8
1 ej.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

Paginación Diversa

"INTERNET: LA RED DE REDES ENFOCADA DESDE TCP/IP SUS PROTOCOLOS DE COMUNICACION"

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A :

PEDRO CASTILLO GRANADOS

ASESOR: ING. JUAN GASTALDI PEREZ

México 1998

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

Dedicado con mucho cariño y respeto

A mis padres:

Sr. José C. Castillo Durán

Sra. Isaura Granados Vázquez

Como un testimonio de eterno agradecimiento al apoyo, amor, comprensión y abnegación que siempre en forma incondicional me han brindado, y que ahora me permiten culminar una de mis grandes metas.

Que Dios los bendiga siempre

Y a todas aquellas personas que de una forma directa o indirecta contribuyeron para hacer realidad este trabajo.

ÍNDICE

página

Página

página

INTRODUCCIÓN

Cuando un lector pretende conocer qué es Internet y cómo trabaja, generalmente lo hace investigando a partir de la bibliografía disponible, encontrandose por un lado principalmente con libros que le explican los servicios, recursos y beneficios que se pueden obtener al utilizar esta red. Se menciona en estos libros que Internet es una enorme red de redes de computadoras que cubre varias decenas de países y que da servicio a millones de usuarios, y qué, para lograr que las miles de redes que la componen interactuen, hace uso de dos elementos primordiales. Uno de estos elementos es la infraestructura de comunicaciones establecida en base a los ruteadores que hacen las veces de una interface física, y que permite el enlace de todas las redes y el otro elemento es un conjunto de protocolos que actuan como una interface lógica que permite que todas las redes se puedan comunicar mediante un lenguaje común. Este conjunto de protocolos es identificado con el nombre genérico de TCP/IP, pero tales libros no explican su operación dentro de Internet.

Por otro lado cuando se revisa la bibliografía referente a TCP/IP el lector se encuentra con libros que hablan de temas demasiados técnicos y que presuponen un cierto conocimiento de redes de computadoras de tecnologías, estándares, etc., es decir, están enfocados a un auditorio especializado como pueden ser los administradores y diseñadores de redes. Estos libros usualmente muestran como implementar una red usando la familia de protocolos TCP/IP y mencionan a Internet como un ejemplo clásico, pero igualmente no explican de forma explícita su uso dentro de esta red.

Como se puede ver se adolece de información que explique cómo están implementados estos protocolos dentro de la red de computadoras más grande del mundo, y como consecuencia evita que lector curioso conozca como trabaja Internet.

Esta situación motivo la realización del presente trabajo, y con el cual se pretende investigar y hacer una aportarcion que auxilie al lector a conocer cómo trabaja Internet para poder dar los servicios y recursos que gozan millones de usuarios a través de todo el mundo.

Este estudio de Internet se enfoca por lo tanto desde la familia de protocolos TCP/IP, es decir, se analiza el porque del uso de estos protocolos, la interacción que existe entre ellos y su relación con el hardware de red para dar como resultado la super carretera de la información.

Se pretende ofrecer una información equilibrada que fusione tanto el aspecto teórico como técnico, que ayude a tener una idea clara de lo que es Internet y a partir de esta idea obtener los máximos beneficios para el usuario.

El presente trabajo está dividido en cuatro capítulos, al definir a Internet como una red de redes, se hace necesario explicar los conceptos relacionados con éstas, tales como los diferentes tipos que existen, los elementos que las componen, las diferentes topologias que utilizan, así como los servicios que ofrecen a los usuarios finales. Todos estos aspectos son explicados dentro del Capitulo I, el cual también tiene como finalidad sentar las bases de conocimiento para los capítulos siguientes.

El Capitulo II describe la historia evolutiva de Internet, este capitulo se presenta con el fin de mostrar al lector qué es Internet, cuales fueron los motivos que provocaron su surgimiento, y su gran desarrollo a través de sus casi tres décadas. Este capitulo muestra con detalle como Internet es el producto de una serie de esfuerzos cooperativos por parte de diferentes entidades, las cuales van desde las instituciones militares, la comunidad cientifica y académica hasta llegar a la organizaciones comerciales. Se describe como Internet fue y ha sido su propio generador de nuevas ideas, experimentos, pruebas , etc., culminando en servicios y productos que en un inicio sirvieron para satisfacer las necesidades de comunicación interna de sus diseñadores, y finalmente con el paso del tiempo han sido ofrecidas al usuario final.

Así mismo, este capitulo nos muestra la evolución y robustecimiento de los protocolos TCP/IP como un producto de la necesidad de soportar y acomodar el crecimiento explosivo que ha manifestado la red.

El Capitulo III constituye la parte medular de este trabajo, en el cual se presenta como están implementados los protocolos TCP/IP dentro de Internet, se muestra como este importante conjunto de protocolos son los responsables de que redes de computadoras de diferentes tecnologías y plataformas se puedan comunicar permitiendo la conectividad universal. En este capitulo se manifiesta con mayor notoriedad la interacción de los diversos protocolos, ya que para llevar a cabo las tareas de comunicación de la red, los sistemas complejos de comunicación requieren subdividir los problemas y delegárselos a un protocolo en particular.

Con el fin de tener una perspectiva más amplia y facilitar al lector el entendimiento del papel de TCP/IP dentro de Internet, en este capitulo se explican tópicos como la conmutación de paquetes en una red, la estratificación de los protocolos, asi como una repaso a la tecnología Ethernet.

Además, se tratan en detalle los aspectos de direccionamiento y enrutamiento de la información dentro de Internet y su interacción con los dispositivos de hardware tales como los ruteadoes y las computadoras receptoras de la información , pero siempre vistos desde el enfoque de los protocolos encargados de llevar a cabo estás tareas.

El capitulo IV hace mención de los principales servicios que ofrece una red implementada con la familia de protocolos TCP/IP como es el caso de Internet, haciendo especial enfasis que estos servicios están soportados también por protocolos.

Existen una gran variedad de servicios disponibles a los usuarios de Internet y cada día aparecen más, lo cual deja de manifiesto el poder de la tecnología. En este capitulo no se pretende describir todos los servicios que existen, ya que cómo se menciona al inicio de esta introducción existen varios libros dedicados exclusivamente para tal propósito, y éste no es fin del presente trabajo. Más bien lo que se quiere mostrar en este capitulo son las aplicaciones o servicios típicos que una red con TCP/IP ofrece a sus usuarios, describiendo la situación particular en la cual cada uno de ellos es utilizado, pero además de esto, mostrar cómo funcionan internamente y que relación tienen con los demás protocolos.

De esta manera se describen los protocolos Telnet, el Protocolo de Transferencia de Archivos (FTP), y el Protocolo Simple de Transferencia de Correo (SMTP), así mismo dentro de este capitulo se mencionan a grandes rasgos algunos servicios adicionales con el fin de mostrar las herramientas que tiene a su disposición el usuario para explorar y explotar la red de redes.

El apéndice A ofrece al lector una lista con direcciones electrónicas de interés dentro de Internet, que le permitirán introducirse, conocer y circular de una manera más fácil dentro de Internet.

Cómo cualquier área del saber humano que integra su propio lenguaje y terminología, Internet posee una gran cantidad de términos, abreviaturas, siglas y acrónimos; que en ocasiones son difíciles de recordar, es por eso que se incluye en el apéndice B un glosario para auxiliar al lector en la interpretación de los mismos.

CAPITULO I

INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

1.1 INTRODUCCIÓN

Internet también conocida como "La Red", "La Red de Redes", o "La Madre de Todas Las Redes"; entre otros términos, involucra en todos estos nombres un factor común la palabra "RED" . ¿Pero qué es una red de computadoras?, ¿Qué elementos la conforman?, ¿Cómo funcionan?. Son todas estas preguntas las que dan motivo para presentar un capitulo introductorio a las redes de computadoras, presentando los conceptos y términos fundamentales que las rigen.

No se pretende agotar el tema, sino, presentar un panorama general pero no por esto somero o parcial de los conceptos básicos, así como sentar las bases o antecedentes de conocimiento para los capítulos subsiguientes.

Este capitulo aborda lo relativo a una red de computadoras desde su definición, tipos existentes, los elementos que las conforman desde el punto de vista de hardware (elementos físicos) y software (elementos lógicos, como programas), un análisis de los medios de transmisión (cables) que se utilizan, así como las diferentes formas de enlazar los nodos situación que da origen al termino de topología de redes.

Este capitulo también habla sobre los protocolos estándares establecidos, así como su implementacion en los diversos productos comerciales que existen en el mercado. Y por último presenta una panorámica del campo de aplicación, en cuanto a los servicios y beneficios que una red proporciona a los usuarios finales.

1.2 QUE ES UNA RED DE COMPUTADORAS ?

Una red de computadoras es un conjunto coordinado de elementos de hardware (tales como computadoras, terminales, cables, etc.) y elementos de software (sistemas operativos de red, programas de administración, seguridad, etc.) que interconectan computadoras aisladas y que tienen como finalidad compartir recursos (como discos duros, impresoras, CD Rom, etc.) proporcionar servicios (como correo electrónico, actividades de cómputo en grupos de trabajo) así como transferir e intercambiar información.

1.3 TIPOS DE REDES DE COMPUTADORAS

Una forma de clasificar a las redes de computadoras es de acuerdo al área geográfica que cubren derivándose las siguientes:

1.3.1 REDES LAN

Las redes LAN (Local Area Network-Red de Área Local) por lo general son aquellas redes que operan en un departamento, edificio o compañía, es decir, funcionan en una área geográficamente limitada. A través del presente capitulo se verán diversas características de este tipo de redes ya que actualmente son las más utilizadas en el mundo y dan pauta a la creación de las redes WAN (Wide Area Network-Red de Área Amplia).

1.3.1.1 REDES INALÁMBRICAS

Dentro del contexto de las redes locales existen las redes inalámbricas estas constituyen una tecnología relativamente nueva en cuanto a la interconexión de computadoras tomando como medio físico de transmisión el aire.

Para su operación se basan principalmente en dos tecnologías: Ondas de radio o espectro distribuido (en el rango de UHF y microondas) y luz infrarroja.

La forma física en que se colocan los nodos de la red para su comunicación en un sistema inalámbrico se denomina esquema lógico de transmisión y se emplean dos métodos fundamentalmente: en el primero; cada nodo se comunica con todos los demás.

En el segundo, existe un dispositivo central a través del cual se conectan todos los módulos. Una ventaja asociada al uso de un controlador central es la de poder incorporar sistemas de administración y control de acceso.

Estas redes se caracterizan en que a mayor velocidad de transmisión de la información menor área de cobertura de la señal y viceversa. Algunos ejemplos son:

- " El sistema Wavelan de NCR opera a una velocidad de 2 Mbps (Megabits por segundo) con un alcance máximo de alrededor de 300 mts.
- ARLAN de Telesystems trabaja a 1.3 Mbps con una área de cobertura de 400 mts.
- FREEPORT de Windata tiene una velocidad de 5.7 Mbps y 85 mts de alcance" [1]

1.3.2 REDES MAN (Metropolitan Area Network-Red de Área Metropolitana)

Este tipo de redes hacen una cobertura de áreas geográficas mayores a 5 kms. y máximo el área geográfica de una ciudad , aunque el termino "Metropolitana" se utiliza en forma genérico para describir áreas hasta del tamaño de una ciudad; también pueden referirse a instalaciones grandes multiedificios (como universidades).

Este tipo de redes además de la transmisión de datos respaldan la transmisión de voz e imágenes de video.

1.3.3 REDES WAN (Wide Area Network-Red de Área Amplia)

Las redes de área amplia cubren grandes extensiones geográficas equivalentes a la conexión de puntos entre estados, países o continentes; para lograr dicha conexión se apoyan en dispositivos que permiten su conectividad usando líneas telefónicas, servicios públicos de transmisión de datos o enlaces satelitales. Cuando se menciono lo referente a una red de área local, se hacia alusión de que tales redes marcaban la pauta para la creación de las redes WAN, ya que en la medida que las redes locales van creciendo en tamaño y complejidad, y conforme las instituciones van confiando en estas redes labores cada día más criticas surge la necesidad de comunicarlas entre si, en ciudades o paises distantes.

[1] Oropesa Talavera Enrique.Personal Computing México,Las Redes Inalámbricas; una opción más.Junio 1994, pags. 76-77

1.4 ELEMENTOS QUE CONFORMAN UNA RED

Como se estableció en la definición de una red, éstas se conforman tanto por elementos de hardware como por elementos de software, algunos de estos elementos son comunes para los diversos tipos de redes mencionados con anterioridad, pero también existen elementos específicos para algunas de ellas.

A continuación en este apartado se verán los principales elementos que conforman a una red ya se LAN, MAN, WAN, etc., y donde una red determinada puede incluir algunos o todos estos elementos dependiendo su tamaño y propósito.

1.4.1 COMPUTADORA CENTRAL O SERVIDOR

En ciertos ambientes de trabajo la computadora central también denominada servidor es el elemento más importante, ya que al ser la computadora más poderosa en la red en cuanto a velocidad de procesamiento, capacidad de almacenamiento entre otras cosas; sirve o comparte sus recursos con las demás computadoras denominadas terminales, estaciones de trabajo o clientes

1.4.2 TARJETAS DE INTERFASE O ADAPTADORES DE RED

Para poder enlazar los nodos y establecer una red, se requiere de un enlace físico que nos permita conectar una computadora con otra a través de cables en las redes alambradas o a través del aire para las redes inalámbricas. Los elementos que nos permiten tal enlace son las tarjetas de interfase o adaptadores de red, típicamente son tarjetas electrónicas que se deslizan dentro de alguna ranura de expansión de la computadora , servidor o impresora (como se puede ver también las impresoras pueden ser un nodo mas de la red), estas tarjetas proveen un conector hacia el exterior adecuado al tipo de cable que se va a utilizar, también cabe hacer mención que existen ciertas computadoras que en su tarjeta principal o madre ya traen incorporados estos dispositivos salvando una valiosa ranura de expansión.

Las tarjetas de interface poseen la electrónica necesaria para establecer la comunicación entre los diversos nodos de la red, empaquetando los datos y transmitiéndolos a cierta velocidad y cumpliendo ciertas características de envío a través del medio físico (cable o aire).

1.4.3 CABLEADO

Es el elemento principal o vertebral de un sistema de red, ya que es a través de este medio que se transporta la información de un nodo a otro. No cualquier cable sirve para alambrar una red, es decir, éste debe cumplir con ciertos requisitos o características que lo hagan propio para ser utilizado para una red, inclusive existen ciertos estándares que determinan que tipo de cables son los apropiados, mas adelante en este capitulo se verán con más detalle las características de estos elementos.

1.4.4 ESTACIONES DE TRABAJO

Por lo general son las computadoras con menor poder de computo que accesan los recursos del servidor y en algunos casos ayudan al procesamiento de la información.

1.4.5 PUENTES

A medida que el numero de nodos en una red aumenta, implica que el tráfico de información en la red también aumentará, llegando al grado que la transferencia se vuelva lenta e ineficiente.

Una forma de solucionar este problema es utilizando un dispositivo denominado "Puente" (Bridge). Las redes que presentan una sobrecarga por lo general son divididas en pequeños segmentos para asegurar un mejor control del tráfico y son enlazados por medio del puente, es decir, los segmentos se convierten en una red lógica.

Los puentes hacen uso de tablas de direcciones de destino que son capturadas manualmente, aunque ya existen ciertos puentes inteligentes que construyen sus propias tablas a partir de la configuración de la red. Los puentes examinan la dirección de destino de los paquetes de información y permiten pasar solamente aquellos que están destinados para el segmento de la red que está del otro lado del puente.

Los puentes requieren de una mínima configuración y están mejor orientados hacia redes pequeñas y poco complejas.

1.4.6 HUBS/REPETIDORES

Como se verá más adelante existen diversas formas físicas de conectar los nodos de una red (topología), y para cumplir con tal propósito algunas configuraciones requieren de ciertos dispositivos como los hubs/repetidores. Se encuentran por lo general en la topología en estrella y sirven como un punto central de reunión para los cables de las computadoras, servidores y periféricos. Es posible que no agreguen nada a la transmisión (pasivos) o que el hub pueda ser un repetidor no inteligente, es decir, solamente resincroniza y reamplifica las señales. El hub también puede ofrecer inteligencia utilizando software, lo cual le permite administrar, monitorear y controlar el tráfico de la red.

1.4.7 RUTEADORES

Los ruteadores al igual que los puentes, también enlazan dos o más segmentos de red separados físicamente, pero para el caso de los ruteadores los segmentos permanecen lógicamente separados, y pueden funcionar (y de hecho lo hacen) como redes independientes.

Los ruteadores tiene acceso a un mayor nivel de conocimiento de la red, en comparación con el que está disponible a los puentes. Información del nodo fuente, nodo destino, distancia de las rutas, y en algunos casos, el status del segmento; están contenidos en las tablas de los ruteadores. Con este conocimiento, los ruteadores pueden ejecutar funciones avanzadas tales como calcular la distancia más corta entre los nodos fuente y destino.

Los ruteadores son generalmente más costosos que los puentes y se requiere de experiencia en su manejo. Están mejor orientados para redes corporativas grandes, redes WAN; donde el tráfico debe ser segmentado y aislado basado principalmente en un protocolo.

1.4.8 COMPUERTAS (GATEWAYS)

Son dispositivos altamente complejos usados para enlazar dos o más redes con diferentes arquitecturas (protocolos) de comunicación, es decir, realizan la conversión y

traducción entre protocolos diferentes para que dos redes heterogéneas se puedan comunicar. Por ejemplo, una compuerta podría proveer conversión y traducción entre el protocolo utilizado por una LAN de computadoras personales y una computadora maiframe IBM.

1.4.9 MODEMS

Un dispositivo fundamental en la comunicación de dos computadoras a través de líneas telefónicas es el módem. Debido a que las computadoras trabajan con señales digitales (0 y 1) y las líneas telefónicas con señales analógicas (señales continuas) se presenta un incompatibilidad entre ellos, la cual es solucionada con el uso de un módem.

La palabra módem es un termino corto para modulación/demodulación. Un módem provee la interface entre los mundos analógico y digital, así como la capacidad de transmitir de un dispositivo digital a través de un canal analógico para que sea recibido por otro dispositivo digital. En otras palabras la computadora transmisora pasa los datos en forma binaria a su módem el cual mediante una señal de diferente frecuencia denominada portadora le modifica ya sea su amplitud, frecuencia o fase, y transporta la señal a la computadora receptora, la cual a su vez tiene conectado otro módem que recibe la señal modulada y hace el proceso contrario, es decir, demodula la señal suprimiendo la portadora y finalmente pasa los datos en forma digital a la computadora receptora.

1.4.10 SISTEMAS OPERATIVOS DE RED

Si el cableado es un elemento primordial desde el punto de vista de hardware para una red, el Sistema Operativo de red lo es desde el punto de vista de software.

El Sistema Operativo es un programa de control y administración, la funcionalidad, la facilidad de uso, el rendimiento, la seguridad de los datos y la seguridad de acceso son funciones propias de él. Sin un Sistema Operativo de red, los componentes permanecerían aislados aunque físicamente estuvieran enlazados.

1.4.11 SOFTWARE ADICIONAL DE RED

Además del sistema operativo de red como un elemento de software, existen productos adicionales que permiten monitorear, auditar, controlar, e incrementar la seguridad de la red, entre otras funciones y que facilitan la tarea de administrar una red.

1.5 MEDIOS DE TRANSMISIÓN (CABLEADO)

Como se dijo anteriormente los cables que se utilizan para enlazar los nodos en una red deben poseer ciertas características para cumplir con su objetivo como es el de además de enlazar físicamente los dispositivos de la red, el de transmitir la información entre los nodos de una manera confiable. Existen tres tipos de cables que se utilizan principalmente en el establecimiento de una red: cable coaxial, cable par trenzado también denominado telefónico y el cable de fibra óptica.

Cada uno de ellos con características propias que los distinguen para ser tomados en cuenta en determinadas necesidades (ancho de banda, longitud máxima, susceptibilidad al ruido, etc.) a satisfacer.

Por otro lado también hay que tener en cuenta que todos los medios de transmisión tiene limitaciones en su capacidad de transmitir datos debido a factores como son el ruido, la atenuación, etc.

El ruido en una línea es un problema que es inherente a la línea en sí misma y no puede ser eliminado, resulta del movimiento constante y aleatorio de los electrones en el conductor y disminuye la capacidad del rango de frecuencias contenidas en el canal de transmisión (ancho de banda).

La atenuación se refiere a la perdida de potencia de una señal a medida que recorre cierta distancia en un canal dado, un método de incrementar la señal es colocando amplificadores en la línea.

A continuación se presentan las principales características de los tres cables mencionados arriba.

1.5.1 CABLE PAR TRENZADO O TELEFÓNICO

El cable par trenzado o telefónico se forma principalmente de dos alambres de cobre que se encuentran aislados por una cubierta plástica y trenzado uno contra el otro.

Es esta característica la que los distingue con el nombre de par trenzado o torcido. El par trenzado, a su vez, se encuentra cubierto por un capa aislante y protectora en su exterior denominada jacket.

Los alambres se trenzan con el fin de aumentar la inmunidad al ruido, provocado por otras fuentes eléctricas o fenómenos naturales (como motores, relampagos,etc). La proximidad tan cercana que existe entre el canal que lleva la señal y el canal de referencia a tierra provoca que cualquier interferencia causada por diversas fuentes sea captada por ambos alambres, y por lo tanto, el efecto en la señal se reduzca. Además si múltiples pares son incluidos dentro del mismo cable, el trenzado de cada par dentro del cable reduce los efectos de la interferencia entre canales adyacentes fenómeno conocido como crosstalk.

El cable par trenzado está disponible en dos variedades blindado (STP-Shielded Twisted Pair) y sin blindaje (UTP-Unshielded Twisted Pair). El par trenzado sin blindaje es similar al cable usado por los sistemas telefónicos de allí el por que también se le llama cable telefónico, es económico, flexible, fácil de instalar y permite manipular una señal a una distancia máxima de 110 mts. sin el uso de amplificadores[2]

El cable par trenzado sin blindaje está disponible en tres categorías:

Categoría 3	soporta	10		Mhz
Categoría 4	soporta	16	a	25 Mhz
Categoría 5	soporta	100		Mhz

Los cables conductores más gruesos y cubiertos por un jacket son denominados par trenzado blindado. Estos últimos son más costosos y menos flexibles que el par trenzado sin blindaje, pero permiten un rango de operación de hasta 500 mts.

