UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

MIGRACIÓN HACIA IPV6 DE LA RED DE CÓMPUTO DEL INSTITUTO DE ASTRONOMÍA DE LA UNAM

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

ING ~~LICENCIADO~~ **EN COMPUTACIÓN**

P R E S E N T A :

E D U A R D O A G U I L A R O L I V A R E S

ASESOR:
ING. LILIANA HERNÁNDEZ CERVANTES

MÉXICO **2002**

PAGINACION DISCONTINUA

A MI MADRE:
Porque de ti no recibí sino dedicación, amor y cuidados; gracias por ser tu, simplemente la mejor madre que pude haber tenido.

A MI PADRE:
Gracias por siempre procurarme lo mejor, darme la oportunidad de ser alguien de provecho y por sobre todas las cosas, por quererme como soy.

A MI HERMANO:
Gracias por indicarme el camino, porque siempre te has ocupado de mi, por todo tu apoyo y por confiar en mi.

A MARTHA:
Gracias por permitirme crecer a tu lado, por siempre impulsarme a ser mejor, por creer en mi y por sobre todo, gracias por tanto tiempo de amor.

A DON JOSÉ AGUILAR:
El niño que te gustaba cuidar y entretener, al que le ensañaste a jugar, hoy te dice gracias.... ¡HE CUMPLIDO!.

A MI ASESORA
Gracias porque me gúio con paciencia y éxito a lo largo de la realización de esta tesis.

INDICE

INTRODUCCIÓN

Con el auge que han cobrado las telecomunicaciones y los sistemas de cómputo a través de la red Internet y ahora Internet 2, ha sido necesaria una gran investigación y desarrollo de una tecnología que cubra todas estas necesidades ya que la actual, IPV4, no fue diseñada para trabajar ante tal demanda. En sus orígenes, cerca del final de la década de los setenta, esta fue la solución ideal ya que proporcionaba un medio de comunicación entre equipos de cómputo tan eficiente que fue el adoptado; incluso por las redes militares.

Sus ventajas eran muchas ya que uno de sus principios lo hace indiferente al sistema operativo en el que se necesite de su funcionalidad, cumple con las normas determinadas por el Modelo de Referencia OSI, permite un control de flujo y fragmentación, en caso de ser necesaria, de paquetes que viajan a través de la red, estas entre muchas otras razones hicieron que este protocolo fuera difundido a tal grado que se convirtió en la base de la red de redes.

Hoy en día existen numerosas necesidades que es necesario satisfacer, de acuerdo a la infraestructura de las telecomunicaciones así como a las necesidades de centros de investigación, universidades y público en general. Podemos encontrarnos que actualmente existe la educación a distancia, videoconferencias, bibliotecas digitales, transmisión de voz, telefonía celular, servicios de banda ancha, electrodomésticos con integración a Internet, entre muchos otros servicios que necesitan de un soporte por parte de una tecnología emergente que ha venido a perfeccionar y solucionar las carencias que se presentaban hasta hace muy poco, esta es IPV6, que junto con tecnología aplicada en hardware nos permite realizar transmisiones de datos a velocidades infinitamente superiores a su antecesor IPV4, además cuenta con muchas posibilidades mas como son la asignación de prioridades al enviar paquetes, en sistema de envío mas eficiente al simplificar el encabezado de cada paquete, acceso a medios de transmisión de mayor calidad y rapidez, etc.; pero tal vez la mayor aportación que nos puede ofrecer este protocolo a todos los usuarios en general, es su mayor capacidad de direccionamiento, ya que es de conocimiento público que eventualmente las direcciones IP se agotarían, con esta nueva versión, se pueden tener mas direcciones IP que estrellas en nuestro sistema solar.

Hasta ahora se ha hecho mención a las características de estos protocolos, pero hay que recordar que para que puedan llevar a cabo su función necesitan del apoyo de un conjunto de programas denominado Sistema Operativo. Un sistema operativo es, en esencia, un conjunto de programas integrados de tal forma que permiten al usuario interactuar con todos los dispositivos que componen una computadora, con la finalidad de obtener un beneficio. Existe una variedad de estos sistemas operativos en el mercado, pero en este proyecto nos enfocaremos como es necesario a los que se encuentran en funcionamiento en el Instituto de Astronomía de la UNAM, éstos son: Linux Red Hat 7.2, Solaris 8 y Microsoft Windows en sus versiones 98, 2000 Server y XP Profesional. Para la correcta implementación del protocolo IPV6 se deben conocer las características de cada uno de ellos, así como el correcto procedimiento de implementación y configuración de este protocolo.

Otro factor importante para que se pueda llevar a cabo la migración de la red de cómputo de éste instituto hacia IPV6, será conocer perfectamente bien cual es el proceso y las técnicas propias de la acción de migrar, es decir, se debe conocer las características y necesidades de la red para poder utilizar ya sea un túnel, un sistema de pila doble de protocolos o la simple traducción de encabezados de paquetes, éstas serán las técnicas que nos permitirán de una forma planificada y con apoyo en un estudio del estado que guarda la red, una migración exitosa hacia IPV6.

La finalidad de este proyecto es que el Instituto de Astronomía de la UNAM pueda contar con tecnología de vanguardia para poder ofrecer un servicio de mayor calidad a la población, es por ello que aquí se plantea el proceso que sufrió la red de cómputo de este Instituto para ser una red de gran velocidad con base en el protocolo IPV6 que solucionara los problemas actuales y, brinda la posibilidad de crecimiento conforme surjan nuevas tecnologías o necesidades, además, también se propone la creación de una biblioteca digital, ésta solucionaría, sin destituir el sistema bibliotecario tradicional, las carencias que existen en nuestra casa de estudios, ya que al estar disponible en la red, cada usuario que se pueda conectar será capaz de consultar no sólo los datos bibliográficos del título en cuestión, además, tendrá a su disposición los índices alfabéticos y temáticos así como la multimedia que lo acompañe, además de poder consultar las tesis de alumnos pertenecientes a

generaciones anteriores y un salón de charla donde podrán discutir acerca de algún tema de investigación o título en particular de su área de desempeño.

Así pues, me permito invitarle a que lea estas páginas que es mi deseo sean de utilidad tanto para nuestra casa de estudios como para generaciones de futuros Ingenieros en Computación.

Capitulo I

"Descripción IPV4"

PROTOCOLO DE INTERNET VERSIÓN 4

1.1 INTRODUCCIÓN AL IPV4.

El Protocolo Internet es uno de los más utilizados en el enlace de redes y está diseñado para su uso en sistemas interconectados de redes de comunicación de equipos de cómputo por intercambio de paquetes.

IP implementa dos funciones básicas: el encaminamiento y la fragmentación. Para la primera de las funciones se sirve de uno de los campos que aparecen la cabecera de los datagramas, se trata de la dirección IP del host destino. Esta dirección es utilizada para transmitir los datagramas hacia el host correspondiente.

La segunda de las funciones está influenciada por el nivel que se encuentra situado justo debajo de la capa IP, se trata del nivel de enlace. Los datagramas generados por IP deben amoldarse al tamaño máximo que es capaz de tratar la red, es cual está limitado por la capa del nivel de enlace.

En cierto sentido una red de redes[1] es una abstracción de una red física porque, en los niveles inferiores, proporciona la misma funcionalidad: acepta paquetes y los entrega. En los niveles superiores el software de la red de redes aporta la mayor parte de las funciones más elaboradas que percibe el usuario.

Conceptualmente una red TCP / IP proporciona tres conjuntos de servicios y su distribución sugiere una dependencia entre ellos en el nivel inferior, un servicio de entrega sin conexión proporciona el fundamento sobre el cual se apoya el resto. En el siguiente nivel un servicio de transporte confiable proporciona una plataforma de alto nivel de la que depende el siguiente nivel que es un servicio de la aplicación.

[1] Una red de redes se compone de muchas redes físicas, interconectadas por computadoras conocidas como ruteadores. Cada ruteador tiene conexiones directas hacia dos o más redes.

Una de las ventajas más significativas de esta separación de conceptos es que es posible reemplazar un servicio sin afectar a los otros. El software de Internet está diseñado en torno a estos tres conceptos de red arreglados jerárquicamente; muchos de los éxitos alcanzados se deben a esta arquitectura sorprendentemente robusta y adaptable.

El servicio más importante de la red la red de redes consiste en un sistema de entrega de paquetes, el servicio se define como un sistema de entrega de paquetes sin conexión. El servicio se conoce como no confiable porque la entrega no está garantizada. Los paquetes se pueden perder, duplicar, retrazar o entregar sin orden, pero el servicio no detectará estas condiciones ni informará al emisor o al receptor.

Una secuencia de paquetes que se envían de una computadora a otra puede viajar por diferentes rutas, alguno de los cuales puede perderse mientras otros se entregan. La no confiabilidad aparece solo cuando los recursos están agotados o la red subyacente falla. Así podemos definir que la función o propósito del Protocolo Internet es mover datagramas a través de un conjunto de redes interconectadas.

1.2 DESCRIPCIÓN Y FUNCIONAMIENTO

La función del IP es encaminar datagramas a través de una serie de redes interconectadas. Este proceso se lleva a cabo pasando los datagramas desde un módulo Internet hacia otro, hasta alcanzar el destino deseado. Se entiende por módulo de Internet aquellos servicios que lleva a cabo la capa de red dentro de una arquitectura TCP/IP.

1.2.1 ENCAMINAMIENTO.

Cuando se habla de encaminamiento, es importante saber diferenciar entre un nombre de host, una dirección IP y una ruta. Se puede decir que el nombre indica el host que buscamos, la dirección indica dónde se encuentra y la ruta cómo llegar hasta él.

Cuando fue estandardizado IP por primera ocasión en septiembre de 1981, la especificación requirió que cada sistema asociado a IP tuviera asignado un único valor de 32 bits en su dirección de Internet, Algunos sistemas, tales como ruteadores, que tengan interfases a más de una red, se debe asignar una dirección única de IP para cada interfase de red.

Una dirección IP (en esta versión) está formada por cuatro números enteros, cada uno de ellos de un byte y separados por un punto. Las direcciones IP se componen de dos partes, la primera parte de una dirección de Internet identifica la red en la cual el ordenador principal reside, mientras que la segunda parte identifica el ordenador principal determinado en la red dada.

Para proveer la flexibilidad requerida para apoyar redes diferentes tamaño, los diseñadores decidieron que el espacio de la dirección de IP se debe dividir en cuatro clases diferentes de la dirección:

Clase A. Destinan un byte para identificar la red y tres bytes para identificar a los hosts dentro de dicha red. El bit más significativo del byte destinado a la red tiene el valor de cero, por lo que los rangos de redes posibles van desde 1 hasta 126. mediante los tres bytes destinados a los hosts se direccionan más de 16 millones de host en cada red. Un ejemplo de red de la clase A es: 12.100.20.30 que representa la red 12 y el host 100.20.30 dentro de dicha red.

Clase B. Destinan dos bytes para identificar la red y dos bytes para identificar los host dentro de ella. Los dos bits más significativos de los destinados a identificar la red tienen el valor uno y cero respectivamente. Esto significa que los rangos de redes permitidos van desde 128.1 hasta 191.254. Mediante los dos bytes destinados a los hosts se pueden representar más de 65,000 equipos. Un ejemplo de dirección de clase B es el siguiente: 141.17.90.239, que representa la red 141.17 y el host 90.239 dentro de ella.

Clase C. Destinan tres bytes para identificar la red y un byte para identificar a los host. Los tres bits más significativos de los bytes que identifican la red valen uno, uno y cero respectivamente. Esto permite rangos que van desde 192.1.1 hasta 223.254.254, y mediante el byte destinado a los hosts se puede identificar a 254 equipos.

Clase D. Son redes cuya dirección IP es especial, ya que está reservada para grupos de multienvío. Su primer byte puede valer cualquier número entre 224 y 239, estos números indican la red, los tres bytes restantes indican el número de multienvío.

Existe una serie de direcciones que están reservadas para propósitos especiales. Por ejemplo, en una red clase C, como se dispone de un byte para representar a los hosts de la red, se podrían direccionar 256 equipos, sin embargo, la dirección cero y la dirección 255 están reservadas, con lo que el número total de equipos que se puede direccionar es de 254. La dirección cero está reservada para identificar a la red en sí, y la dirección 255 está reservada para envíos en forma *broadcast*[2].

Cada clase fija el límite entre el prefijo de la red y el número del ordenador principal en una punta diferente dentro de la dirección de 32 dígitos binarios. Existen además una serie de direcciones especiales como se muestra en la figura 1.1

DIRECCIÓN	DESCRIPCIÓN
0.0.0.0	Se utiliza como origen de una solicitud de configuración de arranque.
127.0.0.0	Reservada.
127.0.0.1	Interna (loopback). Cliente y servidor están en la misma máquina.
127.0.0.2 – 127.255.255.255	Reservadas.
128.0.0.0	Reservada.
191.255.0.0	Reservada.
192.0.0.0	Reservada.
10.0.0.0 – 10.255.255.255	Clase A reservada para Internet.
172.16.0.0 – 172.31.255.255	Clase B reservada para Internet.
192.168.0.0 – 192.168.255.255	Clase C reservada para Internet.
255.255.255.0	Reservada.
244.0.0.0 – 255.255.255.254	Reservada.
255.255.255.255	Broadcast. A todos los nodos de la red.

Fig. 1.1. Direcciones IP especiales.

1.2.2 MÁSCARA DE SUBRED.

[2] La técnica para enviar un mensaje a todos los nodos de una red es colocar todos los bits destinados a identificar los hosts con valor uno. A esta técnica se le conoce con el nombre de *broadcast*.

La parte de red de una dirección de clase A, B, o C tiene un tamaño fijo, sin embargo, las diferentes empresas u organizaciones pueden tener la necesidad de variar este tamaño y decidir cuantos bits se van a destinar para identificar las redes y cuantos para identificar los host. Por este motivo, los ruteadores deben ser capaces de saber a priori cuantos bits se han destinado para identificar una red y así poder encaminar los paquetes en este sentido o en otro. Para llevar a cabo dicho propósito se utiliza el concepto de *máscara de subred*. La máscara de subred es una secuencia de 32 bits, dentro de los cuales aquellos que tengan el valor uno identifican la red y los que tengan el valor cero identifican a los host.

1.2.3 DIRECCIONES SIN CLASE (CIDR)

El método de manejo de direcciones de red del tipo A, B y C es bastante ineficiente. Lo ideal sería que cada empresa o institución pudiera elegir cuantos bits necesita realmente para direccionar cada uno de los equipos de una red o subredes. Esto se consigue mediante la implementación de redes utilizando la técnica CIDR (Classless Internet Domain Routing).

Antes de 1992, el crecimiento exponencial del Internet comenzaba a levantar preocupaciones serias entre los miembros del IETF[3] acerca de la capacidad del sistema del encaminamiento de Internet al crecimiento del futuro de la escala y del apoyo. Estos problemas fueron relacionados con:

El agotamiento cercano del término del espacio de la dirección de la red de Class B
El crecimiento rápido en el tamaño de los vectores de encaminamiento globales de Internet
El agotamiento eventual del espacio de la dirección de 32 bits en IPv4

El crecimiento proyectado de Internet calculaba que era posible que los primeros dos problemas llegaran a ser críticos antes de 1994 o 1995. La respuesta a estos desafíos inmediatos era el desarrollo del concepto de Supernetting o de Classless Inter-Domain Routing (CIDR). El tercer problema, que era de una naturaleza más a largo plazo, está

[3] Internet Engineering Task Force (IETF)

siendo explorado actualmente por el grupo de funcionamiento de IP Next Generation (IPng o de IPv6) del IETF.

CIDR fue documentado oficialmente en septiembre de 1993 en RFC 1517, 1518, 1519, y 1520. CIDR apoya dos características importantes que benefician el sistema global del encaminamiento de Internet:

CIDR elimina el concepto tradicional de las direcciones de la red de clase A, B, y C. Esto permite la asignación eficiente del espacio de la dirección de IPv4 que permitirá el crecimiento continuo del Internet hasta que se despliegue IPv6.

CIDR soporta la adición de ruteo, dónde una sola entrada del vector de encaminamiento puede representar el espacio de la dirección quizás de millares de rutas tradicionales. Esto permite que una sola entrada del vector de encaminamiento especifique cómo encaminar el tráfico a muchas direcciones individuales de la red.

Sin el despliegue rápido de CIDR en 1994 y 1995, los vectores de encaminamiento de Internet tendrían en el exceso de 70.000 rutas (en vez del 30.000+ actual) y el Internet no estaría funcionando probablemente hoy!

1.2.4 CIDR PROMUEVE LA ASIGNACIÓN EFICIENTE DEL ESPACIO DE LA DIRECCIÓN DE IPV4

CIDR elimina el concepto tradicional de las direcciones de la red de Clase A, de Clase B, y de Clase C y las substituye por el concepto generalizado de un " prefijo de la red. " Los ruteadores utilizan el prefijo de la red, mejor que los primeros tres dígitos binarios de la dirección IP que se utiliza para determinar división entre el número de la red y el número del ordenador principal. Consecuentemente, CIDR apoya el despliegue de redes arbitrariamente clasificadas entre los 8, 16 o 24 bits dentro de su dirección IP.

En el modelo de CIDR, cada pieza de información del encaminamiento se anuncia con una máscara de dígitos binarios (o longitud del prefijo). La longitud del prefijo es una manera de especificar el número de dígitos binarios contiguos desde la izquierda en la porción de la

red de cada entrada del vector de encaminamiento. Por ejemplo, una red con 20 dígitos binarios en el número de la red y 12 dígitos binarios en el número del ordenador principal sería anunciada con una longitud del prefijo de 20 dígitos binarios (a / 20). Los ruteadores que utilizan CIDR confían en la información de la longitud del prefijo provista con la ruta.

En un ambiente sin clase, se ven los prefijos como bloques contiguos del espacio de la dirección de IP. Por ejemplo, todos los prefijos con el prefijo a / 20 representan la misma cantidad de espacio de la dirección (212 o 4.096 direcciones del ordenador principal). Además, el prefijo a / 20 se puede asignar a un número tradicional de la red de clase A, B o C.

Por ejemplo, una dirección de red 162.195/16 indica que la dirección de red es la 162.195 y que se utilizan 16 bits para la macara de subred.

Otro beneficio importante de CIDR es que desempeña un papel importante en controlar el crecimiento de los vectores de encaminamiento de Internet. La reducción de la información del encaminamiento requiere que el Internet esté dividido en dominios que dirigen. Dentro de un dominio, la información detallada está disponible acerca de todas las redes que residen en el dominio como se muestra en la figura 1.2. Fuera de un dominio que dirige, solamente se anuncia el prefijo común de la red. Esto permite que una sola entrada del vector de encaminamiento especifique una ruta a muchas direcciones individuales de la red.

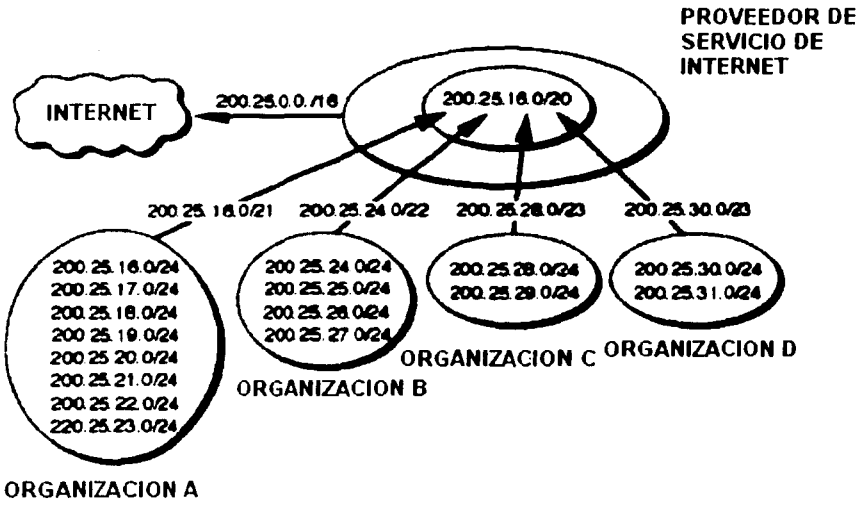


Figura 1.2. Redes residentes en un dominio.

1.2.5 SUBNETTING

El despliegue de subnetting dentro de la red privada provee varios beneficios:

El tamaño del vector de encaminamiento global de Internet no crece porque el administrador del sitio no necesita obtener el espacio adicional de la dirección y los anuncios del encaminamiento para todos los subnets se combinan en una sola entrada del vector de encaminamiento.

El administrador local tiene la flexibilidad de desplegar subnets adicionales sin la obtención de un nuevo número de la red del Internet.

La ruta que aletea (es decir, el cambiar rápido de rutas) dentro de la red privada no afecta el vector de encaminamiento de Internet puesto que las rebajadoras de Internet no saben acerca de el reachability de los subnets individuales - justo saben acerca de el reachability del número de la red del padre.

1.2.6 MÁSCARA DEL SUBNET

Los estándares que describen protocolos modernos del encaminamiento refieren a menudo a la longitud del extendido-red-prefijo más bien que a la máscara del subnet. La longitud del prefijo es igual al número de los dígitos binarios contiguos uno en la máscara tradicional del subnet. Esto significa que especificar la dirección 130,5,5,25 de la red con una máscara del subnet de 255,255,255,0 se puede también expresar como 130,5,5,25/24.

El despliegue de un plan que dirige requiere pensamiento cuidadoso de parte del administrador de la red. Hay cuatro preguntas claves que deben ser contestadas antes de que cualquier diseño sea emprendido:

¿Cuántos subnets totales necesita hoy la organización?

¿Cuántos subnets totales necesitará en el futuro la organización?

¿Cuántos equipos de cómputo principales hay en el subnet más grande de la organización hoy?

¿Cuántos equipos de cómputo principales estarán en el subnet más grande de la organización del futuro?.

1.3 FORMATO DE LA CABECERA IP (DATAGRAMA).

El protocolo Internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. También se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

En una red física la unidad de transferencia es una trama que contiene un encabezado de datos, donde el encabezado contiene información sobre la dirección de la fuente (física) y la del destino. La red de redes llama a esta unidad de transferencia básica *datagrama*, a

veces *datagrama IP* o simplemente *datagrama.* Un datagrama se divide en áreas de encabezados y datos. El encabezado contiene la información de la fuente y del destino.

No existen mecanismos para aumentar la fiabilidad de los datos entre los extremos, control de flujo, secuenciamiento u otros servicios que se encuentran normalmente en otros protocolos host-a-host. El protocolo Internet trata cada datagrama de Internet como una entidad independiente no relacionada con ningún otro datagrama de Internet.

El servicio básico Internet está orientado a datagramas y posibilita la fragmentación de datagramas en las pasarelas, teniendo lugar el reensamblaje en el módulo Internet de destino en el host de destino. En la figura 1.2 se muestra la estructura de un datagrama.

A continuación describiré brevemente los campos que componen un datagrama como el mostrado en la figura 1.2, así como de su tamaño en bits:

<table>
<tr><td colspan="4">0 1 2 3</td><td colspan="4">4 5 6 7</td><td colspan="8">8 9 0 1 2 3 4 5</td><td colspan="8">6 7 8 9 0 1 2 3</td><td colspan="6">4 5 6 7 8 9 0 1</td></tr>
<tr><td colspan="4">Versión</td><td colspan="4">Identificación</td><td colspan="8">Tipo de Servicio</td><td colspan="14">Longitud Total</td></tr>
<tr><td colspan="22">Identificación</td><td colspan="3">Flags</td><td colspan="7">Posición</td></tr>
<tr><td colspan="8">Tiempo de Vida</td><td colspan="14">Protocolo</td><td colspan="10">Suma de Control de Cabecera</td></tr>
<tr><td colspan="32">Dirección de Origen</td></tr>
<tr><td colspan="32">Dirección de Destino</td></tr>
<tr><td colspan="25">Opciones</td><td colspan="7">Relleno</td></tr>
</table>

Fig. 1.2 Ejemplo de Cabecera de un Datagrama Internet

Versión: 4 bits. El campo Versión describe el formato de la cabecera Internet.

Identificación: 4 bits. Longitud de la Cabecera Internet (Internet Header Length), es la longitud de la cabecera en palabras de 32 bits, y por tanto apunta al comienzo de los datos.

Tipo de Servicio: 8 bits. El Tipo de Servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet.

Longitud Total: 16 bits. La Longitud Total es la longitud del datagrama, medida en octetos, incluyendo la cabecera y los datos.

Identificación: 16 bits. Es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un datagrama.

Flags (indicadores): 3 bits. Son diversos indicadores de control.

Bit 0: reservado, debe ser cero.

Bit 1: (DF) No Fragmentar. 0 = puede fragmentarse, 1 = No Fragmentar.

Bit 2: (MF) Más Fragmentos. 0 = Último Fragmento,1 = Más Fragmentos.

Posición del Fragmento: 13 bits. Este campo indica a que parte del datagrama pertenece este fragmento.

Tiempo de Vida: 8 bits. Este campo indica el tiempo máximo que el datagrama tiene permitido permanecer en el sistema Internet. El tiempo de vida es una indicación de un límite superior en el periodo de vida de un datagrama. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado.

Protocolo: 8 bits. Este campo indica el protocolo del siguiente nivel usado en la parte de datos del datagrama.

Suma de Control de Cabecera: 16 bits. Suma de Control de la cabecera solamente. Dado que algunos campos de la cabecera cambian (p. ej. el tiempo de vida), esta suma es recalculada y verificada en cada punto donde la cabecera es procesada. La Suma de control de cabecera proporciona una verificación de que la información utilizada al procesar el datagrama ha sido transmitida correctamente.

Dirección de Origen: 32 bits. La dirección de origen.

Dirección de Destino: 32 bits. La dirección de destino.

Opciones: Variable. Las opciones pueden o no aparecer en los datagramas. Las Opciones proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes.

1.3.1 OTROS CAMPOS DE ENCABEZADO DE DATAGRAMA.

El campo PROTOCOLO es análogo al campo tipo en una trama de red. El valor en el campo PROTOCOLO especifica que protocolo de alto nivel se utilizó para crear el mensaje que se está transportando en el área DATOS de un datagrama.

El campo SUMA DE CONTROL DE CABECERA asegura la integridad de los valores del encabezado. La suma de verificación IP se forma considerando al encabezado como una secuencia de enteros de 16 bits, sumándolos juntos mediante el complemento aritmético a uno, y después tomando el complemento a uno del resultado. Es importante notar que la suma de verificación sólo se aplica a valores de encabezado IP y no para los datos.

1.4 OPCIONES PARA LOS DATAGRAMAS INTERNET

El campo OPCIONES del IP aparece a continuación de la dirección de destino y no se requiere en todos los datagramas; las opciones se incluyen en principio para pruebas de red o depuración. Sin embargo, el procesamiento de las opciones es parte integral del protocolo IP, por lo tanto, todos los estándares de implementación se deben incluir.

Cuando las opciones están presentes en un datagrama, aparecen contiguas, sin separadores especiales entre ellas. Cada opción consiste en un solo octeto de código de opción que debe llevar a continuación un solo octeto y un conjunto de octetos de datos para cada opción. El octeto de código de opción de divide en tres campos como se muestra en la figura 1.3

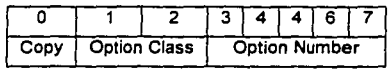


Fig. 1.3 División de octeto del código de opción.

El campo consiste en una bandera de un bit, llamada COPY, un segmento de dos bits, OPTION CLASS, y un segmento de cinco bits, OPTION NUMBER. La bandera COPY controla la forma en que los ruteadores tratan las opciones durante la fragmentación. Cuando el bit COPY esta puesto a uno, especifica que la opción se debe copiar en todos los fragmentos. Cuando esta puesto a cero el bit COPY significa que la opción sólo se debe copiar dentro del primer fragmento y no en todos los fragmentos.

Los bits OPTION CLASS y OPTION NUMBER especifican la clase general de opción y establecen una opción específica en esta clase. La tabla de la figura 1.4 lista las opciones posibles que pueden acompañar a un datagrama IP y muestra los valores para OPTION CLASS y OPTION NUMBER.

OPTION CLASS	OPTION NUMBER	LONGITUD	DESCRIPCIÓN
0	0	-	Fin de la lista de opciones. Se utiliza si las opciones no terminan al final del encabezado.
0	1	-	No operación. Se utiliza para alinear octetos en una lista de opciones.
0	2	11	Seguridad y restricciones de manejo.
0	3	Variable	Ruteo no estricto de fuente. Se utiliza para rutear un datagrama a través de una trayectoria específica.
0	7	Variable	Registro de ruta. Se utiliza para registrar el trayecto de una ruta.
0	8	4	Identificador de flujo. Se utiliza para transportar un identificador de flujo SATNET
0	9	Variable	Ruteo estricto de fuente. Se utiliza para establecer la ruta de un datagrama en un trayecto específico.
2	4	Variable	Sello de tiempo Internet. Se utiliza para registrar sellos de hora a lo largo de una ruta.

Fig. 1.4 Tabla de opciones posibles IP.

1.4.1 OPCIÓN DE REGISTRO DE RUTA.

Las opciones de ruteo y sello de hora (timestamp) son las más interesantes porque proporcionan una manera de monitorear o controlar la forma en que la red de redes maneja las rutas de los datagramas. La opción *registro de ruta* permite a la fuente crear una lista de direcciones IP y arreglarla para que cada ruteador que maneje el datagrama añada su propia dirección IP a la lista. La figura 1.5 muestra el formato de la opción de registro de ruta.

0	8	16	31
Code	Lenght	Pointer	
First IP Adress			
Second IP Adress			
...			

Fig. 1.5 Formato de una opción de registro de ruta.

El campo Code contiene la clase de opción y el número de opción (cero y siete para el registro de rutas). El campo Lenght especifica la longitud total de la opción como aparece en el datagrama IP, incluyendo los tres primeros octetos. El campo comienza con un First IP Adress que comprende el área reservada para registrar las direcciones de la red de redes. El campo Pointer especifica el desplazamiento dentro de la opción de la siguiente ranura disponible. Cada vez que una máquina maneja un datagrama que tiene activada la opción de registro de ruta, la máquina añade su dirección a la lista del registro de ruta.

El IP soporta dos formas de ruteo de fuente. Una forma, conocida como *ruteo estricto de fuente*, especifica una vía de ruteo incluyendo una secuencia de direcciones IP en la opción como se muestra en la figura 1.6.

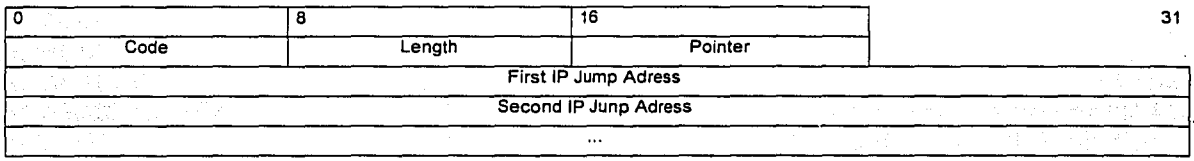


Fig. 1.6 opción de ruta estricta de fuente.

El ruteo estricto de fuente significa que las direcciones especifican la ruta exacta que los datagramas deben seguir para llegar a su destino. La ruta entre dos direcciones sucesivas de la lista debe consistir en una sola red física. La otra forma, conocida como *loose source routing (ruteo no estricto de la fuente)*, también incluye una secuencia de direcciones IP. Ésta especifica que el datagrama debe seguir la secuencia de direcciones IP, pero permite múltiples saltos de redes entre direcciones sucesivas de las lista.

El formato de una opción de ruta de fuente recuerda al de la opción de registro de ruta, mostrada anteriormente. Cada ruteador examina los campos Pointer y Lenght para ver si la lista está completa. Si es así, el campo puntero es mayor que la longitud y el ruteador establece la ruta del datagrama hacia su destino como lo hace normalmente. Si la lista no está completa, el ruteador sigue al puntero, toma la dirección IP, la reemplaza con la dirección del ruteador y establece la ruta para el datagrama utilizando la dirección que obtuvo de la lista.

1.4.2 OPCIÓN DE SELLO DE HORA.

La opción de sello de hora trabaja como la opción de registro de ruta. La opción de sello de hora contiene una lista inicial vacía y cada ruteador, a lo largo de la ruta, desde la fuente hasta el destino, escribe sus datos en la lista. Cada entrada a la lista contiene dos datos de 32 bits: la dirección IP del ruteador que proporciona la entrada y un entero de sello de hora de 32 bits. La figura 1.7 muestra el formato de la opción sellos de hora.

