internet, permitirá tareas como: el encendido, calentamiento y refrigeración de equipos de control.

Transmisión y recepción de datos, voz y vídeo

Se espera mejorar las redes multimedia, mediante aplicaciones iteractivas que proclaman la creación de un protocolo más versátil, capaz de transmitir y recibir señales de datos, voz y video en tiempo real, sin sobrecargar la red con información de control y permita la comunicación de grandes cantidades de clientes en un servidor. Dadas éstas características, se ha previsto que la computadora y la televisión serán cada vez más parecidas.

Para lograr los requisitos de rapidez de transmisión, es esencial un IP que dirija datagramas a gran escala y permita la autoconfiguración, además de la simplicidad de encabezados que garanticen a los ruteadores menores procesos de lectura y se proyecten en costos bajos.

Cambio en la administración de direcciones internet

El número de redes existentes y las venideras demandan cambios de políticas de administración y de la jerarquía de las clases de redes Internet. La administración actual de redes Internet necesita modificar sus políticas, respecto al esquema de direcciones, debido a que ha originado desperdicios de las capacidades de cada clase y, el registro y control de las mismas se ha vuelto complejo.

CONCLUSIONES

La propuesta de integración de IPv6 en el protocolo TCP/IP elimina las deficiencias de direccionamiento implementadas en la versión actual IPv4. Los fundamentos de IPv6 para lograr un alto rendimiento de direccionamiento son los siguientes :

- La longitud de bits de una dirección IPv6 soportará la demanda de direccionamiento de todos los hosts futuros, lo que para IPv4 será imposible aproximadamente en el año 2001, ya que el crecimiento exponencial de Internet demanda mayor capacidad de direcciones IP.

- El formato del encabezado en su interior y en la operabilidad de cada uno de sus campos, coloca a IPv4 en desventaja. El formato de la cabecera IPv6 esta simplificado, de tal manera que se podrán omitir o incluir cabeceras suplementarias de acuerdo a las características de operación requeridas sin alterar los propósitos básicos de la capa Internet.

- La integración de IPv6 no permitirá el cese de ejecución de IPv4, es decir permitirá la interoperabilidad entre ambos. La decisión para cambiar el uso de IPv4 a IPv6 es discrecional, solo será coercitiva en la medida que la tecnología subyacente lo permita y en base a las aspiraciones de operabilidad de cada red.

- La interoperabilidad de IPv6 se logra mediante téenicas sencillas, aunque la transición total de la versión actual a la nueva de IP sea compleja, debido al gran número de hosts que cuentan con los servicios de Internet y además por el carácter evolutivo que implica aún IPv6.

- La demanda del usuario general requiere del rediseño de la versión actual de acuerdo a la tendencia de nuevas tecnologías de telecomunicaciones y de otros ámbitos que han estado relacionándose cada vez más.

- Internet y su grupo de colaboradores son los indicados para desarrollar los estándares de comunicación, puesto que es la red de redes más extensa del mundo. Si Internet no propone un modelo lo suficientemente confiable se desarrollarán muchos que quizá aumenten los problemas de compatibilidad.

- El nuevo modelo IPv6 no pretende eliminar a IPv4, sino que proporciona mejoras que están a disposición de quien decida integrarlas al protocolo TCP/IP en virtud de convivir con los avances tecnológicos actuales y del futuro. IPv6 tampoco se propone descalificar el logro obtenido por IPv4, el cual en su momento cubrió necesidades de su tiempo; ahora IPv6 trata de hacer lo mismo.

BIBLIOGRAFÍA

1. Bradner, S. "The Recommendation for the IP Next Generation Protocol

2. Carballar, José A. Internet: El Mundo en sus Manos. Wilmington. RA-MA. 1994. 372 p.

3. -----. El Libro de las Comunicaciones del PC: Técnicas, Programación y Aplicaciones. México. RA-MA. 1996. 743 p.

4. Castillo Rojas, O. ...[ET. AL.]. Administración Básica de los Servicios de Red en Solaris 2.X a través de TCP/IP. México, 1995. [S. P.]. Tesis (Lic. Informática). UNAM, FES-C.

5. Comer, Douglas E. Redes Globales de Información con Internet y TCP/IP: Principios Básicos, Protocolos y Arquitectura. 3 ed. México. Prentice-Hall. 1996. 621 p.

6. Cypser, R. J. Communications for Cooperating Systems: OSI,SNA and TCP/IP. New York. Addison-Wesley. 1992. 743 p.

7. Hinden, Robert M. y Deering, Stephen E. "IP Version 6 (IPv6) Specification". RFC 1883. Ipsilon Networks y Xerox PARC. Diciembre 1995. 37 p.

8. -----. "IP Version 6 Addressing Architecture". RFC 1883. Ipsilon Networks y Xerox PARC. Diciembre 1995. 18 p.

9. Hunt, Craig. TCP/IP: Network Administration. Sebastopol. O'Relly. 1994. 472 p.

10. Feit, Sidnie. TCP/IP: Architecture, Protocols and Implementation. New York. McGraw-Hill. 1993. 466 p.

11. Postel, Jon y Reynolds, Joyce. "Internet Official Protocol Standars". RFC 1720. USC/Information Sciences Institute. Noviembre 1994. 30 p.

12. Santifaller, Michael. TCP/IP and ONC/NFC: Internetworking in a UNIX Environment. 2 ed.Wokingham. Addison-Wesley, 1994. 288 p.

13. Stallings. William. Data and Computer Communications. New York. Macmillan. 1991. 847 p.

14. Stephen A., Thomas. IPng and the TCP/IP Protocols: Implementing the Next Generation Internet. New York. John Wiley. 1996. 500 p.

15. Tanenbaum, Andrew S. Computer Networks. 2 ed. Englewood Cliffs. Prentice-Hall. 1991. 658 p.