En general el cable par trenzado viene en conjuntos de 2,3,4,6,12,16 y 25 pares de cables, sin embargo, para redes locales de tipo sin blindaje sólo se necesitan dos

[2] Ramirez Alejandro.RED, Cables para redes locales.1991, pags. 32-34

pares de cables para conectar cada nodo a la red. La figura 1.1 muestra un esquema del alambre par trenzado con y sin blindaje.

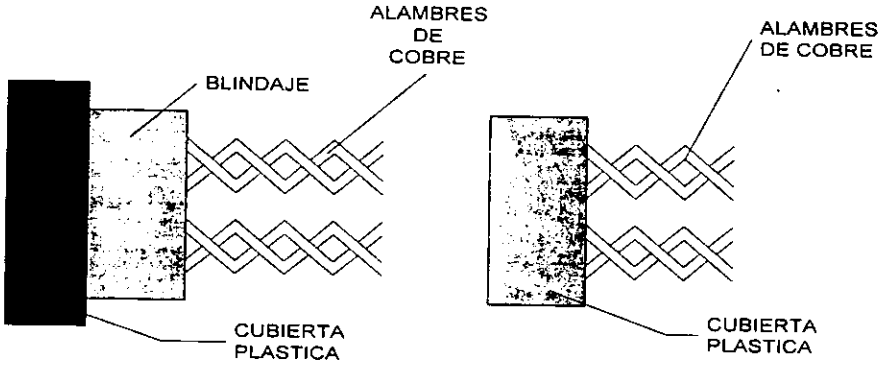


Figura 1.1 Esquema del cable par-trenzado con y sin blindaje

1.5.2 CABLE COAXIAL

El principal factor limitante de un cable de par trenzado es causado por un fenómeno conocido como el "efecto piel": a medida que la tasa de transferencia (y por lo tanto la frecuencia) de la señal transmitida se incrementa, la corriente circulante en los alambres tiende hacerlo únicamente en la superficie exterior del alambre, por lo tanto hace un menor uso de la sección transversal. Esto tiene el efecto de incrementar la resistencia eléctrica de los alambres para señales de frecuencias altas, lo cual causa una mayor atenuación de la señal transmitida. Además, a altas frecuencias, una cantidad creciente de potencia de la señal se pierde debido al efecto de radiación. Por tanto, para aquellas aplicaciones que demandan una tasa alta de transferencia, es normal usar otro tipo de medio de transmisión. Un tipo de línea de transmisión que minimiza ambos de estos efectos es el cable coaxial.

El cable coaxial se conforma de un alambre de cobre como conductor básico el cual es cubierto por un aislante plástico, a continuación sobre el aislante plástico se

coloca un conductor secundario que actúa como tierra y finalmente todo el conjunto está protegido por una cubierta exterior también aislante (figura 1.2).

Debido a sus dos capas de blindaje, el cable coaxial es relativamente inmune al ruido eléctrico, que pueden provocar motores, y puede ser tendido a grandes distancias sin degradación de su desempeño.

El cable coaxial existe en una variedad de tipos y tamaños. Pero para las redes locales se usan dos tamaños principalmente, denominados cable coaxial grueso y cable coaxial delgado. El cable coaxial tiene la característica de que a mayor grosor mayor distancia cubierta por una señal eléctrica, pero suele ser más caro y menos flexible. Hoy en día el cable coaxial delgado es el más común en el cableado de redes por su relación costo beneficio que es muy buena.

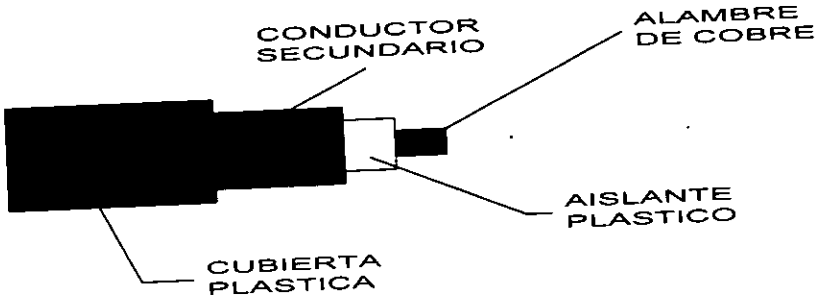


Figura 1.2 Esquema del cable coaxial

1.5.3 FIBRA ÓPTICA

Aunque la geometría del cable coaxial reduce significativamente los efectos de varios factores limitantes, la máxima frecuencia de la señal, y por lo tanto, la tasa de transmisión de información, que puede ser transmitida usando un conductor sólido (normalmente cobre), aunque muy alta, es limitada; este es el caso también para los cables de par trenzado.

Estos factores condujeron a la tercera tecnología de cables que se utilizan en las redes de área local, y que es la fibra óptica.

El uso de la fibra óptica se justifica para cubrir principalmente tres necesidades: para aquellos casos en donde las grandes distancias son un factor determinante para la implantación de una red, cuando se requieren tasas de transferencia de datos muy altas en el orden de cientos de megabits por segundo, y cuando el ruido o cualquier tipo de interferencia son factores a considerar.

El cable de fibra óptica se compone de una fibra muy delgada elaborada de dos tipos de vidrio con diferentes índices de refracción, uno para la parte interior y otro para la parte exterior. Esta diferencia en la refracción previene que la luz penetre en una parte de la fibra óptica hasta la parte exterior, evitando así la perdida de la información. La fibra óptica a su vez se encuentra cubierta por una placa aislante y protectora en la parte más exterior para darle mayor integridad estructural al cable (Figura 1.3). Transmite la información vía fotones o luz, puede propagar una señal sin necesidad de amplificadores a distancias de hasta 2000 mts., se puede transmitir voz, vídeo y datos por el mismo canal, no genera señales eléctricas o magnéticas, es inmune al ruido y tiene un ancho de banda de hasta 200 megabits por segundo. Sin embargo, el costo de instalación y mantenimiento de la fibra óptica permanece alto por estación de trabajo.

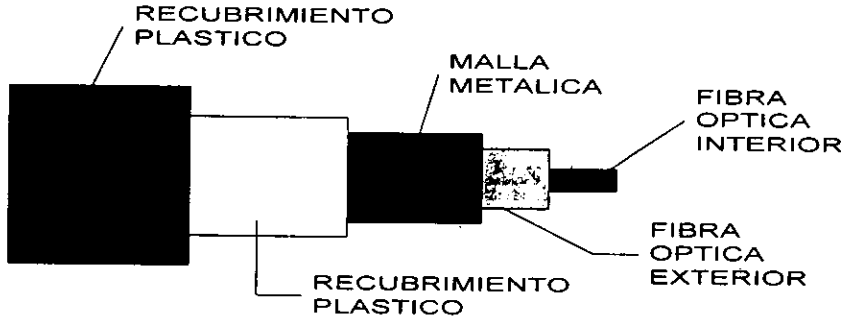


Figura 1.3 Esquema del cable de fibra óptica

1.6 TOPOLOGÍA DE REDES

Existen diversas formas de configurar físicamente los nodos en una red, hecho que da lugar al termino de topología de red. El termino topología es prestado de la

geometría, la cual se encarga de investigar la relación y posición relativa de las figuras geométricas. Esto aplicado a las redes de computadoras nos quiere dar a entender, que se pueden enlazar los nodos de una red de diversas formas dando como resultado que físicamente adquieran una "figura" o forma muy particular.
La topología que se seleccione va a depender de los métodos de acceso al medio (los cuales se verán en el siguiente apartado) y del tipo de cables que se instalaran. Además de los dos factores anteriores, el diseñador de una red debe considerar tres metas cuando pretenda establecer cierta topología:

- Proveer la máxima confiabilidad posible para asegurar una recepción apropiada de todo el tráfico (rutas alternas).

- Enrutar el tráfico a través de la ruta menos costosa dentro de la red (aunque dicha ruta no puede ser elegida si otros factores como la confiabilidad, son más importantes).

- Dar al usuario final la mejor respuesta posible en tiempo, especialmente en sesiones interactivas o por otro lado la transmisión de la máxima cantidad de datos en un periodo dado.

Cabe hacer notar que en redes pequeñas suele existir un tipo de topologia y en redes grandes que cubren una área física amplia pueden usar una combinación de ellas.

A continuación se presentan las topología más usuales:

1.6.1 TOPOLOGÍA EN BUS

Esta topología es muy popular al implementar una red de área local, ya que una característica distintiva de esta topología es su bajo costo de establecimiento. Es económico su establecimiento por que consiste de un cable continuo principal con terminadores en sus extremos, los cuales hacen la función de absorber la señal emitida por un nodo y no sea reflejada de regreso sobre el canal provocando interferencia.

Todos y cada uno de los nodos se enlazan directamente a este cable (Figura 1.4). La topología en bus presenta una desventaja, principalmente derivada del hecho que usualmente un sólo canal de comunicación existe para servir a todos los dispositivos en la red. Consecuentemente en el caso de una falla del canal, la red se perderá o como se dice comúnmente se caerá la red. Otro problema es la dificultad en detectar y aislar las fallas a cualquier componente en particular unido al bus. Este esquema de alambrado se denomina no estructurado, entendiéndose como un alambrado sin un punto de concentración, que nos permita monitorear la red para detectar fallas.

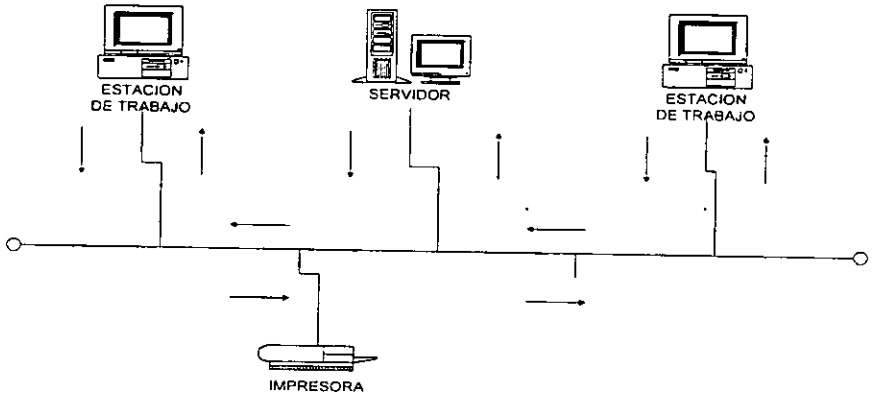


Figura 1.4 Topología en bus

1.6.2 TOPOLOGÍA EN ESTRELLA

En este tipo de topología los nodos van conectados a un dispositivo central (hub) como los rayos de las ruedas de una bicicleta (Figura 1.5).

Esta topología cuenta con un esquema de alambrado estructurado (punto de concentración central), y debido a que todo el tráfico de la red pasa a través del hub, éste puede desconectar un puerto si presenta una falla, reunir estadísticas, monitorear , entre otras cosas. En esta topología sin un nodo falla, usualmente no afectará a los demás nodos.

Las principales desventajas de esta topología son debidas a su centralización, ya que el hub al ser el responsable de enrutar el tráfico hacia los diferentes nodos de la red, provoca problemas de cuello de botella (la información no es distribuida por el hub con la misma velocidad que la recibe, provocando retrasos y por lo tanto una disminución en el desempeño de la red) y además si llega a fallar el hub traerá como consecuencia la caída de la red.

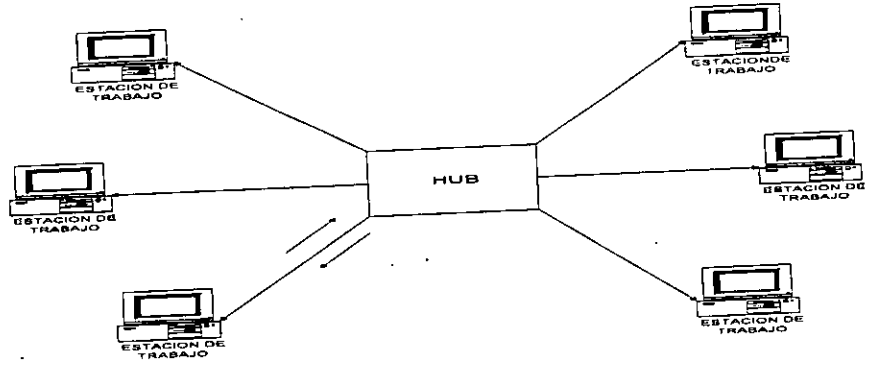


Figura 1.5 Topología en estrella

1.6.3 TOPOLOGÍA EN ANILLO

En este tipo de topología los nodos se enlazan uno tras otro formando un anillo o un circulo (Figura 1.6). También se le denomina así debido al aspecto circular en el flujo de los datos.

Los paquetes de datos en la mayoría de los casos viajan en una sola dirección alrededor del anillo de un dispositivo de la red al siguiente, el cual los toma y los retransmite a la siguiente estación , el proceso se continua así sucesivamente hasta recorrer todo el anillo.

La principal ventaja de esta topología es que raramente presenta cuellos de botella en la distribución de la información. Sin embargo, como todas las topología presenta deficiencias. La principal se deriva del hecho de contar con un canal único que

une a todos los componentes en el anillo, si un canal entre dos nodos falla, entonces la red se pierde.

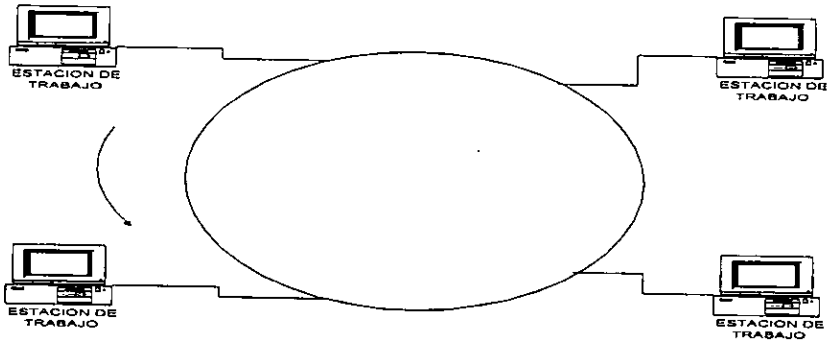


Figura 1. 6 Topología en anillo

1.6.4 TOPOLOGÍA FÍSICAMENTE ESTRELLA LÓGICAMENTE ANILLO

Esta topología toma las ventajas de las topología en estrella y anillo, las incorpora en una sola. Es decir, la red se configura físicamente en estrella y opera lógicamente como una red con topología en anillo (Figura 1.7).

Esta topología esencialmente ha reemplazado la topología en anillo en su uso practico. Obviamente se requiere del servicio de un hub que actúa como un anillo lógico, con los paquetes de información viajando en secuencia de un puerto a otro. Tal como una topología en estrella si un nodo falla , la red seguirá operando.

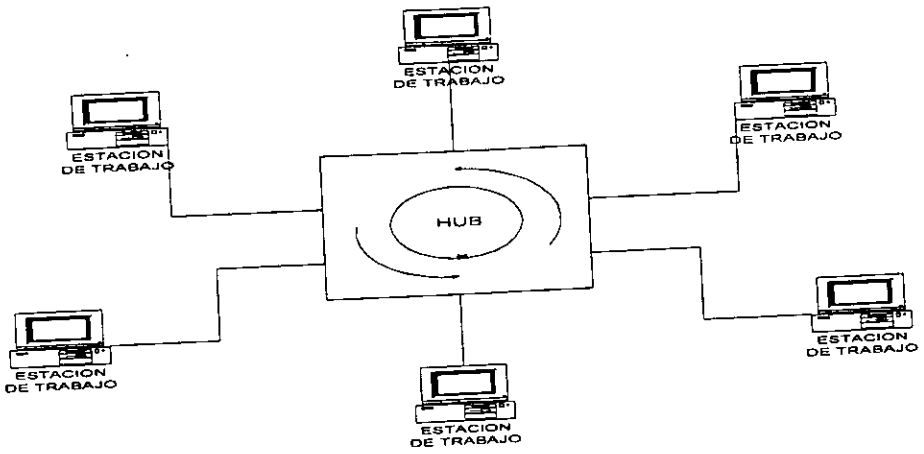


Figura 1.7 Topología físicamente estrella-lógicamente anillo

1.6.5. TOPOLOGÍA EN MALLA.

La topología en malla se ha venido utilizando con mayor frecuencia en los últimos años. Su atracción es su relativa inmunidad a cuellos de botella y fallas. Debido a la multiplicidad de rutas (redundancia) para transportar los paquetes, el tráfico puede ser enrutado alrededor de componentes dañados o nodos ocupados (Figura 1.8). Aunque este modelo es una empresa costosa, algunos usuarios prefieren la confiabilidad de la topología en malla que las de otras topologia, especialmente para redes que cuentan con pocos nodos a ser conectados.

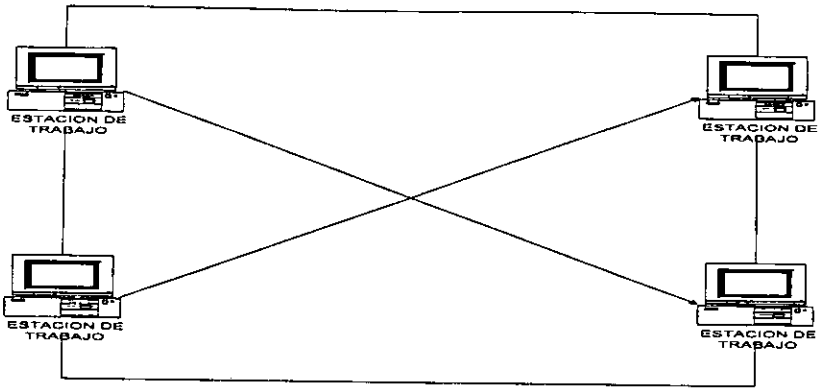


Figura 1.8 Topología en malla

1.7 ESTÁNDARES DE CONTROL DEL ACCESO A LOS MEDIOS

En el mundo de la computación existen diversos organismos y agrupaciones como el IEEE (Institute of Electrical and Electronics Engineers) con sede en la ciudad de Nueva York, OSI (International Standars Organization) con sede en Ginebra y el CCITT (Consultative committee for International Telephony and Telegraphy) también con sede en Ginebra, entre otros que se dedican a la elaboración de estándares.

Son organismos neutrales compuestos por representantes gubernamentales, militares y fabricantes de diversas empresas de productos de cómputo. Por otro lado, un estándar define las especificaciones que deben tomar en cuenta los fabricantes para la elaboración de un producto, y así evitar la proliferación de técnicas.

Las ventajas de tener estándares son muchas entre otras está el de dar origen y fomentar los "Sistemas Abiertos", esto significa que existe la posibilidad que el hardware de diversos fabricantes se mezclen en una misma red (compatibilidad entre productos), trayendo como consecuencia precios competitivos para el consumidor.

A la situación contraria, es decir, cuando una computadora, red, etc.; requiere hardware exclusivo del fabricante de dicho equipo se le denomina "Sistema Propietario".

Un organismo muy involucrado en la elaboración de estándares para las redes de área local es el IEEE, y un proyecto que ha instituido muchos de los estándares usados hoy en día de este organismo es el proyecto 802.

De los estándares del proyecto 802 del IEEE destacan los estándares para controlar el acceso a los medios de transmisión, y que tienen que ver con los métodos para permitir que un nodo determinado transmita en el canal de transmisión de datos disponible para él.

A continuación se presentan los estándares para el control del acceso al medio propuesto por el comité 802 del IEEE.

1.7.1 CSMA/CD (IEEE 802.3)

Carrier Sense Multiple Access/Collision Detection (Portadora Sensa Multiples Accesos/Deteccion de Colision). Este protocolo encuentra su aplicación principal en las redes con topología en bus, entendiéndose como protocolo al conjunto de instrucciones, señales o comandos necesarios para que dos computadoras se puedan comunicar.

En este protocolo cada nodo antes de transmitir un paquete sensa la línea, es decir, "escucha" si no hay tráfico en el canal de comunicación para entonces enviar su información la cual viaja hacia ambos extremos del cable. Por lo tanto, el primer mensaje que se envía es el primero en atenderse.

Cuando dos o más estaciones transmiten simultáneamente ocurren colisiones, sin embargo, CSMA/CD monitorea el canal por una colisión durante la transmisión.Si el paquete de datos de una estación no checa con una estación receptora, se sabe que ha ocurrido una colisión, el protocolo entonces se asegura que todas las demás estaciones sepan de la colisión y espera cierta cantidad de tiempo en forma aleatoria para que las estaciones vuelvan a transmitir, cuando la línea no tenga tráfico y de esta forma se evita la perdida de datos.

Por otro lado cuando un paquete llega a una estación el nodo receptor checa la dirección de destino del paquete, para decidir si el paquete debe ser procesado por éste, si es así, el nodo responde sincronizándose con la señal entrante. Y a medida que los bits van llegando son decodificados y traducidos a datos binarios, además de verificar la integridad de los datos mediante una secuencia de chequeo.

1.7.2 TOKEN BUS (IEEE 802.4)

Este protocolo al igual que CSMA/CD hace uso de una topología en bus, pero la transferencia de información sigue un patrón circular o forma de anillo (anillo lógico).
Este anillo lógico se forma identificando cada una de las estaciones mediante una secuencia en donde la última estación apunta a la primera cerrando el anillo. Por lo tanto, las estaciones pasan los tokens (señales electrónicas) colocando la dirección del siguiente recipiente lógico, en el encabezado del paquete de datos también denominado frame[3].
La señal o token pasa a través del bus y es físicamente monitoreado por todas las estaciones pero el token va a ser recibido solamente por la estación que indica el campo destino del encabezado. En el caso de que un token sea pasado a un nodo fallidamente, el nodo emisor de la señal esperará un momento, retransmitirá un determinado numero de veces y en caso de persistir la falla tiene la capacidad de transmitir el token a la estación sucesora.

En este protocolo, como se puede ver es posible establecer prioridades entre los nodos, pasando el token a las estaciones en orden descendente numérico basado en las direcciones de las estaciones. Cuando el token llega a cierta estación en ese momento la estación puede transmitir datos y cuando termina la transmisión pasa el token a la siguiente estación en el anillo lógico.

Por esta forma de operar del estándar token bus, se concluye que es un protocolo libre de colisiones, dado que el acceso al sistema es siempre secuencial y bajo circunstancias normales los derechos de acceso pasan de estación en estación. Con esto se garantiza que todas las estaciones tendrán la misma oportunidad de transmitir y que un solo paquete viajará a la vez en la red.

1.7.3 TOKEN RING (IEEE 802.5)

Los protocolos token passing (paso de señal) pueden residir en una topología de anillo como en el caso del estándar Token Ring. Sin embargo, también se le ve con

[3] Frame: grupo de bits que constituyen un bloque elemental de datos para su transmisión mediante ciertos protocolos.

mucha frecuencia operar en la topología físicamente estrella-logicamente anillo, donde el hub hace las veces del anillo lógico.