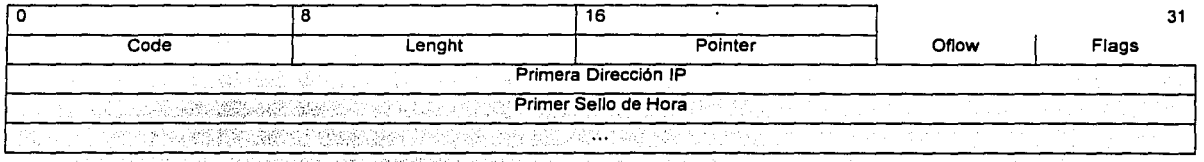


Fig. 1.7 Formato de una opción de sellos de hora.

Los campos Lenght y Pointer se utilizan para especificar la longitud del espacio reservado para la opción y la localización de la siguiente ranura no utilizada. El campo de cuatro bits Oflow contiene un contador entero de ruteadores que podría no proporcionar un sello de hora si la opción fue demasiado pequeña. El valor del campo Flags de cuatro bits controla el formato exacto de la opción y establece como los ruteadores deben suministrar el sello de hora.

El sello de hora define la hora y la fecha en la que un ruteador manejó el datagrama, expresado en milisegundos desde la media noche Tiempo Universal (Hora del Meridiano de Greenwich). Si la representación estándar para la hora no está disponible, el ruteador puede utilizar cualquier representación de tiempo local disponible activando el bit de orden superior en el campo de sello y hora.

Cada máquina reportará una hora de acuerdo a su reloj local y los relojes pueden diferir. Así, el sello de hora deberá considerarse como una estimación, independientemente de la representación.

1.5 TIPO DE DATAGRAMAS DE SERVICIOS Y PRIORIDAD DE DATAGRAMAS.

Conocido informalmente como *Type Of Service (TOS)*, el campo de ocho bits *Tipo de Servicio* especifica como debe manejarse el datagrama; el campo está subdividido en cinco subcampos, como se muestra en la figura 1.8.

0	1	2	3	4	5	6	7
Prioridad			D	T	R	Sin Uso	

Figura 1.8 Tipo de servicios.

Tres bits en el campo Prioridad especifican la prioridad de datagrama, con valores que abarcan de 0 (prioridad normal) a siete (control de red), permitiendo con ello indicar al emisor la importancia de cada datagrama. Este es un concepto importante dado que proporciona un mecanismo que permite controlar la información, que tendrá prioridad en los datos.

Los bits D, T y R especifican el tipo de transporte deseado para el datagrama. Cuando está activado, el bit D solicita procesamiento con retardos cortos, el bit T, solicita un alto desempeño y el bit R solicita alta confiabilidad.

Hay que pensar en una solicitud de transporte como una simple indicación para los algoritmos de ruteo, no como un requerimiento obligatorio. Si un ruteador no conoce más que una posible ruta para alcanzar un destino determinado puede utilizar el campo de tipo de transporte para seleccionar una con las características más cercanas a la petición deseada.

Los datagramas que acarrean la información tecleada por un usuario hacia una computadora remota pueden tener el bit D activado, solicitando que la entrega sea lo más rápido posible, mientras que el transporte de datagramas en la transferencia de un archivo de datos grandes podría tener activado el bit T, solicitando que el recorrido se haga a través de una ruta que incluya un satélite de alta capacidad.

1.6 ENCAPSULACIÓN DE DATAGRAMAS.

A diferencia de las tramas de las redes físicas que pueden ser reconocidas por el hardware, los datagramas son manejados por el software. Estos pueden tener cualquier longitud seleccionada por el diseño de protocolo. El formato de los datagramas actuales asignan solamente 16 bits al campo de longitud total, limitando el datagrama a un máximo de 65,535 octetos. Sin embargo, ese límite puede modificarse en versiones de protocolos recientes.

Los datagramas se mueven de una máquina otra, éstos deben transportarse siempre a través de una red física subyacente. Para hacer eficiente el transporte en la red de redes, se debe garantizar que cada datagrama pueda viajar en una trama física distinta.

La idea de transportar un datagrama dentro de una trama de red es conocida como *encapsulación*. Para la red subyacente un datagrama es como cualquier otro mensaje que se envía de una máquina a otra. El hardware no reconoce el formato del datagrama ni entiende las direcciones de destino IP.

1.7 TAMAÑO DE DATAGRAMA, MTU DE RED Y FRAGMENTACIÓN.

En un caso ideal, el datagrama IP completo se ajusta dentro de una trama física haciendo que la transmisión a través de la red física sea eficiente. Cada tecnología de conmutación de paquetes establece un límite superior fijo para la cantidad de datos que pueden transferirse en una trama física. Por ejemplo, Ethernet limita la transferencia de datos a 1,500 octetos, mientras que FDI permite aproximadamente 4,4700 octetos por trama.

La *Unidad de Transferencia Máxima (MTU)* de una red puede tener un tamaño muy pequeño, algunas tecnologías de hardware limitan la transferencia a 128 octetos o menos. La limitación de los datagramas para que se ajusten a la MTU más pequeña posible en una red de redes hace que la transferencia sea ineficiente cuando estos datagramas pasan a través de una red que puede transportar tramas de un tamaño mayor, es por ello que es lugar de diseñar datagramas que se ajusten a las restricciones de la red física, el software TCP/IP

selecciona el tamaño de datagrama más conveniente desde el principio y establece una forma para dividir datagramas en pequeños fragmentos cuando el datagrama necesita viajara a través de una red que tiene una MTU pequeña. Las pequeñas piezas dentro de un datagrama dividido se conocen con el nombre de fragmentos y el proceso de división de un datagrama se conoce como *fragmentación*. La fragmentación por lo general se da en un ruteador a lo largo del trayecto entre la fuente del datagrama y su destino final.

El tamaño de cada fragmento se selecciona de manera que cada uno de éstos pueda transportarse de la red subyacente en una sola trama. Además dado que el IP representa el desplazamiento de datos en múltiplos de ocho octetos más cercano a la MTU de la red no es usual dividir el datagrama en fragmentos de tamaños iguales; los últimos fragmentos por lo general son más cortos que los otros.

Los fragmentos se deben reensamblar para producir una copia completa del datagrama original, antes de que pueda procesarse en su lugar destino. El protocolo IP no limita los datagramas a un tamaño pequeño, ni garantiza que los datagramas grandes serán entregados sin fragmentación, la fuente puede seleccionar cualquier tamaño de datagrama que considere apropiado; la fragmentación y el reensamblado se dan automáticamente sin que la fuente deba realizar ninguna acción especial. Las especificaciones IP establecen que los ruteadores pueden aceptar datagramas con una longitud equivalente al valor máximo de la MTU de las redes a las que están conectados. Además, un ruteador siempre maneja datagramas de hasta 576 octetos.

Cada fragmento contiene un encabezado de datagrama que duplica la mayor parte del encabezado del datagrama original seguido por tantos datos como puedan ser acarreados en el fragmento siempre y cuando la longitud total se mantenga en un valor menor a la MTU de la red en la que debe viajar.

1.7.1 REENSAMBLADO DE LOS FRAGMENTOS.

En una red de redes TCP/IP, una vez que un datagrama se ha fragmentado, los fragmentos viajan como datagramas separados hacia su destino final donde serán reensamblados. Preservar los fragmentos en todo el trayecto hasta su destino final tiene dos desventajas. Primero, dado que los datagramas no son reensamblados inmediatamente después de pasar a través de una red con una MTU pequeña, los fragmentos pequeños deben transportarse en esa forma desde el punto de fragmentación hasta el destino final. Segundo, si se pierde cualquier fragmento, el datagrama no podrá reensamblarse. La máquina de recepción hace que arranque un *temporizador de reensamblado* cuando recibe un fragmento inicial. Si el temporizador termina antes de que todos los fragmentos lleguen, la máquina de recepción descartará los fragmentos sin procesar el datagrama. Así, la probabilidad de perder un datagrama se incrementa con la fragmentación ya que la pérdida de un solo fragmento provoca la pérdida del datagrama completo.

1.7.2 CONTROL DE FRAGMENTACIÓN.

Tres campos en el encabezado del datagrama, IDENTIFICACION, FLAGS y FRAGMENT OFFSET, controlan la fragmentación y reensamblado de los datagramas. El campo IDENTIFICACION debe copiarse. Su propósito principal es que el destino tenga información acerca de qué fragmentos pertenecen a qué datagramas. Conforme llega cada fragmento, el destino utiliza el campo IDENTIFICACION junto con la dirección de la fuente del datagrama para identificar el datagrama. Las computadoras que envían datagramas IP deben generar un valor único para el campo IDENTIFICACION por cada datagrama.

Para un fragmento, el campo FRAGMENT OFFSET especifica el desplazamiento en el datagrama original de los datos que se están acarreando en el fragmento, medido en unidades de ocho octetos, comenzando con un desplazamiento igualа cero. Para reensamblar el datagrama, el destino debe obtener todos los fragmentos comenzando con el fragmento que tiene asignado un desplazamiento igual a cero hasta el fragmento con el desplazamiento de mayor valor. Los fragmentos no necesariamente llegarán en orden,

además no hay comunicación entre el ruteador que fragmento el datagrama y el destino que trata de ensamblarlo.

Los dos bits de orden menor del campo de tres bits FLAGS controlan la fragmentación. El primer bit de control ayuda en esta prueba especificando en que momento se debe fragmentar un datagrama. Se le conoce como *bit de no fragmentación* porque cuando está puesto a uno especifica que el datagrama no debe fragmentarse. Cada vez que un ruteador necesita fragmentar un datagrama que tiene activado el *bit de no fragmentación*, el ruteador descartará el datagrama y devolverá un mensaje de error a la fuente. El bit de orden inferior en el campo FLAGS especifica si el fragmento contiene datos intermedios del datagrama original o de la parte final. Este bit es conocido como *more fragments*. Cuando un fragmento llega, el campo TOTAL LENGHT en el encabezado consulta el tamaño del fragmento y no el tamaño del datagrama original; de esta manera el destino no puede utilizar el campo TOTAL LENGHT para determinar si ha reunido todos los fragmentos. El bit *more fragments* resuelve este problema con facilidad: cada vez que, en el destino, se recibe un fragmento con el bit more fragments desactivado, se sabe que ese fragmento acarrea datos del extremo final del datagrama original. Examinando FRAGMENT OFFSET y TOTAL LENGHT un receptor puede establecer en que momento los fragmentos que ha reunido contiene toda la información necesaria para reensamblar el datagrama original completo.

1.7.3 TIEMPO DE VIDA (TIME TO LIVE TTL)

El campo TIME TO LIVE especifica la duración en segundos del tiempo que el datagrama puede permanecer en el sistema de red de redes. Cada vez que una máquina introduce un datagrama se establece un tiempo máximo durante el cual el datagrama puede permanecer ahí. Los ruteadores y los anfitriones que procesan los datagramas deben decrementar el campo TIME TO LIVE cada vez que pasa un datagrama y eliminarlo de la red cuando su tiempo ha concluido.

Cada ruteador, a lo largo de un trayecto, desde una fuente hasta un destino, es configurado para decrementar por uno el campo TIME TO LIVE cuando se procesa el campo

del datagrama. Cada vez que un campo TIME TO LIVE llega a cero, el ruteador descarta el datagrama y envía un mensaje de error a la fuente. La idea de establecer un temporizador para los datagramas es interesante ya que garantiza que los datagramas no viajaran a través de la red indefinidamente, aun cuando una tabla de ruteo se corrompa. y los ruteadores direccionen los datagramas en un ciclo.

1.8 RUTEO DE DATAGRAMAS IP

1.8.1 RUTEO EN UNA RED DE REDES

En un sistema de conmutación de paquetes, el ruteo es el proceso de selección de un camino sobre el que se mandarán paquetes y el ruteador es la computadora que hace la selección. Dentro de una red de área amplia que tenga muchas conexiones físicas entre conmutares de datos, la red por sí misma es responsable de rutear paquetes desde que llegan hasta que salen. Las máquinas en el exterior no pueden participar en las decisiones; sólo ven la red como una entidad que entrega paquetes.

El ruteo IP selecciona un camino por el cual se debe enviar un datagrama. El algoritmo de ruteo IP debe escoger como enviar un datagrama pasando por muchas redes físicas.

De forma ideal, el software de ruteo examinaría aspectos como la carga de la red, la longitud del datagrama o el tipo de servicio que se especifica en el encabezado del datagrama, para seleccionar el mejor camino. Sin embargo, la mayor parte del software de ruteo es mucho menos sofisticado y selecciona rutas basándose en suposiciones sobre caminos más cortos.

1.8.2 ENTREGA DIRECTA E INDIRECTA.

Hablando sin formalismos, podemos dividir el ruteo en dos partes: *entrega directa y entrega indirecta*. La entrega directa, es la transmisión de un datagrama desde una máquina a través

de una sola red física hasta otra. Dos máquinas solamente pueden llevar a cabo la entrega directa si ambas se conectan directamente al mismo sistema subyacente de transmisión física (por ejemplo una sola red Ethernet). La entrega indirecta ocurre cuando el destino no es una red conectada directamente, lo que obliga al transmisor a pasar el datagrama a un ruteador para su entrega.

1.8.3 ENTREGA DE DATAGRAMAS SOBRE UNA SOLA RED.

Para transferir un datagrama IP, el transmisor encapsula el datagrama dentro de una trama física, transforma la dirección IP en una dirección física y utiliza la red para entregar el datagrama.

La forma más fácil de pensar en la entrega directa es como el paso final de cualquier transmisión de datagramas, aun si el datagrama atraviesa muchas redes y ruteadores intermedios. El último ruteador del camino entre la fuente del datagrama y su destino siempre conectará directamente a la red física de la máquina destino.

1.8.4 ENTREGA INDIRECTA.

La entrega indirecta es mas difícil que la directa porque el transmisor debe identificar un ruteador para enviar el datagrama. Luego, el ruteador debe encaminar el datagrama hacia la red de destino. Cuando un anfitrión quiere enviar un datagrama a otro, lo encapsula y lo envía hacia el ruteador más cercano. Sabemos que se puede alcanzar un ruteador debido a que todas las redes físicas están interconectadas, así que debe existir un ruteador conectando a cada una. Por lo tanto, el anfitrión de origen puede alcanzar un ruteador en una sola red física. Una vez que la trama llega al ruteador, el software extrae el datagrama encapsulado y el software IP y selecciona el siguiente ruteador a lo largo del camino hacia el destino. De nuevo, se coloca el datagrama en una trama y se envía a través de la siguiente red física hacia un segundo ruteador, y así sucesivamente, hasta que se puede entregar en forma directa.

1.8.5 RUTEO IP CONTROLADO POR TABLA.

El algoritmo usual de ruteo IP emplea una *tabla de ruteo Internet* (a veces conocida como una tabla de ruteo IP). En cada máquina se almacena información sobre los posibles destinos y sobre como alcanzarlos. Las tablas de ruteo solo necesitan contener prefijos de red y no direcciones IP completas.

Si cada tabla de ruteo contuviera información sobre cada posible dirección de destino, seria imposible mantener actualizadas las tablas. Además, como el número de destinos posibles es muy grande, las máquinas no tendrían suficiente espacio para almacenar tanta información.

1.8.6 RUTEO CON SALTO AL SIGUIENTE.

Utilizar la porción de red de una dirección de destino en vez de toda la dirección del anfitrión hace que el ruteo sea eficiente y mantiene reducidas las tablas de ruteo. También es importante, porque ayuda a ocultar información al mantener los detalles de los anfitriones específicos confinados al ambiente local en el que operan. Por lo común, una tabla de ruteo contiene pares (*N,R*), donde *N* es la dirección IP de una red de destino y *R* la dirección IP del *"siguiente"* ruteador en el camino hacia la red *N*. El ruteador R es conocido como el *salto siguiente* y la idea de utilizar una tabla de ruteo para almacenar un salto siguiente para cada destino es conocida como *ruteo con salto al siguiente*. La tabla de ruteo en el ruteador *R* sólo especifica un paso a lo largo del camino *R* a su red destino.

Todos los ruteadores listados en la tabla de ruteo de la máquina *M* deben residir en las redes con las que *M* se conecta de manera directa. Cuando el datagrama está listo para dejar *M*, el software IP localiza la dirección IP de destino y extrae la porción de red. Luego *M*, utiliza la porción de red para tomar una decisión de ruteo, seleccionando un ruteador que se pueda alcanzar directamente.

El tamaño de la tabla de ruteo depende del número de redes en la red; solamente crece cuando se agregan nuevas redes. Sin embargo, el tamaño y contenido de la tabla son independientes del número de anfitriones individuales conectados a las redes.

1.8.7 RUTAS ASIGNADAS POR OMISIÓN.

Otra técnica utilizada para ocultar información y mantener reducido el tamaño de las tablas de ruteo, es asociar muchos registros a un ruteador asignado por omisión. La idea es hacer que el software de ruteo IP busque primero la tabla de ruteo para encontrar la red de destino. Si no aparece una ruta en la tabla, las rutinas de ruteo envían el datagrama a un ruteador asignado por omisión.

El ruteo asignado por omisión es de gran ayuda cuando un sitio tiene pocas direcciones locales y sólo una conexión con el resto de la red de redes.

1.8.8 RUTAS POR ANFITRIÓN ESPECÍFICO.

Tener rutas por anfitrión le da al administrador de red local mayor control sobre el uso de la red, le permite hacer comprobaciones y también se puede utilizar para controlar el acceso por razones de seguridad. Cuando se depuran conexiones de red o tablas de ruteo, la capacidad para especificar una ruta especial hacia una máquina individual resulta ser especialmente útil.

1.8.9 EL ALGORITMO DE RUTEO IP.

```
Extraer la dirección IP de destino D, del datagrama y computar el prefijo de red N;
Si N corresponde a cualquier dirección de red directamente conectada
        Entregar el datagrama al destino D sobre dicha red;
Si no
        Si la ruta contiene una ruta con anfitrión especifico para D
                Enviar el datagrama al salto siguiente especificado en la tabla;
        Si no
                Si la tabla contiene una ruta para la red N
                        Enviar el datagrama al salto siguiente especificado en la tabla;
                Si no
                        Si la tabla contiene una ruta asignada por omisión
                                Enviar el datagrama al ruteador asignado por omisión especificado en la tabla;
                        Si no
                                Declarar error de ruteo.
                        Fin Si.
                Fin Si.
        Fin Si.
Fin Si.
```

Capitulo II

"Descripción IPV6"

PROTOCOLO INTERNET, VERSIÓN 6 (IPV6)

2.1 INTRODUCCIÓN AL IPV6

El IP versión 6 (IPV6) es la nueva versión del Protocolo Internet, aunque también es conocida como IPNG (Internet Protocol Next Generation). Es la versión 6, debido a que la 5 no pasó de la fase experimental. La compatibilidad con la versión 4 es prácticamente total, ya que se han incluido características de compatibilidad.

Algunas de las modificaciones, están encaminadas a mejorar la seguridad en la red, que apenas existía en la versión cuatro. La nueva versión del protocolo Internet (IPV6) intenta dar respuesta a algunos problemas planteados con la versión cuatro. Entre ellos la disponibilidad de direcciones IP, la gestión de direcciones, la seguridad en las trasferencias de información y la optimización de las comunicaciones multimedia. Los cambios del IPV4 al IPV6 recaen principalmente en las siguientes categorías:

- **Capacidades de Direccionamiento Extendida**. El IPV6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una auto configuración más simple de direcciones. El número de direcciones diferentes se ha multiplicado de una manera exagerada. Teóricamente, es posible tener 2128 direcciones diferentes. Este número quiere decir que se podrían llegar a tener más de 665.000 trillones de direcciones por metro cuadrado, aunque si siguieran una jerarquía, este número decrece hasta 1564 direcciones por metro cuadrado en el peor caso o tres trillones siendo optimistas. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos. El cambio mas significativo en las direcciones ha sido, que ahora, se refieren a un interfaz y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a estos mediante su interfaz.
- **Simplificación del Formato de Cabecera**. Algunos campos de la cabecera IPV4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso

de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPV6.

- **Soporte Mejorado para las Extensiones y Opciones**. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.
- **Capacidad de Etiquetado de Flujo**. Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".
- **Capacidades de Autenticación y Privacidad**. Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPV6.

IPV6 proporciona un soporte mejorado de aplicaciones multimedia y de tiempo real, como la videoconferencia, el audio conferencia o las aplicaciones de control, gracias a la incorporación de dos nuevas características: las prioridades y las etiquetas de flujo.

La gestión de prioridades de los paquetes se hace en función de la naturaleza de la información que transportan. Así en el caso de la videoconferencia, el audio es considerado más prioritario que el video, y el video de baja definición tendrá prioridad sobre el video de alta definición.

Las etiquetas de flujo permiten a los paquetes entre dos direcciones específicas recibir una gestión particular por parte del RSVP (Resource Reservation Protocol (Protocolo de Reservas de Recursos)) manteniendo una secuencia lógica de paquetes para garantizar el encaminamiento perfecto.

2.2 DESCRIPCIÓN Y FUNCIONAMIENTO

2.2.1 DIRECCIONES IP VERSIÓN 6

En el IPV6 existen tres tipos básicos de direcciones:

- **Direcciones unicast**: Están dirigidas a una única interfaz en la red. Actualmente se dividen en varios grupos, y existe un grupo especial que facilita la compatibilidad con las direcciones de la versión 4.
- **Direcciones anycast**: Identifican a un conjunto de interfaces de red. El paquete se enviará a cualquier interfaz que forme parte del conjunto. En realidad son direcciones unicast que se encuentran asignadas a varios interfaces.
- **Direcciones multicast**: Identifican a un conjunto de interfaces de la red, de manera que cada paquete es enviado a cada uno de ellos individualmente.

Las direcciones **broadcast** de IPV4 que van dirigidas a toda una red son tratadas en IPV6 como MULTICAST.

Para esta versión del protocolo IP la longitud del direccionamiento ha sido multiplicado por 4, pasando de 32 bits a 128 bits, con lo que se aumenta el número de direcciones posibles. Se prevé la creación de jerarquías de direcciones para simplificar y reducir las tablas de encaminamiento de los "ruteadores" en Internet.

Las direcciones IPV6 se dividen en 8 grupos de 16 bits expresados en hexadecimal y separados por dos puntos ":". Por ejemplo **"A500:0000:0000:0000:83AC:000E:0000:052D"**.

Está notación se puede simplificar eliminando los ceros de mayor peso (los de más a la izquierda) en cada palabra **(A500:0:0:0:83AC:E:0:52D)** o sustituyendo un grupo de palabras de valor cero por ":" **(A500::83AC:E:0:52D)**.

La estructura de la dirección IPV6 facilita la migración a partir de las redes IPV4 actuales. Una parte del espacio de direcciones de IPV6 ha sido reservado a las direcciones

IPV4. Existe una convención que permite escribir direcciones IPV4 en direcciones IPV6, usando las dos últimas palabras. Por ejemplo, **193.146.141.4** quedaría como **0:0:0:0:0:0:193.146.141.4** o abreviando **::193.146.141.4**.

2.2.2 AUTOCONFIGURACION

Una de características de IPV6 es su capacidad para configurar automáticamente un puesto con una dirección IP única o bien de forma dinámica (parecido al DHCP). Esta nueva prestación reduce bastante la sobrecarga administrativa y de gestión de direcciones que caracterizaba hasta el momento al protocolo IP

2.3 FORMATO DE LA CABECERA.

Formato de la Cabecera del IPV6

Octeto 0								Octeto 1								Octeto 2								Octeto 3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Versión								Clase de tráfico								Etiqueta de Flujo															
Longitud de carga Útil																Siguiente Cabecera								Límite de Saltos							
Dirección de Origen (128 bits)																															
Dirección de Destino (128 bits)																															

Esta cabecera ocupa el doble que la anterior, pero se ha simplificado omitiendo algunos campos y haciendo que otros sean opcionales. De esta manera, los ruteadores no tienen que procesar tanta información. Los campos son los siguientes:

- **Versión**: Este campo ocupa 4 bits, y contiene el número de versión del IP, en este caso 6.
- **Clase de tráfico**: Campo clase de tráfico de 8 bits.
- **Etiqueta de Flujo**: Ocupa 24 bits. Indica que el paquete requiere un tratamiento especial por parte de los ruteadores que lo soporten.

- **Longitud de la carga útil**: Entero sin signo de 16 bits. Longitud de la carga útil IPV6, es decir, el resto del paquete que sigue a esta cabecera IPV6, en octetos. (Notar que cualquiera de las cabeceras de extensión presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud).
- **Siguiente Cabecera**: Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPV6. Utiliza los mismos valores que el campo Protocolo del IPV4.
- **Límite de saltos**: Entero sin signo de 8 bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es decrementado hasta cero.
- **Dirección de origen**: Ocupa 128 bits (16 octetos), y es el número de dirección del originador del paquete.
- **Dirección de Destino**: Ocupa 128 bits (16 octetos). Es el número de dirección del destino (posiblemente no el último recipiente, si está presente una cabecera de Enrutamiento).

2.4 CABECERAS DE EXTENSION.

En el IPV6, la información de capa Internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPV6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguiente distinto. Un paquete IPV6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el campo Cabecera Siguiente de la cabecera precedente.

Las cabeceras de extensión no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega de un paquete, hast` que el paquete alcance el nodo (o cada uno del conjunto de nodos, en el caso de multienvío) identificado en el campo Dirección Destino de la cabecera IPV6.

El contenido y la semántica de cada cabecera de extensión determinan si se procede o no a la cabecera siguiente. Por lo tanto, las cabeceras de extensión se deben procesar

estrictamente en el orden que aparecen en el paquete; un receptor no debe, por ejemplo, examinar a través de un paquete buscando un tipo en particular de cabecera de extensión y procesar esa cabecera antes de procesar todas las precedentes.

Si, como resultado de procesar una cabecera, un nodo necesita proceder a la cabecera siguiente pero el valor Cabecera Siguiente en la cabecera actual es desconocido por el nodo, debe descartar el paquete y enviar un mensaje ICMP de Problema de Parámetro al origen del paquete, con un valor Código ICMP de 1 ("encontrado tipo de Cabecera Siguiente desconocido") y el campo Puntero ICMP conteniendo el desplazamiento del valor desconocido dentro del paquete original. La misma acción se debería tomar si un nodo encuentra un valor Cabecera Siguiente de cero en cualquier cabecera con excepción de una cabecera IPV6.

Una implementación completa del IPV6 comprende la implementación de las siguientes cabeceras de extensión:

- **Opciones de Salto a Salto**
- **Enrutamiento (Tipo 0)**
- **Fragmento**
- **Opciones de Destino**
- **Autenticación**
- **Seguridad del Encapsulado de la Carga Útil**

2.4.1 ORDEN DE LAS CABECERAS DE EXTENSIÓN

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

- **Cabecera IPV6**
- **Cabecera Opciones de Salto a Salto**

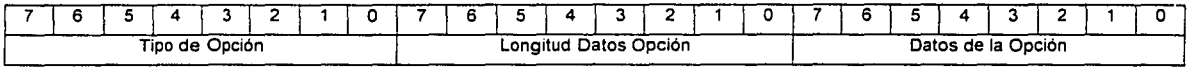
- **Cabecera Opciones de Destino**[1]
- **Cabecera Enrutamiento**
- **Cabecera Fragmento**
- **Cabecera Autenticación**[2]
- **Cabecera Seguridad del Encapsulado de la Carga Útil**
- **Cabecera Opciones de Destino**[3]
- **Cabecera de Capa Superior**

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

Los nodos IPV6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden y cualquier número de veces que ocurran en un mismo paquete, a excepción de la cabecera Opciones de Salto a Salto la cual está restringida a aparecer sólo inmediatamente después de una cabecera IPV6. No obstante, se aconseja fuertemente que los originadores de paquetes IPV6 se apeguen al orden recomendado arriba.

2.4.2 OPCIONES

Dos de las cabeceras de extensión actualmente definidas -la cabecera Opciones de Salto a Salto y la cabecera Opciones de Destino- llevan un número variable de "opciones" codificadas tipo-longitud- valor (TLV), de la siguiente forma:



[1] Para las opciones a ser procesadas por el primer destino que aparece en el campo Dirección Destino IPV6 más los destinos subsiguientes listados en la Cabecera Enrutamiento.

[2] Recomendaciones adicionales con respecto al orden relativo de las cabeceras Autenticación y Seguridad del Encapsulado de la Carga Útil se dan en el RFC-2406.

[3] Para las opciones a ser procesadas solo por el destino final del paquete.

- **Tipo de Opción.** Identificador de 8 bits del tipo de opción.
- **Longitud Datos Opción.** Entero sin signo de 8 bits. Longitud del campo Datos de la Opción de esta opción, en octetos.
- **Datos de la Opción.** Campo de longitud variable. Datos específicos del Tipo de Opción.

Los identificadores **Tipo de Opción** se codifican internamente de tal manera que sus 2 bits de más alto orden especifican la acción que se debe tomar si el nodo IPV6 en proceso no reconoce el Tipo de Opción:

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

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

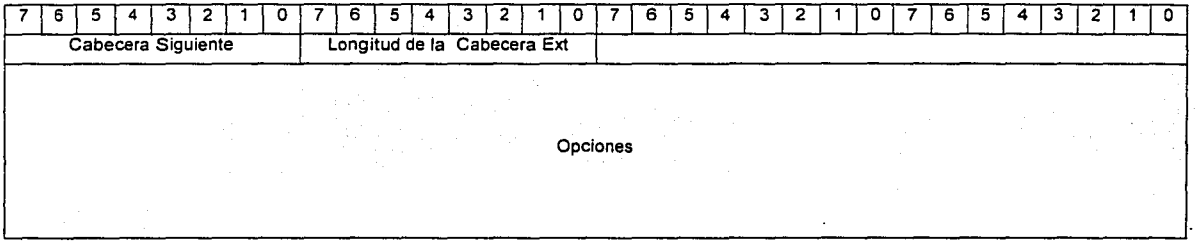
- **0**. Los Datos de la Opción no modifican el enrutado.
- **1**. Los Datos de la Opción pueden modificar el enrutado.

El mismo espacio de enumeración del Tipo de Opción se usa tanto para la cabecera Opciones de Salto a Salto como para la cabecera Opciones de Destino. Sin embargo, la

especificación de una opción en particular puede restringir su uso a solamente una de esas dos cabeceras.

2.4.3 CABECERA OPCIONES DE SALTO A SALTO

La cabecera Opciones de Salto a Salto se usa para llevar información opcional que debe ser examinada por cada nodo a lo largo de la ruta de entrega de un paquete. La cabecera Opciones de Salto a Salto se identifica por un valor Cabecera Siguiente de 0 en la cabecera IPV6 y tiene el siguiente formato:



- **Cabecera Siguiente**. Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Salto a Salto. Utiliza los mismos valores que el campo Protocolo del IPV4.
- **Longitud de la Cabecera Ext**. Entero sin signo de 8 bits. Longitud de la cabecera Opciones de Salto a Salto en unidades de 8 octetos, no incluye los primeros 8 octetos.
- **Opciones**. Campo de longitud variable, de longitud tal que la cabecera Opciones de Salto a Salto completa es un entero múltiplo de 8 octetos de largo.

2.4.4 CABECERA ENRUTAMIENTO

La cabecera Enrutamiento es utilizada por un origen IPV6 para listar uno o más nodos intermedios a ser "visitados" en el camino hacia el destino de un paquete. Esta función es

muy similar a las opciones Origen Impreciso y Registro de Ruta del IPV4. La cabecera Enrutamiento se identifica por una Cabecera Siguiente de valor 43 en la cabecera inmediatamente precedente, y tiene el siguiente formato:

7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Cabecera Siguiente								Longitud de la Cabecera Ext								Tipo de Enrutamiento								Segmentos Dejados							
Datos Específicos del tipo																															

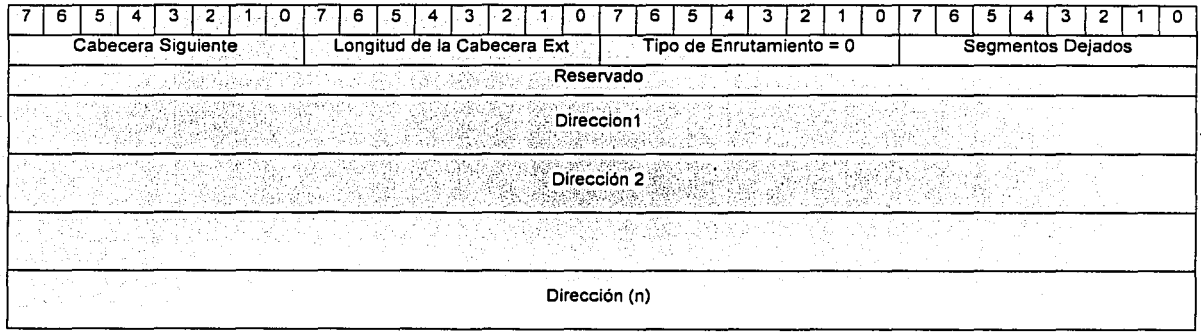
- **Cabecera Siguiente**. Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPV4.
- **Longitud de la Cabecera Ext**. Entero sin signo de 8 bits. Longitud de la cabecera Enrutamiento en unidades de 8 octetos, no incluye los primeros 8 octetos.
- **Tipo de Enrutamiento**. Identificador de 8 bits de una variante en particular de cabecera Enrutamiento.
- **Segmentos Dejados**. Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.
- **Datos específicos del tipo**. Campo de longitud variable, de formato determinado por el Tipo de Enrutamiento, y de longitud tal que la cabecera Enrutamiento completa es un entero múltiplo de 8 octetos de largo.