Como se mencionó anteriormente un token es una señal electrónica que es pasado de estación en estación en el anillo físico de la red. El token circula en una dirección lógica y está disponible a cualquier estación que tiene datos para colocarlos en éste.

Cuando el token circula y no lleva datos se dice que está libre, y al llegar a una estación que tiene datos para enviar los toma cambiando su estatus a ocupado, entonces el token se hace circular a las siguientes estaciones. Cada estación consecutiva entonces, checa la dirección destino de los datos para determinar si debe procesar los datos o no, aquí cabe hacer notar la diferencia con token bus, que los paquete de datos viajan de estación en estación de acuerdo a la configuración física del anillo y no a un orden preestablecido. Finalmente cuando el token hace todo el recorrido del anillo (obviamente alguna de las estaciones ya tomó los datos para ser procesados) y llega a la estación origen, le descarga los datos y le cambia su estatus, ahora nuevamente a libre y lo lanza a la red para que sea tomado por otra estación que requiere transmitir información.

Uno de sus inconvenientes es, que al llegar el token a un nodo se regenera con la dirección destino del siguiente nodo. Esto origina cierto retraso en la transmisión y por lo tanto una reducción en el rendimiento de la red pero por otro lado se asegura una transmisión exitosa desde la primera vez que se envía el mensaje.

Como se puede ver tanto Token Ring como Token Bus (Protocolos Token Passing) son protocolos diseñados para evitar colisiones entre las señales que se transmiten en la red.

1.8 IMPLEMENTACION COMERCIAL DE LOS ESTÁNDARES

Como se mencionó en el apartado anterior existen ciertos organismos internacionales que establecen las reglas, por decirlo así, de las técnicas que deben seguir los fabricantes de equipo de cómputo en la elaboración de los productos para el establecimiento de una red. Los fabricantes a su vez, con el fin de que sus productos sean compatibles con los demás productos de otras empresas, y como consecuencia al

existir una amplia gama de equipo que realiza la misma función (al cumplir con los estándares), se ven obligados por un lado a dar precios razonables al usuario y por otro lado elevar la calidad de sus productos para tener ventaja competitiva sobre otros fabricantes.

En este apartado se mencionaran algunas de las implementaciones comerciales de los estándares. Destacando Ethernet, Token Ring, Arcnet como métodos de acceso al medio usados principalmente para enlazar maquinas de escritorio (como servidores, estaciones de trabajo, impresoras) a la red; y por otro lado Fast Ethernet, FDDI, ATM son usados principalmente en redes con alta velocidad de acceso (servidores de archivos) ya que son tecnologías de alta velocidad de transferencia (100 megabits por segundo).

1.8.1 ETHERNET

En los años 70´s Digital Equipment Corporation (DEC), Intel, y Xerox establecieron las primeras especificaciones para Ethernet (DIX Ethernet).

Ethernet cumple con la norma IEEE 802.3 (CSMA/CD), y ha emergido a través de los últimos años como el método de acceso al medio más popular. Debido a que este estándar de la industria no propietario ha sido acogido por fabricantes de equipo de redes en todas partes, los componentes Ethernet de múltiples vendedores trabajaran juntos y se comunicaran sin complicaciones, se puede configurar en bus para cable coaxial delgado o grueso, pero cuando se utiliza cable telefónico o fibra óptica, el concepto de bus lineal se altera ya que en este tipo de cableado la topología utilizada es de tipo estrella. Se utiliza un hub, que internamente mediante su electrónica, lleva el bus lineal para la conexión de los nodos. Este esquema presenta ventajas como instalación más fácil, facilidades para monitorear y administrar la red, y una forma más sencilla de expander la red.

Ethernet transmite datos a tasas de transferencia de 10 Mbps o 100 Mbps (Fast Ethernet). Por otro lado, es necesario mencionar que en el proyecto 802, el IEEE estableció especificaciones para los cables que transportan señales Ethernet, proponiendo el siguiente formato: 10BASE-5, 10BASE-2, 10BASE-T, 100BASE-T y 10BASE-F; refiriedose a cable coaxial grueso, cable coaxial delgado, cable par trenzado sin blindaje y fibra óptica respectivamente. Donde el "10" y "100" se refieren a las tasas

de transmisión de datos de 10 y 100 Mbps, y por último "BASE" se refiere a banda base (baseband) es decir, un canal simple de comunicaciones en cada cable.

Originalmente , el último carácter se refería a la máxima distancia del cable en cientos de metros. Esta convención cambio, sin embargo, con la introducción de 10BASE-T y 10BASE-F. En estos casos, la T y F se refieren a los tipos de cable par trenzando y fibra óptica respectivamente.

1.8.2 TOKEN RING

Token Ring cumple con la norma IEEE 802.5 (Token Ring) fue desarrollado por IBM Corporation a mediados de los años 80´s y subsecuentemente definido por el IEEE.

Debido a que Token Ring es el método preferido de IBM para armar redes, se le encuentra principalmente en instalaciones que cuentan con minicomputadoras y mainframes IBM.

Las redes Token Ring trabajan con las topología en anillo y físicamente estrella-logicamente anillo. Cuando hace uso de la topología físicamente estrella-logicamente anillo lo hace sobre cables par trenzado ya sea blindado o no blindado con el apoyo de un hub central referido como MAU (Multiple Access Unit- Unidad de Acceso Múltiple), el cual se encarga de la operación lógica de anillo. Token Ring transmite datos a una tasa de transferencia de 4 Mbps y 16 Mbps.

1.8.3 ARCNET

Arcnet cumple con la norma IEEE 802.4 (Token Bus), opera en una topología en bus, utiliza cable coaxial o par trenzado, siendo el primero el más utilizado.

Físicamente seria conflictivo tender una red que forme un anillo, ya que agregar o eliminar un nodo a la red seria muy complicado. En la actualidad, este tipo de red se maneja por centros de alambrado, repetidores o hubs, los cuales se encargan de implementar ese anillo.

Arcnet posee una tasa de transferencia de datos de 2.5 Mbps y se recomienda ampliamente cuando el trabajo o el procesamiento en la red no es muy fuerte.

1.8.4 FAST ETHERNET (100BASE-T)

Fast Ethernet se refiere a Ethernet de 100 Mbps. Usa CSMA/CD al igual que Ethernet "estándar" . Lo que diferencia 100BASE-T de Ethernet de 10 Mbps es el incremento en la velocidad de la capa MAC (Medium Access Control-Control de Acceso al Medio,el cual define quien puede usar la red cuando múltiples computadoras están tratando de accesar simultáneamente) en un factor de 10.

1.8.5 FDDI/TP-PMD

FDDI (Fiber Distributed Data Interface-Interfase de Distribucion de Datos Mediante Fibra Óptica), el cual entrega un base estándar de 100 Mbps sobre cable de fibra óptica, es ampliamente difundido en "redes centrales", que pueden entrelazar múltiples localidades, y a las cuales pueden conectarse redes más pequeñas (a estas redes centrales también se les denomina Backbones).

Su base secundaria o alterna en cables de cobre llamado TP-PMD (Twisted Pair Physical Medium Dependent) usa una variación del MAC para proveer 100 Mbps sobre cableado de cobre.

Las virtudes principales de FDDI/TP-PMD son redundancia, manejo y acceso garantizado a la red. Una desventaja clara de esta implementacion, es que el costo por puerto permanece demasiado alto para ser considerado una solución viable de red para computadoras típicas de escritorio.

1.8.6 ATM

Una red ATM (Asynchronous Transfer Mode-Modo de Transferencia Asincrona) usa una configuración en estrella usando fibra óptica (y en algunas configuraciones nuevas, par trenzado).Aunque no es implementacion de un estándar es digna de mencionar dentro de las tecnologías de alta velocidad de transmisión.

ATM es una tecnología escalable que ofrece transferencia de datos de 25 Mbps a 622 Mbps y más. Un conmutador en el centro de la estrella establece un circuito dedicado

entre las estaciones emisora y receptora. Con ATM se pretende manejar aplicaciones multimedia interactivas en tiempo real que combinen voz, vídeo y datos.

ATM sin embargo, requiere adaptadores nuevos de red y, en la mayoría de los casos, conexiones de fibra óptica. Además sus implementaciones son limitadas y propietarias.

1.9 SERVICIOS QUE PROPORCIONA UNA RED

Se ha descrito hasta este momento, como se ve físicamente, en términos de topología, cableado, y componentes una red, así como, su funcionamiento interno desde el punto de vista de sus protocolos; en este apartado tomando en cuenta al usuario final que poco o nada le interesan los detalles técnicos, se dará un descripción breve de los beneficios que una red puede proporcionar.

1.9.1 SERVICIOS DE MANEJO DE ARCHIVOS

Los servicios de manejo de archivos permiten a los usuarios compartir información y aplicaciones a través de la red. Por ejemplo, se puede accesar a un archivo en otra computadora, usar un programa de aplicación o revisar el reporte de ventas del último mes tomando los datos de un base de datos compartida. Estas tareas son llevadas a cabo por medio de los servicios de manejo de archivos.

1.9.2 SERVICIOS DE CORREO ELECTRÓNICO

Los servicios de correo permiten enviar y recibir correo electrónico (e-mail) en una red. El correo electrónico facilita la comunicación hacia el interior o exterior de una compañía. Usando un paquete de correo electrónico, se pueden programar juntas de trabajo, enviar archivos a otros departamentos y difundir información a una organización entera.

1.9.3 SERVICIOS DE IMPRESIÓN

Los servicios de impresión permiten imprimir documentos en un impresora, usando servidores de impresión. Algunas redes están diseñadas de tal forma que se puede enviar el documento a ser impreso a un cola de impresión en un servidor. El servidor después maneja la impresión del documento, descargándolo de la computadora. Además los

servicios de impresión dan a cada usuario de red acceso a múltiples impresoras, expandiendo la capacidad de impresión.

1.9.4 SERVICIOS DE FAX

Los servicios de fax dan la habilidad de enviar y recibir faxes directamente desde la estación de trabajo del usuario. Uno o más modems con líneas telefónicas dedicadas son conectados a un servidor en la red y proveen servicios de fax a todos los usuaria de la red.

1.9.5 SERVICIOS DE EMULACIÓN DE TERMINAL

Los servicios de emulación de terminal dan acceso a diferentes tipos de estaciones de trabajo con diferentes sistemas operativos. Por ejemplo. si se deseara accesar a la información contenida en el mainframe de una red desde una Macintosh, los servicios de emulación permiten llevar a cabo esta operación.

1.9.6 SERVICIOS DE COMUNICACIÓN

Los servicios de comunicación permiten a usuarios remotos accesar a la red, usando un módem, y hacer uso de los recursos y servicios de dicha red. También permite a los usuarios comunicarse otros servicios de comunicación como Compuserve o AppleLink entre otros.

Por último cabe hacer notar que, algunos Sistemas Operativos de red populares como Novell Netware, Microsoft LAN Manager, Appleshare y Banyan Vines ; proveen algunos, sino es que todos, los servicios mencionados; de la misma forma, también hay productos adicionales disponibles que se especializan en cada uno de los servicios.

CAPITULO II

HISTORIA DE INTERNET

2.1 INTRODUCCIÓN

Poco tiempo después del termino de la Segunda Guerra Mundial los Estados Unidos de Norteamérica (E.U.) y la Unión de Repúblicas Socialistas Soviéticas (URSS), surgieron como las dos potencias predominantes a nivel mundial, cada una líder de un sistema económico-político antagónico entre si, es decir, la URSS encabezando el bloque socialista y los E.U. encabezando el bloque capitalista.

Este hecho produjo una competencia y una campaña de desacreditación entre ambos países, cuyo objetivo era el de demostrar que sistema político era el mejor, y al cual las demás naciones deberían aspirar o imitar. Todo esto con el fin, de establecer una superioridad sobre el otro y así obtener el liderazgo político absoluto a nivel mundial.

Como producto de esta confrontación se derivo una situación de tensión que dio lugar a una guerra conocida como "Guerra Fría", con el termino "Fría" se manifiesta que las relaciones políticas entre el éste y el oeste quedan paralizadas creándose un ambiente hostil, pero sin llegar al uso de las armas.

Las principales características de esta guerra fría fueron: la concentración militar, con especial énfasis en el armamento nuclear (situación que se vio reflejada en una carrera armamentista entre los países involucrados), se propiciaron condiciones de incertidumbre que se trataron de aprovechar aumentando el temor del adversario (amenazando con un enfrentamiento armado), cada una de las partes en conflicto trato de denigrar al máximo a su rival y un aspecto muy importante fue el establecimiento de un impulso continuo a la competición en todos los ámbitos (ya sean científico, deportivo, artístico, cultural, etc.).

Como una consecuencia directa de esta guerra fría se empezaron a desarrollar muchos proyectos y a crear instituciones con una aplicación orientada hacia el aspecto bélico. Un hecho que comprueba lo anterior se presento en el año de 1957, cuando la URSS lanza el Sputnik, el primer satélite artificial y en respuesta, los E.U. crean La Agencia de Proyectos Avanzados de Investigación (Advaced Research Projects Agency (ARPA)) dentro del Departamento de Defensa en el año de 1958, con el objetivo de colocar a los E.U. como líder en la ciencia y en la tecnología aplicable al aspecto militar.

ARPA auspicio muchos proyectos, entre los cuales se encontraron principalmente, la investigación en el campo de la computación y muy especialmente en las redes de computadoras, investigaciones y proyectos que a la postre vendrían a culminar en la creación de la red WAN conocida como ARPANET y ésta a su vez, vendría a ser la red central a partir de la cual se desarrollaría INTERNET.

2.2 LA DÉCADA DE LOS 60's

2.2.1 LAS PRIMERAS IDEAS SOBRE LAS REDES DE CONMUTACIÓN DE PAQUETES

Como se mencionó en el apartado anterior algunos de los sentimientos que prevalecían en el medio político y militar de los E.U. a fines de los años 50's y principio de los años 60's a consecuencia de la Guerra Fría eran el temor y la incertidumbre a un ataque nuclear por parte de la URSS. Estos sentimientos provocaron que la corporación RAND, la institución americana más avanzada en el estudio de la Guerra Fría se planteara un extraño problema estratégico: Cómo podría la armada de los E.U. proteger sus sistemas de comunicación en caso de un ataque nuclear?, y aun más, Cómo podrían comunicarse las autoridades exitosamente después de una conflagración nuclear? [1]

En efecto, E.U. después de un ataque nuclear requeriría de una red que enlazara a las ciudades, estados, instituciones y bases militares; pero se presentaba la situación que cualquier instalación física central seria un blanco fácil para el ataque enemigo, por

[1] Sterling Bruce, The Magazine Of Fantasy And Science Fiction, Internet, Febrero 1993

muy blindada o protegida que estuviera cualquier red concebible simplemente en cualquier ataque quedaría reducida a escombros.

Esta situación derivo en una investigación para analizar y encontrar posibles respuestas a tales preguntas, siendo encomendada a Paul Baran, miembro de la corporación RAND y patrocinada por la Fuerza Aérea de los E.U.

Paul Baran se abocó a explorar varios modelos para formar sistemas de comunicación y evaluar su vulnerabilidad, también realizó el análisis de redes con topología en malla contra las topologías en estrella. Los resultados de la investigación fueron escritos por Baran en una serie de reportes que se llamaron "On Distributed Communications Networks" (Redes de Comunicaciones Distribuidas) y fueron publicados por la corporación RAND en 1964.

Los principios que Paul Baran sugería en su reportes eran simples. Proponía un sistema de comunicación (red) donde no existiera un comando central y tampoco un punto de control, pero en el caso de un ataque en cualquier punto de la red que todos los nodos sobrevivientes tuvieran la capacidad de restablecer contacto, así el daño a una parte no destruiría la red totalmente y su efecto seria mínimo.

La red sería diseñada desde el inicio para operar bajo las más difíciles condiciones, por lo tanto su operación seria considerada como no confiable todo el tiempo, cada uno de los nodos en la red serian iguales con respecto a los demás, es decir, cada nodo tendría la capacidad y autoridad para originar, pasar y recibir mensajes.

Los mensajes serian fragmentados en subpartes llamados paquetes para su transmisión (enrutamiento), cada paquete individual tendría la dirección del nodo origen y la dirección del nodo destino, y serian lanzados de nodo en nodo dentro de la red más o menos en la dirección de su destino, al tener una topología en malla existirían diversas rutas alternas para llegar al nodo destino (principio que Baran llamo "redundancia de conectividad"), sí grandes porciones de la red fueran bombardeadas, simplemente no habría problemas ; ya que los paquetes seguirían viajando a través del campo por cualquier nodo que hubiera tenido la suerte de sobrevivir (cambio de ruta dinámico) y así llegarían a su destino final donde serian ordenados y reensamblados.

Así mismo, dentro de las recomendaciones que Baran proponía en sus reportes, destacaba el establecimiento de un servicio publico nacional de transmisión de datos, que operara en una forma similar al sistema telefónico.

Los reportes que Paul Baran escribió, fueron la primera descripción de lo que ahora conocemos como "Redes de Conmutación de Paquetes".

2.2.2 ARPA: AUSPICIA LA INVESTIGACIÓN SOBRE REDES DE COMPUTADORAS

En el año de 1962 a ARPA se le asignaba la tarea de investigar como emplear el presupuesto otorgado a los militares en cuestión de cómputo, a través de su oficina de Comando y Control de Investigaciones[2]. El Dr. J.C.R. Licklider fue elegido para encabezar este trabajo. Licklider se incorporaba a ARPA proveniente de la empresa Bolt, Beranek and Newman Inc. en Octubre de 1962. Combinaba estudios de ingeniería y psicología fisiológica que lo proveían con una inusual perspectiva entre los ingenieros.

A partir de su llegada a ARPA, la mayoría de los contratos de investigación del departamento con las corporaciones independientes se cambiaron, otorgándoselos a los mejores centros académicos de cómputo del país. Poco tiempo después la oficina de Comando y Control de Investigaciones era renombrada como lá Oficina de Técnicas de Procesamiento de la Información (Information Processing Techniques Oficce (IPTO)).

Licklider estaba interesado en la relación entre las computadoras y las comunicaciones, veía particularmente a la computadora como un dispositivo de comunicación y le apasionaba la cuestión de como la computadora podía ayudar a los seres humanos a comunicarse mejor.

Licklider se interesaba en la interconexión de las comunidades informáticas, fue el primero en percibir el espíritu de comunidad, creada entre los usuarios de los primeros sistemas de tiempo compartido y facilitó la forma de pensar acerca de la interconexión de dichas comunidades. Profèticamente, apodaba al grupo de especialistas en cómputo que había reunido como "La Red Intergalactica". La visión de Licklider de una red intergalactica conectando personas representaba una concepción importante que daba un giro en el pensamiento en las ciencias de la computación de esa época.

Derivado de este pensamiento el trabajo soportado por ARPA/IPTO y por consecuencia el presupuesto de los militares en cuestión de cómputo, se decidió

[2] Hauben Michael, Behind the Net: The untold history of the ARPANET, Publicado Electronicamente

aplicarse explícitamente a la investigación y desarrollo de las comunicaciones y las redes de computadoras; que dirigió al éxito de la primera red de ARPA denominada ARPANET.

Licklider fue uno de los primeros pioneros en computación en ayudar a hacer la red global de computadoras una realidad, su visión de una red intergalactica de computadoras atrajo a otros científicos que se inspiraron en sus ideas para el desarrollo de trabajos posteriores.

Pioneros como Paul Baran y J.C.R. Licklider en sus ideas proponían el desarrollo de una nueva tecnología en una dirección que no se había desarrollado anteriormente, es decir, la aplicación de la computadora como un medio de comunicación y no como se veía en su época simplemente como una máquina aritmética.

2.2.3 LA PROPUESTA PARA ARPANET

Durante el periodo de 1962-1964, Licklider fomento la investigación de los sistemas de tiempo compartido, algunos experimentos se efectuaron en MIT (Compatible Time Sharing System) y en Dartmouth (Dartmouth Time Sharing System). Animados por el hecho, de que sí era posible que varios usuarios trabajaran simultáneamente en una computadora, el enlace de computadoras remotas entonces también era factible.

Entre 1966 y 1967 el Laboratorio Lincoln del Instituto Tecnológico de Massachusetts en Lexington y la System Development Corporation (SDC) en Santa Monica California gracias a un contrato otorgado por el Departamento de Defensa, desarrollaron un estudio llamado "Redes Cooperativas de Computadoras de Tiempo Compartido" y comenzar asi la investigación en el enlace de computadoras a través de E.U. El objetivo era establecer una "red de prueba" para ver en donde estarían los posibles problemas al enlazar computadoras.

En éste estudio se logró el enlace directo de dos computadoras diferentes (incompatibles), la computadora TX-2 del Laboratorio Lincoln y la computadora Q-32 de SDC en California , sin el uso de la tecnología de conmutación de paquetes.

El problema que se visualizó en este estudio fue con respecto a la tecnología telefónica de conmutación, ya que era inadecuada para llevar a cabo sus metas de comunicación.

Así este experimento estableció las bases para justificar la investigación en el desarrollo de una red de cobertura nacional que utilizara conmutación de paquetes.[3]

Durante este periodo, ARPA estuvo patrocinando la investigación en el campo de las redes de cómputo en varias universidades y laboratorios de investigación de E.U. Y decidió enlazarlos en una red experimental, llamándola eventualmente ARPANET.
El plan para construir ARPANET fue hecho publico en Octubre de 1967 dentro del Simposio de la Association for Computing Machinery (ACM) con el tema "Principios de Operación" en Gatlinburg, Tenessee.

Lawrence Roberts miembro del equipo de Licklider y fuertemente influenciado por las ideas de éste, fue elegido para dirigir a IPTO (quien auspiciaba el trabajo) y guiar la investigación.

2.2.4 SE APRUEBA LA CREACIÓN DE ARPANET

Cabe hacer mención que las computadoras que predominaban en la década de los 60's (mainframes y minicomputadoras) se caracterizaban por ser sistemas propietarios, es decir, no había compatibilidad entre las computadoras de los diferentes fabricantes, tanto en software como hardware, que permitiera enlazarlas directamente.

Por lo cual en el simposio se mencionaría que, para desarrollar una red con computadoras de diferentes tipos (incompatibles), dos problemas principales tenían que ser resueltos:

1. Con el fin de eludir los problemas de conectar directamente computadoras incompatibles y proporcionar una interface estándar a la cual se conectaran las computadoras. Se proponía construir una "subred" constituida de circuitos telefónicos y nodos de conmutación cuya confiabilidad, capacidad en sus características de retardo, y costo facilitaran la incorporación de los hosts y permitiera la compartición de sus recursos. A los nodos de conmutación se les llamo Interface Procesadora de Mensajes (Interface Message Processor (IMP)).

[3] Hauben Michael y Hauben Ronda, Netizens: On the History and Impact of Usenet and The Internet,The Birth and Development of the ARPANET, Publicado Electronicamente

2. Entender, diseñar e implementar los protocolos y procedimientos dentro de los sistemas operativos de cada computadora conectada, para permitir el uso de la subred por parte de las computadoras que fueran a compartir recursos.

En el simposio se empezaron a discutir las especificaciones que deberían cubrir tanto los IMPs como los protocolos. La red se formaría básicamente por una subred de IMPs constituida por minicomputadoras dedicadas, unidas a cada una de las computadoras participantes (hosts), los IMPs leerían las direcciones de cada paquete, aceptándolos o pasándolos al siguiente nodo, reensamblandolos en un mensaje y finalmente traduciéndolo al lenguaje del mainframe receptor. Para cerrar la red los IMPs serían unidos vía líneas telefónicas.

Para fines de 1967 ARPA daba un contrato al Stanford Research Institute (SRI) para que escribiera las especificaciones de las comunicaciones (protocolos) de la red, que se empezaba a desarrollar.

Las especificaciones estuvieron listas para ser discutidas con los principales investigadores de ARPA en Junio de 1968 elaborándose un plan para implementarlas en ARPANET . El plan denominado "Resource Sharing Computer Networks" (Compartición de Recursos en Redes de Computadoras) fue entregado el 3 de Junio de 1968 por IPTO al director de ARPA, quien lo aprobó el 21 de Junio de 1968.[4]

2.2.5 QUIEN CONSTRUIRÍA LA SUBRED ?

La red propuesta (ARPANET) era impresionante ya que suministraría beneficios inmediatos a los centros de investigación que estuvieran conectados a la red, así como a los militares. Los objetivos establecidos por ARPA eran experimentar con interconexiones variadas de conmutación de paquetes, con el fin de compartir recursos en un intento de mejorar la productividad en la investigación del campo de la computación.

Ya establecidas las especificaciones dentro de un plan ahora se requería de su implementación, para lo cual en Julio de 1968 ARPA lanzaba una convocatoria, con el fin

[4] Hauben Michael, Behind the Net: The untold history of the ARPANET, Publicado Electronicamente

de encontrar una organización que diseñara y construyera la red física, es decir, la subred de IMPs.

Dentro de los requerimientos se pedía crear una red de cobertura amplia operando, con la participación de cuatro lugares y además proveer el diseño de una red que pudiera incluir 16 lugares.

Los cuatro lugares seleccionados de acuerdo a contratos contraidos con ARPA fueron: La Universidad de California en Los Ángeles (UCLA), El Stanford Research Institute (SRI), La Universidad de California en Santa Barbara (UCSB) y la Universidad de Utah.

2.2.6 LOS PRIMEROS INTENTOS EN LA OBTENCIÓN DE UN PROTOCOLO

La propuesta inicial para ARPANET requería que los sitios seleccionados trabajaran juntos en la solución del problema técnico que representaba el conseguir que los hosts se comunicaran entre si. Para tal efecto se formo un grupo con representantes de cada uno de los cuatro lugares elegidos, nombrándolo el Grupo de Trabajo de la Red (Network Working Group (NWG)). ARPA confiaba que los programadores en cada lugar serian capaces de modificar sus sistemas operativos para conectar sus sistemas a la subred, además de desarrollar el software necesario para accesar los otros hosts en la red.

Elmer Shapiro fue elegido como presidente del NWG pertenecia a SRI, y en el verano de 1968 convocaba a una reunión, en la cual estuvieron presentes Steve Carr de Utah, Stephen Crocker de UCLA, Jeff Rulifson de SRI y Ron Stoughton de UCSB. Esta reunión tomo lugar varios meses antes de que apareciera el primer IMP, obviamente surgieron muchas preguntas en esta primera reunión del NWG, entre otras cómo serian conectados los IMPs a los hosts?, cómo se comunicarían los host? y qué aplicaciones serian soportadas?[5]. Nadie tenia respuestas, pero se mostraban entusiastas ante el reto. Una decisión concreta del primer encuentro fue continuar con reuniones similares a ésta en los demás lugares.

[5] Crocker Stephen, RFC 1000: The Request For Comments Reference Guide, The Origins Of RFCs, pag. 2

Los primeros encuentros fueron muy abstractos y sin tener una idea clara de como funcionaria el hardware, el diseño inicial de un protocolo llevo al "Lenguaje-Decodificador-Codificador" (Decode-Encode-Language DEL) y a una versión posterior llamada "Lenguaje de Red de Intercambio" (Network Interchange Language NIL).

Pocos meses después cuando el desarrollador del hardware proporcionara detalles acerca del IMP, se darían cuenta que estos lenguajes eran mas avanzados de lo necesario, y por lo tanto no funcionarían.

2.2.7 BOLT, BERANEK AND NEWMAN GANA LA CONVOCATORIA

Para Enero de 1969 ARPA anunciaba el ganador de la convocatoria para establecer la subred de IMPs, siendo otorgada a la compañía Bolt, Beranek and Newman Inc (BBN).

Como se menciono en párrafos anteriores la red haría uso de minicomputadoras dedicadas para servir como nodos de conmutación (IMPs), para las computadoras anfitrionas (hosts). Las minicomputadoras que BBN eligió fueron las Honeywell DDP-516, las cuales estaban configuradas con memorias de 12 KB en palabras de 16 bits, y eran consideradas entre las mejores máquinas de su época.

Poco tiempo después de haber empezado a trabajar BBN en el desarrollo de los IMPs, proporcionaba detalles acerca de la unión host-IMP, especialmente del lado del IMP. Esta información dio al NWG algunos puntos definitivos de inicio a partir de los cuales construirían los protocolos.

En Febrero de 1969 miembros del NWG, de BBN y de la Network Analysis Corporation (empresa contratada por ARPA para especificar el diseño topológico de ARPANET y analizar su costo, desempeño y confiabilidad.) se reunían por primera vez, en un intento más de diseñar los protocolos. Como todas las partes tenían diferentes prioridades en mente, el encuentro fue un tanto difícil. BBN estaba interesada en hacer una conexión física confiable al más bajo nivel. Y el NWG estaba interesado en conseguir que los hosts se comunicaran entre si mediante programas de alto nivel. Por lo tanto, BBN no se considero en los planes de diseño para los protocolos.

2.2.8 LOS DOCUMENTOS "PETICIÓN DE COMENTARIO"

Un paso de increíble importancia en el desarrollo de ARPANET de dio en Abril de 1969. Después de una reunión del NWG en Utah, los participantes y en particular Stephen Croker decidieron que era tiempo de empezar a escribir sus discusiones en una forma consistente. Tenían notas del diseño de DEL y otros asuntos, y optaron por reunirlos en una serie de reportes. Pero como eran estudiantes en ese tiempo y por lo tanto no tenían autoridad, el temor de ofender a alguien con sus notas estaba presente, tenían que encontrar una forma de documentar lo que estaban haciendo sin actuar como si estuvieran imponiendo algo a alguien. "Las reglas básicas eran que cualquier persona pudiera decir cualquier cosa y que esto no fuera oficial. Y para enfatizar el punto nombre las notas "Petición de Comentario" (Request For Comments (RFC))"[6].

De esta manera el primer documento Petición de Comentario se titulo "Host Software" (Software para Anfitrión) y fue escrito por Stephen Croker.

Paradójicamente estos reportes se convertirían en la documentación oficial y se distribuirían libremente, sobre la red que se discutía en esta notas.

2.2.9 EL DISEÑO DE UN PROTOCOLO HOST A HOST

En la primavera y verano de 1969 el NWG siguió trabajando en el diseño de los protocolos de comunicación host a host. Estaban conscientes que para cualquier diseño que realizaran, iban a necesitar una interface de software entre el IMP y el host, así como tener acceso a los sistemas operativos, para implementar los protocolos.

Era claro que necesitaban accesar remotamente a los demás hosts con el fin de iniciar una sesión (login) y tener una operación interactiva, mas tarde conocido como Telnet; además de transferir archivos entre maquinas conocido también mas tarde como FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos).

Estas aplicaciones requerían trabajar en un esquema cliente/servidor pero desafortunadamente, los sistemas operativos de esta época tendían a verse a si mismos como el centro del universo; la cooperación simétrica no existía para ellos. En particular,

[6] Ibid pag. 3

únicamente relaciones asimétricas usuario-servidor eran soportadas, es decir, se manejaba el esquema de procesamiento centralizado, donde las terminales no inteligentes (sin capacidad de procesamiento) se conectaban a una minicomputadora o a un mainframe.

Por otro lado en UCLA se trabajaba en la construcción de una interface de software que permitiera la comunicación entre el host de esa universidad una máquina Scientific Data Systems (SDS) Sigma 7 y el IMP.

Normalmente las conexiones físicas host-IMP, fueron conexiones directas con tarjetas electrónicas de propósito especial que se instalaban directamente al bus de entrada/salida de la computadora y se conectaban con el IMP. Cuando se programaba correctamente la interface de hardware, la computadora contactaba el IMP y le permitía enviar y recibir paquetes.

Michael Wingfield estudiante de esta universidad fue quien construyo la interface de software, conocida como BBN 1822, tomando el nombre de acuerdo al numero del reporte técnico que la describía y la cual corria a 400 kbps, considerada muy rápida en ese tiempo.

Desafortunadamente, la interface 1822 nunca pudo ser un estándar de la industria. Ya que pocos fabricantes construían las tarjetas electrónicas, dificultando la conexión de nuevas maquinas.

2.2.10 NACE ARPANET

El 30 de Agosto de 1969, BBN entregaba la primera IMP a la Universidad de California en Los Ángeles, convirtiéndose esta universidad en el primer nodo de la red, la IMP fue conectada a la computadora SDS Sigma 7 la cual usaba el sistema operativo GENIE. La segunda IMP fue entregada en Octubre del mismo año al Stanford Research Institute, la IMP fue conectada a una computadora SDS-940 que utilizaba el sistema operativo SEX. Poco después en la Universidad de California en Santa Barbara, la IMP fue conectada a una IBM 360/75 la cual trabajaba con el sistema operativo OS/MTV. Y en

la Universidad de Utah, el cuarto nodo, la IMP fue conectada a una DEC PDP-10 que usaba el sistema operativo TENEX.[7]

Para fines de 1969, los primeros cuatro IMPs habían sido conectados a los hosts en sus respectivos lugares y las conexiones a la red entre los IMPs vía línea telefónica estaban operando. Físicamente nacía ARPANET.

Como se menciono el primer sitio en recibir la IMP fue UCLA , lugar donde se encontraba el profesor Leonard Kleinrock, quien había realizado trabajos sobre teoría de colas, trabajos que le proporcionaban una base para desarrollar técnicas de medición y monitoreo de redes. Las técnicas del profesor Kleinrock se penso que serian útiles en el monitoreo del desempeño de ARPANET. Y para asegurarse que las estadísticas tuvieran datos correctos con fines de análisis, se estableció que en uno de los primeros dos o tres nodos tendría que estar el lugar en donde se efectuaran las mediciones. De esta manera fue como a UCLA se le designo como el Centro de Medición de la Red.

SRI el segundo nodo, se nombro como el Centro de Información de la Red (Network Information Center,(NIC)) su objetivo era recaudar información acerca de la red, incluyendo los recursos de los hosts, y al mismo tiempo generar herramientas de software para almacenar y accesar la información recolectada.

BBN se encargo del control y operación de los IMP, de tal manera que se le denomino como el Centro de Operación de la Red (Network Operation Center (NOC)).

2.2.11 NCP EL PRIMER PROTOCOLO DE ARPANET

Se tenia resuelto el problema de hardware, pero el problema técnico relativo al software seguía esperando a ser resuelto. Es decir, el conjunto de acuerdos estándares sobre las señales de comunicación (llamados protocolos), que permitirían a los hosts comunicarse entre si a través de la subred.

Pero ahora con el establecimiento físico de la red los investigadores y científicos ya podían empezar a identificar los problemas que tendrían que resolver para desarrollar un red donde hubiera comunicación de host a host.

[7] Hauben Michael y Hauben Ronda, Netizens: On the History and Impact of Usenet and The Internet, The Birth and Development of the ARPANET, Publicado Electronicamente

Con la presión de obtener algo trabajando el NWG definió que el primer conjunto de protocolos incluiría sólo Telnet y FTP .

En Diciembre de 1969, se reunió el NWG y gente de ARPA comandada por Lawrence Roberts en Utah. Roberts al supervisar el trabajo del NWG les indico que no estaba bien orientado, y por lo tanto, tenia que ser replanteado. Después del consejo de Roberts, los siguientes meses el NWG diseño finalmente un protocolo de comunicación host a host, conocido como Network Control Program, ("NCP" más tarde vino a ser el nombre para el protocolo), este programa originalmente se identifico como parte del sistema operativo y se encargaba de establecer, cortar y conmutar las conexiones, además, de controlar el flujo de información.[8]

Con el advenimiento del protocolo host a host, también se tuvo la visión de la creación de una serie de protocolos jerárquicos construidos sobre éste protocolo básico (estratos), tales como Telnet y FTP.

Para 1970 la red empezó a operar con el protocolo NCP y el experimento fue declarado como un éxito, así surgía una de las primeras redes de área amplia operando con la técnica de conmutación de paquetes, conocida como ARPANET. La red de comunicaciones que algún día Paul Baran había imaginado era una realidad.

2.2.12 LAS REDES EN EL MUNDO A FINES DE LOS 60'S

Durante los años 60's el concepto intrigante de red a prueba de bombas y descentralizada utilizando conmutación de paquetes fue enfrentada por algunas instituciones en diversos países: en el Reino Unido Donald W. Davies quien acuño el termino "paquete" propuso la arquitectura de una red de conmutación de paquetes, la cual fue difundida en el periodo de 1965 a 1966. Culminando en lo que probablemente fue la primera red local que uso esta tecnología en el año de 1968 en los National Physical Laboratories.

Otro trabajo referente a la conmutación de paquetes fue conducido por la Societe Internacionale de Telecommunications Aeronautiques de 1968-1970, en el que fue

[8] Crocker, op. cit., pag. 4

organizada la red que interconectaba los sistemas de reservación de distintas compañías aéreas.

Al comienzo de los años 70's, se desarrollo en Francia la red CYCLADES, interconectando varios centros de investigación. Poco tiempo después, se instalo la red Reseau Communication par Paquet (RCP). En esta época también se creo la red European Informatics Netwak, esta red interconectaba varios centros de investigación europeos.

La mayoría de las redes mencionadas tenían un carácter experimental en la investigación sobre la tecnología de redes de computadoras.

2.3 LA DÉCADA DE LOS 70's

2.3.1 ARPANET SE EXPANDE

En el año de 1970 se iniciaba en la Universidad de Hawaii el proyecto ALOHANET dirigido por Norman Abrahamson, que consistía en la implementación de una red de conmutación de paquetes utilizando ondas de radio (packet radio). ALOHANET vendría a conectarse a ARPANET en 1972.

Por otro lado, en la medida que los problemas en el establecimiento de la red con los cuatro nodos de ARPANET fueron identificados y resueltos, la red se expandió a otros lugares más. En Abril de 1971, había 15 nodos y 23 hosts en la red[9]. Los nodos se ubicaban en:

1. Universidad de California en Los Ángeles
2. Instituto de Investigación Stanford (SRI)
3. Universidad de California en Santa Barbara
4. Universidad de Utah
5. Bolt,Beranek and Newman Inc.
6. Instituto Tecnológico de Massachusetts (MIT)

[9] Hauben Michael y Hauben Ronda, Netizens: On the History and Impact of Usenet and The Internet,The Birth and Development of the ARPANET, Publicado Electronicamente

7. RAND Corp.
8. System Development Corporation
9. Harvard
10. Lincoln Laboratories
11. Stanford
12. Universidad de Illinois, Urbana
13. Universidad Case Western Reserve
14. Universidad Carnegie Mellon
15. NASA-AMES

El avance en un principio era lento ya que había una gran variedad de máquinas propietarias con su correspondiente variedad de sistemas operativos propietarios, a las cuales se les necesitaba implementar tanto interfaces de hardware como software.

Como se menciono, los primeros hosts de la red se conectaron a los IMPs Honeywell DDP-516, después la minicomputadora Honeywell 316 fue utilizada. La Honeywell 316 era compatible con la DDP-516 pero estaba disponible a la mitad de costo que ésta. Algunos nodos fueron configurados usando estas minicomputadoras como TIPs (Terminal IMPs) empezando con la NASA-AMES TIP y MITRE TIP.[10]

Del lado del NWG más gente asistía a sus reuniones, además se escenificaban en foros más importantes. Por ejemplo, en el año de 1971 el NWG mantuvo un encuentro con la Spring Joint Computer Conference en Atlantic City.

2.3.2 LA PRIMERA PRESENTACIÓN PUBLICA DE ARPANET

A fines de 1971 Lawrence Roberts con fin de motivar que el desarrollo de ARPANET fuera más rápido, pedía a Robert Kahn de BBN organizar una demostración publica de esta red.

En Octubre de 1972 en el marco de la Conferencia Internacional en Comunicaciones de Computadora (ICCC), se llevo a cabo la presentación. La idea era

[10] Idem

instalar 40 máquinas y un TIP en el sótano del Hotel Hilton de Washington, y permitir que el publico asistente usara ARPANET.

Un grupo de gentes quienes ahora son legendarios en la historia de las redes de computadoras estuvieron envueltos en la presentación. La demostración fue un estruendoso éxito. Asistieron investigadores representantes de proyectos de varias partes del mundo, incluyendo Canadá, Francia, Japón, Noruega, Suecia y La Gran Bretaña.

En esta reunión se discutió la necesidad de empezar a trabajar en el establecimiento de un acuerdo sobre protocolos y fue así como se creo la InterNetworking Working Group (INWG) para empezar las discusiones en la búsqueda de un protocolo común y Vinton Cerf quien había estado involucrado en ARPANET en UCLA fue elegido como su primer presidente. La interconexión internacional de redes fue imaginada como "una malla de redes independientes unidas por compuertas, tal como los circuitos independientes de ARPANET eran interconectados por los IMP's.

2.3.3 LAS PRIMERAS ESPECIFICACIONES PARA LOS PROGRAMAS DE APLICACIÓN

En este año de 1972 Ray Tomlinson de BBN inventaba el programa de correo electrónico (e-mail) para enviar mensajes a través de una red distribuida y Jon Postel creaba la primera especificación para Telnet (RFC 318) titulada "Ad hoc Telnet Protocol", además ARPA era renombrada ahora como la Agencia de Proyectos Avanzados de Investigación de la Defensa (Defense Advance Research Projects Agency (DARPA)).

En Enero de 1973 la red había crecido a 35 nodos de los cuales 14 eran TIPs y se incluía un enlace satelital con ALOHANET, con el cual se conectaba California con un TIP a Hawaii.[11]

El 16 de Febrero de 1973 A. McKenzie presenta la primera especificación del File Transfer Protocol (FTP) en el RFC 454.

En este mismo año, Robert M. Melcafe presentaba su tesis para doctorarse en la cual resaltaba las ideas sobre Ethernet. Más tarde, específicamente en 1979 fundaría la compañía 3Com Corporation.

[11] Idem

2.3.4 DARPA AUSPICIA EL PROYECTO INTERNET

Por otro lado, DARPA se dio cuenta que los militares enfrentarían un problema que algunas organizaciones con varias redes tenían, y que consistía en que cada red conectaba un conjunto de computadoras, pero no existía una ruta que uniera a las redes separadas. Era como tener varias islas sin una ruta de enlace entre ellas.

Por lo cual en 1973 DARPA iniciaba un programa de investigación para encontrar técnicas y tecnologías para interligar redes con conmutación de paquetes de varias clases. Conociendo que el protocolo NCP no sería capaz de soportar una afluencia masiva de hosts, entonces, el objetivo era desarrollar protocolos de comunicación con los cuales se permitiera a las redes de computadoras comunicarse transparentemente a través de múltiples redes enlazadas, implementándolos en una red experimental prototipo (la cual tomaría el nombre de Internet). El conjunto de protocolos que fueron desarrollados a través del curso de esta investigación se conoció como la suite de protocolos TCP/IP, tomado el nombre a partir de estos dos protocolos básicos; Transmission Control Protocol (Protocolo Control de Transmisión) e Internet Protocol (Protocolo Internet)

Una idea clave en la investigación de DARPA fue un acercamiento a la interconexión de redes locales y redes de área amplia tomando a ARPANET como eje central, o troncal (Backbone)[12], esta acción de interconexión de redes llevo al termino "internetwork", usualmente conocido como internet. Los investigadores que trabajaban en DARPA adoptaron la convención de escribir internet con "i" cuando se referían al enlace en general de redes, y escribir Internet con "I" cuando se referían a la red experimental prototipo que pretendían construir, es decir, una red de redes[13]. La convención persiste a la fecha.

En Marzo de 1973 Robert Kahn describía los sistemas de transmisión de paquetes mediante ondas de radio y sistemas satelitales, así como, el problema Internet, el cual lo describía como: conseguir que los host se comunicaran a través de múltiples redes de

[12] Termino utilizado para hacer referencia a una red central que posee muchos ruteadores, por medio de los cuales se enlazan otras redes

[13] Comer Douglas, The Internet Book, The Internet Emerges, pag. 54

paquetes sin importar la tecnología de hardware que éstas tuvieran. Así empezaba la investigación en el enlace de redes auspiciado por DARPA.[14]

2.3.5 ARPANET ES INTERNACIONAL

A mediados de 1973 se presentaban las primeras conexiones internacionales para ARPANET, agregándose mediante líneas de baja velocidad la University College of London de Inglaterra y el Royal Radar Establishment de Noruega.

En Septiembre de este mismo año en un encuentro en la Universidad de Sussex en el Reino Unido, Cerf y Kahn presentan el primer diseño del protocolo TCP, para su revisión por el INWG.

Para este mes ARPANET tenia 40 nodos y 45 hosts, y el tráfico se había expandido de 1 millón de paquetes transmitidos por día en 1972 a la cantidad 2.9 millones.[15]

En Mayo de 1974 Cerf y Kahn publican "A protocol for Packet Network Intercommunication" (Un protocolo para la intercomunicación de redes) en el cual se especificaba en detalle el diseño de un Programa de Control de Transmisión (Transmission Control Program (TCP)), publicado en IEEE Transactions on Communications. Poco después la primera especificación del protocolo TCP fue publicada en Diciembre de 1974.