Si, al procesar un paquete recibido, un nodo encuentra una cabecera Enrutamiento con un valor Tipo de Enrutamiento desconocido, el comportamiento requerido del nodo depende del valor del campo Segmentos Dejados, como sigue:

- Si Segmentos Dejados es cero, el nodo debe ignorar la cabecera Enrutamiento y proceder a procesar la siguiente cabecera en el paquete, cuyo tipo se identifica por el campo Cabecera Siguiente en la cabecera Enrutamiento.

- Si Segmentos Dejados no es cero, el nodo debe descartar el paquete y enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección Origen del paquete, apuntando al Tipo de Enrutamiento desconocido.
- Si, después de procesar una cabecera Enrutamiento de un paquete recibido, un nodo intermedio determina que el paquete será remitido hacia un enlace cuya MTU de enlace es menor que el tamaño del paquete, el nodo debe descartar el paquete y enviar un mensaje ICMP Paquete Demasiado Grande a la Dirección Origen del paquete.

La cabecera Enrutamiento de Tipo 0 tiene el siguiente formato:



- **Cabecera Siguiente**. Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPV4.
- **Longitud de la Cabecera Ext**. Entero sin signo de 8 bits. Longitud de la cabecera Enrutamiento en unidades de 8 octetos, sin incluir los primeros 8 octetos. Para la cabecera Enrutamiento de Tipo 0, Longitud de la Cabecera Ext es igual a dos veces el número de direcciones en la cabecera.
- **Tipo de Enrutamiento**. 0.
- **Segmentos Dejados**. Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.

- **Reservado**. Campo reservado de 32 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
- **Dirección [1 ... n]**. Vector de direcciones de 128 bits, numerados desde 1 hasta n.

Las direcciones multienvío no deben aparecer en una cabecera Enrutamiento de Tipo 0, o en el campo Dirección Destino IPV6 de un paquete que lleva una cabecera Enrutamiento de Tipo 0.

2.4.4.1 ALGORÍTMO DE ENRUTAMIENTO TIPO O

Una cabecera Enrutamiento no se examina o procesa hasta que alcance el nodo identificado en el campo Dirección Destino de la cabecera IPV6. En ese nodo, al despachar el campo Cabecera Siguiente de la cabecera inmediatamente precedente ocasiona que el módulo cabecera Enrutamiento sea invocado, el cual, en el caso de Enrutamiento Tipo 0, lleva a cabo el siguiente algoritmo:

```
Si Segmentos Dejados = 0 {
      Proceder a procesar la cabecera siguiente en el paquete, cuyo tipo se identifica por el campo
      Cabecera Siguiente en la cabecera Enrutamiento
}
Sino Si Lon Cab Ext es impar {
      Enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección Origen, apuntando al
      campo Lon Cab Ext, y descartar el paquete
}
Sino {
      Calcular n, el número de direcciones en la cabecera Enrutamiento, al dividir Lon Cab Ext por 2

  Si Segmentos Dejados es mayor que n {
      Enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección de Origen, apuntando
      al campo Segmentos Dejados, y descartar el paquete
  }
  Sino {
      Decrementar Segmentos Dejados en 1;
      Calcular i, el índice de la dirección siguiente a ser visitado en el vector de dirección,
      substrayendo Segmentos Dejados de n

    Si la Dirección [i] o la Dirección Destino IPV6 es multienvío {
      Descartar el paquete
    }
    Sino {
      Intercambiar la Dirección Destino IPV6 y la Dirección [i]

      Si el Límite de Saltos es menor que o iguala a 1 {
```

```
                Enviar un mensaje ICMP Tiempo Excedido -- Límite de Saitos Excedido en Transito a la
                Dirección Origen y descartar el paquete
            }
            Sino {
              Decrementar el Límite de Saltos en 1;
              Resometer el paquete al módulo IPV6 para la transmisión hacia el nuevo destino
            }
          }
        }
      }
```

2.4.5 CABECERA FRAGMENTO

La cabecera Fragmento es utilizada por un origen IPV6 para enviar un paquete más grande de lo que cabría en la MTU de la ruta hacia su destino. (Nota: a diferencia del IPV4, la fragmentación en el IPV6 sólo se lleva a cabo por los nodos origen, no por los enrutadores a lo largo de la ruta de entrega de un paquete) La cabecera Fragmento se identifica por un valor Cabecera Siguiente de 44 en la cabecera inmediatamente precedente, y tiene el siguiente formato:

7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Cabecera Siguiente								Reservado								Desplazamiento del Fragmento													Res		M
Identificación																															

- **Cabecera Siguiente**. Selector de 8 bits. Identifica el tipo de cabecera inicial de la Parte Fragmentable del paquete original (definido abajo). Usa los mismos valores que el campo Protocolo del IPV4.
- **Reservado**. Campo reservado de 8 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
- **Desplazamiento del Fragmento**. Entero sin signo de 13 bits. El desplazamiento, en unidades de 8 octetos, de los datos que siguen a esta cabecera, relativo al comienzo de la Parte Fragmentable del paquete original.
- **Res**. Campo reservado de 2 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
- **Bandera M**. 1 = más fragmentos; 0 = último fragmento.

- **Identificación**. 32 bits. Número que diferencia al fragmento de los demás.

Para enviar un paquete que es demasiado grande para caber en la MTU de la ruta hacia su destino, un nodo origen puede dividir el paquete en fragmentos y enviar cada fragmento como un paquete separado, para ser reensamblado en el receptor.

Por cada paquete que será fragmentado, el nodo origen genera un valor Identificación. La Identificación debe ser diferente que el de cualquier otro paquete fragmentado enviado recientemente con la misma Dirección Origen y Dirección Destino. Si una cabecera Enrutamiento está presente, la Dirección Destino de interés es la del destino final.

El paquete inicial, grande, no fragmentado es referido como el "paquete original", y se considera que consiste en dos partes, tal como se ilustra:

PAQUETE ORIGINAL:

Parte No Fragmentable	Parte Fragmentable

La **Parte No Fragmentable** consiste en la cabecera IPV6 más cualesquiera de las cabeceras de extensión que debe procesarse por nodos en camino hacia el destino, es decir, todas las cabeceras e incluso la cabecera Enrutamiento si esta presente, sino la cabecera Opciones de Salto a Salto si esta presente, sino ninguna de las cabeceras de extensión.

La **Parte Fragmentable** consiste en el resto del paquete, es decir, cualquiera de las cabeceras de extensión que necesita que sólo se procese por el nodo(s) destino final, más la cabecera de capa superior y los datos. La Parte Fragmentable del paquete original es dividida en fragmentos, cada uno, excepto posiblemente el último ("el de la extrema derecha"), siendo un entero múltiplo de 8 octetos de largo. Los fragmentos se transmiten en "paquetes fragmento" separados tal como se ilustra:

PAQUETE ORIGINAL:

Parte No Fragmentable	Primer Fragmento	Segundo Fragmento	Último Fragmento

PAQUETES FRAGMENTO:

Parte No Fragmentable	Cabecera Fragmento	Primer Fragmento

Parte No Fragmentable	Cabecera Fragmento	SegundoFragmento

▪
▪
▪

Parte No Fragmentable	Cabecera Fragmento	ÚltimoFragmento

Cada paquete fragmento está compuesto de:

1) **La Parte No Fragmentable** del paquete original, con la Longitud de la Carga Útil de la cabecera IPV6 originai cambiada para contener la longitud de tan sólo este paquete fragmento (excluyendo la longitud de la propia cabecera IPV6), y el campo Cabecera Siguiente de la última cabecera de la Parte No Fragmentable cambiado a 44.
2) Una Cabecera Fragmento conteniendo:
   - El valor Siguiente Cabecera que identifica la primera cabecera de la Parte Fragmentable del paquete original.
   - Un Desplazamiento del Fragmento que contiene el desplazamiento del fragmento, en unidades de 8 octetos, relativo al comienzo de la Parte Fragmentable del paquete original. El Desplazamiento del Fragmento del primer ("el de la extrema izquierda") fragmento es 0.
   - Una bandera M de valor 0 si el fragmento es el último ("el de la extrema derecha"), sino una bandera M de valor 1.
   - El valor Identificación generado para el paquete original.
3) El propio **fragmento**.

Deben escogerse las longitudes de los fragmentos tal que los paquetes fragmento resultantes quepan dentro de la MTU de la ruta hacia el(los) destino(s) del paquete.

En el destino, se reensamblan los paquetes fragmento en su forma original, no fragmentada, tal como se ilustra:

PAQUETE ORIGINAL REENSAMBLADO:

Parte No Fragmentable	Parte Fragmentable

2.4.5.1 REGLAS PARA EL REENSAMBLAJE DE FRAGMENTOS.

Las siguientes reglas gobiernan el reensamblaje:

- Un paquete original sólo se reensambla a partir de paquetes fragmento que tienen la misma Dirección Origen, Dirección Destino, e Identificación del Fragmento.
- La Parte No Fragmentable del paquete reensamblado consiste en todas las cabeceras, pero sin incluir, la cabecera Fragmento del primer paquete fragmento (es decir, el paquete cuyo Desplazamiento del Fragmento es cero), con los siguientes dos cambios:
- El campo Cabecera Siguiente de la última cabecera de la Parte No Fragmentable se obtiene del campo Cabecera Siguiente de la cabecera Fragmento del primer fragmento.
- Se calcula la Longitud de la Carga Útil del paquete reensamblado a partir de la longitud de la Parte No Fragmentable y de la longitud y desplazamiento del último fragmento. Por ejemplo, una fórmula para calcular la Longitud de la Carga Útil del paquete original reensamblado es:


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

DONDE

- **LCU.orig** = campo Longitud de la Carga Útil del paquete reensamblado.
- **LCU.inicial** = campo Longitud de la Carga Útil del primer paquete fragmento.
- **LF.inicial** = longitud del fragmento siguiente a la cabecera Fragmento del primer paquete fragmento.
- **DF.final** = campo Desplazamiento del Fragmento de la cabecera Fragmento del último paquete fragmento.
- **LF.final** = longitud del fragmento siguiente a la cabecera Fragmento del último paquete fragmento.

La Parte Fragmentable del paquete reensamblado se construye a partir de los fragmentos siguientes a las cabeceras Fragmento dentro de cada uno de los paquetes fragmento. La longitud de cada fragmento es calculada substrayendo de la Longitud de la Carga Útil del paquete la longitud de las cabeceras entre la cabecera IPV6 y el propio fragmento, su posición relativa en la Parte Fragmentable se calcula a partir de su valor Desplazamiento del Fragmento. La cabecera Fragmento no está presente en el paquete reensamblado, final.

2.4.5.2 POSIBLES ERRORES DURANTE EL REENSAMBLAJE.

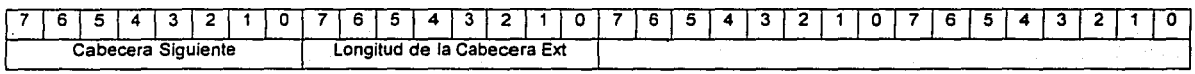
Las siguientes condiciones de error pueden originarse al reensamblar paquetes fragmentados:

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

- Si la longitud de un fragmento, tal como se dedujo a partir del campo Longitud de la Carga Útil del paquete fragmento, no es un múltiplo de 8 octetos y la bandera M de ese fragmento es 1, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Longitud de la Carga Útil del paquete fragmento.
- Si la longitud y el desplazamiento de un fragmento son tales que la Longitud de la Carga Útil del paquete reensamblado de ese fragmento excedería los 65,535 octetos, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Desplazamiento del Fragmento del paquete fragmento.
- El número y contenido de las cabeceras que preceden a la cabecera Fragmento de fragmentos diferentes del mismo paquete original pueden diferir. Cualquiera de las cabeceras que estén presentes, precediendo a la cabecera Fragmento en cada paquete fragmento, se procesan cuando los paquetes llegan, previamente a que los fragmentos hagan cola para el reensamblaje. Sólo aquellas cabeceras en el paquete fragmento de Desplazamiento cero se retienen en el paquete reensamblado.
- Los valores Cabecera Siguiente en las cabeceras Fragmento de fragmentos diferentes del mismo paquete original pueden diferir. Sólo el valor del paquete fragmento de Desplazamiento cero se usa para el reensamblaje.

2.4.6 CABECERA OPCIONES DE DESTINO

La cabecera Opciones de Destino es usada para llevar información opcional que necesita ser examinada solamente por el(los) nodo(s) destino del paquete. La cabecera Opciones de Destino es identificada por un valor Cabecera Siguiente de 60 en la cabecera inmediatamente precedente, y tiene el siguiente formato:



Opciones

- **Cabecera Siguiente**: Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Destino. Utiliza los mismos valores que el campo Protocolo del IPV4.
- **Lon Cab Ext**: Entero sin signo de 8 bits. Longitud de la cabecera Opciones de Destino en unidades de 8 octetos, no incluye los primeros 8 octetos.
- **Opciones**: Campo de longitud variable, de longitud tal que la cabecera Opciones de Destino completa es un entero múltiplo de 8 octetos de largo. Contiene uno o más opciones codificadas TLV.

2.4.7 CABECERA NO HAY SIGUIENTE

El valor 59 en el campo Cabecera Siguiente de una cabecera IPV6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo Longitud de la Carga Útil de la cabecera IPV6 indica la presencia de octetos más allá del final de una cabecera cuyo campo Cabecera Siguiente contiene 59, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

2.5 CUESTIONES FRAGMENTACION

El IPV6 requiere que cada enlace en la Internet tenga una MTU de 1280 octetos o mayor. En cualquier enlace que no pueda llevarse un paquete de 1280 octetos en una pieza, debe proporcionarse fragmentación y reensamblaje especifico al enlace en una capa debajo del IPV6.

Los Enlaces que tienen una MTU configurable deben configurarse para tener una MTU de por lo menos 1280 octetos; se recomienda que sean configurados con una MTU de 1500 octetos o mayor, para alojar posibles encapsulaciones (es decir, tunelizar) sin incurrir en la fragmentación de la capa IPV6.

De cada enlace al cuál un nodo se conecta directamente, el nodo debe poder aceptar paquetes tan grandes como la MTU de ese enlace. Se recomienda fuertemente que los nodos IPV6 implementen el Descubrimiento de la MTU de la Ruta con el propósito de descubrir y tomar ventaja de las rutas con MTUs mayores que 1280 octetos. Sin embargo, una implementación IPV6 mínima puede restringirse simplemente a enviar paquetes no más grandes que 1280 octetos, y omitir la implementación del Descubrimiento de la MTU de la Ruta.

Con el propósito de enviar un paquete más grande que la MTU de la ruta, un nodo puede utilizar la cabecera Fragmento IPV6 para fragmentar el paquete en el origen y tenerlo reensamblado en el(los) destino(s). Sin embargo, el uso de tal fragmentación se desalienta en cualquier aplicación que pueda ajustar sus paquetes para satisfacer la MTU de la ruta medida (es decir, por debajo de los 1280 octetos).

En contestación a un paquete IPV6 que se envía a un destino IPV4, el nodo IPV6 originante puede recibir un mensaje ICMP Paquete Demasiado grande reportando de una MTU del Salto Siguiente menor a 1280. En ese caso, no se exige que el nodo IPV6 reduzca el tamaño de los paquetes subsiguientes a menos de 1280, pero debe incluir una cabecera Fragmento en esos paquetes para que el enrutador traductor de IPV6 a IPV4 pueda obtener un valor Identificación apropiado para usar en los fragmentos IPV4 resultantes.

2.6 ETIQUETAS DE FLUJO

El campo Etiqueta de Flujo de 20 bits en la cabecera IPV6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por

los enrutadores IPV6, tal como la calidad de servicio no estándar o el servicio en "tiempo real".

En este aspecto IPV6 está, al momento de escribir este trabajo, todavía se encuentra en etapa experimental y sujeto a cambio conforme los requisitos para dar soporte a flujos en la Internet se vuelvan más claros. Se exige a los hosts o a los enrutadores que no dan soporte a las funciones del campo Etiqueta de Flujo poner el campo a cero al originar un paquete, pasar el campo inalterado al reenviar un paquete, e ignorar el campo al recibir un paquete.

2.7 CLASES DE TRÁFICO

El campo de 8 bits Clase de Tráfico en la cabecera IPV6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPV6. Hay un cierto número de experimentos en camino en cuanto al uso de los bits Tipo de Servicio IPV4 y/o Anterioridad para proporcionar varias formas de "servicio diferenciado" para paquetes IP, además de a través del uso de un flujo establecido explícito. El campo Clase de Tráfico en la cabecera IPV6 esta proyectado para permitir similar funcionalidad que será soportada en el IPV6.

Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

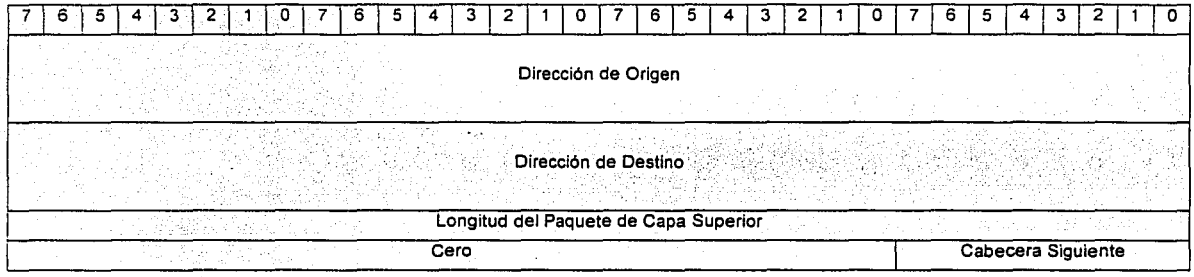
- La interface de servicio para el servicio IPV6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por ese protocolo de capa superior. El valor por defecto debe ser cero para todos los 8 bits.
- Los nodos que soportan un uso especifico de algunos o todos los bits Clase de Tráfico se les permite cambiar el valor de esos bits en los paquetes que ellos originan, reenvían, o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar a cualquiera de los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

- Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido son los mismos que el valor enviado por el origen del paquete.

2.8 PROBLEMAS DE PROTOCOLO DE CAPA SUPERIOR

2.8.1 SUMAS DE VERIFICACIÓN DE CAPA SUPERIOR

Cualquier protocolo de transporte u otro de capa superior que incluya las direcciones de la cabecera IP en su cálculo de suma de verificación debe modificarse para el uso sobre el IPV6, para incluir las direcciones IPV6 de 128 bits en lugar de las direcciones IPV4 de 32 bits. En particular, la siguiente ilustración muestra la "pseudo cabecera" TCP y UDP para el IPV6:



Si el paquete IPV6 contiene una cabecera Enrutamiento, la Dirección Destino usada en la pseudo cabecera es la del destino final. En el nodo originante, esa dirección estará en el último elemento de la cabecera Enrutamiento; en el(los) receptor(res), esa dirección estará en el campo Dirección Destino de la cabecera IPV6.

El valor Cabecera Siguiente en la pseudo cabecera identifica el protocolo de capa superior (por ejemplo, 6 para el TCP, o 17 para el UDP). Diferirá del valor Cabecera Siguiente en la cabecera IPV6 si hay cabeceras de extensión entre la cabecera IPV6 y la cabecera de capa superior.

La Longitud del Paquete de Capa Superior en la pseudo cabecera es la longitud de la cabecera de capa superior y los datos (por ejemplo, la cabecera TCP más los datos TCP). Algunos protocolos de capa superior llevan su propia información de longitud (por ejemplo, el campo Longitud en la cabecera UDP); para tales protocolos, esa es la longitud usada en la pseudo cabecera. Otros protocolos (como el TCP) no llevan su propia información de longitud, en cuyo caso la longitud usada en la pseudo cabecera es la Longitud de la Carga Útil de la cabecera IPV6, menos la longitud de cualquier cabecera de extensión presente entre la cabecera IPV6 y la cabecera de capa superior.

A diferencia del IPV4, cuando los paquetes UDP son originados por un nodo IPV6, la suma de verificación UDP no es opcional. Es decir, siempre que se origine un paquete UDP, un nodo IPV6 debe calcular una suma de verificación UDP sobre el paquete y la pseudo cabecera, y, si ese cálculo produce un resultado de cero, debe cambiarse al hexadecimal FFFF para la colocación en la cabecera UDP. Los receptores IPV6 deben descartar los paquetes UDP que contengan una suma de verificación cero, y deben registrar el error.

La versión IPV6 del ICPM [ICMPV6] incluye la pseudo cabecera citada arriba en su cálculo de suma de verificación; éste es un cambio a diferencia de la versión IPV4 del ICMP, el cual no incluye una pseudo cabecera en su suma de verificación. La razón para el cambio es para proteger al ICMP de una mala entrega o corrupción de aquellos campos de la cabecera IPV6 de los que depende, los qué, a diferencia del IPV4, no son cubiertos por una suma de verificación de la capa Internet. El campo Cabecera Siguiente en la pseudo cabecera para el ICMP contiene el valor 58, que identifica la versión IPV6 del ICMP.

2.8.2 TIEMPO DE VIDA MÁXIMO DE UN PAQUETE

A diferencia del IPV4, no se exigen a los nodos IPV6 cumplir con el tiempo de vida máximo de un paquete. Ésa es la razón por la que el campo "Tiempo de Vida" del IPV4 se renombró a "Límite de Saltos" en el IPV6. En la práctica, muy pocas, si alguna, implementaciones IPV4 adoptan el requisito de limitar el tiempo de vida de un paquete, así que esto no es un cambio en la práctica. Cualquier protocolo de capa superior que depende

de la capa Internet (ya sea IPV4 o IPV6) para limitar el tiempo de vida de un paquete debe actualizarse para proporcionar sus propios mecanismos de detección y descarte de paquetes obsoletos.

2.8.3 TAMAÑO MÁXIMO DE LA CARGA ÚTIL DE CAPA SUPERIOR

Al calcular el tamaño máximo de carga útil disponible para los datos de capa superior, un protocolo de capa superior debe tener en cuenta el tamaño más grande de la cabecera IPV6 relativo a la cabecera IPV4.

2.8.4 CONTESTANDO A PAQUETES QUE LLEVAN CABECERAS DE ENRUTAMIENTO

Cuando un protocolo de capa superior envía uno o más paquetes en contestación a un paquete recibido que incluía una cabecera Enrutamiento, el(los) paquete(s) respuesta no debe(n) incluir una cabecera Enrutamiento que se derivó automáticamente "invirtiendo" la cabecera Enrutamiento recibida a menos que se haya verificado la integridad y autenticidad tanto de la Dirección Origen como de la cabecera de Enrutamiento recibida. En otras palabras, se permiten sólo los siguientes tipos de paquetes en contestación a un paquete recibido que lleva una cabecera Enrutamiento:

- Los paquetes respuesta que no llevan cabeceras Enrutamiento.
- Los paquetes respuesta que llevan cabeceras Enrutamiento que NO se derivaron invirtiendo la cabecera Enrutamiento del paquete recibido (por ejemplo, una cabecera Enrutamiento proporcionada por configuración local).
- Los paquetes respuesta que llevan cabeceras Enrutamiento que se derivaron invirtiendo la cabecera Enrutamiento del paquete recibido SI Y SÓLO SI la integridad y autenticidad de la Dirección Origen y de la cabecera Enrutamiento del paquete recibido han sido verificadas por el contestador.

Capitulo III

"Sistemas operativos de la red"

3.1 LINUX

3.1.1 BREVE HISTORIA DE LINUX

UNIX es uno de los sistemas operativos más populares del mundo debido a su extenso soporte y distribución. Originalmente fue desarrollado como sistema multitarea con tiempo compartido para mini equipos de cómputo y mainframes a mediados de los '70, y desde entonces se ha convertido en uno de los sistemas más utilizados a pesar de su, ocasionalmente, confusa interfaz con el usuario y el problema de su estandarización.

Muchos hackers consideran que UNIX es el auténtico y único sistema operativo. El desarrollo de Linux parte de un grupo en expansión de hackers de UNIX que quisieron hacer su sistema con sus propias manos.

Existen numerosas versiones de UNIX para muchos sistemas, desde equipos de cómputo personales hasta supercomputadores como el Cray Y-MP. La mayoría de las versiones de UNIX para equipos de cómputo personales son muy caras. Linux es una versión de UNIX de libre distribución, inicialmente desarrollada por Linus Torvalds en la Universidad de Helsinki, en Finlandia. Fue desarrollado con la ayuda de muchos programadores y expertos de UNIX a lo largo y ancho del mundo, gracias a la presencia de Internet. Cualquier habitante del planeta puede acceder a Linux y desarrollar nuevos módulos o cambiarlo a su gusto.

El núcleo de Linux no utiliza ninguna línea del código de AT&T o de cualquier otra fuente de propiedad comercial, y buena parte del software para Linux se desarrolla bajo las reglas del proyecto de GNU de la Free Software Foundation, Cambridge, Massachusetts.

Inicialmente, sólo fue un proyecto de Linus Torvalds. Se inspiraba en Minix, un pequeño UNIX desarrollado por Andy Tanenbaum, y las primeras discusiones sobre Linux surgieron en el grupo de News *comp.os.minix*. Estas discusiones giraban en torno al desarrollo de un pequeño sistema UNIX de carácter académico dirigido a aquellos usuarios de Minix que querían algo más.

El desarrollo inicial de Linux ya aprovechaba las características de conmutación de tareas en modo protegido del 386, y se escribió todo en ensamblador. No se anunció nada sobre esa versión, puesto que las fuentes del 0.01 jamás fueron ejecutables: contenían solo rudimentos de lo que sería el núcleo, y se asumía que se tenía acceso a un Minix para poderlo compilar y jugar con él.

El 5 de Octubre de 1991, Linus anunció la primera versión "oficial" de Linux, la 0.02. Ya podía ejecutar bash (el shell de GNU) y gcc (el compilador de C de GNU), pero no hacía mucho más. La intención era ser un juguete para hackers. No había nada sobre soporte a usuarios, distribuciones, documentación ni nada parecido. Hoy, la comunidad de Linux aún trata estos asuntos de forma secundaria. Lo primero sigue siendo el desarrollo del kernel.

Tras la versión 0.03, Linux saltó a la versión 0.10 al tiempo que más gente empezaba a participar en su desarrollo. Tras numerosas revisiones, se alcanzó la versión 0.95, reflejando la esperanza de tener lista muy pronto una versión "oficial". (Generalmente, la versión 1.0 de los programas se corresponden con la primera teóricamente completa y sin errores). Esto sucedía en Marzo de 1992. Año y medio después, en Diciembre del 93, el núcleo estaba en la revisión 0.99.pl14, en una aproximación asintótica al 1.0.

Hoy Linux es ya un clónico de UNIX completo, capaz de ejecutar XWindows, TCP/IP, Emacs, UUCP, software de correo y News. Mucho software de libre distribución ha sido ya portado a Linux, y están empezando a aparecer aplicaciones comerciales. El hardware soportado es mucho mayor que en las primeras versiones del núcleo. Mucha gente ha ejecutado tests de rendimiento en sus sistemas Linux 486 y se han encontrado que son comparables a las estaciones de trabajo de gama media de Sun Microsystems y Digital.

3.1.2 RED HAT LINUX

En Carolina del Norte se fundó un grupo de programadores. Su objetivo era hacer Linux más fácil para la gente con el fin de darle una oportunidad. Como muchos otros de estos grupos, su estrategia era agrupar todas las unidades y piezas necesarias en una

distribución cohesionada, relevando a los "novatos" de algunos de los más esotéricos aspectos del arranque desde cero de un nuevo sistema operativo en sus PC.

De cualquier forma, a diferencia de otras distribuciones, ésta era básicamente distinta. En vez de ser una imagen de un disco duro con una copia operativa de Linux, o un conjunto de disquetes a partir de los cuales se rehacían las diferentes partes del sistema operativo, la distribución se basaba en paquetes.

Cada paquete proporciona una parte diferente del software, completamente probado, configurado, y listo para ejecutarse. Por ejemplo si desea probar un nuevo editor sólo copie el paquete e instálelo, en segundos puede evaluarlo. Si no le gusta, ejecute un solo comando, y el paquete será eliminado. Si esto es todo lo que puede ofrecer, esta distribución sería muy limitada. Pero al estar basada en paquetes tiene una ventaja adicional: esta distribución Linux puede ser actualizada fácilmente.

Desde la aparición de Red Hat Linux en el verano de 1994, Linux y Red Hat Software han crecido, logrando soporte para más hardware, enormes avances en la seguridad, y un creciente uso de Linux por parte de las empresas en todo el mundo.

Red Hat Linux se ejecuta en tres plataformas líderes de ordenador: PC compatibles Intel, ordenadores Alpha de Digital, y equipos SPARC de Sun. La estructura unificada de código fuente y los beneficios de la tecnología RPM (Gestor de paquetes Red Hat) permite desplegar Red Hat en cada plataforma con un mínimo esfuerzo. Esto a su vez permite a los gestionar y migrar software entre las tres plataformas lo más fácilmente posible.

Red Hat Linux es fácil de instalar; el sistema en sí mismo es muy flexible. Con RPM[1], puede instalar o eliminar paquetes individuales de software con un mínimo esfuerzo. Debido al uso de paquetes, Red Hat Linux es también fácil de mantener, los paquetes instalados pueden verificarse y corregirse, y los paquetes se instalan y eliminan de forma fácil y segura. Se cuenta con un rico conjunto de herramientas de administración y se suministra el código fuente completo de todos los componentes de libre distribución del sistema.

---

[1] **RPM**

3.1.3 INSTALACION, CONFIGURACION Y PRUEBA DE IPV6

La configuración se realiza en tres principales pasos:

1. Configuración para cada interfase.
2. Configuración global de la red.
3. Puesta en marcha de los "demonios" (daemons).

3.1.3.1 PREINSTALACION

Antes de instalar IPV6 la configuración de IPV4 debe estar hecha para su distribución y funcionando.

3.1.3.2 INSTALACIÓN

La instalación es bastante fácil, sólo siga las indicaciones que aparecen a continuación:

- Obtenga tarball de la siguiente dirección: ftp://ftp.kernel.org/pub/linux/kernel/v2.4/
- Extraiga tarball
- Copie los archivos script a los directorios relacionados.
- Aplique los "parches" (patches) a los archivos existentes, puede descargarlos de la siguiente dirección: ftp://ftp.openwall.com/pub/patches/linux/
- Ejecute el comando Cat file dic | patch
- Examine los archivos y copie la información que es importante para usted. Revise el ejemplo de datos y cámbielo antes de reiniciar.

Este proceso de instalación deberá ser usado por la versiones de Red Hat anteriores a la 7.2, ya que ésta última contiene el protocolo IPV6 en su distribución y sólo deberá configurarlo como se muestra en el siguiente proceso.

3.1.3.3 CONFIGURACION

A continuación se muestran los archivos que deberá cambiar, después del símbolo # se presentan algunos comentarios para una mejor descripción.[2].

/etc/sysconfig/network

- Configuración de los controles globales IPV6
  - NETWORKING_IPV6=yes # Habilita la inicialización global IPV6 #
  - NETWORKING_IPV6=no # Deshabilita la inicialización global IPV6 [default] #
- Control de envío IPV6
  - IPV6FORWARDING=yes # Habilita el envío global de IPV6 #
  - IPV6FORWARDING=no # Deshabilita el envío global de IPV6 [default] #
- Control global de auto configuración IPV6
  - IPV6_AUTOCONF=yes # Habilita la auto configuración global de IPV6 (Sólo si el envío "forwarding" está deshabilitado) [default] #
  - IPV6_AUTOCONF=no # Deshabilita la auto configuración global de IPV6 (Sólo si el envío "forwarding" está deshabilitado) #
- Control automático del Túnel
  - IPV6_AUTOTUNNEL=yes # Habilita el túnel automático para IPV6 #
  - IPV6_AUTOTUNNEL=no # Deshabilita el túnel automático para IPV6 [default] #
- Control de inicialización del Ruteador por default
  - Especificando la dirección de la "puesta de enlace" (gateway)
  - IPV6_DEFAULTGW=<ipv6address[%interfase]> # [optional]
- Especificando el dispositivo puerta de enlace por default
  - IPV6_DEFAULTDEV=<interface> # [optional]

/etc/sysconfig/network-scripts/ifcfg-device

Ejemplo para controlar una red de tipo LAN con configuración especifica IPV6:

- Control de la auto configuración IPV6 para esta interfase
  - IPV6INIT="yes" # Habilita la inicialización de IPV6 para esta interfase #
  - IPV6INIT="no" # Deshabilita la inicialización de IPV6 para esta interfase [default]
- Especificación de la dirección básica y el prefijo para esta interfase:
  - IPV6ADDR="3ffe:ffff:0000:f101::1/64" # dirección IPV6 básica estática para esta interfase #
- Especificación de una dirección IPV6 adicional y la longitud del prefijo para esta interfase:

[2] También puede revisar el archivo sysconfig-ipv6.txt que está incluido en el tarball para mas información y ejemplos.

- IPV6ADDR_SECONDARIES="fec0:0:0:1::1/64 3ffe:ffff:0000:f101::2/64" # Lista de direcciones secundarias #

- Especificación de la MTU de la red
  - IPV6_MTU="1280" # Especificación de la MTU de la red #

/etc/sysconfig/network-scripts/ifcfg-túnel [tunnel=sitX (X > 0)]
Ejemplo de control dedicado a una interfase de túneles de IPV6 a IPV4

- Especificación del nombre de la interfase (debe ser el mismo del nombre del archivo) y otros valores compatibles:
  - DEVICE="sit1"
  - BOOTPROTO="none"
  - ONBOOT="yes"
- Especificación de un nombre alternativo para el túnel (opcional)
  - IPV6_TUNNELNAME=<name>
- Control de configuración IPV6 para esta interfase:
  - IPV6INIT="yes" # Habilita la inicialización IPV6 para esta interfase #
  - IPV6INIT="no" # Deshabilita la inicialización IPV6 para esta interfase [default] #
- Especificación de la dirección IPV4 para el punto final del túnel
  - IPV6TUNNELIPV4="1.2.3.4" # dirección IPV4 del punto final del túnel #
- Especificación la dirección IPV4 para el punto final del túnel (para nodos con mas de una dirección IPV4 sobre una interfase):
  - IPV6TUNNELIPV4LOCAL="2.3.4.5" # dirección IPV4 del punto final del túnel #
- Especificación de la dirección IPV6 local de un túnel IPV6 a IPV4 numerado:
  - IPV6ADDR="3ffe:b00:c18:1fff:0:0:0:a1f/0" # dirección local de un túnel numerado #
- Especificación de la MTU del túnel
  - IPV6_MTU="1280" # Establece la MTU del túnel #

/etc/sysconfig/static-routes-ipv6
Ejemplo para los ruteadores estáticos IPV6:
Aquí puede especificar ruteadores adicionales para esta interfase:

```
#Device IPv6 network to route        IPv6 gateway address
#eth0   fec0:0:0:2::/64              fec0:0:0:1:0:0:0:20
```

```
#eth0   2000::/3          3ffe:ffff:0000:f102:0:0:0:1
```

y también los ruteadores para los túneles:

```
## Virtual túnel interfase      IPv6 network to route through
# IPv6 official addresses
sit1                           2000::/3
```

3.1.3.4 PROBANDO

Usted puede reestablecer por completo la configuración de la red ejecutando el siguiente comando:

```
/etc/rc.d/init.d/network restart
```

Normalmente, usted no es capaz de ver que es lo que realmente está pasando, por eso la salida es escrita en syslog (RedHat: facility: local7, file: /var/log/boot.log), por eso, es una buena idea mirar la salida en una consola virtual con el siguiente comando:

```
tail -f /var/log/boot.log
```

3.2 WINDOWS 98

3.2.1 INTRODUCCIÓN A WINDOWS 98

Microsoft Windows 98 hace que el ordenador funcione mejor integrando Internet y ofreciendo un mejor rendimiento del sistema y un sistema de diagnósticos y mantenimiento más sencillo, su capacidad para añadir y quitar periféricos lo hacen más accesible para todos los usuarios con respecto a su antecesor **Windows 95**. Al mismo tiempo, mantiene la compatibilidad con otras aplicaciones y tecnologías basadas en versiones anteriores de Windows

3.2.2 CARACTERÍSTICAS GENERALES

Las características de Microsoft Windows 98 ofrecen sacar mucho más partido del PC. Los programas se ejecutan más rápido, pudiendo ganar una media de un 25% o más espacio en disco. La integración de Internet con Windows 98 ahora ofrece una visión integrada de todos los recursos e información.

Windows 98 permite administrar el correo electrónico, leer grupos de noticias, y video conferencias. Además dispone de soporte para periféricos, Una nueva característica de Windows 98 es la Administración Avanzada de Configuración y Energía o ACPI. Con el modelo de controlador para Win32, las empresas que utilicen una combinación de Windows 98 y Windows NT Workstation 5.0 dispondrán de un único juego de controladores, con lo que se reducirá el tiempo necesario para administrarlos y la formación asociada a los mismos.

3.2.3 REQUERIMIENTOS DEL SISTEMA

Los requerimientos mínimos de Windows 98 son:

- ***Procesador*** 486DX / 66 MHz o superior.
- 16 MB de ***memoria RAM***; a más memoria mayor rendimiento.
- Una instalación típica requiere aproximadamente 195 Mb de espacio libre en el ***disco duro***, pero puede variar entre 120 y 295 Mb, dependiendo de la configuración del ordenador y de las opciones que desee instalar.
- ***CD-ROM o DVD-ROM***.
- Monitor VGA o superior.
- Ratón Microsoft o compatible.

3.2.4 WINDOWS 98 E IPV6

Desgraciadamente Windows 98 no está listo para trabajar con IPV6 en forma natural, es debido a esto que aquellos equipos que utilicen este sistema operativo deberán utilizar la técnica de migración conocida como **túnel** para poder comunicarse con el resto de equipos de la red que si pueden utilizar IPV6. Esta técnica se describirá a detalle en el siguiente capitulo.

3.3 WINDOWS 2000

3.3.1 INTRODUCCIÓN A WINDOWS 2000

Windows 2000 representa un esfuerzo por unificar lo que hasta ahora eran dos sistemas operativos distintos, ***Windows 9x*** y ***Windows NT*** por lo que ofrece lo mejor de ambos mundos: la solidez y la seguridad de NT, junto a la facilidad de manejo, soporte de hardware y multimedia de Windows 98.

Las principales características de ***Windows 2000*** son:

- Cuenta con un gran número de herramientas de conectividad.
- Una interfaz amigable,
- Reconocimiento del hardware y estabilidad.
- Soporte de nuevas tecnologías.
- Mejoras en las funciones de informática remota.
- Aplicaciones centralizadas de servicio.

Windows 2000 es una de las versiones más estables de ***Microsoft***. Esto se ha logrado mediante un conjunto de tecnologías como la protección de escritura del modo kernel; y la "***pool tagging***", una técnica que permite que los controladores utilicen memoria asignada de un segmento especial y no de la memoria compartida del sistema. Un método de firma digital encriptada se usa para comprobar la fuente e idoneidad del controlador. Si

este sistema operativo detecta que un controlador procede de una fuente no certificada avisa al usuario y le da la opción de detener o continuar.

La fiabilidad y la capacidad de gestión se han mejorado con herramientas que ayudarán a los usuarios y administradores de red a gestionar de forma mas sencilla sus sistemas, empezando porque el laberinto de las DLL[3] parece resuelto. Windows 2000 permite que las DLL's se instalen en los directorios de sus aplicaciones especificas, y eviten que se eliminen las DLL's compartidas.

La gestión global de un sistema se realiza a través de un módulo denominado ***Administración del equipo***, que organiza los recursos, servicios, dispositivos de almacenamiento y seguridad que utilizan tanto en el sistema local como en equipos de cómputo remotos. El pánel es una herramienta muy valiosa para los administradores de redes y se divide en tres módulos:

- ***Herramientas del Sistema***. Dispone de un visor de sucesos y del Administrador de dispositivos, una síntesis jerarquizada de los dispositivos instalados en el PC y que permite hacer modificaciones y búsquedas para resolver conflictos.
- ***Almacenamiento***. Desde aquí es posible acceder a las propiedades de las unidades de disco, incluyendo unidades extraíbles, y a sus opciones de verificación, comparticiones y copias de seguridad.
- ***Servicios y Aplicaciones***. Da información mas clara sobre los servicios Microsoft y de red implementados. En general, el Administrador del equipo es un mapa completo y detallado de la PC, incluyendo informes sobre la forma en que el usuario lo utiliza.

Puesto que se trata de un sistema operativo orientado al trabajo en red y a la comparición de recursos, la familia Windows 2000 ha integrado sólidas tecnologías de seguridad. La intención es que cada usuario pueda comprender como funcionan estas tecnologías y controlarlas de forma cabal. Esta "infraestructura" de seguridad funciona en tres niveles:

[3] Dymanic Link Libraries (Enlace Dinámico de Librerías).

1. ***Local***. Se refiere a la protección de datos en el ordenador. El sistema esta diseñado para evitar que usuarios no autorizados omitan el sistema de arranque y, por tanto, también las funciones de seguridad. Algunos fabricantes de hardware integran sistemas de contraseña, una solución no muy adecuada para entornos de trabajo compartido. La encriptación de los datos en el disco NTFS es un servicio que se basa en la arquitectura CriptoAPI de Windows para implementar el sistema de llaves públicas. Cada archivo (incluyendo sus temporales de trabajo) se encripta a través de una llave generada aleatoriamente, utilizando algoritmos asimétricos. Este es el primer sistema operativo que implementa encriptación de 128 bits en un proceso transparente, ya que encripta y desencripta los archivos localizando las llaves del usuario, bien desde el almacén del sistema o desde los dispositivos como los Smart Cards.
2. ***Corporativo***. Se refiere a la protección de datos en una red local. Utiliza el protocolo de autentificación ***Kerberos*** versión, 5, un estándar de seguridad en redes locales e intranets que verifica y hace un seguimiento de la actividad de cada usuario dentro de la red. Kerberos permite un control del acceso unificado a casi cualquier entorno de red, eliminando la necesidad de obtener permisos y esperar la respuesta de cada vez que un cliente desea acceder a un nuevo recurso de la red.
3. ***Público***. Utiliza también sistemas de llaves públicas y protocolos de autenticación para mantener la seguridad de las comunicaciones que se realizan por Internet, de forma que verifique la procedencia de mensajes de correo o garantice las fuentes de donde proceden las descargas. Por otra parte, incluye soporte para ***Redes Privadas Virtuales (VPN)***, protocolos encapsulados que crean un canal de comunicación privado a través de redes públicas. El soporte VPN se realiza a través del protocolo ***PPTP (Point to Point Tunneling Protocol), Layer 2 Tunneling Protocol e IPSec***, un protocolo que implementa una gama de funciones sobre una capa de red encriptada.

Un servicio de directorios es un servicio de red que identifica todos los recursos en ella y los vuelve accesibles a los usuarios y a las aplicaciones. ***Active Directory (AD)*** es el servicio de directorio incluido en Windows 2000.

El elemento principal de AD es el directorio, que almacena información sobre los recursos de la red y los servicios que hacen disponible la información. Los recursos almacenados en el directorio, como los datos del usuario, impresoras, servidores, bases de datos, grupos, computadoras y políticas de sistema, se denominan objetos.

AD los organiza jerárquicamente en dominios. Un dominio es una agrupación lógica de servidores y otros recursos de red bajo un mismo nombre de dominio. Cada dominio incluye uno o mas controladores de dominio, que son máquinas que almacenan una réplica de un directorio de dominio. Cada vez que se hace algún cambio en alguno de los controladores, el resto se actualiza automáticamente.

Un objeto es un conjunto de atributos particulares, bajo un nombre específico, que representa un recurso individual de la red. Los atributos se refieren a las características del objeto. Así, los atributos de una cuenta de usuario pueden ser el nombre, departamento y dirección de mail, y los de una impresora, si es láser y si es en color. Algunos objetos funcionan también como contenedores: por ejemplo, un dominio.

3.3.2 VERSIONES DE WINDOWS 2000

La familia Windows 2000 está integrada por cuatro versiones:

- ***Windows 2000 Professional***: Windows 2000 Pro, sucesor de NT Workstation, está destinado a ser un cliente de red seguro y una estación de trabajo corporativa. Soporta hasta 2 procesadores y es útil, como sistema operativo autónomo, para correr aplicaciones de un alto performance, especialmente en diseño gráfico, por ejemplo. Microsoft lo promociona como el principal sistema operativo de escritorio en un entorno de negocios.
- ***Windows 2000 Server***: Sucesor de NT Server, soporta hasta 4 procesadores y está destinado a ser el servidor de impresión, archivos, aplicaciones e, incluso, Web de una empresa pequeña a mediana.
- ***Windows 2000 Advanced Server***: Sucesor de NT Server Enterprise Edition, soporta hasta 8 procesadores y será el servidor departamental de aplicaciones en empresas

medianas a grandes, con más de un dominio y tareas de misión crítica. Entre otras prestaciones, se incluye soporte para RAID y fault tolerance.

- ***Windows 2000 Data Center Server***: Soporta hasta 32 procesadores y sólo se entregará sobre pedido. Está destinado a grandes empresas que requieran data warehousing, análisis econométricos, simulaciones científicas e ingenieriles a gran escala, etc.

3.3.3 REQUERIMIENTOS DEL SISTEMA

Los requerimientos de hardware para Windows 2000 Profesional son:

- ***Procesador*** compatible con Pentium a 133 MHz o superior.
- 64 Mb de ***memoria RAM***.
- 650 Mb de espacio disponible en el ***Disco Duro***.

Los requerimientos de hardware para Windows 2000 Server son:

- ***Procesador*** compatible con Pentium a 133 MHz o superior.
- 128 Mb de ***memoria RAM*** (recomendados 256 Mb).
- 1 Gb de espacio disponible en el ***Disco Duro***.

Los requerimientos de hardware para Windows 2000 Advanced Server son:

- ***Procesador*** compatible con Pentium a 133 MHz o superior.
- 128 Mb de ***memoria RAM*** (recomendados 256 Mb).
- 1 Gb de espacio disponible en el ***Disco Duro***.

Los requerimientos de hardware para Windows 2000 Datacenter Server son:

- CPU con 8 procesadores al menos.
- ***Procesador*** compatible con Pentium III Xenon o superior.
- 256 Mb de ***memoria RAM*** (recomendados 512 Mb).
- 1 Gb de espacio disponible en el ***Disco Duro***.

3.3.4 IMPLEMENTACION DE IPV6

Para instalar la versión preliminar IPV6 de Microsoft para Windows 2000, es necesario que la computadora cuente con este sistema operativo instalado, así como el Service Pack 2 y completar el siguiente procedimiento:

1. Descargue y guarde en su disco duro el archivo ***tpipv6-001205.exe*** de la dirección http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/download.asp en una carpeta local (por ejemplo ***C:\IPv6TP***).
2. Desde su carpeta local (***C:\IPv6TP***) ejecute ***Tpipv6-001205.exe*** y extraiga los archivos a la misma ubicación.
3. Desde su carpeta local (***C:\IPv6TP***) ejecute ***Setup.exe –x*** y extraiga los archivos a una subcarpeta de la carpeta actual (por ejemplo ***C:\IPv6TP\files***).
4. Desde la carpeta que contiene los archivos (***C:\IPv6TP\files***), abra el archivo ***Hotfix.inf*** en un editor de texto.
5. En la sección ***[Version]*** del archivo ***Hotfix.inf*** cambie la línea **NTServicePackVersion=256** a **NTServicePackVersion=512** y guarde los cambios.
6. Desde la carpeta que contiene los archivos extraídos (***C:\IPv6TP\files***), ejecute el archivo ***Hotfix.exe***.
7. Reinicialice su computadora cuando le sea pedido.
8. Después de que su computadora ha reinicializado, continué con la instalación a partir del punto ***tres*** que se encuentra en el archivo ***Readme.htm*** que está ubicado en la carpeta que contiene el archivo ***Setup.exe*** (***C:\IPv6TP***).

3.3.4.1 OBTENCIÓN DE SU DIRECCION IPV6.

Por default, Microsoft configura las direcciones de la red local para cada interfaz que corresponde a un adaptador Ethernet instalado. Las direcciones de red local tienen el prefijo ***FE80::/64***. Usted puede verificar su dirección de red local ejecutando el comando ***ipv6 if***

desde el símbolo del sistema (prompt). Podrá observar en pantalla la dirección de la forma ***aa-bb-cc-dd-ee-ff***.

3.3.4.2 CONFIGURACIÓN MANUAL DE DIRECCIONES IPV6.

Sin un ruteador IPV6, usted puede configurar manualmente las direcciones IPV6 para cada interfaz utilizando el comando ***ipv6 adu***. Con este comando usted puede especificar una interfaz, la dirección, el prefijo y el límite de vida, además si la dirección es unicast o anycast.

Un ejemplo de la sintaxis del comando ***ipv6 adu*** es el siguiente:

- Ipv6 adu ifindex / adress [lifetime validlifetime [/preflifetime]] [anycast] [unicast]

Con este comando usted puede agregar o eliminar una asignación de dirección unicast o anycast a una interfaz, por default la asignación es unicast. Si el límite de vida no es especificado, éste toma el valor de infinito, si solo el valor validlifetime es indicado, preflifetime toma este valor. El valor de lifetime puede ver infinito o especificado en segundos. Si es especificado el valor de preflifetime, éste debe ser menor o igual a lifetime.

El siguiente es un ejemplo de la configuración de una dirección local unicast con un tiempo de vida infinito: Fec0::260:8ff:fe52:f9d8.

3.3.5 TIPOS DE CONFIGURACIONES

3.3.5.1 RED ÚNICA CON DIRECCIONES LOCALES

La primera configuración no requiere configuraciones adicionales mas allá de la instalación de Microsoft IPv6 Technology Preview Protocol. Esta configuración consiste en al menos dos nodos sobre una misma subred. En la terminología IPV6, dos nodos están sobre la misma red si no tienen routeadores intermediarios.

La figura 3.1 muestra la configuración de dos nodos usando direcciones locales

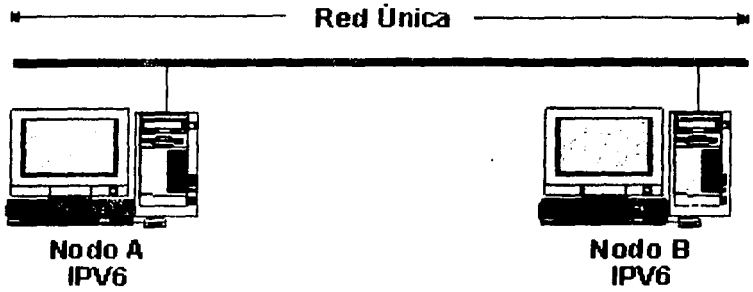


Figura 3.1 Red Única con Direcciones locales

Por defecto, Microsoft IPV6 configura direcciones IP locales para cada interfaz correspondiente al instalar los adaptadores de red Ethernet. Las direcciones locales tienen el prefijo fe80::/64. Los últimos 64 bits de la dirección IP son conocidos como el identificador de la interfase y es derivado de la dirección del adaptador de red.

Usted puede ver su dirección utilizando el comando ***ipv6 if*** como se muestra a continuación:

```
C:\>ipv6 if
Interface 4 (site 1): Local Area Connection
  uses Neighbor Discovery
  link-level address: 00-10-5a-aa-20-a2
    preferred address fe80::210:5aff:feaa:20a2, infinite/infinite
    multicast address ff02::1, 1 refs, not reportable
    multicast address ff02::1:ffaa:20a2, 1 refs, last reporter
  link MTU 1500 (true link MTU 1500)
  current hop limit 128
  reachable time 43500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1
Interface 3 (site 1): 6-over-4 Virtual Interface
  uses Neighbor Discovery
  link-level address: 10.0.0.2
    preferred address fe80::a00:2, infinite/infinite
    multicast address ff02::1, 1 refs, not reportable
    multicast address ff02::1:ff00:2, 1 refs, last reporter
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 34000ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 1
Interface 2 (site 0): Tunnel Pseudo-Interface
  does not use Neighbor Discovery
```

```
  link-level address: 0.0.0.0
    preferred address ::10.0.0.2, infinite/infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
  reachable time 0ms (base 0ms)
  retransmission interval 0ms
  DAD transmits 0
Interface 1 (site 0): Loopback Pseudo-Interface
  does not use Neighbor Discovery
  link-level address:
    preferred address ::1, infinite/infinite
  link MTU 1500 (true link MTU 1500)
  current hop limit 1
  reachable time 0ms (base 0ms)
  retransmission interval 0ms
  DAD transmits 0
```

La interfase 4 es una interfase correspondiente a un adaptador Ethernet instalado con una dirección fe80::210:5aff:feaa:20a2.

3.3.5.1.1 PROBANDO LA CONECTIVIDAD ENTRE DOS ANFITRIONES (HOSTS) LOCALES.

Usted puede hacer un simple ping usando ipv6 entre dos equipos de cómputo sobre una red local, para hacerlo utilice el siguiente procedimiento:

1. Utilice ipv6 if sobre el Host A para obtener la dirección de la interfase local. Por ejemplo la dirección de éste host es fe80::210:5aff:feaa:20a2.
2. Utilice ipv6 if sobre el Host B para obtener la dirección de la interfase local. Por ejemplo la dirección de éste host es fe80::260:97ff:fe02:6ea5.
3. Desde el Host A haga ping al Host B utilizando Ping6.exe de la siguiente manera: ping6 fe80::260:97ff:fe02:6ea5.

3.3.5.2. LA HERRAMIENTA 6TO4CFG.EXE

6to4cfg.exe automatiza su configuración 6 TO 4, automáticamente descubre la dirección del ruteador IPV4 global y crea un prefijo. Esta configuración se realiza directamente, o si prefiere se puede escribir una configuración para revisarla posteriormente.
La sintaxis básica del comando 6to4cfg.exe es: 6to4cfg [-r] [-s] [-u] [-R relay] [-b] [-S address] [filename].

- 6to4cfg [filename] . Escribe la configuración en un archivo si se especifica el nombre del archivo, ésta configuración utiliza ipv6.exe. Si no especifica un nombre de archivo, actualiza la configuración sobre su computadora.
- 6to4cfg –r. Llega al gateway ruteador de su red local y habilita el ruteo sobre todas sus interfaces y prefijos de subred asignados.
- 6to4cfg –s. Habilita el direccionamiento local de su sitio 6 TO 4. Este comando solo es recomendado cuando se utiliza junto con el parámetro –r.
- 6to4cfg –u. Especifica que la configuración 6 TO 4 será invertida.
- 6to4cfg –R relay. Especifica el nombre o la dirección IPV4 de un ruteador 6 TO 4 relay, por defecto, este nombre es 6to4.ipv6.microsoft.com.
- 6to4cfg –b. Especifica que 6to4cfg.exe escoja la mejor dirección relay.
- 6to4cfg –S. especifica la dirección local IPV4 para el prefijo 6 TO 4.

3.3.5.2.1 TRÁFICO SOBRE NODOS QUE SE ENCUENTRAN EN DIFERENTES SUBREDES CONECTADAS MEDIANTE UN RUTEADOR IPV4 (6 TO 4)).

6 TO 4 es un método para conectar anfitriones IPV6 o sitios que existen sobre una infraestructura IPV4 como se muestra en la figura 3.2. Utiliza un prefijo único de dirección para poder aislar los sitios IPV6 sobre el espacio de direcciones IPV6. 6 TO 4 es como un proveedor "PSEUDO-ISP". Usted puede usar 6 TO 4 para comunicarse directamente con otros sitios 6 TO 4, así como con 6bone, 6 TO 4 no requiere el uso de ruteadores IPV6 ya que el tráfico de información es encapsulado con un encabezado IPV4. La siguiente configuración muestra dos nodos sobre subredes separadas usando 6 TO 4 para comunicarse a través de un ruteador IPV4.

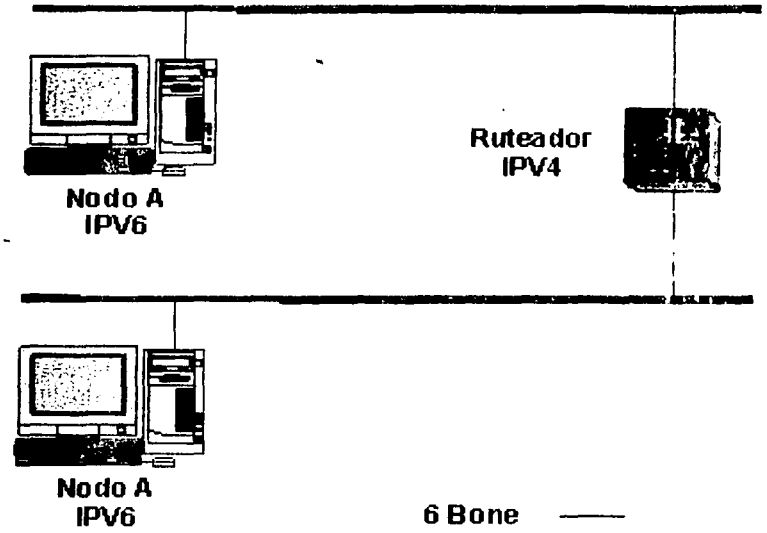


Figura 3.2 Conexión de anfitriones IPV6 sobre una estructura IPV4

El principal requerimiento para usar 6 TO 4 es una dirección IPV4 que englobe su sitio. Suponga que su sitio consiste en una colección de computadoras IPV6 que usted administra (Algunas utilizando el protocolo de Microsoft IPV6 y otras utilizando otras implementaciones IPV6). Asuma también que todas las computadoras IPV6 están directamente conectadas utilizando Ethernet. La dirección global del ruteador IPV4 a una de sus computadoras que están utilizando el protocolo Microsoft IPV6. Esta computadora será su 6 TO 4 Gateway.

3.3.5.3 CONECTÁNDOSE AL 6BONE

La mejor forma de conectarse al 6bone es configurar 6 TO 4 y usar el ruteador Microsoft 6 TO 4 relay. La figura 3.3 muestra la configuración de un nodo usando 6 TO 4 para comunicarse con el 6bone utilizando el ruteador Microsoft 6to4 relay.

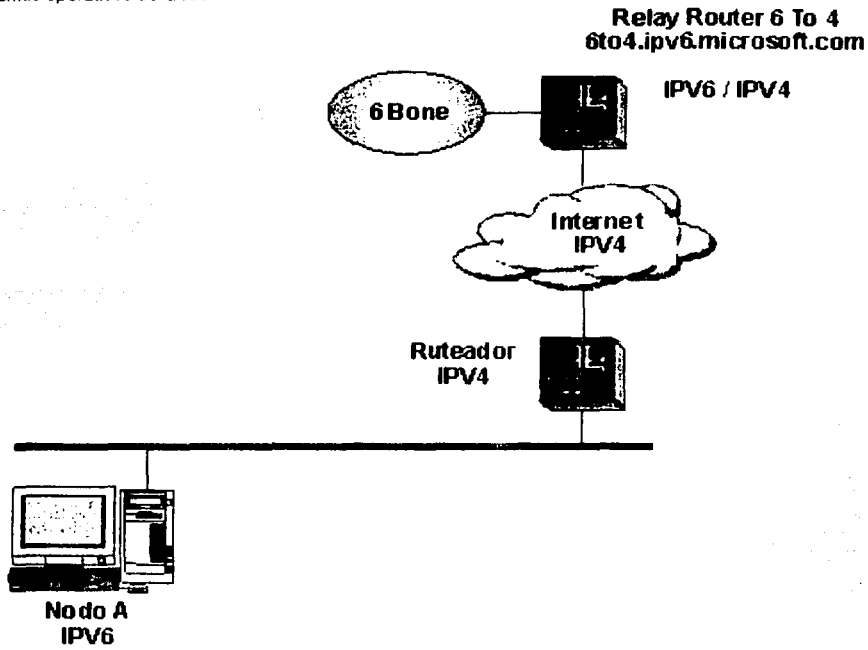


Figura 3.3 Conexión al 6Bone.

Utilizando 6 TO 4 usted puede hacer ping con otras computadoras sobre el 6bone como se muestra en el siguiente ejemplo:

```
ping6 6bone-gw.ipv6.sics.se
ping6 sipper.ipv6.zk3-x.dec.com
ping6 www.6bone.net
ping6 carmen.ipv6.cselt.it
ping6 ipv6.research.microsoft.com
```

3.4 WINDOWS XP PPROFESSIONAL

3.4.1 INTRODUCCION

Windows XP proporciona nuevas pantallas, menús simplificados además en equipos compartidos, cada persona que utiliza el equipo puede crear una cuenta diferente protegida

por contraseña con opciones personalizadas y archivos privados. Puede haber varias cuentas activas en el equipo al mismo tiempo.

Las características de comunicación avanzada de Windows XP Professional ofrecen facilidades que permiten aprovechar las ventajas de las tecnologías de informática móvil y de comunicación inalámbrica más novedosas y vanguardistas. Las conexiones inalámbricas seguras permiten comunicarse y colaborar en tiempo real, en el mismo momento en que suceden las cosas, mediante la voz, vídeo y mensajería instantánea. No hay pérdida de tiempo intentando conectar, automáticamente se le notificará siempre que otro dispositivo inalámbrico esté dentro del alcance. Windows XP Professional permite hasta 10 conexiones de Internet o de uso compartido de archivos al mismo tiempo. Los puentes de red permiten la comunicación a través de conexiones inalámbricas, Ethernet y líneas telefónicas domésticas al mismo tiempo.

La seguridad global se ha mejorado, lo que facilita todavía más las compras y la exploración en Internet. También podrá comunicarse con otras personas en otras redes sin tener que preocuparse por comprometer su privacidad o la seguridad de sus archivos personales.

3.4.2 REQUERIMIENTOS DE HARDWARE

Los requisitos mínimos de hardware para que funcione Windows XP son:

- **Microprocesador** Pentium de 233 MHz o superior (o equivalente)
- Se recomienda 128 megabytes (MB). 64 MB de **RAM** es el mínimo y 4 gigabytes (GB) de **RAM** el máximo
- 1,5 GB de espacio libre en el **disco duro**
- Monitor VGA
- Teclado
- Mouse
- Unidad de CD-ROM o DVD

3.4.3 INSTALACIÓN Y CONFIGURACIÓN DE IPV6

3.4.3.1 INSTALACIÓN

La instalación en este sistema operativo en particular del protocolo IPV6 es muy fácil debido a que ya está incluido en su distribución, basta con sólo ejecutar el comando ***install ipv6*** desde el prompt del símbolo del sistema.

3.4.3.2 CONFIGURACIÓN

Al estar basado Windows XP en la tecnología que utiliza Windows 2000 Server, la configuración se realiza exactamente igual que en éste último[4], también acepta las distintas configuraciones, así que trabajar con los sistemas operativos de Microsoft es muy fácil.

3.5 SOLARIS

3.5.1 INTRODUCCIÓN

El sistema operativo Solaris proporciona características como: portabilidad, escalabilidad, interoperatividad y compatibilidad. Además de esto también posee una gran funcionalidad en áreas con simetría de multiprocesos, funcionalidad de tiempo real, mayor seguridad, y un Sistema de Administración mejorado.

[4] Página 999

3.5.2 CARACTERÍSTICAS GENERALES

Entre las características de Solaris tenemos:

- **PORTABILIDAD**: El software conformado por una ABI[5] se ejecuta con un Shrink-wrapped (Contracción envuelta) el software en todos los sistemas vendidos con la misma arquitectura del microprocesador obliga a los desarrolladores de aplicaciones a reducir el costo del desarrollo del software y traer productos al mercado rápidamente, y obliga a los usuarios a actualizar el hardware mientras retienen sus aplicaciones de software y minimizan sus costos de conversión.
- **ESCALABILIDAD**: Las aplicaciones se usan con más frecuencia en el sobre tiempo, y requiere sistemas más poderosos para soportarlos. Para operar en un ambiente creciente, el software debe ser capaz de ejecutar en un rango de ancho poderosos y debe ser capaz de tomar ventajas del poder adicional que se está procesando.
- **INTEROPERATIBIDAD**: La computación del ambiente heterogéneo es una realidad hoy. Los usuarios compran de muchos vendedores para implementar la solución que necesitan. La estandarización y una clara interfase son criterios para un ambiente heterogéneo, permitiendo a los usuarios desarrollar estrategias para comunicarse por medio de su red. El sistema operativo Solaris puede interoperar con unos sistemas muy populares hoy en el mercado, y aplicaciones que se ejecutan en UNIX se pueden comunicar fácilmente.
- **COMPATIBILIDAD**: La tecnología de la computación continua avanzando rápidamente, pero necesita permanecer en el ámbito competitivo para minimizar sus costos y maximizar sus ingresos.