A partir de ese momento se empezaron a hacer implementaciones concurrentes sobre los protocolos TCP en 3 lugares: en Stanford con Cerf al mando, en BBN con William Plummer y Ray Tomlinson y en la University College London la persona en cargo era Peter Kirstein. Kirstein tenia una gran cantidad de estudiantes trabajando en una DEC PDP-9, así como con un enlace satelital. De esta forma el esfuerzo en el desarrollo de los protocolos para Internet, fue internacional desde el principio.

Por lo tanto para la implementación de los protocolos TCP se contó con la tecnología satelital, con la tecnología de conmutación de paquetes transmitidos con

[14] Cerf Vinton, How the Internet Came to Be, Publicado Electronicamente
[15] Hauben Michael y Hauben Ronda, Netizens: On the History and Impact of Usenet and The Internet,The Birth and Development of the ARPANET, Publicado Electronicamente

ondas de radio y ARPANET. Se evoluciono a través de cuatro versiones de la suite TCP, la ultima de las cuales apareció en 1978.

2.3.6 RFC SINÓNIMO DE DOCUMENTACIÓN "ABIERTA"

La mayoría de los investigadores que DARPA había elegido para el proyecto Internet ya tenían experiencia en el uso de las redes de computadoras. Habían diseñado y construido ARPANET, y habían ideado las aplicaciones. También sabían que podían usar ARPANET para intercambiar información técnica. De tal manera que poco después que empezara el proyecto Internet, decidieron mantener toda la documentación en archivos accesibles a través de ARPANET.

Inicialmente, los investigadores planearon editar los reportes en dos pasos. Después que un reporte fuera escrito, estaría disponible a otros investigadores para que lo comentaran. Después de un tiempo, el autor incorporaría todos los comentarios y se editaría un reporte final. Para implementar los dos pasos, los investigadores establecieron dos series de reportes. Cuando un reporte era editado por primer vez, seria nombrado como "Petición para Comentario" (Request For Comments (RFC)). Después que los demás investigadores enviaran sus comentarios al autor y el reporte fuera pulido, éste tomaría el nombre de "Nota Internet de Ingeniería" (Internet Engineering Note (IEN)).

Pero los investigadores encontraron que algunos de los reportes iniciales eran suficientes y no necesitaban revisión o mejora. Otros reportes eran reescritos totalmente, pero reeditados como un nuevo RFC para otra ronda de comentarios. La mayoría de los investigadores encontraron más productivo continuar investigando nuevas ideas que editar viejos reportes. Al final, los documentos RFC se convirtieron en el registro oficial del proyecto y la serie IEN se elimino.

Cada RFC fue asignado con un numero, y se incluyo dentro de un índice que listaba el titulo de cada numero. En cualquier momento, que un investigador que quisiera conocer los detalles de cualquier software de Internet podía usar ARPANET para obtener el RFC que tuviera la información. Si no se recordaba el numero del documento se podía obtener a partir del índice.

El mantener la documentación del proyecto "abierta" a través de la red permitió que cualquiera que estuviera trabajando en el proyecto coordinara sus actividades y mantuviera el software actualizado con las especificaciones. Mas importante, la rápida comunicación entre los investigadores incremento la velocidad con la cual el proyecto avanzo.

En resumen, el hecho que los reportes RFC que documentaban tanto los detalles técnicos del software (TCP/IP) como el proyecto Internet y que estuviera accesible a través de ARPANET, permitieron que el trabajo avanzara más rápidamente.

2.3.7 EMPRESAS PRIVADAS OFRECEN SERVICIOS DE RED

En Julio de 1975 el manejo operacional de lo que se empezaba a conocer como INTERNET era transferido por DARPA de BBN a la Defense Communications Agency (DCA) conocida ahora como la Defense Information Systems Agency (DISA).

Para esta época la tecnología de conmutación de paquetes para la transmisión de datos paso a ser económicamente ventajosa, lo que atrajo el interés en ofrecer este tipo de servicios por parte de particulares, por ejemplo en Canadá fue creada en 1974 la red DATAPAC, en 1975 BBN establece Telenet la primera implementación comercial de ARPANET, permitiendo que otros grupos diferentes a los investigadores académicos, gobierno y militares tuvieran acceso a esta tecnología. Y así fueron apareciendo redes de este tipo en varias partes del mundo.

En 1976 uucp (unix-to-unix copy) era desarrollado en los Laboratorios Bell de AT&T por Mike Lesk como parte de un proyecto de investigación. Uucp es una utilería para enviar y recibir correo electrónico, transferir archivos, y accesar remotamente otra computadora. Uucp fue distribuido con el sistema operativo Unix en 1977.

Este desarrollo derivo en la creación de varias redes nuevas que buscaban utilizar correo electrónico, transferencia de archivos, computo remoto, etc. En 1977, THEORYNET, una de estas redes, fue creada en la Universidad de Wisconsin por Lawrence Landweber, Richard Demillo y Richard Lipton. THEORYNET proporcionaba correo electrónico a cerca de 100 investigadores en ciencias de la computación.

2.3.8 LA PRIMERA PRESENTACIÓN DE INTERNET

En Julio de 1977 se realizo la primera presentación de Internet con el enlace de tres redes: una red satelital, una red de radiotransmision y ARPANET, con el objetivo de hacer una demostración de la operación de los protocolos.

Para enlazar un sistema de radiotransmisión móvil, en la demostración se estuvo manejando una camioneta en la autopista de la Bahía de San Francisco con dicho sistema corriendo en una computadora DEC LSI-11. Esta máquina fue enlazada mediante una compuerta (gateway) a ARPANET en BBN (Massachusetts). En BBN se monitoreaba la compuerta y se ajustaba manualmente el ruteo en el sistema. Después de cruzar el trafico por ARPANET éste se oriento a través de un enlace satelital punto a punto a Noruega y se transmitió a Londres a la University College London por una linea terrestre. De Londres se regreso la señal a través de SATNET (Atlantic Packet Satellite Network) hacia ARPANET otra vez, donde se dirigió finalmente hacia el Instituto de Ciencias de la Información de la Universidad del Sur de California a una de sus máquinas DEC KA-10.[16]

Esta demostración tenia el fin de simular a un soldado en un escenario bélico haciendo conexión a una red particular, para lo cual el tráfico viajaría a través de una red continental luego atravesaría una red satelital intercontinental, para por fin conectarse a una red alambrada, a un mayor recurso de cómputo en un cuartel general.

Debido a que el Departamento de Defensa estuvo auspiciando este proyecto, se buscaba que las demostraciones se trasladaran a escenarios militares de interés.

Después de esta interesante demostración se trabajo muy fuerte en la finalización de los protocolos TCP/IP. ARPANET se convirtió rápidamente en el backbone de Internet y se utilizo mucho para los experimentos con TCP/IP.

2.3.9 INTERNET SE ESTRUCTURA COMO UNA ORGANIZACIÓN

A fines de 1978, los militares empezaron a interesarse en la tecnología de Internet. Para estas fechas la popularidad del correo electrónico en ARPANET había crecido

[16] Cerf Vinton, How the Internet Came to Be, Publicado Electronicamente

enormemente. En 1979 se distribuyeron sistemas de radiotransmisión en Fort Bragg. Los sistemas satelitales se extendieron para incluir estaciones terrenas en varias partes del mundo. Y se desarrollaron más implementaciones de TCP/IP para los sistemas que no estaban cubiertos.

Mientras tanto en DARPA Vinton Cerf en 1979 establecía la Internet Configuration Control Board (ICCB) presidida por David Clark de MIT con el fin de asistir a DARPA en la planeación y ejecución en la evolución de la suite de protocolos TCP/IP. Este grupo incluía muchos de los investigadores líderes que habían contribuido al desarrollo de TCP/IP.

2.3.10 USENET

En 1979, se estableció USENET (User's Network, Red del Usuario), uno de los primeros sistemas distribuidos de conferencia (grupos de discusión). USENET utiliza uucp para transportar noticias.[17]

USENET se desarrollo a partir de una serie de programas escritos por Steve Bellovin, estudiante graduado de la Universidad del Norte de Carolina (UNC) para automatizar y facilitar las comunicaciones uucp entre UNC y la Universidad de Duke. Estos programas fueron posteriormente reescritos por Steve Daniel y Tom Truscott en el lenguaje de programación C. El experimento utilizo a USENET como una versión computarizada de un tablero de mensajes, el cual permite la colocación de notas, así como la lectura de nuevos mensajes y noticias.

USENET inicialmente sirvió a la comunidad universitaria y, mas tarde a las organizaciones comerciales. A principio de los 80's redes más coordinadas como CSNET y BITNET, empezaron a proveer servicios de red a nivel nacional a las comunidades científicas y académicas. Cabe hacer la aclaración que estas redes originalmente no fueron parte de Internet, pero años mas tarde con conexiones especiales (compuertas) se hizo posible el intercambio de información entre ellas.

[17] Mensajes de correo electrónico relativos a un tema cualquiera

2.3.11 LAS REDES EN EL MUNDO A FINES DE LA DÉCADA DE LOS 70's

A partir de mediados de los 70's empezó la proliferación de las redes de computadoras en todo el mundo, conforme la tecnología avanzaba tanto en software como en hardware (varios fabricantes introdujeron pequeñas minicomputadoras con suficiente poder de cómputo para manejar muchos usuarios) el establecimiento de las redes se fue facilitando. Grandes corporaciones por un lado o gobiernos mediante el financiamiento a universidades promovieron su desarrollo.

Los países europeos no fueron ajenos a este desarrollo, por ejemplo Alemania estableció la red de investigación HMInet en 1974, Francia figuro con la red CYCLADES y Australia con CSIROnet en 1972. En 1975 empezó a operar la Red Europea de Informática.

Las tecnologías vía transmisión de ondas y satelital también se vieron fuertemente desarrolladas por ejemplo, en 1976 empezaba a operar la Packet Radio Network, así como la Atlantic Packet Satellite Network (SATNET).

En 1977 Tymshare pone en servicio Tymnet y Nueva Zelanda DSIRnet; en 1978 Francia establece TRANSPAC, y Australia ACSnet (La Red Australiana en Ciencias de la Computacion).

2.4 LA DÉCADA DE LOS 80's

2.4.1 EMPIEZA A FIGURAR LA FUNDACIÓN NACIONAL PARA LA CIENCIA

A principio de los 80's, Internet operaba confiablemente, interconectaba instituciones académicas y de investigación. Convencidos de la viabilidad de la red, el ejercito de los E.U. empezó a conectar computadoras a Internet y a usar el software TCP/IP.

En 1981 la Fundación Nacional para la Ciencia (National Science Foundation (NSF)) la agencia federal gubernamental responsable del patrocinio de la investigación y educación en ciencia e ingeniería en E.U., reconoció la importancia del enlace de las

redes de computadoras. Un pequeño grupo de investigadores propuso implementar una red a la NSF. Su meta era hacer una red que pudiera comunicar a todos los investigadores de cómputo de E.U. que no tuvieran acceso a ARPANET. La ausencia de acceso a ARPANET era percibida como una substancial desventaja en la investigación y en el reclutamiento de estudiantes y profesores.

NSF auspicio la construcción de la red CSNET (Computer Science Network, Red de Computadoras de la Ciencia) con la colaboración de algunos científicos en computación, la Universidad de Delaware, la Universidad de Purdue, la Universidad de Wisconsin, la Corporación RAND y BBN. CSNET proporciono principalmente el servicio de correo electrónico entre los científicos.

CSNET utilizo el protocolo Phonenet MMDF para la distribución de correo electrónico basado en líneas telefónicas, en su auge tuvo 200 sitios participante y conexiones internacionales con aproximadamente 15 países.[18]

En este mismo año de 1981, BITNET (Because It's Time Network, Por que este es el tiempo de la redes) era establecida en la Ciudad Universitaria de Nueva York con una conexión a la Universidad de Yale, su objetivo era distribuir correo electrónico y proporcionar herramientas llamadas "listserv" para distribuir información. BITNET adopto originalmente la suite de protocolos RSCS de IBM y su contribución con el correo electrónico hacia ARPANET a través de compuertas fue muy significativo en los 80's. Desde su origen y hasta la actualidad los hosts de BITNET han sido grandes computadoras
(como mainframes IBM o DEC, no PCs ni estaciones de trabajo).

Redes como BITNET, CSNET, USENET y otras fueron importantes, por que, a pesar de que no formaron parte inicialmente de Internet, sus datos serian transportados en el futuro por ésta red, y se convertirían en parte de su expansión.

2.4.2 TCP/IP EL CONJUNTO DE PROTOCOLOS DE INTERNET

En 1982 se crea la Defense Data Network. En este año DCA y DARPA deciden que todos los sistemas en ARPANET dejen de usar NCP para ser sustituido por TCP/IP,

[18] Cerf Vinton, A Brief History of the Internet and Related Networks, Publicado Electronicamente

además el Departamento de Defensa elige a Internet como su sistema primario de comunicación.

Esto llevo a una de las primeras definiciones de un "internet" como un conjunto de redes enlazadas, específicamente aquellas que usan el protocolo TCP/IP, e "Internet" como al conjunto de internets TCP/IP conectadas.

En este año Internet había crecido para albergar más de 200 hosts, a través de E.U. y parte del mundo (cerca de 22 países tenían IMPs, para entonces).[19]

A diferencia de NCP, TCP/IP fue diseñado desde el inicio para proveer capacidades de interconexión de redes de diferentes clases de computadoras y utilizar un amplio arreglo de tecnologías de comunicación como: redes de área local, radio transmisión y enlaces satelitales. Es decir, su éxito (hasta la actualidad) se basa en la habilidad que tiene de enlazar virtualmente cualquier clase de computadora a cualquier otra, aunque sean de diferente tipo, sobre casi cualquier forma concebible de medio de red o tecnología. En el campo de pruebas, TCP/IP demostró una superioridad técnica sobre NCP, y una vez que éstas terminaron se concluyo que TCP/IP era el camino para satisfacer las futuras necesidades de interconexión de redes.

Usando TCP/IP, ya no se requería el uso de software y hardware propietario costoso para construir una red, ni tampoco se limitaba a un modelo particular o marca de computadora.

De acuerdo a la decisión de cambiar de NCP a TCP/IP se estableció una fecha de corte. Y el 1 de Enero de 1983 ARPANET y sus redes militares asociadas dejaban de correr el viejo software de comunicación NCP. Todas las conexiones fueron cambiadas para usar TCP/IP, y cualquier computadora que no lo entendiera, no seria capaz de comunicarse. Esta fecha se considera el inicio "oficial" de Internet.

2.4.3 PERO, QUÉ ES TCP/IP?

TCP/IP es el nombre común para una familia de cerca de 100 protocolos de comunicación de datos usado para organizar computadoras y equipos de comunicación de datos para compartir recursos dentro de redes de computadoras.

[19] Robbins Margaret, Internet Access Essentials, Introducing TCP/IP, pag. 24

Dos protocolos del software Internet destacan particularmente. El Protocolo Internet (IP) y el Protocolo Control de Transmisión (TCP). En discusiones informales, los investigadores identificaban el conjunto de protocolos por las iniciales de estas dos importantes partes.

Cuando un nombre mas formal era necesario para el conjunto de las especificaciones de software, los investigadores usaban el nombre "La Suite de Protocolos TCP/IP de Internet".

TCP es el protocolo responsable de fragmentar los mensajes en paquetes también llamados datagramas, reensamblarlos en el nodo destino, retransmitiendo paquetes que se hayan perdido, y poniéndolos en el orden correcto.

IP es el protocolo responsable de enrutar los paquetes individuales hasta su destino final. Podría parecer que el protocolo TCP hace todo el trabajo, pero aunque es cierto para redes pequeñas, sin embargo en Internet, simplemente llevar un paquete a su destino puede ser un trabajo complejo.

Ya que una transmisión puede requerir que los paquetes crucen a través de diferentes redes de diferentes tecnologías, mantener la pista de las rutas a través de los diversos destinos y manejar las incompatibilidades entre los diferentes medios de transporte se convierte en un trabajo difícil.

2.4.4 INTERNET: UN SISTEMA ABIERTO

Para motivar el uso de la tecnología Internet, DARPA decidió hacer públicos los resultados de la investigación. Siempre que un investigador descubriera una nueva técnica, midiera el desempeño de la red, o extendiera el software TCP/IP, DARPA les solicitaba que documentaran los resultados en un reporte.

Todas las especificaciones necesarias para construir el software TCP/IP, y toda la experiencia en su instalación y uso fueron documentadas. Y DARPA hizo disponibles a cualquier persona estos reportes (RFCs).

La practica de DARPA de publicar las especificaciones de la red fue sorprendente debido a que la mayoría de las compañías comerciales que habían diseñado ciertas tecnologías de red mantenían sus descubrimientos en secreto. Propiciando que los sistemas cerrados o también llamados propietarios predominaran.

Por lo tanto, desde sus inicios el proyecto Internet aspiro a producir un sistema abierto que permitiera que las computadoras de todos los fabricantes se comunicaran. La filosofía de un sistema abierto significo que los investigadores publicaran todos sus descubrimientos acerca de Internet y todas las especificaciones necesarias para construir el software TCP/IP.

2.4.5 1983 UN AÑO DE GRAN DESARROLLO PARA INTERNET

Con el constante crecimiento de ARPANET, la red empezó a ser difícil de manejar, en particular por el creciente aumento de tráfico en la red, debido a esta situación la DCA en 1983 decidió dividir a ARPANET en dos secciones separadas, una para investigación y la otra para la comunicación de los sitios militares. La red de investigación mantuvo el nombre de ARPANET; la parte militar, la cual era un poco más grande, se nombro como la red militar (military network , MILNET) y fue integrada dentro de la Defense Data Network. Las dos redes permanecieron comunicadas gracias a TCP/IP, el cual daba la posibilidad de dirigir el tráfico de una red a otra conforme fuera necesario.

En 1983, un numero importante de desarrollos siguieron a la introducción y amplia difusión de TCP/IP, junto con la adopción del termino Internet en el vocabulario de las redes de computadoras.

2.4.5.1 SERVIDORES DE NOMBRES Y UN SISTEMA DE NOMBRES DE DOMINIO

Las computadoras que se conectan a Internet se denominan anfitriones, las cuales para su identificación dentro de la red, cada una recibe un numero único. Una computadora para comunicarse con otra debe conocer su correspondiente dirección. Este

numero único asignado a la computadora es llamado dirección Internet, normalmente conocido como dirección IP.

La dirección IP consta de 32 bits los cuales están organizados en cuatro grupos de ocho bits traducidos a su equivalente decimal, de tal manera que, por ejemplo, el numero 140.186.81.1 podría ser la dirección IP de algún anfitrión. Cabe recordar que cada paquete enviado a través de la Internet contiene la dirección IP de la computadora a la cual esta siendo enviado.

Esta nomenclatura es utilizada por la computadora pero, para el usuario común y corriente le es difícil memorizar estas direcciones, de tal manera que también se permitió usar nombres alfabéticos para hacer referencia a las computadoras de una red, Internet permite tales nombres.

Desde los inicios de Internet, todos los nombres de los anfitriones y sus direcciones IP asociadas fueron grabadas en un archivo llamado hosts.txt administrado por el Centro de Información de la Red (NIC), el cual lo transmitía vía FTP a cada uno de los nodos. Sí un usuario deseaba hacer conexión con un anfitrión en particular, requería revisar el archivo localizar el nombre y obtener su correspondiente dirección IP. Aunque, apropiado en los inicios de la red cuando había pocos anfitriones, para principios de los años 80's con el crecimiento de la misma, este esquema presentaba las siguientes desventajas:

- En la medida que crecía el numero de anfitriones en Internet también crecía el archivo.
- Cada vez era más difícil distribuir versiones nuevas del archivo a todos los sistemas, debido al ancho de banda que se requería, provocaba que la carga en el host del NIC fuera considerable.
- Era casi imposible mantener actualizado el archivo, debido a la incorporación de nuevos anfitriones.
- Las aplicaciones tendían a ser mas sofisticadas y creaban la necesidad de un servicio de nombres de propósito general.

Para solucionar este problema se implementaron servidores de nombres desarrollados en 1983 en la Universidad de Wisconsin. Y en 1984 se acompletaba el esquema mediante el Sistema de Nombres de Dominio (DNS).

El DNS proporciona un servicio que automáticamente traduce el nombre alfabético del anfitrión con el cual cierta aplicación desea comunicarse, a la dirección numérica IP que le corresponde. Se vale de una base de datos y servidores de nombres distribuidos a través de la red.

Para la correcta operación del DNS, se requiere que los nombres de los anfitriones sigan un formato especial y que consiste en una serie de cadenas alfabéticas separadas por puntos por ejemplo: arachnid.qdeck.com

El nombre anterior se denomina nombre de dominio, y es un nombre jerárquico que se lee de derecha a izquierda, es decir, la palabra mas a la derecha se conoce como el dominio de más alto nivel en este caso com, que significa que se trata de un sitio comercial. La siguiente parte es un subdominio de com, es decir, qdeck y es el nombre de la compañía Quarterdeck Inc. La siguiente parte es un subdominio de qdeck y es el nombre del anfitrión en particular dentro de la compañía, conocido como arachnid.

El DNS usa la arquitectura cliente-servidor, cuando una aplicación necesita traducir el nombre de una computadora a su dirección IP, la aplicación se convierte en un cliente del DNS. Ésta contacta un servidor de nombres de dominio, y le envía el nombre alfabético de un anfitrión. Entonces el servidor busca la respuesta, y regresa la dirección numérica IP correcta.

Este esquema simplifico grandemente el acceso a la red y facilito a los usuarios emplear los recursos tan ampliamente distribuidos dentro de la red.

2.4.5.2 MAS AVANCES EN 1983

La Red de Computadoras de la Ciencia (Computer Science Network (CSNET)) era enlazada a ARPANET, vía una compuerta la cual movia el tráfico (principalmente correo electrónico) entre las dos redes. Esto abrió los recursos por completo a la comunidad académica de computo, y envolvió a una generación entera de profesores y estudiantes que serian el núcleo de la enorme comunidad Internet de hoy en dia.

1983 fue el año en el cual la IBM PC fue lanzada. Esto trajo poder de computo al escritorio y engendro una revolución en el área de las redes que aun continua.

En Europa, se establecia la Red Académica y de Investigación Europea (European Academic and Research Network (EARN)), operando de la misma manera que la red BITNET de los E.U. a la cual también fue enlazada.

En 1983, DARPA al ver el rápido crecimiento de Internet decidió que la ICCB debería tener una estructura más formal y tener más responsabilidad para coordinar la investigación de TCP/IP y el desarrollo de Internet. Por lo cual reemplaza este organismo, estableciendo el Consejo de Actividades de Internet (Internet Activities Board (IAB)).

2.4.5.3 UNIX DISEMINA TCP/IP

Paralelo al desarrollo de Internet, otra tecnología se había desarrollado y en el año de 1983 se encontraban, ésta tecnología se refiere al Sistema Operativo Unix desarrollado en los Laboratorios Bell propiedad de AT&T . A continuación se describe su desarrollo a grandes rasgos:

El año de 1969, Ken Thompson de los Laboratorios Bell Telephone escribe la primera implementación de lo que eventualmente se convirtió en el sistema operativo Unix. En esta época los fabricantes de computadoras vendían sistemas operativos propietarios para cada una de sus computadoras, escritos en lenguaje ensamblador. Debido a que los Laboratorios Bell usaban una gran variedad de computadoras, los investigadores pensaron hacer el sistema más general (portable a cualquier máquina). En 1973 Dennis Ritchie y Ken Thompson reescriben el sistema operativo en el lenguaje de programación C, y Unix se convirtia en el primer sistema operativo en ser implementado en un lenguaje de alto nivel dándole portabilidad.

Los laboratorios Bell permitieron a las universidades que obtuvieran copias del sistema Unix para ser utilizado en la enseñanza y la investigación. Debido al interés de medir la portabilidad del sistema en el año de 1974, AT&T empezó a licenciar el sistema a bajo costo a universidades proporcionando el código fuente.

Una de estas copias llego a la Universidad de California en Berkeley, y en 1975 Ken Thompson (quien realizaba un curso sabático) junto con una serie de estudiantes empezaron a hacerle una serie de mejoras al sistema. Le agregaron nuevas

características y experimentaron con programas que trabajaran en una red local. Para hacer el trabajo disponible a otras universidades Berkeley distribuyo el código fuente a cualquiera que tuviera una licencia para manejar el código fuente de Unix de AT&T. La versión del sistema Unix de Berkeley, se denomino como BSD UNIX (Berkeley Software Distribution UNIX). El BSD UNIX fue muy aceptado en muchas universidades de los E.U.

Para 1983, DARPA con el fin motivar a los investigadores universitarios en adoptar y usar la suite de protocolos TCP/IP, hizo una implementación a bajo costo, se dio cuenta que BSD alcanzaba muchas universidades y decidió utilizarlo para diseminar el software Internet. Negociaron un contrato de investigación con Berkeley, en el cual DARPA daba a los investigadores en Berkeley una copia del software TCP/IP que había sido desarrollado como parte del proyecto Internet y Berkeley incorporaba el software en su versión del sistema operativo Unix y modificaba los programas de aplicación para que usaran TCP/IP.

Fue así como TCP/IP se incorporo al BSD UNIX release 4.2, y vendedores de estaciones de trabajo como Sun y Apollo empezaron a entregar máquinas para escritorio basadas en Unix alrededor de E.U. y el mundo, la mayoría de las cuales incluían capacidades de red basadas en TCP/IP.

El TCP/IP llego en un momento particularmente significativo, ya que empezaba la proliferación de las tecnologías de redes de área local, es decir, muchas instituciones empezaban a adquirir su segunda o tercer computadora las cuales conectaban en red. Las instituciones necesitaban protocolos de comunicación y no había otro software disponible.

El BSD UNIX fue muy popular debido a que, ofrecía más que los protocolos básicos TCP/IP. Además de los programas de aplicación estándar de TCP/IP, Berkeley ofrecía un conjunto de utilerías para servicios de red y el software conocido como socket que permitía a los programas de aplicación accesar los protocolos de comunicación.

En este punto, el enfoque de conexión a Internet cambio, ya que la necesidad de interconectar grandes sistemas de tiempo compartido en sitios ampliamente distribuidos, se derivaba a la interconexión de redes locales compuestas de múltiples máquinas por sitio.

2.4.6 EL BACKBONE NSFNET

Del año de 1983 a 1985 se produjo un periodo de consolidación para Internet. Los protocolos TCP/IP fueron ampliamente implementados.

En 1984 casi se duplicaba el numero de computadoras instaladas con respecto al año anterior (1983 500 hosts, 1984 ~1000 host)[20] Otras dependencias gubernamentales diferentes a DARPA empezaron a construir sus propias redes usando los mismos protocolos de comunicación que ARPANET utilizaba. Entre estas nuevas redes la mas importante fue la NSFNET, patrocinada por la Fundación Nacional para la Ciencia (National Science Foundation (NSF)).

A mediados de los años 80's la NSF contaba con cinco centros de supercomputo distribuidos en todo el país. Por lo tanto hasta esta fecha, las computadoras mas rápidas habían estado disponibles únicamente para los desarrolladores de armamento y para pocos investigadores de las grandes corporaciones. Preocupada la NSF en que los investigadores, académicos y científicos contaran con este tipo de recursos, fue como decidió crear estos centros de supercomputo, pero debido a su alto costo solamente pudieron construir cinco.

Este esquema presentaba ciertas desventajas, ya que cualquier investigador requería trasladarse físicamente al centro de supercomputo mas "cercano". Para solucionar esta situación la NSF decidió enlazar los cinco centros de supercomputo para compartir sus recursos de una manera más fácil, ahora mediante este esquema el investigador solamente tenia que enviar sus datos y programas mediante un enlace con las supercomputadoras, esperar su proceso y recibir los resultados de regreso.

Esto creo un problema técnico de comunicación, ya que se necesitaba una forma de conectar los centros de supercomputo y permitir a los usuarios accesarlos. Al principio, la NSF trato de usar ARPANET para comunicarlos, pero esta estrategia fallo debido a que los administradores de ARPANET (específicamente la DCA) se negaron a proporcionar las conexiones con estos centros de supercomputo, citando una ya abrumadora carga de trabajo para la red y a un deseo de limitar sus actividades mas estrictamente a necesidades gubernamentales y de defensa.

[20] Hobbes Zakon Robert, Hobbe's Internet Timeline v2.4a, Publicado Electronicamente

En respuesta la NSF en 1986 decidió construir su propia red basada en la tecnología TCP/IP, enlazando sus cinco centros de supercomputo siendo éstos: el Centro de Supercomputo John von Newman (JvNC), en Princeton NJ; el Centro de Supercomputo de Pittsburgh (PSC); el Centro Nacional para Aplicaciones de Supercomputo (NCSA), en la Universidad de Illinois en Urbana-Champaing; el Centro de Supercomputo de San Diego (SDSC), y el Centro Teórico Cornell; además del Centro Nacional para la Investigación Atmosférica (NCAR).

Como resultado se obtuvo el Backbone denominado NSFNET, el cual utilizaba líneas telefónicas de 56 kbps (esto equivale aproximadamente a transferir dos páginas completas de texto por segundo. Aunque lenta para los estándares modernos, esta velocidad era razonablemente rápida a mediados de los 80's). En cada uno de los sitios se utilizaron las minicomputadoras DEC LSI-11 como ruteadores y corrían el software conocido como "Fuzzball"[21]. Desarrollado por Dave Mills de la Universidad de Delaware, cada fuzzball accesaba a las computadoras en los centro de supercomputo usando una interface convencional Ethernet. Los fuzzballs contenían tablas con las direcciones de los posibles destinos y las utilizaba para direccionar (enrutar) cada paquete hacia su destino.

2.4.7 EL ESQUEMA NSFNET-REDES REGIONALES-REDES DE CAMPUS

Poco tiempo después de la creación de NSFNET, éste se conecto con ARPANET. La conexión primaria entre el backbone NSFNET y el resto de Internet se localizo en la Universidad Carnegie Mellon (CMU), la cual tenía nodos tanto de ARPANET como de NSFNET y operaba mediante el siguiente esquema: cuando un usuario, conectado al backbone NSFNET, enviara trafico hacia un sitio de ARPANET, los paquetes viajarían a través de NSFNET hacia CMU donde el fuzzball los enrutaría hacia ARPANET vía un enlace Ethernet local. Similarmente, el fuzzball entendería que los paquetes provenientes de ARPANET y destinados para NSFNET deberían ser aceptados del Ethernet y enviados a través de NSFNET al sitio apropiado.[22]

Por otro lado, se presentaba el problema, que si la NSF intentaba conectar cada una de las universidades directamente al backbone quebraría, debido al costo del tendido

[21] El origen exacto del termino "fuzzball" a la fecha no es claro
[22] Comer Douglas, Internetworking With TCP/IP, Volume I, The Original NSFNET Backbone, pag. 41

de líneas telefónicas. Por lo cual ideo un esquema de conexión jerárquico de tres niveles, que consistía de redes de "nivel medio" o "regionales", cada una de las cuales cubrían una pequeña área geográfica; y redes de "campus" (redes universitarias) o "acceso". En el modelo jerárquico de la NSF, las redes regionales se enlazarían al backbone NSFNET y las redes de campus a su vez se enlazarían a las redes regionales. Las redes regionales fueron avisadas desde el inicio que su financiamiento sería por un periodo limitado de tiempo, por parte de la NSF, de tal manera que tenían que pensar en el futuro como podrían ser autosuficientes económicamente.

Con este esquema los investigadores en las universidades se podían comunicar con sus colegas en sus campus mediante la red local, pero también lo podían hacer con investigadores fuera de ésta, ya que sus maquinas podían enrutar el trafico, tanto hacia las redes regionales como al backbone.

Esta solución provoco una explosión de conexiones, especialmente por parte de las universidades, al poco tiempo el tráfico de la red se incremento considerablemente hasta el grado que las computadoras que controlaban la red y las líneas telefónicas que las conectaban fueran saturadas. Era necesario aumentar la potencia del backbone NSFNET.

2.4.8 EL SEGUNDO BACKBONE NSFNET

En 1987, la NSF emitía una convocatoria abierta para aquellos grupos que estuvieran interesados en establecer y operar un nuevo backbone NSFNET. Las propuestas de diversas compañías fueron entregadas en Agosto. Y el 24 de Noviembre de 1987, la NSF anunciaba que el ganador era una sociedad constituida por: MERIT Network Inc. una organización que instalaba redes y operaba un red que conectaba escuelas en el estado de Michigan, MCI Inc. una compañía de telefonía de larga distancia , IBM Corporation y el Estado de Michigan; y les otorgaba un contrato por cinco años cuyo vencimiento seria en Octubre de 1992.

La misión de MERIT y sus socios no seria únicamente cubrir los requerimientos inmediatos para mejorar el desempeño de la red, sino que también tendrían que ofrecer

un medio ambiente dinámico donde nuevas tecnologías pudieran ser probadas e implementadas para beneficiar el servicio del backbone.

Los socios prometieron construir un segundo backbone, estableciendo el centro de control y operación de la red en la Universidad de Michigan en Ann Arbor, prometiendo su operación para el siguiente verano. El nuevo backbone tenía que enlazar a los seis centros de supercomputo y a siete redes regionales.

La forma mas fácil de ver la división del trabajo entre los tres grupos era la siguiente: MERIT estaba a cargo de la planeación, y establecimiento de la red; además de ser el centro de operación de la red, IBM contribuyo con máquinas y mano de obra de sus laboratorios de investigación para auxiliar a MERIT a desarrollar, configurar y probar el hardware y software necesario, y MCI un portador de larga distancia proporcionando el ancho de banda de comunicación mediante el uso de fibra óptica ya instalada para su red de voz.

En este año de 1987 Internet rompia la barrera de los 10,000 hosts y aparecía el documento RFC numero 1,000 editado por J. Postel y J. Reynolds titulado "Guía de Referencia de RFC"[23]

Para Julio de 1988, el hardware estaba instalado y NSFNET empezó a usar su segundo backbone corriendo a una velocidad de 1.544 Mbps (el equivalente de 50 paginas de texto por segundo) conectando 13 sitios: MERIT, BARRNet (Bay Area Regional Research Network), NCAR (National Center for Atmospheric Research), MIDnet, Westnet, NorthWestNet, SESQUINET, SURAnet y los cinco centros de supercomputo. Dos redes regionales, NYSERNet y JVNCnet, fueron también servidas por el backbone, debido a que cada una de ellas estaban colocadas dentro de un centro de supercomputo.

La tecnología elegida para el segundo backbone fue interesante. En esencia el backbone era una red de área amplia compuesta de ruteadores basados en la tecnología IBM RT, interconectados por líneas telefónicas que manejaban velocidades de transmisión de 1.544 Mbps (conocidos como circuitos T1, por cierto proporcionados por MCI). Como en el primer backbone, el ruteador en cada nodo conectaba tanto la red del lugar vía un enlace Ethernet, como las líneas de comunicación que se dirigían a los

[23] Hobbes, op. cit.

demás nodos. Poco después, el primer backbone NSFNET fue dado de baja y desconectado.

2.4.9 INTERNET ES ATACADO POR UN VIRUS

En el año de 1988, sucede un echo singular en la historia de Internet, el 1 de Noviembre es atacada la red por un virus llamado "gusano", afectando aproximadamente a 6,000 de los 60,000 hosts instalados.

Robert T. Morris un estudiante graduado en ciencias de la computación fue el autor de un programa autoreplicante (genera copias de si mismo) y autopropagable, que provocaba que las computadoras de aquellos sitios que corrían cierta variación del sistema operativo Unix se "congelaran". Por primera vez, una parte de la red se "rompía", muchas computadoras fueron afectadas en lugares como universidades y sitios militares. El programa se aprovecho de un error del programa sendmail y el comando finger del sistema Unix. Gente de la Universidad de California en Berkeley y MIT obtuvieron copias del programa y lo desensamblaron (regresarlo a su formato fuente) para determinar como funcionaba. Equipos de programadores trabajaron hasta encontrar una solución y prevenir su propagación. Después de 12 horas, el equipo en Berkeley encontró un método que ayudaría a retardar la propagación del virus. Otro método fue también descubierto en Purdue siendo ampliamente publicado. Morris fue acusado de infringir la Ley de fraude y abuso en cómputo, siendo sentenciado a tres años de libertad condicional, 400 horas de servicio a la comunidad y una fianza de 10,050 dólares. Su apelación, presentada en Diciembre de 1990 fue rechazada en Marzo siguiente.[24]

Uno punto interesante de este hecho, fue que Internet sobrevivió a este ataque debido a su diversidad tanto en hardware como en software. Es decir, no todas las redes que comprenden Internet, por ejemplo, fueron vendidas por un solo fabricante, no todas corren el mismo sistema operativo, y además éstas corren diferentes implementaciones de los protocolos TCP/IP.

Derivado de este suceso DARPA creo El Equipo de Respuesta en Emergencias de Computo (Computer Emergency Response Team (CERT)).

[24] P. Kehoe Brendan, Zen and The Art of Internet, The Internet Worm, pag. 63

Por otro lado, en este año de 1988 Jarkko Oikarinen en Finlandia desarrolla el servicio Internet Relay Chat (IRC), el cual permite tener un "conversación" en línea entre usuarios de la red. Este servicio le permite a un grupo de usuarios comunicarse a través de la red usando un teclado. Cada grupo crea un canal al cual envía mensajes, y cada participante activo para un canal dado recibe una copia del mensaje enviado pudiendo contestar entablando una "conversación".

2.4.10 NSFNET SUPERA A ARPANET

Como consecuencia del mejor desempeño del backbone de la NSF con respecto al de ARPANET, muchas instituciones empezaron a cambiarse hacia NSFNET, además de que los nuevos países que se agregaban a Internet lo hacían también, conectándose a éste backbone. Países como Canadá, Dinamarca, Finlandia, Francia, Islandia, Noruega y Suecia se enlazaban a NSFNET en el año de 1988, así como las primeras redes regionales canadienses: Onet vía Cornell, RISQ vía Princeton y Bcnet vía la Universidad de Washington.

Después de medir el tráfico de NSFNET por un año, en 1989 el centro de operaciones reconfiguro la red agregando alguno circuitos T1 y quitando otros. Para entonces, la carga de tráfico en el backbone se había incrementado a cerca de 500 millones de paquetes por mes, representando un 500% de incremento en un solo año. Cada siete meses, el tráfico en el backbone se estaba duplicando, y esta tasa de crecimiento exponencial estaba creando enormes retos para el equipo de la NSF.[25]

Este crecimiento exponencial en el tráfico era una consecuencia directa del numero de hosts que se estaban agregando a la red, ya que de los 10,000 hosts que se tenía en el año de 1987 para 1989 se rompía la impresionante cantidad de 100,000 hosts instalados[26]

En el año de 1989, en Europa se crea RIPE (Reseaux IP Europeens, Redes IP Europeas) formada por proveedores de servicio de red europeos, con el fin de tener una

[25] R. Harris Susan y Gerich Elise, Retiring the NSFNET Backbone Service: Chronicling the End of an Era, Publicado Electronicamente

[26] Robbins Margaret, Internet Access Essentials, The National Science Foundation, And Acceptable Usage, pag. 27

coordinación administrativa y técnica, que permitiera la comunicación de todas las redes IP europeas.

Se forma también la Corporación para la Investigación y la Educación en Redes (Corporation for Research and Education Networking (CREN)) con la unión de CSNET dentro de BITNET.

2.4.11 IAB, IETF E IRTF

Como se menciono en apartados arriba el Consejo de Actividades de Internet (Internet Activities Board (IAB)), es el consejo coordinador para el diseño, manejo e ingeniería de Internet. Está dirigida por un presidente por un lapso de dos años y es elegido por sus propios miembros. El IAB se enfoca en la evolución de la suite de protocolos TCP/IP y las extensiones del sistema Internet para soportar múltiples suites de protocolos. El IAB desempeña las siguientes funciones:[27]

1) Establece los estándares para Internet
2) Maneja el proceso de la publicación de los RFCs
3) Supervisa la operación del IEFT y IRTF
4). Ejecutar la planeación estratégica para Internet, identificando problemas y oportunidades
5) Resuelve las situaciones técnicas que no pueden ser tratadas dentro del IEFT o IRTF.

En el año de 1989, la IAB crea la Fuerza de Trabajo de Ingeniería de Internet (Internet Engineering Task Force (IETF)) y la Fuerza de Trabajo de Investigación de Internet (Internet Research Task Force (IRTF)).

Cada una de estas fuerzas de trabajo es dirigida por un presidente y guiada por un Grupo Coordinador el cual reporta a IAB a través de su presidente. A su vez, cada una de las fuerzas de trabajo se dividen en grupos de investigadores o grupos de trabajo los cuales llevan a cabo los programas.

Todas las decisiones del IAB son hechas publicas a través los RFCs.

[27] G. Malkin y A.Marine. RFC 1206: Answers to Commonly asked "New Internet Users" Questions, What is the IAB? , pag. 9

2.4.11.1 IETF

En 1989, Internet había crecido para agrupar un gran numero de redes geográficamente dispersas en comunidades académicas y de investigación. Proporcionaba una infraestructura para una amplia comunidad con intereses variados. Además, la familia de protocolos de Internet y los componentes del sistema se habían movido del desarrollo experimental al desarrollo comercial. Para ayudar a coordinar la operación, manejo y evolución de Internet, el IAB estableció la IETF.

El IETF es una gran comunidad abierta de diseñadores de redes, operadores, vendedores, e investigadores relacionados con Internet y sus protocolos. Tiene la responsabilidad de la evolución de TCP/IP y la integración de otros protocolos dentro de la operación de Internet (por ejemplo, los protocolos de Interconexión de Sistemas Abiertos (OSI)).

2.4.11.2 IRTF

Para promover la investigación en el campo de las redes de computadoras y el desarrollo de nueva tecnología, el IAB estableció la IRTF. La IRTF es una comunidad de investigadores de redes, generalmente con un enfoque hacia Internet.

2.4.12 INTERNET Y SU USO COMERCIAL

En 1989, se efectuaban las primeras transmisiones entre portadores comerciales de correo electrónico e Internet. MCI Mail intercambiaba correo a través de la Corporación Nacional de Iniciativas de Investigación (CNRI) y Compuserve lo hacía a través de la Universidad Estatal de Ohio. Este fue el primer uso comercial de Internet.

En el mismo tenor, las redes regionales también empezaron a aceptar clientes comerciales, en un esfuerzo por convertirse económicamente autosuficientes.

En este año los paises que se conectan a NSFNET fueron: Australia, Alemania, Israel, Italia, Japón, México, Holanda, Nueva Zelanda, Puerto Rico, y el Reino Unido.

2.5 LA DÉCADA DE LOS 90's

2.5.1 ANSNET: UN BACKBONE MAS RÁPIDO PARA INTERNET

La nueva velocidad y capacidad del backbone de la NSF motivo nuevos e innovativos usos de la red para la investigación y la educación. Un gran salto intelectual ocurrió cuando la gente se dio cuenta de que la red podía ser usada no solamente para la transferencia de datos entre las computadoras. La popularidad del correo electrónico y otras formas de colaboración, así como el cómputo remoto, provocaron un incremento del trafico en la red del 15% mensual.

Para manejar la tasa de crecimiento exponencial del tráfico, MERIT y sus socios introdujeron un plan para actualizar el servicio del backbone, para que operara a una velocidad de 45 Mbps. La NSF también propuso incrementar el número de nodos de 13 a 16, incluyendo Cambridge con NEARNET, el Laboratorio Nacional Argonne de Chicago y Atlanta con SURAnet.[28]

A fines de Mayo de 1990, el acuerdo de MERIT y sus socios con NSF fue modificado para cubrir este trabajo adicional.

En Junio de 1990, el backbone ARPANET dejaba de funcionar como tal, habiendo sido rebasado y reemplazado por el backbone NSFNET, con un bien desarrollado conjunto de redes regionales y metropolitanas.

Para fines de 1990, la NSF y otras agencias gubernamentales se dieron cuenta que Internet estaba creciendo mas allá de su dominio académico y científico. Mas compañías nuevas de todo el mundo seguían conectándose a Internet y el uso no referente a la investigación se incrementaba rápidamente. El trafico sobre NSFNET crecia cada vez más y la capacidad de 1.5 Mbps se estaba volviendo insuficiente para algunos circuitos. Un mayor ancho de banda era necesario, ya que el backbone NSFNET alcanzaría rápidamente su máxima capacidad. La NSF también se dio cuenta que el gobierno federal no podria tener recursos para auspiciar indefinidamente a Internet.

[28] R. Harris Susan y Gerich Elise, op. cit.

Como resultado, el gobierno de E.U. empezó una política de comercialización y privatización. NSF decidió mover el backbone a una compañía privada y comenzar a hacer cargos a las instituciones por las conexiones.[29]

Respondiendo a la nueva política del gobierno en Septiembre de 1990, IBM, MERIT y MCI formaban una compañía no lucrativa llamada Red Avanzada y Servicios (Advanced Network and Services (ANS)). ANS empezó a proporcionar servicios para NSFNET como un subcontratista de MERIT, con IBM, MCI.