3.5.3 CARACTERISTICAS PARA LOS USUARIOS

Dentro de las características de los usuarios tenemos:

[5] (Aplicación de Interfaces Binaria, Application Binary Interface)

- **ESPACIO DE TRABAJO PARA EL ADMINISTRADOR** (A workspace manager): cuenta con una ventana de manejo de servicios rápidos (open, close, more, etc.), así como herramientas que le permiten al usuario ajustar su espacio de trabajo a sus necesidades personales.
- **INTEGRACION DE SERVICIOS DESKTOP** (Desktop Integration Services): incluyen ToolTalk, Drag and Drop (arrastrar y soltar), y cut and paste (cortar y pegar), proporcionando la base para que a las aplicaciones puedan integrarse unos con otros.
- **BIBLIOTECAS GRÁFICAS** (Graphics Libraries): incluye XGL, Xlib, PEX, y XIL, proporcionando soporte para aplicaciones de 2D y 3D.
- **ADMINISTRADOR DE CALENDARIO** (Calendar Manager): posee una aplicación de administrador de tiempo que despliega citas y todos los compromisos del día, semana, o un mes en una ojeada. También contiene un Multibrowse que hace un programa de reuniones entre un grupo de usuarios más fácil. Varios calendarios pueden ser cubiertos simultáneamente para determinar la conveniencia de la hora de una reunión en una ojeada.
- **HERRAMIENTA DE IMAGEN** (Image Tool): permite cargar, ver y salvar imágenes en 40 diferentes formatos incluyendo PICT, PostScript (TM), TIFF, GIF, JFIF, y muchas más.

Otras herramientas incluyen una herramienta de impresión, audio, shell, reloj, y editor de texto.

3.5.4 CARACTERISTICAS PARA EL ADMINISTRADOR DEL SISTEMA

El Sistema Solaris ofrece una variedad de herramientas nuevas para el administrador como lo son:

- **Dispositivo de Información**: los administradores pueden usar estos accesorios opcionales para obtener información sobre dispositivos instalados incluyendo nombres, atributos, y accesibilidad.

- **Sistema de Administración de Archivo**: estos accesorios permiten a los administradores crear, copiar, amontonar, depurar, reparar y desmontar sistemas de archivos, crear y remover cadenas de archivos y nombrar tuberías o pipes, y manejar volúmenes.
- **Manejo del Proceso**: este controla la agenda de control del sistema. Usando estos accesorios, administradores pueden generar reportes sobre el desempeño, entrada de identificación, ubicación del acceso a discos, y buscar la manera de afinar el desempeño del sistema.
- **Usuarios y el manejo del grupo**: con estos accesorios, un administrador puede crear y eliminar entradas en grupos y entradas de identificación del sistema, y asignar grupos y ID's de usuario.
- **Seguridad**: El ASET (Automated Security Enhancement Tool) es un accesorio que incrementa la seguridad porque permite a los administradores de sistemas revisar archivos del sistema incluyendo permisos, pertenencia, y contenido del archivo. El ASET alerta a los usuarios acerca de problemas de seguridad potencial y donde es apropiado colocar el sistema de archivos automáticamente de acuerdo a los niveles de seguridad especificados.

3.5.5 PAQUETES DE SOFTWARE Y CLUSTERS

El software del sistema de Solaris es entregado en unidades conocidas como paquetes. Un paquete es una colección de archivos y directorios requeridos para el producto de un software. Un cluster es una colección de paquetes. Hay 4 tipos de clusters:

- **Núcleo del Soporte del Sistema** (Core System Support): es el software de configuración mínima; contiene solo el software necesario para iniciar el funcionamiento del computador y ejecutar el ambiente operativo Solaris.
- **Sistema de Soporte para Usuarios Finales** (End User System Support): contiene el Núcleo del Soporte del Sistema más el Sistema de soporte para usuarios finales, como lo es el Open Windows sistema de ventanas y aplicaciones de archivos DeskSet relacionados; este cluster incluye el software recomendado para un usuario final.

- **Soporte de Sistemas Desarrollados** (Developer System Support): contiene soporte de usuario final del sistema más librerías, incluye archivos y herramientas que se necesitan para desarrollar el software en el sistema de Solaris. Compiladores y depuradores no están incluidos en el sistema de Solaris 2.5.

3.5.6 ADMINISTRACION DEL PAQUETE

El manejo de paquetes de software simplifica la instalación y actualización del software. La administración es simplificada porque el método de manejo del software del sistema y aplicaciones de terceros son ahora consistentes. Las herramientas para crear paquetes de software están en un paquete de aplicaciones de herramientas de biblioteca.

Hay 2 herramientas que se pueden utilizar para instalar y remover paquetes:

- **Programa de Interface Gráfica** (A graphical user interfase program): se puede instalar un software en un sistema local o en un sistema remoto con Admintol (comenzando con el comando Admintol). Se utiliza Admintol para:
  - Ver el software instalado en un sistema local.
  - Instalar o remover un software en un sistema local.
- **El comando de línea de accesorios** (The command-line utilities): se utiliza para instalar, remover, y revisar la instalación del paquete de software.

3.5.7 SERVICE ACCESS FACILITY (SAF)

El SAF es una herramienta usada para administrar terminales, módems, y otros dispositivos de red. En particular, el SAF permite:

- Añadir y administrar (ttymon and listen) monitores en puertos (usando el comando sacadm)

- Añadir y administrar (ttymon) servicios de monitores en puertos (usando los comandos pmadm y ttyadm)
- Añadir y administrar (listen) servicios de monitores en puerto (usando los comandos pmadm y nlsadmin)

El SAF no es un programa. Es una jerarquía de últimos procesos y comandos de administración. El nivel tope del programa SAF es el SAC. El SAC (Service Access Controller) controla monitores de puerto que se pueden administrar por el comando ***sacdm***. Cada puerto de monitor puede manejar uno ó más puertos

3.5.8 CONTROLADORES DE INTERFACES DE DISPOSITIVOS

La intención de Solaris 2.5 SPARC DDI/DKI es de proporcionar una compatibilidad de los dispositivos que soporten las plataformas y para todas las futuras innovaciones del ambiente de Solaris 2.5 en esas plataformas. En el ambiente operativo de Solaris 2.5 hay un nuevo conjunto de dispositivos de interfaces.

Los dispositivos de interfase en el ambiente operativo Solaris2.5 están formalizados y son referidos como Solaris 2.5 SPARC DDI/DKI. El término DDI/DKI es derivado de la especificación original que se utiliza como suministro del SVR4 (System V Release 4). DDI/DKI significa device driver interface/driver kernel interface. Las interfaces se dividen en 3 grupos:

DDI/DKIDKI onlyDDI onlyDDI/DKI: se estandarizó en el SVR4, y son genéricos a lo largo de todas las implementaciones del SVR4, independientemente de la plataforma en la que se ejecuta.

DDI only: son genéricos como las interfaces de DDI/DKI y son soportados en todas las implementaciones del SVR4. Por otro lado, no son garantizados para ser soportados en el Solaris V.

DKI only: están destinados a ser de una arquitectura específica; por ejemplo, métodos para accesar y controlar dispositivos y sistemas de hardware específico (archivos de E/S, servicios de DMA, interrupciones, y memoria de mapeo). Estas interfaces no están garantizadas para trabajar en otras implementaciones de SVR4.

Estos dispositivos, combinados con un gran número de plataformas SPARC, son una ayuda a nuevos desarrolladores de hardware. En el Solaris 2.5 DDI/DKI solo el DDI only son genéricos a todos los sistemas Solaris basados en SPARC que soportan Solaris 2.5 DDI/DKI.*KERNEL*

El kernel del Solaris tiene multithread. En vez de una llave maestra, hay muchas llaves pequeñas que protegen pequeñas regiones de código. Por ejemplo, puede haber una llave de kernel que protege el acceso a un nodo particular, y uno que protege un nodo. Solo un procesador puede estar ejecutando códigos relacionados con ese nodo a la vez, pero otro podría estar accesando un nodo. Esto permite mayor concurrencia. El kernel de multithread tendrá mayor impacto en como está diseñado el controlador.

3.5.10 IMPLEMENTACION Y CONFIGURACIÓN DE IPV6 PARA SOLARIS

Lo primero que necesita para poder instalar IPV6 en su sistema Solaris es obtener la última versión de este protocolo, para ello debe visitar el sitio oficial de Sun en Internet en la siguiente dirección: http://www.sun.com/solaris/ipv6. Esta distribución se encuentra en forma de parche, de acuerdo con su plataforma puede ser el107788 para Sparc y 107916 para x86. Los archivos que usted descargará deben ser algo parecido a esto:

```
-rw-r--r--   1 acd      root     7815169 Jul 15 19:00 107788-01.tar.gz
-rw-r--r--   1 acd      root     5453436 Jul 21 17:23 107916-01.tar.Z
-rw-r--r--   1 acd      root        9768 Jul 21 17:23 README.107788-01
-rw-r--r--   1 acd      root        7864 Jul 21 17:23 README.107916-01
```

Dependiendo de su plataforma puede no necesitar todos los archivos. Obtenga el ultimo README y léalo, contiene información esencial que necesitará saber.

La parte agradable de este formato de distribución es que es realmente muy fácil de utilizar. Simplemente descomprima (un-tar) los archivos, después, en el directorio donde se encuentran éstos; escriba algo como esto:

patchadd –d . 107788-01

Sustituya 107788-01 con 107916-01 si esta utilizando una PC, patchadd reemplazará los archivos existentes por los que necesitará para ejecutar IPV6. Ahora debe reiniciar su equipo.

Algunos cambios son muy evidentes en la forma en que trabaja IPV4 para Solaris y la forma en que lo hace IPV6. no hay equivalente del archivo defaulrouter, se espera que lo autodescubra IPV6 por la vía del descubrimiento del vecino (neighbor), afortunadamente no tiene que preocuparse por esto.

Presumiblemente usted querrá hacer una auto configuración sobre sus interfaces IPV6. Éste es el método más conveniente. Para ello, solo cree el archivo /etc/hostname6.* sin entradas, es decir, en blanco. Eso auto configurará las direcciones IPV6 mediante el ruteador IPV6.

3.5.10.1 CONFIGURANDO TÚNELES (TUNNELS)

Los túneles son bastante fáciles sobre Solaris. Existen dos tipos, automático y configurado, ambos deben ser preparados. Para preparar un túnel automático, cree un archivo llamado /etc/hostname6.ip.atun0[6]. En este archivo coloque una línea como la siguiente:

tsrc SU_DIRECCIÓN_IPV4 ::SU_DIRECCION_IPV4/96 up

[6] La "a" en atun0 especifica que es un túnel automático.

Donde SU_DIRECCIÓN_IPV4 se encuentra en la notación tradicional como 192.168.0.2. A continuación se presenta un ejemplo de esta línea completa:

tsrc 209.112.190.80 ::209.112.190.80/96 up

para un túnel configurado aquí está la línea que debe ser agregada al archivo /etc/hostname6.ip.tun0:

tsrc SU_DIRECCION_IPV4 tdst TUNNEL_V4_ADDRESS up

si usted además quiere tener una dirección IPV6 en este túnel, también agregue:

addif SU_HOSTNAME_IPV6/mask TUNNEL_V6_HOSTNAME up

Si utiliza hostname asegúrese que están definidos en el archivo /etc/inet/ipnodes para IPV6 y /etc/hosts para IPV4. Como este es un enlace punto a punto, probablemente este utilizando una mascara /128 (ruta del Ruteador).

El siguiente es un ejemplo de un túnel configurado:

tsrc 209.112.190.80 tdst 209.112.190.25 up
addif snowy.woods.net/128 r2.ipv6.greatland.net up

Esto crea un túnel IPV6 en IPV4 desde 209.112.190.80 (snowy.woods.net) hacia 209.112.190.25 (r2.anchorage.greatland.net), entonces configura IPv6 en ese túnel que usa las direcciones especificadas en /etc/inet/ipnodes para esos hostnames.

Estos son los archivos que necesita editar en orden para tener una configuración IPV6 cliente funcional:

/etc/inet/ipnodes Agrega direcciones y hostmanes IPV6 así

	como IPV4.
/etc/hosts	Agrega hostnames y direcciones IPV4 para las interfaces locales.
/etc/hostname6.*	Creado pero en blanco.
/etc/hostname.*	Direcciones IPV4 para cada interfase
/etc/defaultrouter	Ruteador IPV4 por default
/etc/inet/ndpd.conf	configuración de "Descubrimiento de Vecino (Neighbor Discovery)" para un ruteador.
/etc/nsswitch.conf	Agrega DNS para lookups, nodos ip y hosts
/etc/hostname6.ip.atu*	Auto-túnel.
/etc/hostname6.ip.tun*	túneles configurados.

Capitulo IV

"Migración de protocolos"

4.1 MODELO DE ARQUITECTURA PARA LA INTERCONEXIÓN DE SISTEMAS ABIERTOS.

Este modelo, conocido por las siglas OSI, y cuya actividad vio a luz a principios de 1977 y obtuvo el grado definitivo de estándar internacional en 1983, trata de establecer las bases para la definición de protocolos de comunicación entre sistemas informáticos. Su principal objetivo es la interconexión de sistemas de diferentes fabricantes, es decir, de sistemas abiertos. Por ellos OSI constituye un marco para la coordinación de las actividades de normalización de los sistemas de telecomunicaciones e información.

La base de la normalización es el Modelo de Referencia. Cada sistema abierto está lógicamente formado por un conjunto ordenado de subsistemas –para OSI son siete como se muestra en la figura 4.1- que junto con el medio físico proporcionan un conjunto completo de servicios de comunicación.

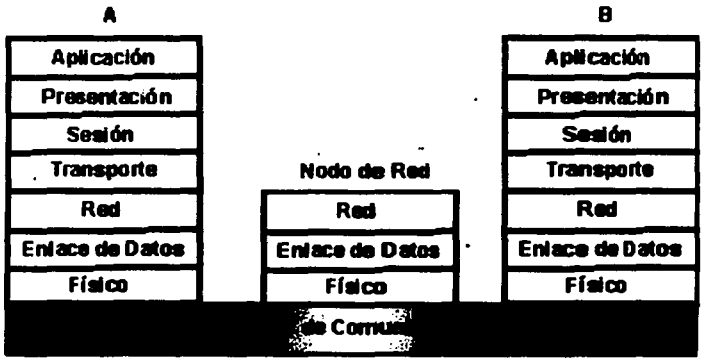


Figura 4.1 Niveles OSI

4.1.1 CONCEPTOS BÁSICOS DE OSI

El modelo de referencia OSI es el modelo que se ha estructurado mas recientemente, por lo que, a pesar de no existir muchas implementaciones OSI, sí puede afirmarse que se trata del modelo que proporciona un nivel de formalización más abstracto. Por este motivo es el que

se emplea habitualmente en la literatura y en el mundo académico como marco e hilo conductor para desarrollar los conceptos de redes y sistemas teleinformáticos.

Dentro del modelo de referencia OSI se establecen tres niveles de abstracción:

- **La arquitectura OSI**. Define los elementos básicos de los sistemas abiertos abstractos, es decir, de que manera debe verse un sistema desde el exterior.
- **Las especificaciones de servicio OSI**. Define los servicios proporcionados a los usuarios en cada nivel, es decir, los servicios proporcionados por un nivel al nivel superior.
- **Las especificaciones de protocolos OSI**. Definen la información de control transmitida entre los distintos sistemas, así como los procedimientos para la interpretación de dicha información de control.

El modelo de referencia OSI es un modelo de redes estructuradas en capas o niveles. El objetivo es tratar de manera estructurada la totalidad de un sistema teleinformático. El conjunto de funciones del sistema se divide en niveles, facilitando su estudio y desarrollo, que sean fácilmente controlables de forma individual y que en conjunto resultan satisfactoriamente las necesidades de comunicación.

Cada nivel se desarrolla sobre el anterior, de tal forma que recibe una serie de servicios sin conocer los detalles de cómo se realizan dichos servicios. Las diferentes funciones de la arquitectura OSI han sido estructuradas en siete niveles, siendo las funciones asignadas a cada uno de ellos complementarias. La figura 4.2 muestra la arquitectura de una red que utiliza el modelo OSI.

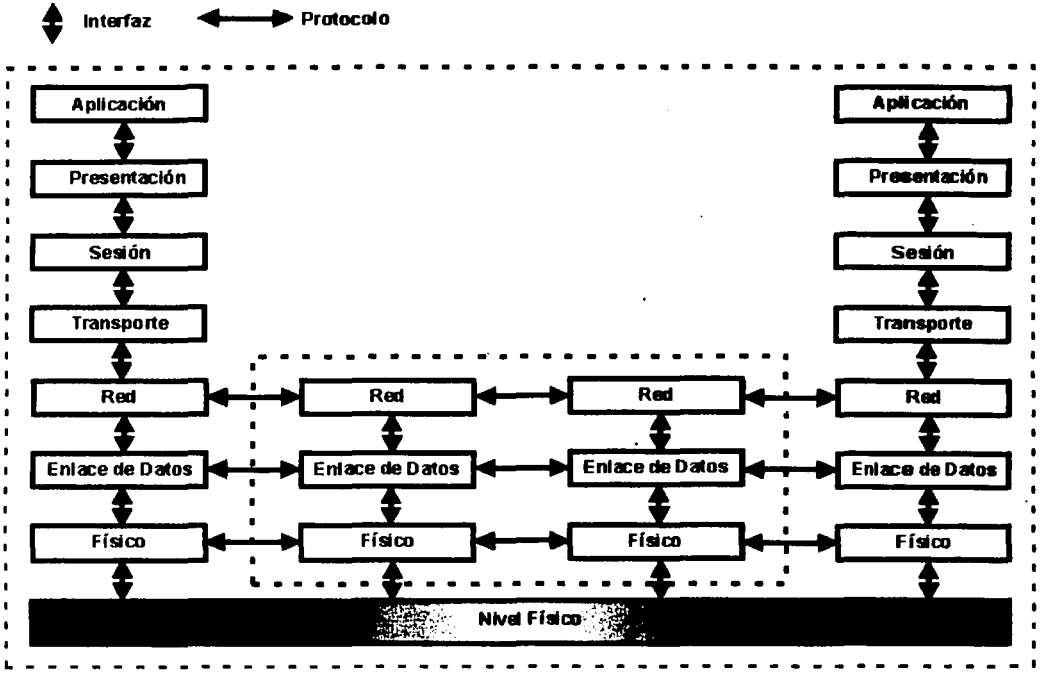


Figura 4.2 Arquitectura de una red basada en el modelo OSI.

La estructura de una red de comunicaciones se compone de una serie de nodos que pueden estar formados por el sistema central, una unidad central de comunicaciones o una terminal. En ella se define el término usuario final como el elemento que da origen o es receptor de la información. Este usuario puede ser tanto una aplicación como un dispositivo de entrada / salida.

Por el término nivel entendemos cada una de las particiones en que se ha dividido el sistema teleinformático. Unidad funcional o entidad es un proceso que se ejecuta dentro de un mismo nivel e implementa funciones de ese nivel.

Cada nivel se relaciona con el nivel inmediatamente superior o inferior a través del concepto de interfaz, que representa el conjunto de elementos lógicos y físicos existentes entre dos niveles adyacentes.

Los procesos que una unidad funcional realiza y cuyos resultados son ofrecidos o empleados por el nivel superior se denominan servicios de nivel. Estos servicios se proporcionan a través de los puntos de acceso al servicio (SAP, Service Access Points) de la interfaz.

Se define como protocolo el conjunto de reglas o convenciones que controlan el intercambio de información entre unidades funcionales del mismo nivel, tanto en la transmisión como en el control y recuperación de errores.

La figura 4.3 muestra la estructura interna de un nivel y su relación con los niveles adyacentes.

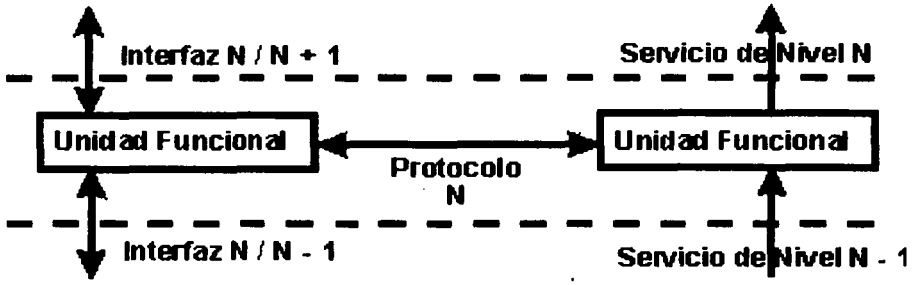


Figura 4.3 Estructura Interna de un Nivel.

4.1.2 TRANSMISIÓN DE DATOS EN OSI.

La comunicación entre dos nodos de una red significa que los correspondientes niveles de ambos nodos o niveles que están "hablando" entre ellos. Para que dicha comunicación sea posible cada nodo debe tener idénticos protocolos de nivel. Ésta comunicación se mantiene mediante el intercambio de mensajes con un formato común denominados unidades de datos de protocolos (Protocol Data Unit PDU).

Para ejemplificar como se realiza la transmisión de datos a través del modelo de referencia OSI suponga que existen dos nodos, el emisor y el receptor. El nodo emisor pone a disposición de su nivel de aplicación los datos que desea transmitir. El nivel de aplicación

incorpora a los datos pasados por el nodo información propia del nivel mediante datos de cabecera y cola (datos situados al principio y al final del mensaje respectivamente); la totalidad de la información cabecera mas datos mas cola es entregada al nivel de presentación, quien a su vez, añade una nueva cabecera y cola propias del nivel, transfiriendo el resultado al nivel de sesión. Este proceso se repite en el resto de los niveles por los cuales va pasando el mensaje hasta llegar al nivel físico. En el nivel físico es desde donde se realiza realmente la transmisión de la información. En el nodo receptor el mensaje recibido sufre el proceso inverso al que se vio sometido en el emisor. A medida que el mensaje asciende por los niveles de la torre OSI del nodo receptor, se le quieta la información de cabecera y cola correspondiente de cada nivel. De esta forma, finalmente, los datos llegan al nodo receptor idénticos a como fueron enviados por el nodo emisor.

Como se observa, no existe una comunicación directa entre los niveles, a excepción del nivel físico. Cuando se realiza una comunicación entre usuarios de diferentes sistemas se establece una relación lógica utilizando el protocolo de nivel 7. Este protocolo requiere los servicios del nivel 6, obligando, por lo tanto, a los dos niveles 6 a comunicarse a través de su propio protocolo de nivel 6 y así sucesivamente hasta llegar al nivel 1 donde se realiza realmente la comunicación.

La figura 4.4 ilustra la transmisión de datos en una red con arquitectura OSI. Además se muestra la clasificación de los niveles en dos grupos.

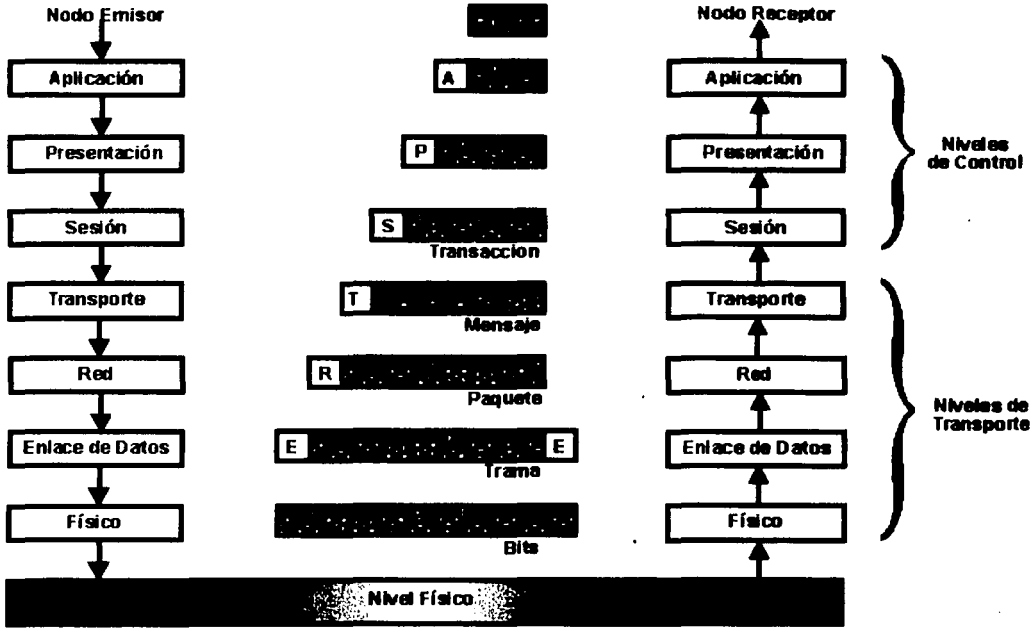


Figura 4.4 Transmisión de datos en el modelo OSI

4.1.3 NIVELES OSI.

A continuación se describen las funciones básicas y los elementos de cada nivel del modelo de referencia OSI:

- **Aplicación**. Es el nivel superior de las arquitecturas OSI y tiene como misión controlar y coordinar las funciones a realizar por los programas de usuarios de manera que les permita el acceso al entorno OSI. Los procesos de aplicaciones se comunican entre sí por medio de las entidades de aplicación utilizando servicios de presentación (de su nivel inferior inmediato, nivel 6).

  Se pueden distinguir tres tipos de procesos de aplicación:

  - **Procesos del propio sistema**. Son los que ejecutan funciones para controlar y supervisar operaciones de los sistemas conectados a la red de comunicación.

- **Procesos de gestión de aplicaciones**. Son los encargados de controlar y supervisar las operaciones de los procesos de aplicación.
- **Procesos de aplicación de usuario**. Son los que procesan la información real para los usuarios finales.

- **Presentación**. Es el encargado de la transferencia de los datos contenidos en los protocolos de aplicación. En este nivel intervienen los aspectos sintácticos de la información o, lo que es igual, la forma o código en que se presentan los datos. A través de este nivel, los procesos de aplicación adquieren independencia de la representación de los datos e incluyen en su entorno las posibles transformación es de códigos. Los servicios que proporciona el nivel de presentación serán, por tanto, la transformación de la sintaxis de los datos y la sintaxis de la presentación de los mismos.

- **Sesión**. Los cuatro niveles siguientes son lo que proporcionan los mecanismos para un correcto y seguro intercambio de datos entre sistemas. Sin embargo, determinadas aplicaciones podrían requerir otras opciones que no proporciona este servicio básico, como por ejemplo la comparición de una conexión de nivel transporte para de esta forma ordenar el diálogo, o la introducción de puntos de sincronización en el flujo de la información para de esta forma permitir la recuperación de la comunicación o la realización de copias de seguridad.

  Los servicios proporcionados por el nivel de sesión son los siguientes:

  - **Establecimiento de la conexión de sesión**. Se realiza la conexión de dos entidades de presentación a petición del usuario.
  - **Intercambio de datos**. Es el servicio que permite la transferencia de datos. Puede ser en un sentido, en otro o en ambos.
  - **Liberación de la conexión de sesión**. Una vez finalizado el intercambio de datos se procede a la desconexión.
  - **Sincronización y mantenimiento de la sesión**. Se realiza la sincronización y control de la comunicación de manera que se produzca un intercambio ordenado de datos.

- **Transporte**. El objetivo del nivel de transporte es proporcionar un mecanismo fiable para el intercambio de datos entre procesos en diferentes sistemas. Este mecanismo independiza al nivel de sesión y niveles superiores de los elementos de comunicación que constituyen la red; es decir, oculta a los niveles superiores los detalles específicos de la red a través de la cual se transmite la información. El nivel de transporte pasa los datos del nivel de sesión al nivel de red, fragmentados en unidades más pequeñas si es necesario y asegurando que todos llegan correctamente a su destino. Para ello emplea funciones de direccionamiento, multiplexación, establecimiento de la conexión y desconexión y de transferencia y control de flujo de los datos.

  El nivel de transporte puede, además, ofrecer servicios de detección y corrección de errores, para asegurar la integridad de los datos, así como niveles de calidad de servicio. Por ejemplo, una entidad de sesión podría especificar tasa de errores, retardo máximo y prioridad. Como ejemplo de protocolo de nivel de transporte es el TCP (Transmission Control Protocol).

- **Red**. La comunicación generalmente tiene lugar en el ámbito de una red, sea ésta pública o privada, compuesta por nodos. Este nivel es el responsable de asegurar que la información se transmite correctamente a través de la red. Proporciona a las entidades del nivel de transporte de transferencia de datos transparente. En este sentido, libera al nivel de transporte de la necesidad de conocer los mecanismos de transmisión de datos o tecnologías utilizadas para conectar sistemas. El nivel de red tiene como funciones la conexión y desconexión de redes, sincronización y control de flujo de las transferencias y la detección de errores en la transmisión, recuperándolos en caso necesario. En el caso de que hubiera mas de una red implicada en la transmisión también tiene como función el encaminamiento entre redes. Como ejemplo de este protocolo está el Internet Protocol (IP).

- **Enlace de Datos**. El nivel de enlace de datos es el responsable de mantener la integridad de los datos de una transmisión sobre un canal de comunicaciones. Es decir, proporciona un canal fiable para la transmisión de datos sobre un medio

físico, por lo general, no exento de ruido. Para ello, entre sus funciones se encuentras las de detección y corrección de errores de transmisión que pudieran ocurrir en el nivel físico. Los protocolos del nivel de enlace definen el establecimiento y liberación de un enlace de datos, controlan la correcta transferencia de información y recuperación de anomalías, así como la gestión del propio nivel.

- **Físico**. El nivel físico es el responsable de la definición de las características mecánicas, eléctricas y funcionales de la transmisión y recepción de la información utilizando un medio de comunicación especifico. Entre sus funciones básicas se encuentran la identificación de los circuitos de datos, el secuenciamiento de los mismos y la gestión del nivel.

4.2 INTERNET

El mundo está cambiando muy rápidamente: algunas personas dirían que, además, se hace cada vez más pequeño. Este fenómeno está íntimamente relacionado con el impacto de la tecnología: la revolución de las redes de computadoras. Internet ha supuesto una revolución sin precedentes en el mundo de la informática y las telecomunicaciones. El telégrafo, teléfono, radio, televisión y la computadora sentaron las bases para integrar capacidades nunca antes vistas. Internet constituye al mismo tiempo un mecanismo de difusión mundial, de propagación, interacción, y colaboración entre individuos y computadoras, independiente de su localización geográfica.

Internet inicia con un experimento de la ARPA (Advanced Research Projects Agency) en la década de los 60, con una red llamada ARPANET ideada entre otros por Leonard Kleinrock, Lawrence G. Roberts, I. Sutherland y Bob Taylor bajo la teoría de la conmutación de paquetes. En esta década y en los 70, más y más computadoras fueron enlazándose al embrión de Internet. En 1972 Ray Tomlinson escribió el software para el correo electrónico: la aplicación estrella de aquella época. La ARPANET evolucionó hacia Internet bajo la idea de federar varias redes que usaran la conmutación de paquetes y un protocolo de enlace

llamado NCP. En 1972, Khan desarrolló un nuevo protocolo más poderoso que NCP, que carecía de control de errores y no tenía capacidad para direccionar redes ni máquinas fuera de la ARPANET. El nuevo protocolo, llamado TCP/IP (transmision-control protocol/Internet protocol) estaría llamado a ser un protocolo de comunicaciones, basado en algoritmos de corrección de errores, reenvío de mensajes, redes independientes, funciones de pasarelas para redirigir los paquetes, interacción de diversos sistemas operativos, enrutado y división de paquetes si fuera necesario, entre otros detalles. En los años 80, el desarrollo de LANs (Local Area Networks), PC´s y estaciones de trabajo permitió el florecimiento de Internet. Como resultado de este crecimiento, se produjo un cambio en la gestión de la red: ahora las máquinas servidores (hosts) podían aspirar a tener un nombre y no sólo una dirección numérica. Esto llevó a la invención del DNS (Domain Name System) por Paul Mockapertris. DNS permitía un mecanismo escalable y distribuido para resolver jerárquicamente los nombres de los hosts en direcciones de Internet: lo que permite usar por ejemplo **www.lania.mx** en lugar del críptico 192.100.158.-254. TCP/IP sobrevivió como protocolo estándar y, en 1985, Internet estaba firmemente establecida como una tecnología que ayudaba al trabajo de investigadores y desarrolladores en sus comunicaciones diarias. Con el impulso de organismos como NFS, el backbone de Internet había hecho una transición desde la comunidad de investigación a usar equipos comerciales. En ocho años y medio el backbone había crecido desde seis nodos con enlaces de 56 Kbps a 21 nodos con enlaces de 45 Mbps. Internet contaba con más de 50,000 redes en los cinco continentes. El financiamiento de 200 millones de dólares entre 1986 y 1995 del programa NSFNET, permitió que TCP/IP sustituyera o marginara a la mayor parte de los protocolos restantes y se convirtiera en el portador de la "Infraestructura Global de Información". Pero la red Internet ha llegado a un punto de saturación en sus servicios. La comunidad académica ha reaccionado con una nueva propuesta de redes de comunicaciones, con más capacidades y servicios para satisfacer la creciente demanda de información.