ANS propuso construir un backbone mas rápido para Internet (a una velocidad de 45 Mbps conocida como T3). A diferencia de las redes de cobertura amplia anteriores usadas en Internet las cuales habían sido propiedad del gobierno de los E.U., ANS sería el dueño del nuevo backbone denominándolo ANSNET.

Para fin de año, MERIT, SDSC, y NCSA eran conectados a un primer servicio T3 y empezaban las pruebas de nuevos ruteadores con tráfico real. Además, una red T3 de prueba era implementada para hacer un paralelo a la existencia de la red T1.

Cambios importantes en arquitectura y equipo vinieron con la nueva red T3. El corazón del equipo del backbone fue movido de las universidades y los centros de supercomputo a puntos de presencia[30] pertenecientes a MCI, y los ruteadores IBM RT usados en la red T1 eran reemplazados por ruteadores IBM RS/6000. Muchas de las técnicas introducidas en los ruteadores RS/6000 han sido adoptadas por vendedores comerciales de este tipo de equipo.

2.5.2 LA NSF Y SU POLÍTICA DE USO ACEPTABLE DE LA RED

Desde mediados de los años 80's, el asunto del "uso aceptable" o "uso apropiado" de las instalaciones de Internet había sido un asunto delicado.

Al principio, sólo se permitía usar la red por aquellas organizaciones que contribuyeran al desarrollo y despliegue de Internet, típicamente con situaciones que se relacionaran con la defensa de los E.U., así como con la investigación.

[29] Comer Douglas, Internetworking With TCP/IP, Volume I, ANSNET, pag. 44
[30] Lugar donde existe un gran colección de equipo de telecomunicaciones, usualmente líneas telefónicas y ruteadores multiprotocolos.

En 1990 la NSF publico una guía con la "Política de Uso Aceptable" del backbone NSFNET. Este programa permitía a cualquier colegio o universidad de los E.U. conectarse con la NSFNET; pero las actividades comerciales, como publicidad, o el envío de trafico relacionado con un propósito lucrativo no era permitido.

El papel de la NSF sobre el backbone ayudo a clarificar el problema, ya que ésta establece que su rol es apoyar las actividades de investigación y educación en los E.U., por lo tanto el trafico que circulara sobre NSFNET tenia que estar relacionado con estos temas.

Este anuncio fue significativo por que ninguna restricción era establecida a aquel que se conectara mientras respetara la política de uso. Generalmente bajo esta política, cualquier uso que resaltara la educación o las metas de la comunidad investigadora era permitido. También, los usuarios podían usar NSFNET para intercambiar correo con compañías comerciales así como recibir servicios y productos electrónicamente. Sin embargo, para las compañías lucrativas estaba prohibido usar el backbone para publicitarse o mantener otros propósitos con carácter comercial.

2.5.3 ALGUNOS SERVICIOS DE INTERNET

En 1990, aparece Archie desarrollado por Peter Deutsch, Alan Emtage, y Bill Heelan en la Universidad McGill en Canadá. Archie es un servicio de búsqueda automático de archivos disponible en Internet. El usuario le proporciona el nombre del archivo y Archie proporciona la(s) direccion(es) de los anfitriones donde se localiza. El nombre Archie se deriva de la palabra archive (archivo).

También en 1990, la utilería Hytelnet es distribuida por Peter Scott de la Universidad de Saskatchewan en Canadá. Hytelnet es un programa de Hipertexto[31] diseñado para asistir al usuario en la consulta a catálogos, sistemas de información de universidades, servicios de boletines electrónicos, bases de datos, etc.; mediante el uso de Telnet.

En Noviembre del mismo año, producto de un proyecto de hipertexto iniciado en Marzo de 1989 se obtiene el primer prototipo de una herramienta que provocaría mas

[31] Sistema de almacenamiento de paginas de texto que contienen referencias (conexiones) a otras paginas de información, tambien de texto.

adelante una explosión aun mayor de conexiones a Internet: el World Wide Web desarrollado por Tim Berners-Lee en el Laboratorio Europeo de Física de Partículas, ubicado en Ginebra Suiza y mejor conocido como CERN por sus siglas en francés.

Por otro lado, se empiezan a formar los primeros backbones nacionales, como el CA*net el backbone canadiense constituido por 10 redes regionales con conexión directa a NSFNET.

Los países que se incorporaron a NSFNET en este año fueron: Argentina, Austria, Bélgica, Brasil, Chile, Grecia, India, Irlanda, Corea del Sur, España y Suiza.

2.5.4 ANSNET REEMPLAZA A NSFNET

Durante 1991, después de un año de refinar la tecnología del backbone, las redes T1 (NSFNET) y T3 (ANSnet) trabajaban en paralelo. Ciertas dificultades para poner a punto la nueva tecnología evitaron a la red moverla a su total producción hasta fines de año, cuando los 16 nodos que comprendían NSFNET fueron conectados a la nueva infraestructura nacional T3 ANSnet.

La actualización del servicio del backbone NSFNET a T3 no fue solamente un reto tecnológico y organizacional del mas alto orden. Si no que también precipito una gran necesidad, aunque contenciosa, de un dialogo acerca de la evolución y comercialización de Internet.

2.5.5 INTERNET COMERCIAL

Dado que algunas organizaciones o compañías comerciales deseaban usar Internet para actividades contrarias a la política de uso establecida para NSFNET, el surgulmiento de una implementacion cien por ciento comercial de un Internet era inevitable.

Desde años anteriores, proveedores comerciales con servicios similares a los que proporcionaba Internet estuvieron surgiendo a través de todo E.U., desde proveedores

locales hasta grandes compañías que proporcionaban servicios T1 y eventualmente servicios T3, así como servicios y productos TCP/IP.

De esta forma en 1991, se formo la asociación de Intercambio Comercial de Internet (Commercial Internet Exchange (CIX)), la cual es una asociación "no lucrativa" de proveedores comerciales de servicios de enlace de redes. Formada con la cooperación de un gran numero de proveedores de servicio internet, para establecer claramente el uso legitimo de negocios dentro de Internet. CIX tuvo interconexiones con las redes regionales, cada uno de los miembros de CIX transportaban el trafico de los demás miembros de la asociación sin cargo alguno. Con el surguimiento de CIX, todos los miembros que la formaban estuvieron tranquilos que ninguna restricción seria establecida en el tipo de trafico entre las redes miembro. Así, no hubo temor de violar la política de uso aceptable de la red, la cual prohibía la circulación de trafico con carácter comercial.

Esta organización se formo con la unión de CERFnet de General Atomics, PSInet de Performance Systems International y AlterNet de UUNET Technologies, constituyendo una extensión de Internet que estaba disponible a cualquiera que pudiera pagar el equipo necesario y los cargos de uso.

2.5.6 BUSCANDO EN INTERNET

En 1991, Internet obtuvo otro gran avance de diferente tipo con la distribución de dos tecnologías, llamadas WAIS y Gopher. El primero, el Servidor de Información de Área Amplia (Wide Area Information Server (WAIS)), inventado por Brewster Kahle y distribuido por Thinking Machines Co., proporciona un servicio de búsqueda automática en Internet, examinando el contenido de los documentos en la red, permitiendo a los usuarios accesar fácilmente bases de datos de todo el mundo proporcionando palabras simples.

El segundo, Gopher, fue un programa de búsqueda desarrollado por Paul Linder y Mark P. McCahill en la Universidad de Minnesota diseñado para permitir el acceso a los usuarios a muchas de las fuentes de información de Internet en una forma simple y consistente. Usar Gopher es tan simple como hacer selecciones desde un menú.

Estas herramientas representaron un paso adelante en el mejoramiento del uso de la información disponible en Internet, haciéndola accesible a usuarios casuales.

En Marzo de 1991, CERN distribuía la primera versión en modo de línea (no gráfica) del WWW limitada a algunos modelos de máquinas. Y el 12 de Junio en un seminario hablaba sobre la tecnología WWW.

En este año el trafico sobre el backbone pasa la gran cantidad de los 10 billones de paquetes por mes.[32]

Los países que se conectaban a Internet eran: Croacia, La República Checa, Hong Kong, Hungría, Polonia, Portugal, Singapur, Sudáfrica, Taiwan y Túnez. Rompiendo el numero de 600,000 hosts en Internet.

2.5.7 LA SOCIEDAD INTERNET

En 1992, Internet rompía la marca del millón de hosts instalados alrededor de muchos países del mundo.[33] Ya que Internet se había movido fuera de sus raíces gubernamentales estadounidenses, una sociedad se formo para fomentar la participación en él. Llamada la Sociedad Internet (Internet Society (ISOC)), el grupo es una organización internacional inspirada por la National Geographic Society. La sociedad Internet fue formada como una organización profesional internacional para promover la evolución y uso de la tecnología Internet a través de todo el mundo, estandarizacion, etc. La sociedad actualmente publica bimestralmente On the Internet y patrocina las reuniones internacionales sobre Internet.

En este año las obligaciones de IAB (Internet Activities Board) y su interacción con otros grupos fue reorganizada nuevamente, de hecho en esta segunda reorganización que sufría, la IAB mantenia el mismo acrónimo pero cambiaba su nombre al de Internet Architecture Board (Consejo de Arquitectura de Internet). Además pasaba a formar parte de la Sociedad Internet. La IAB se despojo de algunas de sus responsabilidades técnicas, pasando mas control a grupos subordinados, y dejando el consejo como el último arbitro para las políticas y estándares.

[32] Hobbes, op. cit.
[33] Robbins Margaret, Internet Access Essentials, Moving into the Present-and Beyond, pag. 29

Para 1992, la amplia difusión y uso de la tecnología Internet fue evidente, desde la cobertura en televisión, periódicos, revistas, así como en el medio informático. Palabras como la Infraestructura Nacional de Información y la Infraestructura Global de Información se convirtieron en parte del lenguaje político, así como de la retórica técnica.

2.5.8 MAS SERVICIOS DE INTERNET

En 1992, se hacia la primera distribución publica del World Wide Web (WWW) para Internet. El WWW es un servicio que organiza la información utilizando hipermedia, es decir, cada documento o página puede contener ligas que hacen referencia a imágenes, audio, texto, o vídeo. Un usuario al estar consultando la información de una página siguiendo las referencias, da la sensación de que esta "navegando" sobre él.

También en este año es distribuido por la Universidad de Nevada la herramienta de búsqueda conocida como veronica (Very Easy Rodent Orient Net-wide Index to Computerized Archives). Es un servicio de búsqueda automático a través de gopher. Veronica permite buscar a través de menús gopher por una cadena de caracteres dada, obteniendo como resultado un menú con el resultado de la búsqueda.

2.5.9 CONVOCATORIA PARA UNA NUEVA ARQUITECTURA DE LA RED

Durante 1992, el Consejo Nacional de La Ciencia autorizo una extensión del acuerdo de cooperación con MERIT por dieciocho meses mas a partir de Octubre, fecha en la cual expiraba el contrato. Con el fin de que la NSF desarrollara una convocatoria para un proyecto nacional de red, que permitiera acomodar el creciente rol de los proveedores comerciales de Internet y permitir a la NSF regresar del papel actual de patrocinador y operador de la red, a su importante misión de apoyo a las iniciativas de investigación y educación en el desarrollo de tecnología de punta.[34]

[34] R. Harris Susan y Gerich Elise, op. cit

NSF publico una convocatoria solicitando diseños iniciales para su comentario por la comunidad investigadora en 1992, y una nueva convocatoria seria editada en Mayo de 1993.

Por lo mientras los países que se agregaban a Internet en 1992 eran: Camerún, Chipre, Ecuador, Estonia, Kuwait, Letonia, Luxemburgo, Malasia, Eslovaquia, Eslovenia, Tailandia y Venezuela.

2.5.10 INTERNIC

La NSF con el fin de proporcionar servicios de información específicos, tanto a la comunidad comercial como a los proveedores de servicios públicos de Internet, así como a una mayor y cada vez mas creciente comunidad de usuarios, hacia publica la licitación para obtener un contrato cuyo objetivo era el de formar el Internet Network Information Center (INTERNIC) (Centro de Información de la Red Internet).

Ya que la tecnología TCP/IP no pertenece a ninguna empresa, sociedad profesional u órgano de estandarizacion, entonces la documentación de los protocolos, estándares, y políticas, obviamente no podían ser obtenidas por parte de ellos. Por lo cual se hacia necesario la formación de un grupo que mantuviera y distribuyera la información relativa acerca de TCP/IP y en general de Internet. De esta forma INTERNIC manejaría muchos detalles administrativos para Internet, así como la distribución de la documentación.

En 1993, la NSF daba a conocer los nombres de las empresas que formarían INTERNIC siendo: AT&T una empresa de telecomunicaciones, la que tomaría el rol de proporcionar servicios de directorio y bases de datos, la empresa Network Solution Inc. estaría a cargo de los servicios de registro de la nuevas redes y también de los servicios de acceso a la información, y por ultimo la empresa General Atomics/CERFNET proporcionaría servicios de información.

2.5.11 MOSAIC

En Febrero de 1993, el Centro Nacional para Aplicaciones de Supercomputo (NCSA) en Illinois, con base en el código de Marc Andreessen distribuía el primer

visualizador gráfico para el WWW conocido como Mosaic. Mosaic dio poder a cualquier usuario para bajar de la red imágenes, texto, sonido, etc.

En este año el numero de anfitriones Internet rebasa los dos millones, incorporándose importantes instituciones y organismos gubernamentales como la Casa Blanca sede del gobierno norteamericano, así como la Organización de la Naciones Unidas[35]. Los países que se agregaron a Internet en este año fueron: Bulgaria, Costa Rica, Egipto, Fiji, Ghana, Guam, Indonesia, Kazajistan, Kenya, Liechtenstein, Perú, Rumania, La Federación Rusa, Turquía, Ucrania, y las Islas Vírgenes.

2.5.12 UNA ARQUITECTURA NUEVA PARA INTERNET

A principios de 1994, y como resultado de la convocatoria de la NSF para un proyecto nacional de red, se proponía la siguiente arquitectura para Internet: que la función del principal backbone de E.U. y de Internet (ANSNET) pasara a la iniciativa privada, es decir, que el trafico ahora circulara a través de las diferentes redes interconectadas de los diferentes proveedores servicios de red; de tal manera que le permitiera a la NSF regresar a patrocinar un backbone de investigación. Es decir, un backbone comercial y un backbone de investigación.

En la nueva arquitectura (backbone comercial) las redes regionales serian desconectadas del backbone, pero por otro lado obtendrían su conectividad interregional a partir de Proveedores de Servicios de Red (Network Service Providers (NSPs)). Los NSPs tendrían las siguientes funciones:

1. Se conectarían a centros llamados Puntos de Acceso a la Red, (Network Access Points (NAPs)), donde el trafico seria intercambiado.
2. Enrutarian y transportarían el trafico a/desde cualquier localidad de investigación
3. Harían las rutas disponibles a un servicio de arbitro de ruteo.

[35] Hobbes, op. cit.

La NSF permanecería enfocada en proporcionar servicios avanzados a la comunidad investigadora e ingenieril. Para este fin, otorgaba un acuerdo de cooperación para proveer servicios de información Internet y un segundo acuerdo para establecer un backbone de muy alta velocidad (very high speed backbone network service (vBNS)) para operar como una red de investigación. El vBNS conectaría los centros de supercomputo y proporcionaría una red con un alto ancho de banda para los investigadores de aplicaciones, y permitirles empujar las barreras de la tecnología de interconexión de redes.

Los contratos (cinco años) para construir la nueva arquitectura fueron dados a MERIT y al Instituto de las Ciencias de la Información (ISI) de la Universidad del Sur de California para el servicio de Arbitro de Ruteo, a MCI para el vBNS, y a tres proveedores para los Puntos de Acceso a la Red: Sprint, MFS Datanet, y Bellcore representando a Ameritech y PacBell. La NSF también otorgaba nuevamente una extensión al contrato previo de MERIT que empezaba en Mayo de 1994 y duraría hasta Abril de 1995, cuando el servicio del backbone ANSNET fuera retirado y todas las conexiones fueran cambiadas al nuevo servicio.

2.5.13 PLAZOS Y COMPROMISOS

Mover el backbone ANSNET a una nueva arquitectura en los meses comprendidos entre Febrero de 1994 (fecha en la cual se nombro a los ganadores de la licitación) y el 30 de Abril de 1995 fue un gran reto para las redes regionales, los proveedores de servicio de Internet y la NSF. Antes de que el backbone pudiera ser dado de baja, cuatro tareas principales se tenían que llevar a cabo para poder hacer el cambio:

- Establecer lo Puntos de Acceso a la Red (NAPs).
- Enlazar a los NAPs el bakbone ANSNET y los proveedores de servicio de Internet que proporcionan servicio a las redes regionales.
- Desarrollar el servicio de Arbitro de Ruteo colocando los servidores de ruteo en los NAPs y establecer un registro de ruteo.

- Mover las redes regionales fuera de ANSNET y enlazarlas a las redes operadas por los proveedores de servicio Internet.

2.5.14 MANTENIENDO EL NUEVO INTERNET JUNTO (NAP Y ARBITRO DE RUTEO)

Los Puntos de Acceso a la Red (NAPs) y los servicios de Arbitro de Ruteo (RA) son los mecanismos por medio de los cuales el vBNS y los proveedores de servicio de red (los cuales transportan el trafico de las redes regionales) serian enlazados. Para asegurarse que Internet permaneciera totalmente interconectada cuando ANSNET dejara de funcionar, la NSF incluyo NAPs y servicios RA en la nueva arquitectura.

Los NAPs actuarían como compuertas para hacer posible que las redes de los proveedores de servicio de red, muchas redes regionales, así como backbones domésticos y extranjeros y el vBNS permanezcan integrados completamente en la ausencia de lo que fue usualmente un backbone, el ANSNET. Los NAPs auspiciados por la NSF se establecerían en: Hayward CA operado por PacBell, Chicago IL, operado por Ameritech, Pennsauken NJ operado por Sprint y Washington DC. operado por Metropolitan Fiber Systems.

Sin embargo, el construir los NAPs y pasar las redes regionales a proveedores de servicios de red comerciales no garantizaba la continuación de una Internet totalmente interconectada. Otro elemento era necesario para esta interconexión total de Internet, siendo éste un adecuado servicio de ruteo para la nueva arquitectura.

Bajo la nueva arquitectura, el servicio de Arbitro de Ruteo, es el responsable de mantener un coherente y consistente política de ruteo a través de Internet vía Servidores de Rutas localizados en los Puntos de Acceso a la Red. El Arbitro de Ruteo mantendrá una base de datos de rutas y manejara el intercambio de rutas entre los NAPs.

Para recibir auspicio por parte de la NSF de acuerdo con la licitación, a las redes regionales se les requería conectarse a un proveedor de servicio de red, el cual a su vez se tendrían que conectar a cada uno de los NAPs. El vBNS debería ser también conectado a cada NAP.

Esta arquitectura física soportaría una completa interconexión e interoperabilidad del nuevo Internet.

2.5.15 CONECTIVIDAD INTERREGIONAL

Así como el viejo backbone NSFNET fue desfasado, el trafico del backbone ANSNET se movería a proveedores comerciales de acceso a Internet. Por lo tanto, una segunda parte de la nueva arquitectura de la red consistía en el apoyo directo a las redes regionales enlazadas a ANSNET para su transición metódica hacia los proveedores de servicio. Los proveedores de servicios de red no serian financiados directamente por NSF, en su lugar, NSF financiaría el enlace de las redes regionales a los proveedores de servicio, con un apoyo económico en una base descendente de cuatro años (tiempo que se considera se haga la transición), para ayudar a la conectividad interregional.

A diferencia del tiempo cuando el viejo NSFNET fue creado, en 1994 había varios proveedores capaces de soportar un servicio a nivel nacional de Internet para las redes regionales.

Al final de los cuatro años del periodo de transición la NSF ya no financiara a ninguna red regional, con excepción del vBNS y el RA. La NSF continuara auspiciando a instituciones merecedoras de acceso a Internet, bajo el programa Nuevas Conexiones, pero la NSF ya no estará en el negocio de construir y mantener backbones.

2.5.16 EL BACKBONE DE MUY ALTA VELOCIDAD (vBNS)

La nueva arquitectura de Internet incluye el servicio de un backbone de muy alta velocidad o vBNS por sus siglas en inglés.

El vBNS proporcionara una red experimental de un gran ancho de banda para investigar aplicaciones y estará abierta a organizaciones que requieran altas velocidades para sus aplicaciones tales como el cómputo científico. Este backbone desarrollara tecnología y aplicaciones que se espera beneficien a los usuarios de Internet. El vBNS únicamente estará disponible para investigación y no será utilizado para el trafico general de Internet.

El vBNS inicialmente proporcionara una interconexión de alta velocidad entre los centros de supercomputo de la NSF y las conexiones a los Puntos de Acceso a la Red (NAPs), es una plataforma experimental para el desarrollo de servicios para Internet y equipo para el futuro.

El vBNS operara inicialmente a una velocidad de transmisión de 155 Mbps, y está proyectado como un recurso único para los investigadores en redes y aplicaciones de E.U. con el fin de explorar su desempeño con las nuevas tecnologías. El vBNS conecta cinco centros de supercomputo: el Centro de Supercomputo de Pittsburgh (PSC); el Centro Nacional para Aplicaciones de Supercomputo (NCSA), el Centro de Supercomputo de San Diego (SDSC), y el Centro Teórico Cornell; además del Centro Nacional para la Investigación Atmosférica (NCAR). También se conecta los Puntos de Acceso a la Red auspiciados por la NSF.

2.5.17 EL WWW CRECE

Debido a la interfaz gráfica (Mosaic) y la habilidad para desplegar imágenes y vídeo, reproducir sonidos, y el poder obtener toda esta información, el crecimiento del World Wide Web hasta la fecha ha sido extraordinario. Simplemente en Diciembre de 1993 el WWW estaba colocado en el lugar numero 11 de todos los servicios de la red, en términos del total del trafico, siendo que 12 meses antes, estaba colocado en el numero 127. En 1994 poco a poco el WWW alcanzo a Telnet para convertirse en el segundo servicio mas popular de la Red detrás de FTP, resultado basado en el porcentaje de paquetes y bytes transmitidos sobre ANSNET.[36]

Esta tasa de crecimiento exponencial es increíble, ya que la empresa Network Solucions Inc. reportaba que mantenía un registro de nombres de dominio a un ritmo de 2000 por mes, trayendo como consecuencia que para Junio se rompiera la marca de los tres millones de anfitriones en Internet y se tuviera un trafico de diez trillones de bytes por mes.[37]

[36] Ibid
[37] Ibid

Esta tendencia trajo como consecuencia que la NSF recomendara moverse a un esquema en el cual se cobrara el registro de los nombres de dominio tan rápido como fuera posible.