4.3 INTERNET 2

El Proyecto de Internet2 está enfocado al desarrollo de recursos para una nueva familia de aplicaciones avanzadas que cumplen con los nuevos requerimientos universitarios

de investigación, enseñanza y aprendizaje. Los principales objetivos del proyecto Internet2 son:

1. La creación y el sostenimiento de una red con tecnología de liderazgo con la capacidad de cubrir las necesidades de la comunidad de investigación.
2. Dirigir los esfuerzos del desarrollo de la red para permitir la creación de una nueva generación de aplicaciones que exploten al máximo las capacidades de las redes de alto ancho de banda.
3. Trabajar para transferir rápidamente los nuevos servicios de red y aplicaciones a todos los niveles de educación y a la comunidad Internet en general.

4.3.1 HISTORIA DE INTERNET 2

En Octubre de 1996 inicia el proyecto de crear una red de alta velocidad, de entre 100 y 1000 veces más rápida que las redes actuales, con alrededor de 40 universidades de Estados Unidos. En 1997 nacen las iniciativas: NGI (Next Generation Internet) y UCAID (University Corporation for Advanced Internet Development) formada por 100 universidades, 17 organizaciones y 25 empresas. Internet-2 involucra dos grandes aspectos: el uso de nuevas tecnologías de comunicación: ATM, protocolos nuevos, gran ancho de banda por una parte y por otra la Integración de nuevas aplicaciones: Bibliotecas digitales, Teleinmersión, Videoconferencias, Laboratorios virtuales, Telemedicina y Educación a Distancia entre otras. Internet-2 no es una red superpuesta a Internet, ni tampoco la sustituye: es una red académica de alta velocidad que será el embrión de las nuevas redes del futuro.

Internet-2 hace uso del protocolo IP versión 6 (IPv6), que debe permitir a las aplicaciones: una muy alta fiabilidad, una alta capacidad (ancho de banda), soporte de selección de calidad de servicio (QoS: Quality of Service) y herramientas de monitoreo, distribución de cargas y variaciones en rendimiento y planificación dinámicas en función de las aplicaciones.

La ingeniería en Internet-2 tiene como objetivo minimizar los costos de acceso a las universidades participantes, proporcionando circuitos de conexión de alta velocidad. Además, mediante una arquitectura flexible es posible una interconexión de otros servicios regionales. Para servicios de áreas extensas un solo servicio será necesario: el gigaPoP (gigabits Point of Presence), que es un punto de interconexión de tecnología avanzada y alta capacidad, donde todos los participantes de Internet-2 pueden intercambiar tráfico de servicios avanzados entre sí. Las universidades de una región geográfica se pueden unir en un gigaPoP regional para conseguir los servicios de Internet 2.

Las nuevas aplicaciones de Internet-2 son, principalmente, las siguientes:

- **Software Educativo** (Learning-ware) y el **Instructional Management System** (IMS), para educación a distancia y con contenidos sobre demanda.
- **Bibliotecas Digitales**. El esfuerzo de Digital Libraries patrocinado por DARPA/NASA/NSF ya permite ofrecer catálogos en línea, resúmenes, indexación, y contenidos en forma electrónica. Las nuevas capacidades de Internet-2 ofrecen oportunidades para extender los programas de bibliotecas digitales a nuevas áreas. Un ancho de banda amplio permitirá la difusión de videos y audio digital en forma continua. Se permitirá además un acceso de todos estos materiales por canales dedicados actualmente, en forma casi exclusiva, a materiales textuales. La recuperación inteligente será una prioridad para acceder a estos materiales. Internet-2 proveerá el medio adecuado para que las computadoras de cualquier usuario tengan acceso a las nuevas tecnologías de visualización de la información, y las consultas en tiempo real o consultas por medio de videoconferencias incorporadas a la interfaz del usuario.
- **Teleinmersión**. Es la combinación eficaz de sistemas avanzados de telecomunicaciones que permitan aplicaciones colaborativas de manera fluida, así como la ampliación de la tecnología de "cavernas informáticas" para reconocer la presencia y el movimiento de individuos dentro de ellas, rastrear su presencia y movimientos y permitir su proyección en entornos de inmersión múltiple, geográficamente distribuidos, en los cuales los individuos pueden interactuar sensorialmente. La teleinmersión puede cambiar los paradigmas científicos y de fabricación. Los individuos pueden manipular datos, compartir simulaciones y

experiencias como si estuvieran en el mismo cuarto, participar juntos en simulación, diseños o procesos.

- **Laboratorios Virtuales** (LAV). Un LAV es un entorno distribuido heterogéneo de resolución de problemas que permitirá a investigadores, esparcidos por el resto del mundo, poder trabajar en proyectos comunes. Al igual que en laboratorios convencionales, las herramientas y técnicas son específicas del dominio de investigación, pero los requisitos de infraestructura básica se comparten entre las distintas disciplinas.
- **Telemedicina**. La telemedicina permitirá utilizar las nuevas tecnologías de comunicación para realizar intervenciones quirúrgicas y de diagnóstico a distancia, salvando así obstáculos geográficos. Un médico puede operar a distancia, mientras un robot esclavo reproduce fielmente sus movimientos, gracias al ancho de banda de Internet-2, el médico puede tener una realimentación sensorial y visual en tiempo real de la cirugía que realiza.
- En otras partes del mundo se están haciendo esfuerzos para crear redes de alta velocidad; en Canadá, por ejemplo, las nuevas redes de alta velocidad están agrupadas bajo CANARIE - CAN*Net; en Singapur existe SIGAREN, y en Taiwan, TAINET. Como proyectos internacionales se encuentran el Asia-Pacific Advanced Network Consortium (APAN) integrado por Australia, Japón, Corea, Singapur, Hong Kong, Indonesia, Tailandia y Malasia, con enlaces a: Canadá, Estados Unidos y Europa. En Europa, el grupo TEN34 es un esfuerzo que coordina multitud de redes nacionales de alta velocidad de los siguientes países: Alemania (DFN), Austria (AcoNET), Bélgica (BELNET), República Checa (CESNET), Francia (RENATER), España (RedIRIS), Grecia (GSRT), Hungría (HUNGARNET), Inglaterra (UKERNA), Italia (INFN), Luxemburgo (RESTENA), Holanda (SURFnet), Dinamarca - Finlandia - Noruega - Suecia (NORDUnet), Portugal (FCCN), Eslovenia (ARNES) y Suiza (SWITCH).

Los investigadores e ingenieros de Internet, Internet-2 y de las nuevas redes telemáticas y de las aplicaciones inteligentes están construyendo un mundo nuevo, intercomunicado y al alcance de un número cada vez mayor de individuos: un mundo que será muy diferente del que ahora vivimos.

4.3.2 ANTECEDENTES DE INTERNET 2

Siguiendo el desarrollo mundial de redes de datos de mayor capacidad y velocidad, para utilizarlas en aplicaciones de alta tecnología, en un esfuerzo conjunto, el Gobierno Mexicano, la Comunidad Universitaria y la Sociedad Mexicana en general, toman la iniciativa de desarrollar una red de alta velocidad y unirse a la red internacional denominada Internet-2, con el fin de dotar a la Comunidad Científica y Universitaria de México una red de telecomunicaciones que le permita crear una nueva generación de investigadores, dotándolos de mejores herramientas que les permitan desarrollar aplicaciones científicas y educativas de alta tecnología a nivel mundial.

Para tal efecto se han dado los siguientes pasos que marcan el inicio de este importante avance:

- El 8 de abril de 1999 se oficializó en Los Pinos la constitución de la ***Corporación Universitaria para el Desarrollo de Internet (CUDI)***, con la presencia como testigos de honor, del presidente de la República, Dr. Ernesto Zedillo Ponce de León, y de los Secretarios de Educación Pública, Lic. Miguel Limón Rojas y de Comunicaciones y Transportes Lic. Carlos Ruiz Sacristán.
- El 20 de mayo de 1999, en la ciudad de San Diego, California, representantes de la CUDI firman dos importantes Memorándums de Entendimiento con dos de las más importantes corporaciones universitarias que promueven y coordinan la disponibilidad de redes avanzadas para aplicaciones de investigación y educación en la Unión Americana, las cuales colaborarán conjuntamente con la CUDI en el desarrollo de tecnologías y aplicaciones de la nueva generación de Internet.
- El 20 de mayo de 1999 se firmó un convenio con Telmex participando como Asociado Institucional.
- El pasado 6 de Octubre de 1999, en la ciudad de Ottawa Canadá, se firmó un Memorándum de Entendimiento entre CUDI y CANARIE, esta ultima organización canadiense es la encargada del desarrollo de la red Internet avanzada en aquel país y con dicho acuerdo se podrán establecer programas de investigación, educación y colaboración entre ambos países.

4.3.3 OBJETIVOS DE INTERNET 2

- Crear nuevas aplicaciones que ayuden a los investigadores en sus trabajos.
- Acercar las nuevas tecnologías a la educación y a otras áreas, como la salud y la medicina, donde pueden aportar altos beneficios.
- Transferir la tecnología de Internet 2 a Internet.
- Demostrar que las nuevas aplicaciones pueden mejorar las capacidades de colaboración entre centros académicos y la transmisión de información.
- Mejorar procesos educativos y otros servicios (como los de salud) gracias a la ventaja que ofrece la llamada "proximidad virtual".
- Coordinar la adopción de estándares de trabajo para garantizar la calidad final del servicio.
- Estudiar el impacto de las nuevas infraestructuras, servicios y aplicaciones en la comunidad universitaria y en Internet en general.

4.3.4 PRINCIPALES DIFERENCIAS CON INTERNET TRADICIONAL

Las principales características que diferencian a Internet 2 del que se utiliza comercialmente hoy en día son las siguientes:

- **Mayor ancho de banda**: Una de las características fundamentales de Internet 2 es el manejo de un gran ancho de banda, en la actualidad dependiendo de los recursos disponibles se tienen en realidad velocidades del orden de los cientos de megabits por segundo pero la tendencia es a lograr llegar al rango de los gigabits por segundo.
- **Calidad de los servicios (Quality of Service)**: En Internet, todos los paquetes de información tienen la misma prioridad, de tal forma que si alguien esta enviando vídeo por la red y otras personas están transfiriendo un archivo de datos, ambas aplicaciones compiten por el mismo canal, de tal forma que probablemente los cuadros de vídeo no lleguen en forma continua, con lo cual se tendrá un congelamiento o al menos un deterioro en la calidad de la imagen. En cambio en Internet 2, se le puede dar prioridad al vídeo, de tal forma que se garantice que todos

los cuadros lleguen a tiempo y solo en los espacios que el vídeo deje libre se irán transmitiendo los paquetes del archivo de datos. Esta característica permite también mantener en un nivel adecuado el retardo de la información, esto es importante sobre todo para sistemas de control de dispositivos a distancia.

- **Transmisión Multipunto (Multicast)**: Otro problema que se tiene en Internet, consiste en que cuando queremos transmitir alguna información a un conjunto de usuarios, por ejemplo en la transmisión de un evento en vivo, se mandan los mismos paquetes de la señal de vídeo a cada uno de los usuarios, con lo cual se multiplica el trafico en la red. En cambio en Internet 2 se esta experimentando con una tecnología conocida como multicasting, en la cual se envía una sola vez cada paquete con la información necesaria para que les llegue a todos los usuarios que deben recibirlo.
- **Retardo Reducido (Low Latency)**: En aplicaciones sensibles al retardo de la información es vital reducir este al mínimo posible, en Internet 2 con la combinación de un gran ancho de banda, la priorización de los servicios y técnicas avanzadas de enrutamiento se logran retardos realmente muy pequeños en el orden de los milisegundos. Esto permite desarrollar sistemas de control a distancia de equipos muy sofisticados, en los cuales demasiado retardo de la información de control entre el equipo y el manipulador remoto puede resultar fatal.
- **Seguridad y Privacía**: Otro aspecto importante que se esta experimentando en Internet 2 consiste en la mejora de la seguridad y privacía de la red, utilizando protocolos que permitan autentificar plenamente el origen de los datos y que asegure la integridad y confidencialidad de los mismos.

Todas estas características permiten el desarrollo de aplicaciones de gran utilidad práctica, en diversas áreas tales como: Telemedicina, Educación a Distancia, Colaboratorios, Sistemas de Información Geográfica, Predicción del Clima, Bibliotecas Digitales, Realidad Virtual, Telepresencia, Simulación de Procesos Complejos.

4.3.4.1 COMPARACIÓN DE TECNOLOGÍAS

Aplicación	Internet	REUNA2/Internet2	Competencia
Videoconferencia	H323 hasta 56 Kbps, mala calidad, pérdidas de sincronismo	H323, 300 Kbps - MPEG-2, 8 Mbps, alta calidad, sincronismo garantizado	RSDI Internacional a 512 Kbps, calidad media, sincronismo garantizado
Video a pedido	H323 56 Kbps, mala calidad	H323, 300 Kbps – 8 Mbps MPEG-2, alta calidad	No hay
Acceso a depósitos masivos de datos	Capacidades de transferencia limitadas, en la práctica, a 30 MB/Hora	Capacidades de transferencia de 4,8 GB/Hora	Circuitos dedicados satelitales o terrestres.*Frame Relay* o ATM internacionales
Reserva de espacio (astronomía, medicina)	No disponible	Disponible	ATM internacional
Simulación distribuida	Mala calidad o servicio casi imposible (sincronismo no garantizado)	Calidad garantizada mediante reserva de espacio	Redes privadas con circuitos dedicados o ATM internacionales

4.3.5 PROYECTOS EN LA UNAM

En el Marco de Internet2, la UNAM ha participado activamente prospectando y planeando la realización de proyectos que son beneficiados directamente por las nuevas características que proporciona esta nueva red de alto rendimiento.

Algunos de estos proyectos se encuentran reflejados en este condensado, donde se tienen las caracteristicas esenciales de cada proyecto y las personal responsables de él, para ver a detalle la descripción del proyecto siga la liga correspondiente.

La UNAM cuenta con los siguientes proyectos de aplicación internet 2:

- Sistema de distribución de video y audio **WEBCASTING.** Distribución de contenido a través de la infraestructura de red, en forma de video, audio, presentaciones y documentos referenciales producidos por dependencias universitarias.

- Empleo de un Colaboratorio para intercambio síncrono de imágenes, video, datos y aplicaciones **COLABORATORIO.** Construir una red de grupos académicos donde se realicen labores de investigación apoyados por herramientas de colaboración en tiempo real sobre video, audio, intercambio de datos, edición coordinada de documentos, instrumentos remotos y uso de herramientas comunes de presentación de información.
- Centro de archivo astronómico en México. Proveer a la comunidad Astronómica en México un gran acervo de datos (tanto públicos como de uso restringido) con un acceso de alta velocidad, asi como herramientas que permitan el realizar procesos de búsqueda y análisis de datos recuperados.
- Plataforma de Servicios Distribuidos de Almacenamiento **ALMACEN.** Diseño de una estructura de alimentación, organización, resolución de ubicación, consulta y resguardo de acervos digitales para ser distribuidos a los usuarios de Internet2 de acuerdo a condiciones de frecuencia de solicitud (cache), previsión de acceso (push) y cercanía de servicio.
- Servicio de acceso al acervo astronómico de "Two Micron Survey All Sky Survey"
- **2MASS.** El proyecto detalla los mapas de esfera celeste en el infrarrojo. Esta es una base de datos muy valiosa para los astrónomos, pues es en estas longitudes de onda en la que se detectan procesos de formación estelar, campo en el que sobresale la comunidad nacional de astrónomos.
- Conversión Digital del acervo de TV-UNAM y RadioUNAM para su distribución por Internet2. **HI-BROADCASTING.** Conversión de los diversos formatos analógicos en los que se encuentra el material de la videoteca de TV-UNAM y de la Fonoteca de RadioUNAM a un formato digital que permita el ahorro en medios de Almacenamiento y la distribución del material en diversas aplicaciones.
- Control y transmisión de datos de los Observatorios astronómicos desde los centros de visualización y procesamiento **OBSERVATORIUM.** El proyecto contempla realizar funciones de control de movimiento, enfoque y obtención de datos de los telescopios que el Instituto de Astronomía de la UNAM administra para uso académico nacional e internacional.
- Realización de eventos por videoconferencia empleando alta calidad de video y audio con estándares de H.323 **VIDECONF-I2.** Construcción de una esquema de operación de videoconferencias empleando el estándar H.323 con características de alta

definición (60 cuadros por segundo de imagen) para su uso académico entre instituciones mexicanas e inicialmente la Universidad de Texas A&M.

- Talleres Virtuales. Implementar heramientas y la infraestructura para la realización de talleres y proyectos a distancia, entre universidades, con impacto de presencia virtual (proyeccciones 1:1, sets virtuales, heramientas compartidas).
- Sistema de traducción simultánea para servicios de videoconferencia. Facilitar el acceso de la comunidad universitaria a videoconferencias o servicios de video en demanda que de origen se proporcionan en idiomas distintos al español, asistiéndolos de traductores simultáneos que operen de forma automática.
- Sistemas multiprotocolo para audio y video digital. Incrementar el uso de sistemas de video y audio digital entre la comunidad universitaria, por medio de accesos en función del tipo de red y recursos físicos y lógicos con los que cuente cada usuario.
- Servicios de video en demanda bajo formatos de MPEG 1 y MPEG 2. Proporcionar a la comunidad universitaria acervos de video y audio digital relacionados con materiales didácos en línea a velocidades de transferencia de hasta 6Mbps. Se definen diversos niveles de seguriodad para restringir accesos a bancos de datos de informacion.
- Biblioteca Médica Digital Nacional. **BMND.** Creación de una Biblioteca Digital utilizando la infraestructura de cómputo , telecomunicaciones y acervos Bibliográficos; permitiendo brindar una amplia variedad de servicios y productos de información para alumnos académicos y profesionales en el área de la Salud en el ámbito nacional.
- Operación Remota de Microsonda JEOL **JEOL.** Control y despliegue visual a través de la microsonda JEOL de la muestra analizada por medio de la interconexión de computadoras en redes de alto desempeño.
- Páginas interactivas VRML con capacidades de procesos y monitoreos simples de ambientes complejos **MONITOREO-VRML.** Desarrollar páginas con ambientes virtuales que permitan interactuar al visitante para obtener información especializada y monitoreos en tiempo real.
- Telecontrol en robótica **ROBOTICA.** Operación de robots experimentales con tele-presencia, con manipulaciones a través de visualización simulada.
- Sistemas de Información Geográfica y Percepción remota con ambientes de navegación 2D y 3D, para sistemas de bases de datos de gran escala **GIS-2Y3D.** Generar una aplicación que permita visualizar en ambientes virtuales y su navegación,

topografías e información geográfica de bases de datos muy grandes (la república mexicana, 1.7 Gb, tan solo para el MDE).

- Arte en internet2: Visión 20/21 **ARTE.** La elaboración de un sitio donde sucedan eventos, siguiendo la estructura de "costumbre" del medio artístico.
- Colaboración Médica a través del control remoto de Instrumentos. **PET-I2.** Desarrollar los medios de cómputo que permitan la interacción Médica con instrumentos especializados en forma remota.
- Suite de productos para el trabajo científico en redes de alto rendimiento (habanero, labvis, cumulus) Poner a disposición de los usuarios de ambientes colaborativo en redes de alto rendimiento, una barra de herramientas complementarias, que puedan ser fácilmente explotadas por los usuarios.
- Distribución de tareas de software comercial en redes de alto rendimiento (AVS, Maya): Implementar los despachadores de distribución de tareas para permitir el cómputo distribuido en paquetes comerciales que lo permiten (AVS y Maya y AliasWavefront), para sintonizar su rendimiento en redes con gran ancho de banda.
- Barras de Herramientas para la visualización en línea o colaborativa con software de terceros: Un caso con Grass. Contar con las metodologías (y realizar un ejemplo con Grass) para la creación de barras de herramientas que permitan enviar instrucciones a paquetes instalados en servidores poderosos, para que ejecuten tareas y se desplieguen remotamente en un cliente; permitiendo el trabajo Colaborativo.
- Ambientes colaborativos y visualización en línea Desarrollo de un kernel para la instalación de distintas aplicaciones de Visualización científica, con la posibilidad de trabajos colaborativos y en línea.
- Cómputo Intensivo entre nodos computacionales Evaluación y simulaciones a mayor escala de varios códigos paralelos en nodos computacionales cercanos o lejanos geográficamente.
- Cómputo Paralelo esta relacionado con los algoritmos y con las computadoras multiprocesador. Las máquinas actuales están llegando a su límite físico en el procesamiento de datos, es por eso que desde hace algunos años las máquinas paralelas están teniendo cada vez más auge, pero esto implica cambiar la forma de diseñar los algoritmos y la programación.
- Instrumentación Remota en Mecánica de fluidos **IMPLEMENTACION REMOTA.** Desarrollar los medios de cómputo que permitan el uso remoto de equipo de

anemometría, laso e hilo caliente y sensor de precisión, instalados en el laboratorio del CIE en Temixco.

- Navegación Virtual de sitios Arqueológicos. **CACAXTLA.** Desarrollar los medios de cómputo que permitan realizar visitas y recorridos virtuales de sitios de interés cultural.
- Educación a Distancia

4.3.6 APLICACIONES EN INTERNET-2

En la comunidad de investigación, el cómputo avanzado está emergiendo. Estos sistemas surgen como agregados de recursos de software y hardware que los científicos requieren para resolver problemas extremadamente complejos. Por el lado del hardware, un sistema de cómputo avanzado es una colección de recursos dispersos geográficamente: redes, computadoras, bases de datos y herramientas de visualización y realidad virtual. Por el lado del software, es necesario un "middleware" para integrar este conjunto conformado por múltiples y variadas piezas de forma tal que operen como una sola.

Ian Foster y Carl Kesselman en su libro: "The Grid: A Blueprint for a New Computing Infrastructure" [http://www.mkp.com/grids], proponen una primera clasificación de los servicios de cómputo avanzado, que pueden distinguirse como:

- **Cómputo Distribuido**: Se trata de aplicaciones ejecutándose en paralelo en elementos computacionales dispersos, requiriendo para ello de programadores de interfases y herramientas de asignación de recursos, autorización, autentificación y comunicaciones.
- **Cómputo sobre Demanda**: Consiste en poder acceder remotamente a instrumentos tales como microscopios y aceleradores de partículas.
- **Cómputo Intensivo**: Bases de datos en red que permitan búsquedas y visualización.
- **Cómputo Colaborativo**: Teleinmersión y compartición de espacios de trabajo virtuales tales como Sistemas Colaborativos de Diagnóstico Médico, para los cuales se requiere de acceso a computadoras o bases de datos en tiempo real.

4.4 RDSI

Hoy en día nos damos cuenta de que cuando se utilizó por primera vez la red telefónica para realizar transmisiones a 300 baudios, era lo suficientemente buena para poderse comunicar con algún centro de investigación u otro departamento de la misma empresa, pero la calidad del sonido que nos ofrece la red telefónica no es lo suficientemente buena como para transmitir fax en blanco y negro y que la transmisión de datos a 28 800 bps no resulta eficaz, además de que existe la necesidad de transmitir imágenes, video, etc. La solución fue inventar algo nuevo o simplemente ampliar las posibilidades, esta ampliación se consigue gracias a la introducción de una nueva red llamada Red Digital de Servicios Integrados (RDSI).

La red telefónica está teniendo en los últimos años una profunda transformación, debido a la introducción en la misma de técnicas digitales, logrando lo que se ha venido a llamar Red Digital Integrada (RDI).

La RDSI supone la digitalización completa de todos los componentes, las centrales y medios de transmisión entre los mismos de modo que existe una continuidad digital de extremo a extremo de la comunicación. Además de eso, la RDSI posee un grado de inteligencia que permite ofrecer a los usuarios nuevas facilidades y servicios, en comparación con las redes existentes. De esa manera se obtiene no sólo una mejora en la calidad, sino la posibilidad de ofrecer nuevos servicios.

La capacidad de transferencia de información (voz, datos, video, etc.) entre el acceso de usuario y la RSDI está estructurada en forma de canales de transferencia de información. La RDSI considera los siguientes tipos de canales:

- **Canal B**: canal de 64 Kbps destinado al transporte de la información del usuario (voz, video, datos, etc.).
- **Canal D**: canal de 16 o 64 Kbps destinado principalmente a la transmisión de información de señalización usuario-red para el control de la comunicación, aunque también puede ser utilizado en determinadas condiciones para la transferencia de datos de baja capacidad.

- **Canal H**: son los canales que proporcionan al usuario una capacidad de transferencia de información a velocidades superiores a los 64 Kbps. Hasta el momento se han definido los canales H0 (384 Kbps, equivalente a 6 canales B), H11 (1536 Kbps, equivalente a 24 canales B) y H12 (1920 Kbps, equivalente a 30 canales B).

4.4.1 APLICACIONES DE LA RDSI

APLICACIONES GENERALES		
Transferencia de archivos	Teletrabajo	Teleedición
Aplicaciones multimedia	Trabajo en grupos	Teleconferencia audiográfica
Videoconferencia	Teleeventos	Televigilacia
Interconexión LAN-LAN	Videotex de alta calidad	Telecontrol y telemedida
Interconexión PC-LAN	Telediagnostico	Fax de alta calidad
Teleenseñanza	Acceso a bases de datos de imagen	Rutas de seguridad

APLICACIONES ESPECIFICAS	
SECTOR	**APLICACIÓN**
Publicidad y artes graficas	Telediseño interactivo
Administración	Sistemas de información multimedia
Administración	Gestión documental de grandes volúmenes de información
Industria	Telemantenimiento, teleasistensia
Distribución	Catalogo en centrales de compra
Medios de comunicación	Audio alta calidad.
Sanidad	Telediagnostico (transmisión de radiografías, historias clínicas)
Banca	Autoservicio multimedia en oficinas bancarias
Farmacia	Kiosco de información
Turismo	Servicio de información multimedia
Educación	Formación a distancia
Inmobiliario y construcción	Telecatalogo. Telediseño interactivo
Seguros	Tramitación de siniestros.

4.4.2 TRANSMISIÓN DE DATOS EN RDSI.

Realmente, no se puede hacer una diferenciación entre transmisión de datos y de cualquier otro tipo de señal, ya que la RDSI es una red completamente digital, cualquier tipo de señal que no es digital es convertida a digital antes de ser [illegible] la

red, por lo tanto, al disponer la RDSI de un servicio transparente a 64 Kbps con una interfaz usuario-red normalizada, lo que entre cualquier par de terminales que incorporen dicha interfaz, sin necesidad de utilizar módems. Esta capacidad de transmisión puede llegar incluso a los 128 Kbps en un acceso básico o 2048 en un acceso primario.

La posibilidad de transmitir datos a 64 o más Kbps permite abordar aplicaciones que hasta ahora requerían la utilización de medios específicos. Este es el caso, por ejemplo de las aplicaciones de interconexión de redes de área local, teletrabajo, acceso a bases de datos de imágenes, videodistribución, etc.

4.4.3 RDSI DE BANDA ANCHA.

La RDSI vista hasta ahora es lo que se denomina RDSI de banda estrecha, RDSI-BE, ya que sólo puede soportar la prestación de servicios que requieren el transporte de señales de hasta 2 Mbps. Esta limitación viene impuesta por la tecnología utilizada, que no es adecuada para manejar señales de mas velocidad.

Para aquellos servicios que requieren velocidades superiores a 2 Mbps es para los que se desarrollando la RDSI de banda ancha, RDSI-BA (BISDN Broadband ISDN en inglés). Esta red permitirá la transmisión de datos de hasta 34 Mbps mediante una línea de fibra óptica. Con esta línea se tiene acceso tanto a todos los servicios de la banda estrecha como a los siguientes:

- **Comunicación de datos** a muy alta velocidad (de 3 a 34 Mbps), lo cual es útil para la transferencia de señales de video, para la interconexión de redes de área local o para aplicaciones de diseño, fabricación de ingeniería asistida por el ordenador, CAD/CAM/CAE.
- **Videotelefonía** de alta calidad, que permitirá establecer comunicaciones viendo la imagen del interlocutor con calidad similar a la de la televisión actual.
- **Videotex** de banda ancha, que pondrá imágenes móviles a la información ofrecida.

4.5 TÉCNICAS DE MIGRACIÓN

4.5.1 MIGRACIÓN DESDE IPV4

Los nuevos sistemas IPV6 pueden ser una "pila doble" (dual stack) para ser compatibles con IPV4 y las direcciones mapeadas IPV4. Esta integración tiene dos características especiales. Primero, se pueden convertir direcciones IPV6 a IPV4 y viceversa. La segunda característica de esta integración tiene efecto sobre la suma de verificación (checksum). La mayoría de los protocolos de transporte TCP/IP usa una suma de verificación para asegurar la integridad de los datos, ésta suma de verificación se calcula con la dirección origen, la dirección destino, el encabezado y los datos. Esta integración del formato de direcciones permite implementaciones de transporte que calculan la suma de verificación consistentemente, independientemente si es una dirección IPV6 o IPV4. Si una computadora envía información usando la suma de verificación en direcciones IPV4, mientras que el receptor utiliza solamente direcciones IPV6, éste ultimo podrá recibir los paquetes de información.

4.5.2 EQUIVALENCIA DE ENCABEZADOS.

Debido a la similitud entre los dos protocolos, una migración es cosa fácil. La mayoría de los campos del encabezado se traducen directamente, los que no, pueden ser simplemente convertidos. La siguiente lista muestra los posibles pasos de la conversión:

- La longitud de los encabezados IPV4 es calculada basándose en las opciones presentes en los datagramas IPV6.
- IPV6 no controla las prioridades, por eso recibe la prioridad IPV4 como 0.
- El tipo de servicio IPV4 es ignorado en IPV6; todos los datagramas los recibe como servicio normal IPV4.
- La información de la fragmentación IPV4 se deriva de la cabecera de fragmentación IPV6, si ésta está presente, el fragmento de identificación IPV4 son los 16 bits menos significativos de la cabecera de fragmentación del mensaje IPV6. Un datagrama IPV4 fragmentado resulta en un datagrama IPV6 con cabecera de fragmentación.

- La suma de verificación de un encabezado IPV4 debe ser calculada una vez que se ha formado el encabezado.
- Las etiquetas de seguimiento IPV6 son ignoradas cuando los datagramas son convertidos a IPV4; éstas son puestas a cero sobre los datagramas IPV6 derivados de unos IPV4.

4.5.3 ESTRATEGIAS DE MIGRACIÓN.

Las estrategias de migración hacia IPV6 se componen de tres componentes principales:

- Claramente, los sistemas deben agregar la capacidad de entender IPV6 mediante una ***pila doble*** (dual stack).
- Otra opción es la del ***tunel***, que permite comunicarse con otros sistemas inclusive a través de redes IPV4.
- Cuando la popularidad o necesidad de IPV6 cause que en los sistemas se olvide completamente de IPV4, la ***traducción de encabezados*** ofrece una alternativa para que esos sistemas mantengan contacto con viejos sistemas IPV4.

4.5.3.1 PILA DOBLE (DUAL STACK)

El primer paso en una migración hacia IPV6 es el despliegue de sistemas que pueden entender IPV6. Al menos al principio, esos sistemas es probable que no tengan muchos otros con quienes comunicarse, la mayoría de los otros sistemas seguirán utilizando IPV4. Estos nuevos sistemas entonces probablemente serán unos "sistemas de pila doble", capaces de usar IPV4 e IPV6. La figura 4.5 muestra como las capas sobre IP permanecen igual en cada caso. Los sistemas de pila doble pueden comunicarse con sistemas IPV6 y también se pueden comunicar con sistemas viejos IPV4.

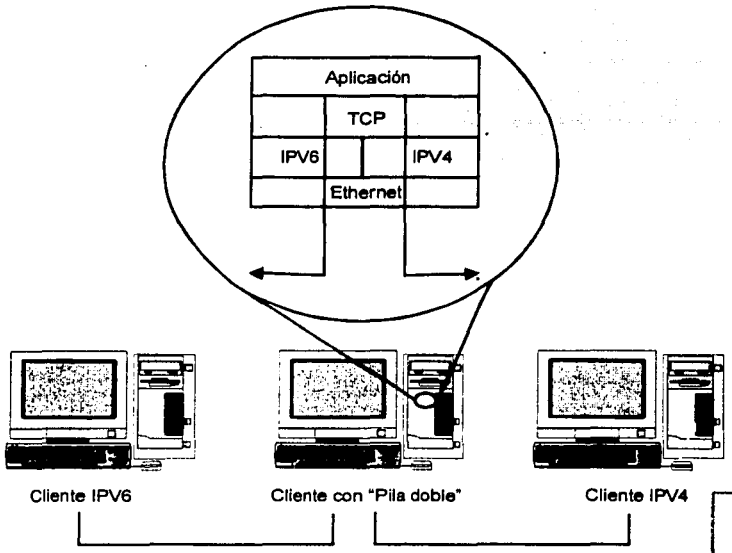


Figura 4.5 Cliente con "Pila Doble" comunicándose con clientes IPV4 e IPV6.

Para determinar que versión del protocolo IP pueden usar, los clientes pueden consultar el Sistema de Dominio de Nombres (DNS). Si el DNS regresa una dirección IPV6 para el destinatario de la información, el cliente puede usar IPV6, de otro modo utilizara IPV4. Para agregar direcciones IPV6 al DNS no se requiere que el servidor DNS soporte comunicación basada en IPV6, de hecho, el cliente DNS puede usar IPV4 para consultar al servidor y el servidor le puede responder usando IPV4, incluso aunque la información sea regresada en una red con direcciones IPV6.

Una vez que el cliente sabe que el destinatario puede entender IPV6, este todavía necesita decidir como enviar el datagrama. La capa IP misma puede hacer esta decisión automáticamente. Si el destino se encuentra sobre la misma red que el origen, entonces la decisión es fácil: utilizará IPV6. Si el destino se encuentra en una red diferente, no obstante, debe escuchar los avisos del ruteador, si alguno llega, entonces el cliente debe usar IPV6 para enviar el datagrama al ruteador. Si la comunicación requiere un túnel, entonces el ruteador puede establecerlo. Sólo si no hay un ruteador IPV6 disponible, el cliente deberá realizar la encapsulación para el túnel él mismo. Esta estrategia fuerza la preferencia de los ruteadores IPV6 sobre los IPV4. Desde que los ruteadores IPV6 entienden ambos

protocolos, probablemente se tiene que poseer un mejor conocimiento de la red como un entero para poder tomar mejores decisiones.

4.5.3.2 TUNEL

Cuando en las redes se introduzcan sistemas de pila doble capaces de soportar IPV6, más sistemas querrán usar IPV6 para comunicarse. Desafortunadamente, las viejas redes IPV4 deben separarse de esos sistemas, los sistemas IPV6 deben "tunelear" mediante la red IPV4.

Cuando un datagrama IPV6 alcanza el límite de la red IPV4, el ruteador lo encapsula en un datagrama IPV4. Como un datagrama IPV4, el nuevo mensaje debe tener una dirección de destinatario IPV4. Para obtener esa dirección el ruteador la extrae del paquete IPV6. La figura 4.6, muestra como el datagrama encapsulado viaja a través de todo el camino hasta su destino, donde el sistema receptor recupera el mensaje IPV6 original. El proceso completo no requiere una configuración especial en algún sistema, esto es, "tunelear automáticamente". En la figura el valor del siguiente encabezado que aparece en el datagrama IPV4, ese valor es 41, indicando que los datos IPV4 son un datagrama IPV6.

Cuando una dirección IPV4 es inalcanzable, el túnel automático no es posible, en esas situaciones hay que configurar el túnel manualmente para permitir a los sistemas IPV6 comunicarse. Un túnel configurado requiere una configuración explicita en el punto de entrada a la red IPV4. Esta configuración especifica el destinatario IPV4 para usar por los datagramas tuneleados.

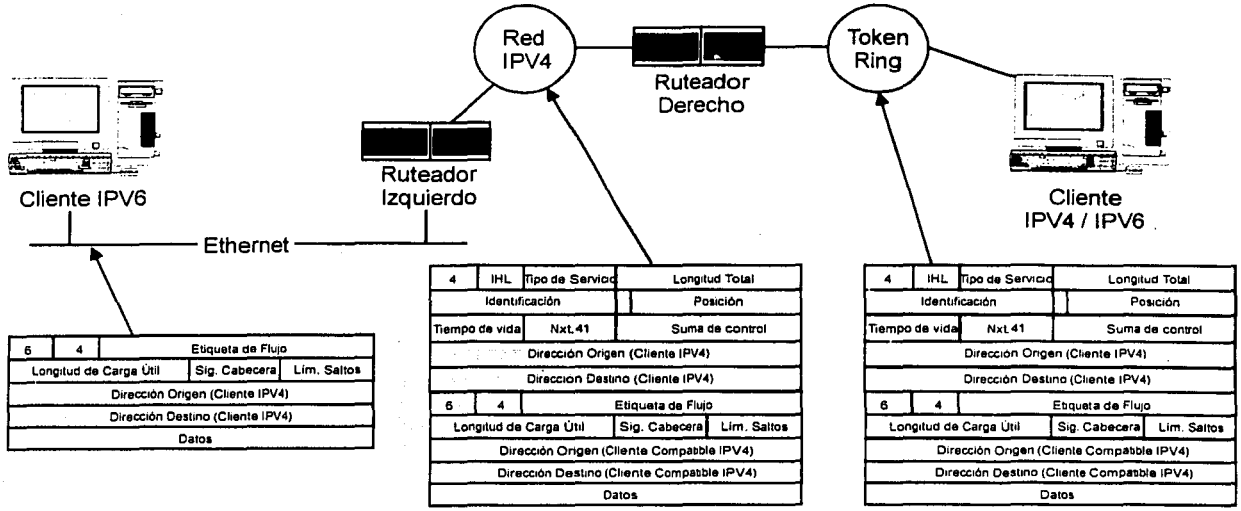


Figura 4.6 Túnel Automático con compatibilidad de direcciones IPV4.

A diferencia del túnel automático, la dirección destino IPV4 no es el último destino para los datagramas, cuando un datagrama encapsulado alcanza el punto final del túnel, el ruteador extrae el datagrama IPV6 de adentro y lo envía a su destinatario real.

La figura 4.7 muestra un túnel configurado atravesando una red IPV4, note que el datagrama tienen tanto la dirección origen como la destino la de dos ruteadores, no de una estación de trabajo o una mini computadora. También note que el datagrama encapsulado (IPV4)no viaja todo el camino hacia el destinatario, el ruteador derecho recupera el mensaje original IPV6 y envía el mensaje a la mini computadora.

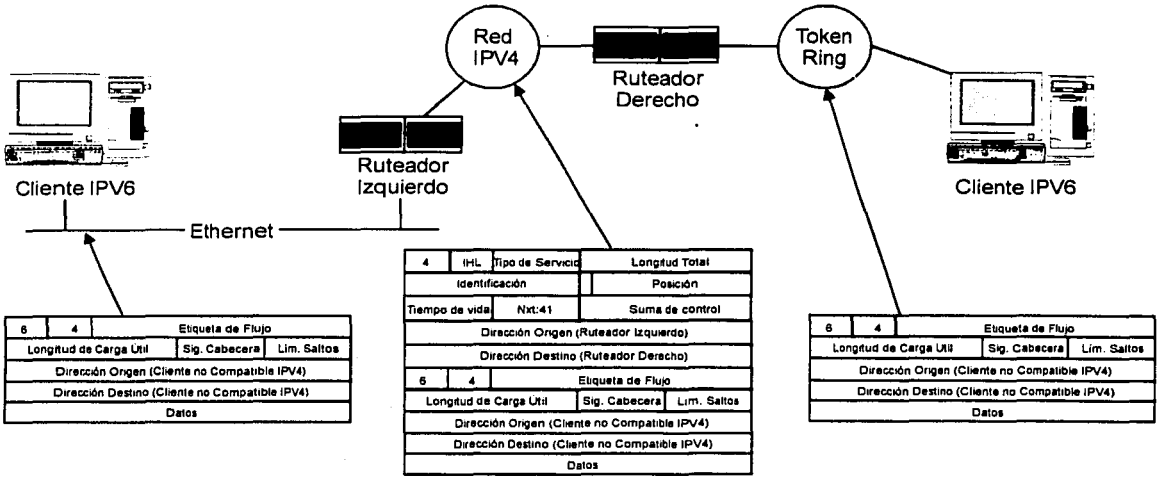


Fig. 4.7 Túnel Configurado para atravesar una red IPV4.

4.5.3.3 TRADUCCIÓN DE ENCABEZADOS

En algún punto durante la migración, los administradores pueden querer eliminar IPV4 de sus redes. Esa estrategia será practicada después de que la mayoría de los sistemas tengan soporte para IPV6, pero incluso en esta etapa quedarán algunos sistemas que solamente entienden IPV4, para comunicarse con esos sistemas se requiere una traducción de encabezados.

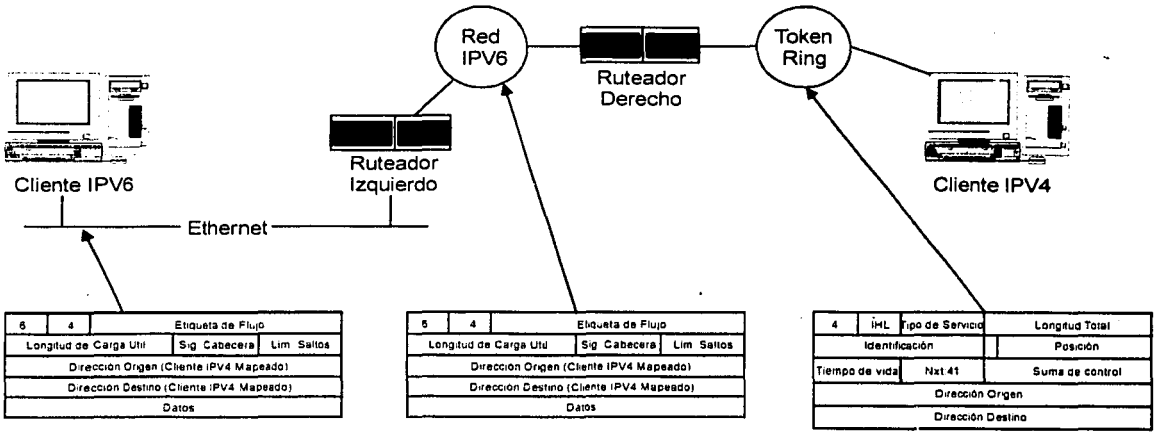


Figura 4.8 Ruteador que convierte datagramas IPV6 a datagramas IPV4.

La figura 4.8 muestra la traducción de encabezados en acción. El mensaje IPV6 viaja casi todo el camino hacia el destino, pero el destinatario no entiende IPV6 y no puede completar el proceso. Para que la computadora pueda enviar un mensaje que pueda entender el destino el ruteador derecho lo acepta y lo convierte en uno de formato IPV4. La traducción de encabezados utiliza direcciones IPV4 mapeadas, note que el ruteador de la derecha quita completamente el encabezado IPV6 del datagrama y lo reemplaza con un encabezado IPV4 equivalente. Cuando la mini computadora responda a este mensaje, el ruteador derecho tiene que realizar el proceso inverso de esta traducción convirtiendo un mensaje IPV4 a IPV6.

4.5.4 PASOS A SEGUIR PARA UNA CORRECTA MIGRACIÓN.

- Actualizar el servidor DNS para que manejen direcciones IPV6.
- Introducir una pila doble en los sistemas para que soporten tanto IPV4 como IPV6.
- Agregar direcciones IPV6 a los registros DNS de esos sistemas.
- Implementar túneles que conecten las redes IPV6 con las redes IPV4.
- Remover el soporte IPV4 de estos sistemas.
- Confiar en la traducción de encabezados para que alcancen los sistemas que solo soportan IPV4.

4.6 RED DE CÓMPUTO DEL INSTITUTO DE ASTRONOMÍA DE LA UNAM

4.6.1 ANTECEDENTES HISTÓRICOS E IMPORTANCIA DE LA RED DE CÓMPUTO.

El desarrollo de la astronomía en México se ha beneficiado significativamente con la utilización de computadoras, estaciones de trabajo y supercomputadoras, así como con las grandes bondades con que se cuenta al tener una red local con acceso a Internet. El Instituto de Astronomía actualmente cuenta con dos unidades foráneas: Ensenada (Baja California Norte) y Morelia (Michoacán); y una en el Distrito Federal, dentro de las instalaciones de la UNAM. Además se cuenta con dos observatorios, el Observatorio Astronómico Nacional (San Pedro Mártir, Baja California Norte) y el observatorio de Tonantzintla (Puebla), que durante muchos años fue el principal Observatorio de América Latina. Los observatorios y los centros de investigación cuentan con acceso a Internet; este medio es utilizado por los investigadores para intercambiar ideas e información con diversos colaboradores.

Los antecedentes históricos recientes de la red de cómputo en el **Instituto de Astronomía de la UNAM (IAUNAM)** los podemos ubicar a finales de la década de los 80. Fue entre 1987 y 1989 cuando se dieron los pasos finales para lograr la conexión del Instituto a la red de la **National Science Fundation (NSF)**. Finalmente, a mediados de 1989 y con la participación de un gran número de personas tanto del IA como de otras dependencias de la UNAM, así corno del gobierno, se logró el primer enlace entre el Instituto y la NSFNet en Boulder Colorado. A partir de este suceso tan notable para la investigación astronómica y del Internet en México, ha ido creciendo el uso e importancia de las redes de cómputo globales, no solo a nivel académico y de investigación, sino en todas las actividades de la vida cotidiana.

A principios de la década pasada se construyó la red de cómputo local para el Instituto en Ciudad Universitaria. Esta red interconectaba a todas las computadoras mediante la tecnología *Token Ring* y más adelante con la tecnología *Ethernet* a través de cable coaxial y repetidores. Con esta red era posible que desde el escritorio de cada investigador se tuviese acceso a todos los servicios que la nueva red ofrecía: compartir información entre la comunidad local y remota en forma rápida y segura, intercambio de mensajes, uso de equipo

de cómputo de otros centros de investigación de forma remota, compartir otros recursos como impresoras, unidades de respaldo, procesamiento, etc.

Posteriormente, a principios de 1997 se hizo una reestructuración de la red local, la cual comprendió cambios en el cableado y equipo de comunicaciones. Se migró a cable UTP y la interconexión a través de *concentradores* y un *switch* central. Esta red ha permanecido operando satisfactoriamente conjuntamente con la red del edificio nuevo del IAUNAM ubicado en Ciudad Universitaria, instalada en 1998.

4.6.2 DESCRIPCIÓN DE LA RED DE CÓMPUTO DEL IAUNAM ANTES DE LA MIGRACIÓN HACIA IPV6

En el IAUNAM, sede ciudad universitaria, se tiene un gran número de computadoras, dentro de los sistemas operativos utilizados tenemos que las estaciones de trabajo usan *Solaris 2.x.* En cuanto a las computadoras personales con *Linux,* utilizan una versión llamada *RedHat 7.x.* Las *PC's* con *Windows* usan alguna de las versiones *98, 2OOO ó XP,* aproximadamente 65 estaciones de trabajo con sistema operativo *Unix,* unas 60 *computadoras personales (PC's)* con sistema operativo *Linux* y alrededor de 110 *PC's* con sistema operativo *Windows,* destinándose los sistemas *Unix / Linux* para las tareas astronómicas principalmente y los sistemas *Windows* para actividades administrativas y algunas otras como elaboración de carteles y presentaciones, debido a sus facilidades para estas otras tareas. De este equipo de cómputo, algunos son de uso público y otros de uso privado, a los de uso público todos los usuarios de la red pueden accesar a ellos sin restricciones y los privados normalmente son equipos para uso de los investigadores y de su grupo de trabajo. Se tienen 5 estaciones de trabajo que realizan las principales tareas de servidores de aplicaciones de red, además de destinarse al uso público.

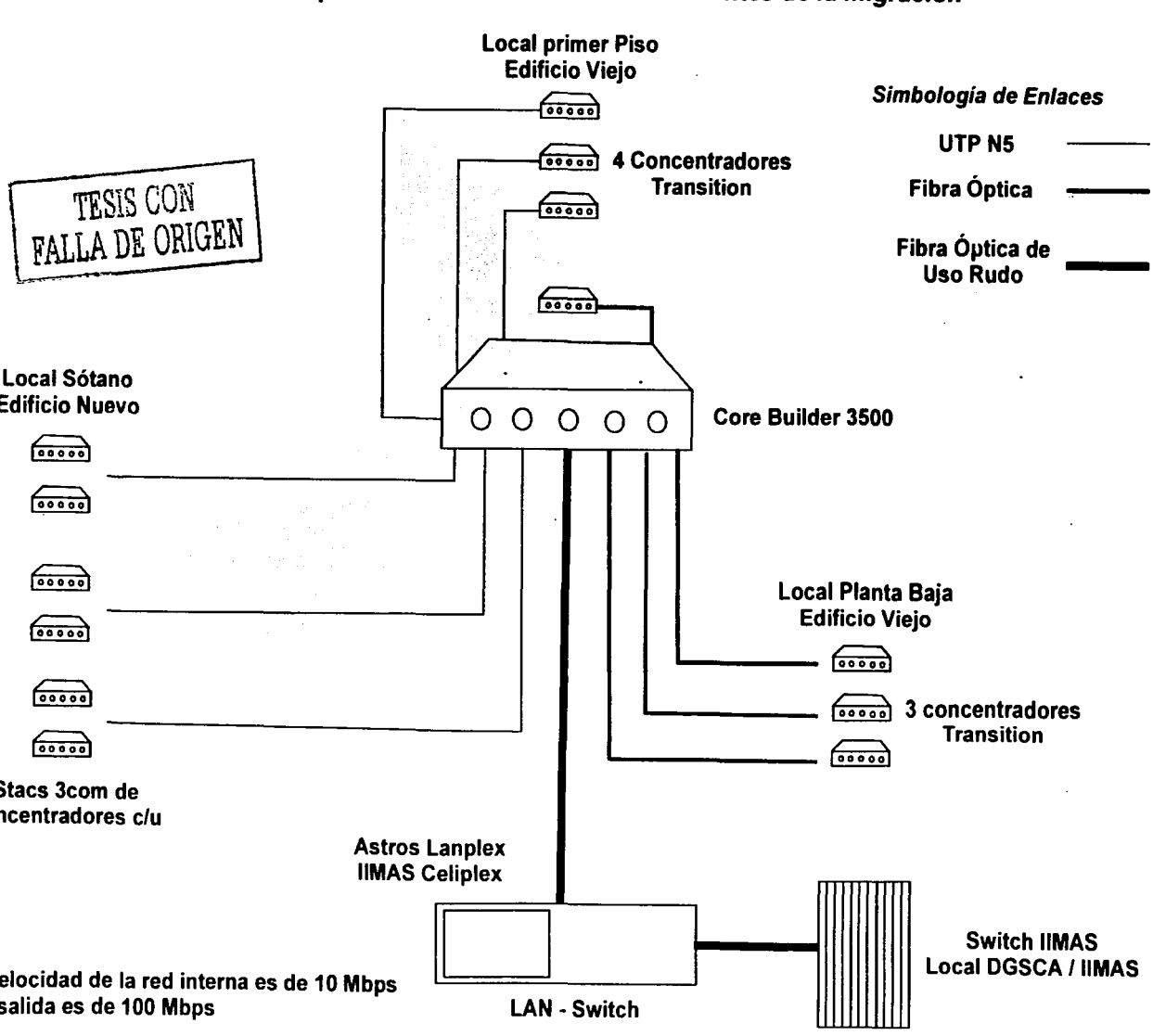
La red del IA es de clase C, que soporta hasta *255* direcciones, en donde dos de las direcciones ya están ocupadas (gateway y broadcast). La red del IA se ubica dentro de los segmentos 132.248.1 y 132.248.230.

En lo relativo a la infraestructura de equipo base de la red y cableado, el IAUNAM - CU actualmente cuenta con una red *Ethernet UTP* a 10 *Mbps* y 10 *concentradores* interconectados a un *switch* central en topología *estrella*. Este esquema ha funcionado satisfactoriamente debido a su robustez y confiabilidad, teniéndose servicio de red en todos los cubículos y oficinas del Instituto. Esta red interconecta a los 2 edificios en una sola red y a su vez se tiene conexión con el resto de las dependencias e institutos a través de *RedUNAM* como se muestra en la figura 4.9

4.6.3 PROPUESTA DE ADECUACIÓN DE LA RED DE CÓMPUTO DEL IAUNAM.

Del análisis previo, observamos que el esquema actual de la red es bueno. Sin embargo, hacen falta algunas adecuaciones en los principales factores con el fin de mejorar su desempeño.

Para este tipo de red, donde se maneja un gran número de computadoras, aplicaciones y usuarios, se hace necesaria una buena administración de los recursos, con el fin de lograr un punto óptimo entre la inversión y el aprovechamiento. El esquema centralizado tiene más ventajas que desventajas en este tipo de redes. Algunas ventajas tienen que ver con una mejor administración de los recursos, mayor uniformidad de la red en cuanto a sistemas operativos y aplicaciones, y una actualización del software instalado. Una de las desventajas es por ejemplo el depender de un servidor central para toda la red en ciertas aplicaciones. Esta se puede aliviar en forma relativamente sencilla, instalando un servidor de respaldo, el cual sirve a su vez para repartir la carga de trabajo del principal, con



"Migración hacia IPV6 de la Red de Cómputo del Instituto de Astronomía de la UNAM"
Capítulo IV: "Migración de Protocolos"
Figura 4.9. Red del Instituto de Astronomía de la UNAM antes de la migración.

Figura 4.9. Red del Instituto de Astronomía de la UNAM antes de la migración.

lo que se elimina la otra desventaja que es el trafico excesivo hacia un solo punto. Cabe mencionar que estos servidores deben ser lo suficientemente robustos para soportar estos requerimientos.

Bajo este esquema centralizado, es necesario además el contar con una buena infraestructura de red. Debido a que existen puntos estratégicos, es necesario proveerlos de enlaces de alta velocidad para que cumplan de forma exitosa sus tareas. Para este punto es necesario adecuar los enlaces y puertos de la red.

Esta actualización consiste básicamente en adecuar la red en el equipo de comunicaciones: *concentradores, switches, enlaces, tarjetas de red,* etc., a fin de contar con una red local más rápida y aprovechar de una mejor manera estos recursos. En este punto se observan algunos cuellos de botella, principalmente en los servidores y en las computadoras viejas.

La importancia de tener una buena infraestructura de red es que es ésta la base para el buen funcionamiento de la misma. Tradicionalmente se han empleado equipos "pasivos" de red como son repetidores y concentradores, los cuales en su momento realizaron un buen trabajo de acuerdo a los requerimientos pasados. Sin embargo, hoy en día la importancia de tener todos los servicios y aplicaciones en red hacen que la demanda de recursos crezca notablemente. Es por eso que el empleo de sistemas de conmutación se vuelve más popular cada día. Esta conmutación se logra empleando dispositivos más "inteligentes", capaces de manejar mejor el tráfico de una red local, estos equipos se les conoce como *"switches",* los cuales están tendiendo a reemplazar a los concentradores debido a esta mejoría en el manejo del tráfico y a su precio muy competitivo. Estos dispositivos manejan velocidades de acceso grandes, ya sea de 100 *Mbps, 150 Mbps o* 1000 *Mbps,* aumentando en al menos 10 veces las velocidades de acceso de la red actual. En un esquema ideal, se recomienda cambiar todos los concentradores por switches. Para esta red, donde el tráfico se da entre ciertas computadoras más que entre otras, es posible reemplazar únicamente esos concentradores, los cuales representan aproximadamente la mitad de los que están operando actualmente.

En lo relativo al cableado de la red, este esta diseñado para soportar velocidades de hasta 100 *Mbps,* por lo que es necesario establecer algunos enlaces a 1000 *Mbps* en la red local. En lo que respecta a la implantación de esta propuesta, considero que entre los pocos factores que podrían demorar su puesta en operación esta el económico, y no es tan grave debido a que ya se cuenta con una buena infraestructura de red y equipamiento, faltando solo las adecuaciones que ya no requieren de una gran inversión. Los factores técnicos y humanos no serian un obstáculo ya que se cuenta con el personal adecuado para llevar esta reestructuración y los elementos tecnológicos están bien probados y estandarizados.

Desarrollar un esquema de reestructuración de la red del Instituto de Astronomía para soportar cualquier aplicación de Internet o Internet 2, utilizando las tecnologías Fast-ethernet y Gigabit-ethernet, así como establecer un estándar de los sistemas operativos y de los programas que se instalaran en las computadoras. Esto brindará al usuario una gran transparencia al utilizar los recursos de la red. Los equipos de cómputo que requieren 100 Mbps utilizaran ci cableado que existe; para los que requieren 1000 Mbps se instalará fibra óptica.

Se recomienda cambiar todos los equipos de comunicaciones por conmutadores nivel 2 (10/100 Mbps) y nivel 3 (100 Mbps y 1000 Mbps). Estos elementos son inteligentes debido a que aíslan el trafico innecesario y disminuyen significativamente la tasa de errores. El desarrollo de esta propuesta permitirá' ofrecer a los usuarios seguridad, disponibilidad, estabilidad y escalabilidad permanentemente.

Es de vital importancia seleccionar un sistema operativo que ofrezca ser estable, soportar el protocolo IPV6, multiusuario, validar los accesos sin importar la plataforma, compartir la información hacia ci usuario transparentemente y soportar programas que aumenten la seguridad. Los programas que cumplen estas características y más son Linux, Windows 2000, Windows XP y Solaris. Todos estos sistemas operativos cuentan con una interfaz de usuario suficientemente amigable, por lo cual resultan fáciles de instalarse, así como de administrar

4.6.4 RED DE CÓMPUTO DESPUÉS DE LA MIGRACIÓN PROPUESTA

Después de varios meses de trabajo, un equipo de profesionales en cómputo del Instituto de Astronomía ha podido realizar la propuesta de migración de la red de cómputo de dicho Instituto aquí presentada obteniendo los resultados esperados en cuanto ala velocidad de transmisión y recepción de información, la nueva forma de asignación de direcciones IP, la estandarización de los sistemas operativos de la red y sobre todo la funcionalidad y transparencia hacia el usuario de ésta red.

Después de lo anterior la red ha quedado instalada físicamente como se muestra en la figura 4.10.

Cave mencionar que toda la red del IA, después de la migración tiene una velocidad de transferencia de 100 Mbps y cuenta con cuatro puntos a 1 Gbps.

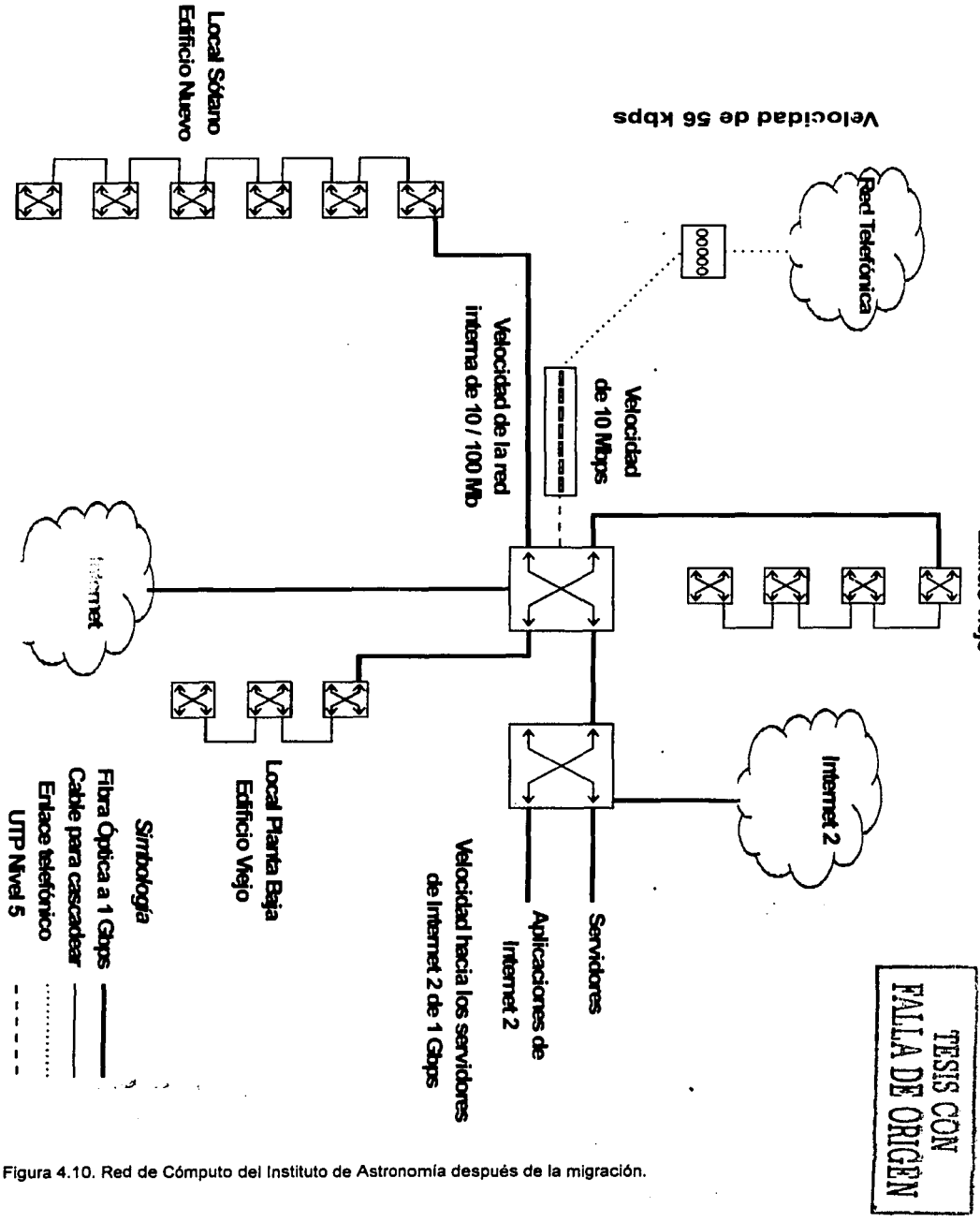


Figura 4.10. Red de Cómputo del Instituto de Astronomía después de la migración.

Capitulo V

"Aplicaciones"

5.1 BIBLIOTECA DIGITAL.

A la fecha de la realización de esta tesis me encontré con que hay muchas deficiencias en el sistema de bibliotecas de nuestra casa de estudios, de entre ellos puedo mencionar: Los catálogos no están actualizados, no hay suficiente cantidad de los libros, los libros existentes no contienen los temas de actualidad, no todas las bibliotecas tienen la misma cantidad de libros, los catálogos electrónicos tampoco están vigentes, etc., por todo esto creo que una posible solución sería la creación de bibliotecas digitales.

Una biblioteca digital podría ofrecer la soluciona todos estos problemas, no necesariamente significa que se reemplacen las bibliotecas tradicionales, pero esta nueva opción tiene un gran potencial al igual que la gente que descubre el mundo de Internet a diario, por ello la cantidad de personas que la utilizaran es cada día mayor.

La principal ventaja de esta propuesta radica en que cualquier persona que se encuentre conectada a la red, podrá acceder a la información que necesita y si no le es suficiente, reducirá el tiempo de búsqueda de algún tema.

También considero que sería una gran oportunidad que incluso se encontrara una sección dedicada a las tesis además de otra que contenga ensayos o trabajos realizados por los alumnos para que sirvan de consulta a las nuevas generaciones.

Las principales ventajas hablando técnicamente se encuentran precisamente en las diferencias entre las características de la versión actual del protocolo IP y su sucesor.

Las bibliotecas electrónicas pueden ofrecerse a través de una gran base de datos indexada que ofrecerá la información tradicional a cerca de las obras de que consta, pero además puede ofrecer un breve resumen del contenido de cada capitulo, así como los índices temáticos y alfabéticos, multimedios y toda la información relacionada con la obra en cuestión.

Una base de datos con las características mencionadas deberá estar implementada en varios servidores e incluso algunos de espejo, hablamos de una gran cantidad de máquinas que participarían en este proyecto y es por ello que se necesitará una gran capacidad de direccionamiento IP como la de 128 bits que aporta IPV6 para que no se vea afectado el sistema actual que es utilizado en la red de cómputo UNAM que sólo soporta 32 bits.

Otra de solución que aporta esta nueva versión del protocolo IP para la implementación de bibliotecas digitales es el ancho de banda, IPV6 cuenta con un ancho de banda (300 Kbps) mucho mayor al actual (56 Kbps) para la transmisión de video. Con esta capacidad será posible que nuestra biblioteca también ofrezca todos los servicios multimedia que actualmente acompañan a la mayoría de títulos publicados, ya sean audio, video y texto; brindando así una posibilidad extraordinaria para que un mayor número de alumnos se beneficien, ya que en el sistema actual de bibliotecas solo un alumno por cada titulo puede tener acceso al mismo tiempo a la herramienta multimedia que acompañe al libro en cuestión.

Todavía existe una mejora de mayor relevancia de este nuevo sistema bibliotecario aquí propuesto en comparación con el sistema tradicional. Propongo que utilizando las nuevas tecnologías y grandes capacidades de almacenamiento, no sólo se pueda consultar los datos bibliográficos de un libro es particular, sino que también se cuente con el índice temático y alfabético, así como un breve resumen de cada capitulo de la obra. Con esto se puede ahorrar muchísimo tiempo de búsqueda de información y sobre todo se acabaría el problema de que se agotara un libro que contiene un tema en particular, ya que se tendría al alcance de un clic los resúmenes de todas las obras de las que dispone la biblioteca.

Por otro lado, considero que seria de gran provecho para los estudiantes actuales y las generaciones futuras, la existencia de una sala virtual de tesis que contuviera todas las tesis en formato PDF que puede ahorrar mucho espacio de almacenamiento. La publicación de estas tesis serviría como material de consulta, ya que áreas como ingeniería, medicina, humanidades, etc, existe un sin fin de conocimientos que permanecen vigentes al paso del tiempo.

Por ultimo, la biblioteca que aquí se propone, deberá contar el servicio de cuartos de charla donde los alumnos puedan comentar la información que solicitan; así como la ayuda mutua entre ellos para la recomendación de textos u otros medios de información, con la finalidad de que sean ellos mismos los que recomienden la adquisición de obras de un tema en particular, si las traducciones de un idioma diferente al español se realizaron en forma correcta, etc. Bien utilizado puede ser el medio mas efectivo para la comunicación entre las autoridades bibliotecarias y los usuarios.

5.2 GENERACIÓN DE DOCUMENTACIÓN HIPERMEDIA EN INTERNET A PARTIR DE INFORMACIÓN MULTIMEDIA EN BASES DE DATOS

El término HIPERMEDIA, combinación de los conceptos HIPERtexto y multiMEDIA, hace referencia a una tecnología de construcción de (hiper)documentos que permite a la audiencia de los mismos encontrar fácilmente la información que realmente necesitan, a través de hiper-enlaces establecidos entre los diferentes elementos de información multimedia (texto, sonido, imagen fija, imagen en movimiento) que conforman los documentos. La aparición del entorno WEB en el ámbito de Internet ha permitido que se pueda publicar y acceder a documentación hipermedia de forma extraordinariamente sencilla y con un costo muy reducido, mediante la utilización de servidores Web para almacenar los documentos publicados, y navegadores para acceder a su contenido multimedia: mediante la visualización de texto e imágenes, la audición de sonidos y la reproducción de vídeo; y para facilitar la navegación entre documentos a través de hiper-enlaces.

Los documentos puestos a disposición de los usuarios de la red normalmente no forman parte de bases de datos en el sentido estricto del término, sino que se suelen distribuir en forma de páginas Web registradas en archivos independientes almacenados en servidores de información, conteniendo estas páginas los enlaces que, con la ayuda de un navegador, permitan que un usuario navegue de un documento a otro, aun cuando estos documentos estén situados en diferentes computadores comunicados a través de la red.

Cuando una persona u organización desea ofrecer un volumen importante de documentación a los usuarios a través de Internet, se plantean algunos problemas cuya resolución dependerá de si se va a adoptar un enfoque tradicional, basado en un sistema de archivos (páginas Web), o un enfoque fundamentado en la utilización de un sistema de gestión de base de datos. Estos problemas son los siguientes:

- **La gestión del almacenamiento de los documentos.** Se refiere a la forma de organizar la información en los soportes físicos de acceso directo (normalmente, discos magnéticos) para almacenar de forma óptima los documentos. Hacerlo mediante archivos sin más estructura que la permitida por el Sistema Operativo, basada en directorios o carpetas, cuando su volumen es muy grande no parece ser lo más adecuado, si se tiene en cuenta la existencia de Sistemas de Gestión de Bases de Datos, especialmente creados para facilitar el registro y la recuperación de grandes cantidades de información con un costo de mantenimiento reducido.
- **La implementación de los hiper-enlaces entre documentos.** Frente al segundo problema, se puede adoptar simplemente la implementación de los enlaces en el interior de los documentos o complementarlo con las posibilidades que ofrec¤ la gestión de índices que incorpora cualquier Gestor de Bases de Datos.
- **El mantenimiento de la documentación**. El mantenimiento de la información que se va a poner a disposición de los usuarios de la red es un importante problema a considerar, ya que actualizar grandes volúmenes de información supondrá un esfuerzo considerable si ésta se almacena directamente a nivel de presentación, es decir, en forma de páginas Web incluidas en archivos y codificadas mediante un lenguaje de marcado como HTML. Es más eficaz adoptar una estructura de la información en forma de base de datos, relacional u orientada a objetos, que, en principio, no considere la forma en que el usuario visualizará tal información (como páginas Web).
- **El mantenimiento de los hiper-enlaces**. En cuanto al mantenimiento de los hiper-enlaces, si se utilizan las facilidades de gestión de índices de un Sistema de Bases de Datos, el propio mantenimiento de la información implicará la actualización automática de los índices de acceso a documentos relacionados.
- **La seguridad de la información**. Frente al problema de la seguridad, es necesario considerar dos aspectos: la seguridad en la información documental almacenada y la

seguridad en la información que se transmite por la red. Si se utiliza un Sistema de Gestión de Bases de Datos, la seguridad del almacenamiento, en cuanto al proceso de transacciones y a la integridad referencial, la garantiza el propio gestor de la base de datos. La seguridad en la red se puede solucionar con el empleo adicional de unas claves públicas entre el software de acceso a la base de datos en el servidor Web y el navegador.

5.2.1 GENERACIÓN DE PÁGINAS WEB VIRTUALES

Como se ha indicado en el apartado anterior, el almacenamiento de la información que contienen los documentos en una Base de Datos puede ofrecer ventajas frente a su almacenamiento en forma de archivos que contienen cada uno de ellos una página Web. Como Sistema de Base de Datos se puede adoptar uno de tipo relacional, el más ampliamente utilizado en la actualidad, aunque el futuro apunta hacia los denominados Sistemas Orientados a Objetos como los más eficientes para gestionar datos de muy diferente naturaleza, como es el caso de los datos multimedia. No obstante, muchos sistemas relacionales permiten utilizar campos BLOBs (Binary Large OBjects) en las Bases de Datos Relacionales para registrar información de tipo multimedia, como sonidos o imágenes.

Para la generación de páginas Web de forma dinámica a partir de la información almacenada en una base de datos, además del programa gestor de dicha base de datos, normalmente comercial, es necesario disponer de otro programa que atienda las peticiones que realizan los usuarios vía Internet y construya, en tiempo real, la página Web "virtual" correspondiente, tomando de la base de datos la información necesaria. Para independizar este segundo programa del gestor comercial de la Base de Datos utilizado, se puede añadir un componente software intermedio, o interfaz, que normalice las relaciones entre ambos programas, de tal forma que si se cambia de gestor de base de datos (por ejemplo, Oracle por Informix, Informix por Microsoft SQL Server, etc.), no sea necesario introducir cambios en el programa que accede a la base de datos para construir páginas Web. En el ámbito de los

Computadores Personales (PCs) la interfaz de este tipo más utilizada es la conocida como ODBC (Open Data Base Conectivity).

Dentro de la estructura de los componentes necesarios para la generación de páginas Web virtuales debe existir una página Web "real", almacenada en el servidor Web en forma de archivo ".htm" con formato HTML. Esta página normalmente será la denominada "default.htm", que es la que se muestra por defecto cuando un usuario accede mediante un navegador a una dirección de "sitio" Web en Internet sin especificar un nombre de página: por ejemplo, es equivalente acceder a la dirección www.unam.mx que a www.unam.mx/default.htm.

La página Web mostrada es de presentación, ofreciendo al usuario el acceso a otras páginas que no existen como tales en el servidor, sino que serán creadas en tiempo real con la información de la Base de Datos. Para ello, los enlaces en la página de presentación no hacen referencia a archivos HTML, sino a un programa que al ejecutarse origina la ejecución de la aplicación que crea dinámicamente la página virtual correspondiente. De esta forma, en lugar de incluir un hiper-enlace del tipo:

<A HREF="Nombre archivo que contiene página Web">
(Por ejemplo: <A HREF="pagina.htm">)

se utilizaría otro que originase la ejecución del programa de creación de la página:

<A HREF="Nombre del programa">
(Por ejemplo: <A HREF="programa.exe">)

También hay que considerar un componente denominado "Interfaz CGI" (Common Gateway Interface); se trata de un programa que permite relacionar aplicaciones desarrolladas en un determinado lenguaje de programación (por ejemplo, C++, Java, etc.) con el mundo Web. Además de esta interfaz que comunica la aplicación encargada de crear las páginas virtuales con Internet, también debe existir otra interfaz que permita su relación con el mundo de las Bases de Datos. Esta interfaz puede ser, como se ha mencionado anteriormente, ODBC, que incluye, como puede apreciarse en la figura, un Drive Manager,

programa encargado seleccionar el controlador (driver[1]) adecuado en función del Sistema Operativo (Windows, LInux, etc.) y del Sistema de Gestión de Base de Datos utilizados.

5.2.2 APLICACIÓN PRÁCTICA

En el Departamento de Ciencias de la Computación de la Universidad de Alcalá se ha llevado a cabo un proyecto piloto para comprobar este método de generación de documentación hipermedia en Internet. Para ello, se ha creado una Base de Datos Relacional, utilizando la herramienta comercial Microsoft SQL Server, con información multimedia sobre los más famosos pintores españoles. En esta base, además de textos, se han incluido fotografías de calidad de sus principales cuadros, explicaciones audibles en forma de sonido digitalizado sobre autores y cuadros, música de la época, y vídeo digital.

Se han creado únicamente dos páginas Web "reales" en fomato HTML, ambas de presentación, con el mismo contenido, aunque una de ellas en español y la otra en inglés. En la página de presentación existen hiper-enlaces, a través de una interfaz CGI, con la aplicación que crea las páginas Web virtuales accediendo a la base de datos mediante órdenes SQL, siendo esto transparente al usuario, y mostrándole su contenido (imágenes, texto, etc.) como si de páginas Web se tratara; páginas que se destruyen cada vez que se solicita una nueva consulta, aunque mediante su navegador, el usuario puede examinar su código HTML y almacenarlas en su computador para su propio uso.

5.3 PROCEDIMIENTO GENERAL PARA EL DESARROLLO DE SISTEMAS DE INFORMACION

Para el desarrollo de este sistema propongo que se siga el procedimiento general para el desarrollo de sistemas de información en cual consta de 7 etapas como se muestra en la figura 5.2:

[1] Un driver, en este contexto, es el programa que procesa todas las órdenes de acceso a la base de datos, normalmente expresadas en un lenguaje de consulta denominado SQL (Structured Query Lenguage), y las convierte en comandos que pueda "entender" el Gestor de la Base de Datos utilizada.

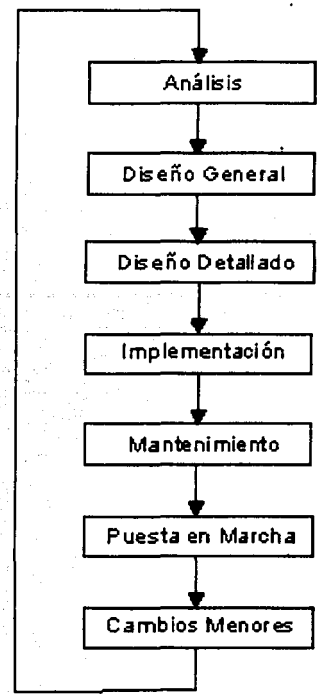


Fig. 5.2 Procedimiento General para el desarrollo de sistemas de información.

Las etapas de este procedimiento se describen a continuación:

- **Análisis.** Involucra la recopilación de datos que pertenezcan a la empresa, incluyen la evaluación del equipo con el que se cuenta y la selección de proveedores en caso de ser necesario.
- **Diseño General.** Se diseñaran mas de dos formas para el manejo del sistema indicando brevemente las características de cada diseño para la posterior selección del diseño que cubra las necesidades de la empresa.
- **Diseño Detallado.** Una vez seleccionado el diseño del sistema se desarrollara cada uno de los puntos indicados en el diseño general.
- **Implementación.** Una vez concluido el diseño detallado se empezara la instalación de cada uno de los puntos de forma independiente, realizando las pruebas de manejo que involucran cada una de las partes.

- **Puesta en Marcha.** Se ira dando de alta cada uno de los puntos que involucran al sistema tomando en cuenta que cada uno de ellos funcione adecuadamente hasta lograr el manejo total del sistema de información.
- **Mantenimiento.** Lo proporciona el grupo de analistas y consistirá en verificar la calidad de la información así como también determinar si el sistema cumple los objetivos para el cual fue diseñado.
- **Cambios Mayores.** Si se detecta que el sistema no cumple con los objetivos será necesario hacer una revisión del sistema y si es necesario volver nuevamente a la etapa de Análisis.

5.4 APLICACIÓN DEL PROCEDIMIENTO GENERAL PARA DESARROLLO DE SISTEMAS DE INFORMACIÓN.

Para poder utilizar éste procedimiento hay que adecuarlo a las características específicas del sistema que queremos desarrollar, por otra parte, se debe tener en cuenta que la duración de las etapas para la creación de este sistema dependerá casi al cien por ciento de las personas que estén colaborando en este proyecto, por tal razón, la duración de cada una es simplemente una estimación del tiempo que considero seria el óptimo para que se cumplan en su totalidad las metas propias de cada etapa, en base a todo lo anterior, las etapas quedarían de la siguiente forma:

Etapa	
Análisis	En esta etapa hay que realizar un estudio minucioso para poder identificar las fuentes de información que alimentarán nuestro sistema, se debe considerar que actualmente en la UNAM ya existen catálogos electrónicos en la mayoría de sus bibliotecas –no con las características que aquí se proponen-. Conjuntamente se debe considerar las características del equipo que vamos a utilizar y de ser necesario, actualizar o adquirir nuevo equipo, primordialmente dispositivos de almacenamiento (Discos duros SCSI) que puedan conectarse entre si de tal modo que formen un arreglo

	que pueda satisfacer la demanda del sistema, considerando que para cada Título existente en nuestro catálogo; se debe destinar un espacio mínimo de 5 Mb para un archivo en formato PDF que contendrá la información relacionada con la obra en cuestión. así como la elección de las herramientas de software (Plataforma operativa y Lenguaje de Programación, Herramientas Multimedia) que nos permitan la creación de este sistema.
Diseño General	Es aquí donde se realiza el bosquejo del sistema, se debe indicar el funcionamiento de cada uno de sus componentes. Normalmente se deben crear dos o mas propuestas para posteriormente realizar la mejor elección de entre ellas.
Diseño Detallado	Se deben evaluar todos los diseños propuestos en base a su relación costo – beneficio en todos los ámbitos como son: tecnológico, económico, social, etc., es ésta posiblemente la etapa más importante de este procedimiento ya que de aquí en adelante se va a trabajar únicamente con lo que se ha estudiado y determinado en base a cada componente (sub sistema).
Implementación.	Se debe crear por separado cada uno de los componentes del sistema y realizarle las pruebas necesarias para poder afirmar que cumple con los objetivos para los que fue diseñado, por tal razón, esta es la etapa que más tiempo demorará.
Puesta en Marcha	Se deberán realizar las ultimas pruebas a cada componente para verificar su correcto funcionamier.to y calidad, incorporándolos en un solo sistema hasta lograr que todos los componentes funciones en plenitud como un solo ente. Es importante mencionara que para este proyecto en particular, estas pruebas se pueden realizar en una Intranet antes de liberarlos al público en general por medio de Internet. Una vez que todas las evaluaciones han sido satisfactorias en sistema puede ser puesta a disposición de los usuarios.
Mantenimiento	Esta etapa en particular y la siguiente no debe preocuparnos en demasía por el momento, ya que como se mencionó, la realizan los analistas en base a deficiencias (bugs) detectadas por parte de los usuarios. Aunque

	esto no quiere decir que deba pasar mucho tiempo para realizar las correcciones pertinentes, como ejemplo tenemos el sistema operativo Windows XP de Microsoft, que a las pocas horas de haber salido este producto al mercado, salió un parche (patch o service pack) para cubrir un problema detectado en su seguridad.
Cambios Mayores	Esta es la etapa que completa el ciclo de vida de todo sistema de información, si se llega hasta esta etapa es porque será necesario hacer un nuevo análisis detallado del diseño actual para que cubra las nuevas necesidades o las deficiencias del sistema, si es posible, esta correcciones se realizarán sobre la versión vigente, de no ser posible, de deberá remontar hacia la primera etapa para la creación de un nuevo sistema.

Así pues, después de haber revisado éste procedimiento, llego a la conclusión de que es difícil pero muy viable la creación de un sistema con las características mencionadas.

Es de vital importancia que en la etapa del análisis se haga una revisión minuciosa de las características físicas del equipo (hardware), primordialmente en lo referente a la red de cómputo, ya ésta es la parte medular del equipo requerido para el desarrollo y funcionamiento del sistema. De lo anterior y los demás resultados que arroja la primera etapa de este procedimiento se pueden deducir algunos de los que serán los requerimientos básicos, de entre ellos se puede mencionar que los equipo de cómputo que serán servidores de estas aplicaciones deberán' contar con las siguientes características mínimas; alta velocidad en ducto (bus) de 200 Mbps, memoria RAM de 512 Mb, tarjetas de red de alta velocidad (100 Mbps o 1 Gbps), tarjetas graficas 3D con 64 Megas, puertos ultra-wide SCSI, cache de 512 Kb y un procesador de 500 MHz. Con esta arquitectura se evitaran cuellos de botella y se disminuirá la latencia en estos equipos además de ofrecer una alta estabilidad de los equipos. Para el manejo de grandes volúmenes de información, lo más recomendable es tener un sistema inicial que pueda ir creciendo conforme las necesidades así lo demanden. Existen dispositivos con capacidad de manejar muchos discos duros en arreglos lógicos, como el modelo **A5000 y A1OOOO** de *Sun Microsystems,* con capacidad de almacenamiento de varios cientos de Gigabytes, dando además de mayor capacidad, una mayor velocidad de acceso. Con un esquema de este tipo, se lograría una mejor

organización de los archivos en los espacios públicos al tenerlos en un solo sitio, así como una mayor facilidad para realizar respaldos y un mejor tráfico en la red.

Para hacer de éste un proyecto más integral hacia la comunidad universitaria, propongo que sea desarrollado por jóvenes estudiantes de la Carrera de Ingeniería en Computación dirigidos por un grupo de personal de nuestra casa de estudios, de esta forma, los alumnos podrían compartir sus habilidades y participar en la creación de un proyecto que servirá a muchas generaciones posteriores a la que pertenecen, además, adquirirían nuevos conocimientos que les serán de gran utilidad en el mercado laboral, para motivarlos aun más, es posible que la UNAM les ofreciera la participación de este proyecto mediante la liberación del servicio social a cada alumno que quiera comprometerse.

De este modo se puede ahorrar la UNAM muchos recursos evitando pagar sueldos a personal que no labora ni pertenece a ésta institución, por otro lado, no será mucho personal el que se requerirá, por tal razón, no habrá descompensación del personal de otras áreas y/o proyectos.

Otro punto a mencicnar favorable para la creación de este sistema es que al igual que en el Instituto de Astronomía y demás Instituciones de la UNAM, actualmente ya se está trabajando con el sistema operativo Linux, es decir, propongo que la biblioteca que aquí menciono sea desarrollada para que sea utilizada bajo este sistema operativo que nos ofrece la gran ventaja mencionada con respecto a sus competidores: es libre. Con las características del protocolo IPV6 no se tendrían problemas de interoperabilidad o comunicaciones entre nuestros servidores y el resto de la red Internet o Internet 2.

CONCLUSIONES

El protocolo IP en su versión 4 es una gran herramienta en el complicado proceso de la comunicación entre equipos de cómputo dentro de una red de cómputo, debido a sus características como la fragmentación, el control de la suma de verificación y el sistema de encaminamiento o ruteo lo convirtieron en uno de los estándares mas utilizados a partir del final de la década de los setentas.

Con el desarrollo de nuevas tecnologías debido a la importancia que ha cobrado el área de las telecomunicaciones y el creciente mercado y progreso en el campo de la computación, las deficiencias de IPV4 han saltado a la vista. Desde su nacimiento, no contaba con un servicio confiable, por eso se dice que es orientado a no-conexión, por si sólo no es un protocolo que sea capaz de garantizar la entrega completamente satisfactoria de todos los paquetes que viajan por la red. Por otro lado, al no contar con asignación de prioridades se ha vuelto obsoleto ante las necesidades actuales, ya que en la actualidad no se puede realizar la correcta transmisión de video o audio que una videoconferencia necesita, además de que no se puede acceder a los medios de transmisión más modernos y eficientes que existen. El mayor problema de IPV4 en la actualidad es que no cuenta con capacidad de direccionamiento para subsistir por mucho mas tiempo, hay que considerar que cuando una máquina se conecta a la red, se le debe asignar una dirección IP, y con el crecimiento que ha mantenido Internet, éstas direcciones se están agotando, los treinta y dos bits con los que cuenta ésta versión, pronto no serán suficientes.

Por otro lado, la versión actual de IP, la 6, soluciona todas las problemáticas que se presentaban con la versión anterior, cuanta con un sustancial aumento en la capacidad de direccionamiento pues ahora cambia a 128 bits, ha perfeccionado la forma de enviar los paquetes ya que ha simplificado el formato del encabezado de cada uno de ellos; transmitiendo sólo las opciones que necesite. Además cuenta con un control de flujo y asignación de prioridades que permiten la correcta transmisión de multimedios sin que se presente algún desfasamiento entre las señales, la capacidad de auto configuración, el sistema de ruteo se ha mejorado, pero una de sus mayores cualidades es la seguridad, ya

que cuenta con una cabecera de extensión llamada "Cabecera de Autentificación" que permite que únicamente el destinatario pueda acceder a la información que fue transmitida.

No todo es bueno en IPV6, tiene un gran problema, y es que por el momento no es muy difundido entre todos los usuarios de equipos de cómputo, la mayoría ni siquiera ha oído de él. Otro gran conflicto, al menos en nuestro país, es que no contamos con la infraestructura de cómputo para adoptar este protocolo, ya que en la mayoría de las empresas se cuenta con equipos que necesitan una actualización en cuanto a su hardware y, por otro lado, cuentan con sistemas operativos tan viejos que no puede funcionar IPV6 de modo natural, por tal razón, habría que utilizar las técnicas de migración, pero eventualmente tendrá que ser reemplazada o actualizada toda ésta infraestructura.

Los sistemas operativos con los que cuenta la red de cómputo del Instituto de Astronomía de la UNAM están casi en su totalidad, salvo Windows 98, listos para trabajar en Internet 2 con el protocolo IPV6 de forma transparente sin tener necesidad de la utilización de alguna técnica de migración, caso contrario a Microsoft Windows 98, aquí se tiene que utilizar la técnica de Túnel para que pueda establecer comunicación con los demás equipos de la red y tener acceso a la red Internet 2.

Existen proyectos que desde su nacimiento son tan bien diseñados que prevalecen al paso del tiempo, incluso de décadas, este es el caso del Modelo de Referencia OSI, que es el estándar a seguir en cuanto a los protocolos, aún las versiones más innovadoras como IPV6 tienen su base en éste modelo.

Un caso similar a este es Internet, es similar porque también está vigente después de décadas de su nacimiento, pero en mi opinión su evolución y crecimiento no ha sido lo mejor, en sus orígenes estaba diseñado para aplicaciones militares y de investigación por parte de las más prestigiadas universidades de Estados Unidos, hoy en día se ha convertido en el más grande catálogo de productos comerciales, algunos tan banales y decadentes como la pornografía. Hoy, con Internet 2, se les brinda a todos los centros de investigación y universidades del mundo una nueva oportunidad de contar con tecnología de vanguardia para el ejercicio de sus actividades, para el intercambio de información científica y cultural,

como el acceso a ésta red es sólo permitido a dichas instituciones, espero que no permitan que se convierta en lo que hoy es Internet, porque hay que recordar que así comenzó todo.

Internet 2 podrá permitir que se difunda el conocimiento generado dentro de las universidades e institutos de investigación, no sólo del Distrito Federal o de México, el alcance así como la red misma es mundial, es por ello que países del llamado tercer mundo podrán tener acceso a información más novedosa.

En cuanto a las aplicaciones que puede tener IPV6 así como Internet 2 son tantas y seguramente con el tiempo surgirán nuevas necesidades de comunicación así como tecnologías que utilizarán éste protocolo como base de desarrollo. Por otro lado, en la aplicación que aquí propongo, considero que el método de generación de páginas Web "virtuales" descrito, ofrece ventajas evidentes que se han puesto de manifiesto en proyectos que se han desarrollado por todo el mundo, caso particular en las universidades de España. Como ventaja principal se puede destacar la facilidad del mantenimiento del gran volumen de información utilizada, al estructurarse en forma de base de datos, además de poder aprovechar todas las facilidades ofrecidas por los gestores de bases de datos comerciales en lo que se refiere a la seguridad de la información y a la integridad de los índices utilizados para implementar los hiper-enlaces de navegación. Confío en que la realización de este proyecto es viable y deseo que no pasen muchas generaciones de ingenieros en computación antes de tener esta valiosa e importante herramienta para el mejor desempeño de los alumnos de esta carrera.

La migración que sufrió la red tiene como objetivo resolver los problemas significativos que se tienen en los servicios que ofrecen los servidores y robustecer la plataforma de comunicaciones para contar con anchos de banda dedicados (10 Mbps, 100 Mbps y 1 Gbps). Estas velocidades y anchos de banda permitirán correr cualquier tipo de información (voz, datos, video y multimedia) y contar con una alta confiabilidad y disponibilidad de la red. También se mencionan los requerimientos mínimos que se necesitan para funcionar en Internet 2 y no tener cuellos de botella local. Todas las configuraciones de software permitirán poder tener un acceso a la red desde cualquier plataforma de manera transparente y segura, ofreciendo al usuario una configuración estándar en la utilización del equipo y de los programas. El acceso remoto para el personal del IA es ya una necesidad,

por lo cual las configuraciones que se dieron permitirán al usuario acceder a la red del IA de una manera sencilla y directa, evitando la saturación que se presenta al hacerlo vía DGSCA.

Con la implementación de todo lo anterior, el usuario ganará una amplia variedad de servicios, disponibilidad y seguridad en la red del IA. Así mismo los administradores ganaran una mayor facilidad y eficiencia en la administración de la red.

Así, mi principal aportación en este complejo proyecto fue la instalación y configuración de todos los equipos de cómputo que conforman la red del Instituto de Astronomía de la UNAM para que puedan intercomunicarse utilizando el protocolo IPV6 de forma transparente al usuario, así como el acceso a la red Internet 2. Además de una extensa documentación de éstos procesos y redes, presento una propuesta de una aplicación pensada en la red Internet 2, dicha aplicación consiste en la creación de una biblioteca virtual con características mucho más allá de las que actualmente operan tanto dentro de nuestra casa de estudios como en el Internet en general.

BIBLIOGRAFÍA

- "Redes de área local y su interconexión".
  Manuel Esteve Domingo, Juan Carlos Guerra Cebollada, Carlos Palau Salvador
  Universidad Politécnica de Valencia
  Valencia, España, 1998

- "Computer Telephony Integration".
  William A. Yarberry, Jr.
  CRC Press LLL
  Florida, Estados Unidos, 2000

- "El libro de las comunicaciones del PC. Técnica, Programación y Aplicaciones".
  José A. Caballar
  RA-MA
  Madrid, España, 1996

- "IP Applications with ATM"
  John Amoss, Ph.D. and Daniel Minoli
  McGraw Hill
  Estados Unidos, 1998

- "Redes Globales de Información con Internet y TCP / IP. Principios Básicos, Protocolos y Arquitecturas".
  Douglas E. Comer
  Prentice may
  México, 1996

- "Utilizando Linux 2ª Edición".
  Jack Tackett Jr., David Gunter
  Prentice Hall
  México, 1996

- "Windows 2000 Server".
  David Garza Marin, Hugo Jiménez Perez
  Prentice Hall
  México, 2000

- "Aprendiendo TCP/IP en 14 días 2ª Edición".
  Timothy Parker, Ph.D.
  Prentice Hall – Hispanoamericana
  México, 1997

- "Linux, recursos para el usuario".
  James Mohr
  Prentice Hall
  México, 1998

- "Strategic Database Technology: Management for the Year 2000".
  Simon, A.R.
  Morgan Kaufmann Publishers, 1995.

- "Redes para proceso distribuido. Área local, arquitecturas, rendimiento, banda ancha".
  Jesús García Tomás, Santiago Ferrando Girón, Mario Piattin Velthuis
  RA-MA
  Madrid, 1997

- "Solaris 7 performance administration tools"
  Frank Cervone, H.
  Mc Graww – Hill
  Nueva York, Estados Unidos, 2000

- "Internet 2000"
  Marco Antonio Tiznado Santana
  Mc Graw – Hill
  Bogotá, Colombia, 1999

- "The Internet Book: Everithing you need to know about computer networking and how the internet works"
  Douglas Comer
  Prentice Hall 1995
  Nueva Yersey, estados Unidos, 1995

- "Internet: Manual de referencia: Una información completa, ideal para todo usuario de Internet"
  Harley Haha
  Mc Graw – Hill
  España 1994

- "Big Book of IPV6 Addressing RFC'S"
  Peter H. Salus
  Morgan Kaufmann
  California, Estados Unidos, 2000

- "TCP/IP and related protocols"
  Uyless Black
  Mc Graw – Hill
  Nueva York, Estados Unidos, 1992

- "Redes ATM"
  Luis Guijarro Coloma
  RA-MA
  Madrid, España, 2000

- "Linux Complete: Linux documentation proyect"
  Grant Taylor
  Sybex
  San Francisco, Estados Unidos, 1999

- "Linux Edición Especial"
  Jack Tackett
  Prentice Hall Hispanoamericana
  México 1996

- "TCP/IP"
  Gary Govanus
  Sybex
  California, Estados Unidos, 1999

- "Windows 2000 complete"
  Ehlen Arumary
  Sybex
  San Francisco, Estados Unidos, 2000

- "Windows 2000 Server: Instalación configuración y administración"
  José Luis Raya
  RA-MA
  Madrid, España, 2000

- "Windows 98 Avanzado"
  José Luis Raya Cabrera
  Alfaomega
  Distrito Federal, México, 1999

- "TCP/IP Protocol Suite"
  Behrouz A. Forouzan
  Mc Graw Hill
  Estados Unidos, 2000

- "TCP/IP" (Clearly Explained)"
  Pete Loshin
  Morgan Kaufmann
  3ª Edición, Estados Unidos, 1999

- "IP Fundamentals"
  Thomas A. Maufer
  Prentice Hall
  Nueva Jersey, Estados Unidos, 1999

URL:

- http:://www.ipv6.unam.mx
- http://www.dgsca.unam.mx
- http://www.redhat.es
- http://www.redhat.com
- http://www.itesm.com.mx
- http://www.ucm.es/info/multidoc/multidoc/revista
- http://www4.uji.es/~al019803/Tcpip.htm
- http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
- http://www.cybercursos.net/tcp-ip.htm
- http://www.bestars.ua.es/asignaturas/rc/trabajos/ip/indice2.html
- http://usuarios.tripod.es/vteforte/ip.html
- http://ttt.upv.es/rmartin/TcpIp/cap02s03.html
- http://ttt.aaa.upv.es/~ferboiar/ip.html
- http://www.3com.com
- http://www.internet2.edu.mx

g

- ftp.rediris.es/docs/rfc/17xx/1752

- ftp.rediris.es/docs/rfc/7xx/791
- http://ttt.aaa.upv.es/~ferboiar/nukes.html
- http://www.microsoft.com
- http://www.ietf.org/html.charters/ipngwg-charter.html .
- http://www.ietf.org/html.charters/ngtrans-charter.html
- http://ttt.aaa.upv.es/rmartin/Tcpip/cap02s02.html
- http://argo.es/~jcea/proyecto/indice.html
- http://www.isc.org/bind.html
- http://www.visc.vt.edu/ipv6/doc/dns.html
- ftp://ds.internic.net/rfc/rfc1897.txt
- http://www.ipv6.org/.
- http://www.opengroup.com
- http://www.6bone.net
- http://www.ipv6.com/.
- http://www.playground.sun.com/ipng/
- http://www.itojun.org/v6/v6faq.html

- http://www.baquia.com/
- http://cs-ipv6.lancs.ac.uk/ipv6/systems/linux/faq/linux-ipv6.faq.html
- http://www.idg.es/pcworld
- http://www.monografias.com
- http://www4.uji.es/~al019803/tcpip.htm
- http://usuarios.tripoid.es/vteforte/transporte.htm
- http://www.sun.com/solaris/ipv6
- http://win6.goto.info.waseda.ac.jp/index.html
- http://www.ipv6.itesm.mx/ligas
- http://www.cis.ohio-state.edu/cs/Services/rfc/rfc.html
- http://www.ucm.es