Los países que se agregaron a Internet en 1994 fueron: Argelia, Armenia, Bermuda, Burkina Faso, China, Francia, Polinesia, Jamaica, Líbano, Lituania, Macao, Marruecos, Nueva Caledonia, Nicaragua, Níger, Panamá, Filipinas, Senegal, Sri Lanka, Suazilandia, Uruguay, y Uzbekistan.

2.5.18 EL INTERNET DE MEDIADOS DE LA DÉCADA DE LOS 90's

En Marzo de 1995, Internet registra el host numero 4,000,000 y el trafico del WWW viene a rebasar el trafico manejado por el protocolo FTP, así el Web se pone a la cabeza en Internet con la mayor cantidad de trafico transportado.[38]

El 30 de Abril, deja de operar el backbone ANSNET operado por MERIT Network Inc. para ser reemplazado por la nueva arquitectura. La nueva arquitectura permitirá a la NSF enfocarse en su misión primaria de promover la investigación científica y la educación en E.U. Pasando el manejo operacional del backbone a otros la NSF perseguirá mas activamente la tecnología de punta relativa a las redes de computadoras.

Por otro lado en este año de 1995, los servicios tradicionales en línea como Compuserve, America Online, Prodigy, etc.; empiezan a proporcionar acceso a Internet como parte de algunos de sus servicios. Se manifiesta un gran desarrollo en las herramientas gráficas para "navegar" en Internet como: Netscape, Explorer, Mosaic, Emisary, etc.

El registro tradicional de nombres de dominio hasta antes del 14 de Septiembre de 1995 había sido gratuito, a partir de esta fecha la NSF y la empresa encargada del registro de nuevos dominios (Network Solutions Inc.) anuncian que este registro ahora requerirá de un cargo. De acuerdo con el nuevo plan los nuevos integrantes de la red deberán pagar una cuota de 50 dólares anuales y también las organizaciones registradas antes de esta fecha deberán de pagar esta cuota en el aniversario de su registro inicial.

[38] Ibid

El Vaticano y el gobierno Canadiense tienen presencia en este año en Internet, se nombra al WWW y a las máquinas de búsqueda en Internet como las tecnologías del año, y a su vez empiezan a emerger nuevas tecnologías como: JAVA, JAVAscript, los medios ambientes virtuales (Virtual Reality Modeling Language (VRML)), Intranets, las suites para navegar en Internet , mecanismos de seguridad (firewalls) y las herramientas de colaboración.

El 15 de Abril de 1996, MCI actualiza el vBNS de una capacidad de 45Mbps a 155Mbps.

CAPITULO III

TCP/IP: LOS PROTOCOLOS DE INTERNET

3.1 INTRODUCCIÓN

Internet al ser una red virtual (una red constituida por una gran cantidad de redes heterogéneas distribuidas en todo el mundo) requiere de un mecanismo adecuado para llevar a cabo la correcta comunicación entre los diversos nodos que la conforman. Para cumplir con este fin Internet se basa en dos elementos fundamentales, a saber desde el punto de vista de hardware, la interconexión física de las redes se realiza por medio de los ruteadores y desde el punto de vista de software el otro elemento lo constituye la familia de protocolos TCP/IP.

El presente capitulo tiene como objetivo presentar como interactuan estos dos grandes elementos que hacen posible el funcionamiento de Internet. En otras palabras, es presentar como trabajan e interactuan los principales protocolos TCP/IP en conjunto con el hardware para dar origen a la super carretera de la información.

El motivo de este capitulo está dado por la falta de documentación que amalgame el aspecto teórico - técnico de TCP/IP con el aspecto relacionado a la operación y los servicios que proporcionan las redes implementadas con este tipo de protocolos, y muy en particular con Internet. Ya que generalmente, la literatura o por un lado habla de los protocolos TCP/IP cien por ciento técnicamente o por otro lado habla de Internet desde el punto de vista de los servicios que proporciona como son correo electrónico, transferencia de archivos, Telnet ,etc.; pero escasamente habla de una relación de ambos. Esta es la aportación que pretende hacer el presente capitulo.

Se revisan aspectos accesorios como la conmutación de la información y la tecnología Ethernet, con el fin de tener un panorama más amplio de conocimiento, que permita una mejor comprensión de los temas tratados.

3.2 INTERNET = RED DE CONMUTACIÓN DE PAQUETES

Internet utiliza la conmutación de paquetes para la comunicación entre los diversos nodos que la constituyen, pero para entender mejor por qué se utiliza esta técnica, es necesario hablar del porque de la conmutación.

En una red de área amplia como Internet el uso de una enlace dedicado (generalmente mediante una linea telefónica), con cada una de las computadoras de la red, de ser posible físicamente, económicamente seria muy costoso. Por ejemplo, considérese el caso general de una red con n computadoras, entonces (1/2)n(n-1) líneas serian necesarias para el enlace total de todas las computadoras, líneas que se utilizaran o no tendría que pagarse su renta.

Por otro lado, el tener una red totalmente conectada entre sus nodos no garantiza un mejor desempeño de la misma, por ejemplo, en la figura 3.1, se muestra una red totalmente conectada o punto a punto (un host se enlaza con cada uno de los demás hosts de la red) con 4 computadoras y 6 conexiones.

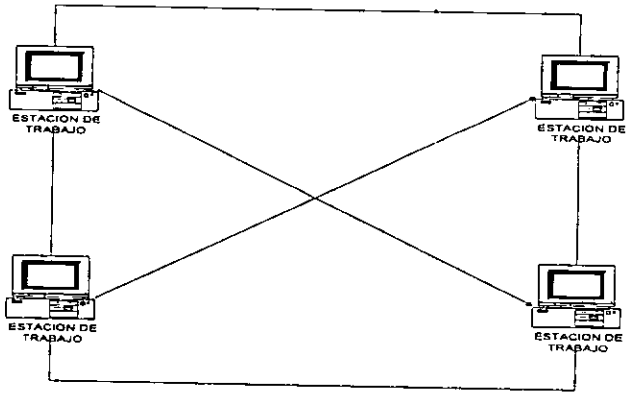


Figura 3.1 Red totalmente conectada o punto a punto

Debido a que, una computadora en un momento dado no se comunica con todas las demás computadoras de la red al mismo tiempo, esto da como resultado que la mayoría de las líneas estén subutilizadas.

Por lo tanto para incrementar la optimización en el uso de las líneas de comunicación en una red, su numero se redujo al mínimo necesario y se introdujo un proceso denominado conmutación. Al reducir el número de enlaces ahora se tendrá una red parcialmente conectada como se muestra en la figura 3.2

Hay tres formas de conmutación que puede ser utilizadas en comunicaciones:

- Conmutación por circuito
- Conmutación por mensaje
- Conmutación por paquete

La **conmutación por circuito** es utilizada generalmente en las redes telefónicas para conectar a los suscriptores del servicio. En la implementación de una red de computadoras utilizando este tipo de conmutación, cada host debe tener una línea dedicada a una central local, y las centrales deben conectarse para formar la red.

Una propiedad importante de la conmutación por circuito es la necesidad de establecer una ruta extremo a extremo antes de que cualquier conjunto de datos pueda ser enviado. En cualquier momento que dos computadoras desean intercambiar información, una ruta física (eléctrica) es establecida entre ellas vía las centrales telefónicas. La ruta después es desconectada cuando la comunicación se termina.

Hay que considerar que, el tiempo transcurrido entre el momento en que se termina de marcar un número y el momento en que se inicia el sonido del timbre del abonado llamado, puede ser fácilmente de 10 segundos, y más en el caso de llamadas de larga distancia. Durante este intervalo de tiempo, el sistema telefónico se encuentra en la etapa de búsqueda de un camino de cobre.

Este método de conexión no en muy utilizado en el establecimiento de redes de computadoras. Las mayores desventajas de la conmutación por circuito son:

1. El costo del equipo es muy alto, además el circuito resultante no es necesariamente de la más alta calidad para la comunicación de computadoras.
2. El circuito resultante sólo puede ser utilizado por dos computadoras a la vez.
3. El tiempo necesario para establecer una ruta física puede ser muy grande en términos de computadora (frecuentemente varios segundos)

La **conmutación por mensaje** supera los problemas en el establecimiento de circuitos físicos vía centrales telefónicas, mediante un esquema que permite a las redes de computadoras usar circuitos permanentes llamados nodos ruteadores que conmutan los datos. Cuando se utiliza esta forma de conmutación, no hay un establecimiento anticipado de la ruta entre el que envía y el que recibe. En una red parcialmente conectada, cada computadora tiene un circuito permanente a un numero de computadoras vecinas dentro de la red, pero no a todas las computadoras.

Para distinguir entre la conmutación por mensaje y la conmutación por paquete es necesario entender que es un mensaje. La forma más fácil de definir un mensaje es decir que es una unidad de información la cual es intercambiada por los usuarios de una red. Esto significa que las características de un mensaje son sólo dependientes del usuario o la aplicación que se esté utilizando. Un mensaje puede ser de algunos bits (una búsqueda dentro de una base de datos) un registro, o aun una base de datos completa. Con la conmutación por mensaje no existe ningún limite para el tamaño del mensaje, lo que significa que los nodos ruteadores deben tener discos para el almacenar temporalmente bloques grandes de información. En un red de conmutación por mensajes el mensaje completo es pasado de un nodo ruteador a otro como una entidad completa.

En la figura 3.2 se muestra una red parcialmente conectada, si la computadora A desea enviar un mensaje a B, el mensaje tiene que pasar ya sea a través de D o C.

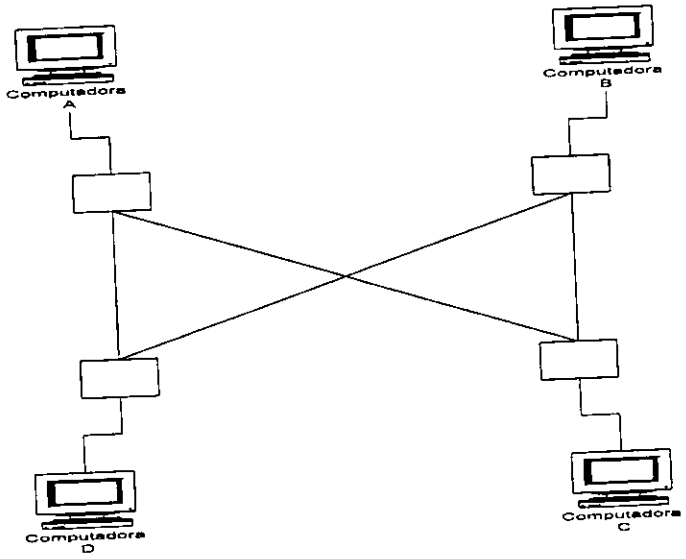


Figura 3.2 Red parcialmente conectada

Los rectángulos en la figura 3.2 son llamados nodos ruteadores. A direccionará el mensaje hacia B, colocando la dirección de B en el encabezado del mensaje. El mensaje y la dirección son después enviados en el circuito a D. En D el nodo inspecciona la dirección; si la dirección es 'D' el mensaje es dado a la computadora; si la dirección no es 'D' el mensaje es lanzado a un circuito donde el nodo cree que el mensaje será recibido. En este caso D lanzará el mensaje a B. Así el nodo en D ha conmutado el mensaje hacia el circuito apropiado. En este ejemplo dos características principales de una red de computadoras se pueden observar:

1. El direccionamiento

   El mensaje es direccionado a un destino remoto (nodo), enviándolo a la siguiente etapa de su ruta.

2. Almacenamiento y Reenvío

   En los nodos cada mensaje es recibido en su totalidad para ser procesado como una unidad completa. Usualmente un chequeo de errores se lleva a cabo después de la recepción completa de cada mensaje. El mensaje después

es inspeccionado con relación a su dirección de destino, de tal forma que el mensaje pueda ser colocado en la cola de salida de un circuito para reenviarlo. Si el mensaje es para una computadora enlazada al nodo ruteador, éste lo pasará directamente a la computadora. Si el mensaje es para un host remoto el nodo debe lanzar el mensaje a otro nodo en la ruta hacia la computadora receptora. Este proceso de almacenamiento y reenvío continua hasta que el mensaje es entregado a su destino final.

Los nodos ruteadores han sido introducidos en la red para llevar a cabo las funciones de ruteo, almacenamiento y reenvío de los mensajes con el fin de que los hosts estén separados de estas cuestiones lo más posible.

Las computadoras nodo son usualmente minicomputadoras elegidas por su habilidad de responder en tiempo real a los dispositivos de comunicación.

La conexión de cualquier nodo ruteador puede ser utilizada para llevar mensajes emitidos de diferentes computadoras, así el equipo físico involucrado es utilizado de una forma más eficiente que en la conmutación por circuito. Este multiplexaje de mensajes es la ventaja más importante de las redes por conmutación de mensajes y paquetes.

Comparada con la conmutación por circuito, una red con conmutación por mensaje tiene las siguientes características:

1. Cualquier computadora o nodo puede comunicarse con cualquier otra computadora sin tener una conexión física directa.
2. Cualquier computadora puede comunicarse con otras usando el mismo equipo mediante la conmutación de mensajes.
3. No hay retraso debido al establecimiento del circuito, pero los mensajes son retrasados cuando pasan a través de los nodos hacia su destino, esperando a ser procesados o reenviados.

Las ventajas de la conmutación por mensaje, sobre la conmutación por circuito son:

- El emisor puede lanzar el mensaje cuando desee, aun si el receptor no está listo, ya que la red (nodo) almacenará el mensaje para su entrega. Sin embargo si los

recursos de la red tales como el almacenamiento se agotan, un mensaje no entregado puede ser borrado y por lo tanto perderse.

- Las computadoras pueden intercambiar información a diferentes velocidades, debido a la caracteristica de almacenamiento de los nodos que controlan el flujo de datos.

- La difusión de un mensaje a través de toda la red (broadcast) puede ser posible.

- El equipo es usado más eficientemente

- Los mensajes pueden ser manejados por prioridad

Sin embargo, en la conmutación por mensaje también se presentan algunas desventajas:

- Un mensaje muy grande evita la salida de otros dentro de la cola , quizás más urgentes, los mensajes muy grandes monopolizan un nodo mientras dura su transmisión, por lo cual las redes de conmutación de mensajes no son apropiadas para el manejo de tráfico interactivo.

- Como un mensaje puede ser muy grande, la computadora nodo no puede tener el suficiente espacio en disco para almacenarlo antes de lanzarlo; en este caso el mensaje se pierde.

- Cuando un mensaje muy grande monopoliza el almacenamiento de un nodo, se presenta el inconveniente que otros mensajes no pueden ser recibidos.

Como se puede ver las desventajas de la conmutación por mensaje se derivan de la posibilidad en la ocurrencia de mensajes 'grandes' donde el valor exacto de grande depende de la red. Si una red pudiera estar cierta de sólo manejar mensajes 'pequeños', las desventajas desaparecerían. Pero como se mencionó, el tamaño de los mensajes en una red por conmutación por mensajes es una característica establecida por el usuario.

Así, una red que cumpla con las necesidades del usuario debe ser capaz de manejar tanto mensajes muy grandes así como mensajes pequeños.

La solución a estos dos conflictivos requerimientos fue dividir el mensaje en pequeños paquetes colocándoles información de protocolo (encabezado[1]) para ser transferidos a través de la red como entidades independientes y reensamblandolos nuevamente al mensaje original en el host destino por parte del receptor.

La figura 3.3 muestra como puede ser dividido un mensaje en paquetes. Hay que notar que el encabezado del mensaje original es reproducido en el encabezado de los paquetes. Este refinamiento produjo la **conmutación por paquete**, siendo la técnica más ampliamente utilizada por las redes de computadoras incluyendo Internet.

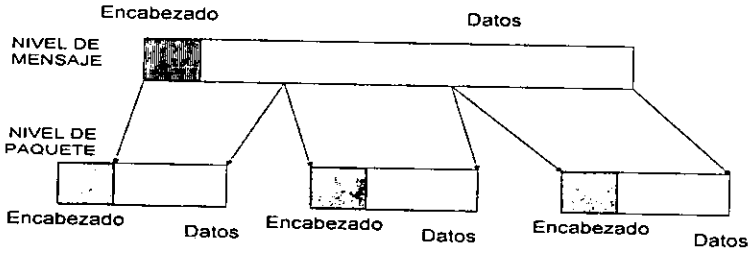


Figura 3.3 División de un mensaje en paquetes

A diferencia de las redes de conmutación por mensaje las redes de conmutación de paquetes fijan un limite superior en el tamaño del bloque, permitiendo que los paquetes sean almacenados en la memoria principal del nodo en lugar de hacerlo en disco.

La organización física de una red por conmutación por paquetes es la misma que para la de conmutación por mensaje. La red es una malla parcialmente conectada de nodos. Por razones practicas la mayoría de las redes usan computadoras nodo especiales para llevar a cabo la conmutación (tradicionalmente conocidos como gateways o ruteadores), y las computadoras de los usuarios se conectan a estos nodos.

[1] El encabezado contiene datos de control, estaciones de origen y destino, tipo de mensaje, nivel de prioridad, etc.

Como se menciono en el capitulo 2 en ARPANET estos nodos fueron llamados Interfaces Procesadoras de mensajes (IMPs) ya que tomaban los mensajes de los usuarios y los dividían en paquetes.

Con el uso de un ruteador las funciones de conmutación de paquetes, tales como almacenamiento y ruteo son liberadas de un host.

Las ventajas que la conmutación por paquete tiene sobre la conmutación por mensaje son:

- El tamaño máximo de un paquete permite que su almacenamiento y manejo sea más fácil por parte del ruteador.

- El tiempo total de transmisión a través de la red se reduce. La diferencia en el tiempo utilizado por la conmutación por mensaje y la de paquete en la transferencia de un mensaje, se incrementa conforme el numero de enlaces a ser recorridos y el tamaño del mensaje aumentan.

- Provee una mejor utilización del equipo

- Teniendo la seguridad de que ningún usuario puede monopolizar una línea de transmisión por más de unas cuantas décimas de milisegundo, las redes de conmutación por paquetes son muy apropiadas para el manejo de tráfico interactivo.

Las ventajas que la conmutación por paquete tiene sobre la conmutación por circuito son:

- La conmutación por circuito reserva, de forma estática y anticipada, el ancho de banda necesario, en tanto que la conmutación por paquete lo adquiere según lo necesita.

- Con la conmutación por circuito, cualquier ancho de banda, que no se utilice en un circuito asignado, se desperdicia. En la conmutación por paquetes, y debido a que los circuitos nunca están dedicados a una tarea especial, pueden ser utilizados por los

paquetes provenientes de cualquier computadora de la red, optimizando el ancho de banda.

- Aunque se presentan situaciones como, la saturación de paquetes en un ruteador provocando la perdida de algunos de ellos, daño en el proceso de su transmisión, llegada a su destino en forma desordenada, o su repetición; no tiene importancia, ya que son controladas y corregidas por un complemento muy importante como lo son los protocolos.

Por estas razones las redes de computadoras deben ser, por lo general, conmutadas por paquete como Internet y ocasionalmente conmutadas por circuito, pero nunca deben ser conmutadas por mensaje.

3.3 IDENTIFICACIÓN DE LOS NODOS EN INTERNET

Como se puede deducir de la explicación anterior, para efectuar una correcta comunicación entre los diversos nodos que conforman a una red, (e Internet no es la excepción), es necesario identificarlos de alguna manera. La identificación dentro de Internet se realiza asignando nombres descriptivos a cada una de las máquinas para comprensión del usuario, mientras que el software trabaja con representaciones binarias más compactas de identificadores conocidos como direcciones IP.

El formato binario elegido para la representación de una dirección IP, fue con el fin de permitir que los ruteadores hicieran cálculos más rápidos para la selección de una ruta.

Obviamente no debe existir un número de dirección repetido dentro de la red, ya que se provocaría un conflicto en la comunicación. Para asegurarse que todas las direcciones sean únicas dentro de Internet, ésta posee una autoridad central que las asigna. La IANA (The Internet Assigned Number Authority, La Autoridad Internet de Asignación de Números), tiene el control sobre los números asignados, así como el establecimiento de políticas. Sin embargo cuando una organización pretende enlazarse a Internet debe solicitar su número de dirección al Centro de Información de la Red Internet (INTERNIC).

De lo anterior se desprende que, aunque es valido que cualquier organización, universidad, institución gubernamental, etc.; puede asignar cualquier dirección IP a sus redes, siempre y cuando no se tenga pensado enlazarse a Internet, por otro lado, se tiene el inconveniente de que si en un momento dado se pretende hacer dicho enlace, las direcciones elegidas por las instituciones pudieron ya haber sido asignadas dentro de Internet evitando por tanto la incorporación (ya que se repetirían las direcciones). De esta forma, la red a ser incorporada requerirá de una reasignacion de direcciones IP únicas dentro de Internet, esta reasignacion quizás para una red relativamente pequeña no sea inconveniente, pero no así para una red grande.

Por esta razón se recomienda que al implementar una red que utilice la familia de protocolos TCP/IP, aunque inicialmente no vaya a ser enlazada a Internet, de todos modos solicite su dirección IP a INTERNIC, ya que si en un futuro desea hacerlo no existirá ningún inconveniente, debido a que no habría duplicidad de direcciones y por lo tanto tampoco conflictos en la comunicación.

3.4 CLASES DE DIRECCIONES IP

Desde un punto de vista conceptual hay que pensar en Internet como una gran red al igual que cualquier otra red física. La diferencia, por supuesto, es que Internet es una estructura virtual implementada totalmente en software, nada en esta red está dictado por el hardware.

Para las direcciones, los diseñadores de TCP/IP eligieron un esquema en el cual cada host o ruteador en Internet fuera identificado con un dirección única de 32 bits llamada Dirección Internet o Dirección IP. La parte inteligente del direccionamiento en Internet es que los números son elegidos cuidadosamente para hacer el ruteo eficiente. Específicamente, una dirección IP codifica la identificación de la red a la cual un host se enlaza así como la identificación de forma única del host dentro de la red.

Conceptualmente, cada dirección es un par (redid, hostid), donde redid identifica a la red , y hostid identifica a un host en dicha red.

INTERNIC asigna a la organización que lo solicite solamente la porción correspondiente a la identificación de la red; una vez que ya se tiene el prefijo de red la organización puede elegir un sufijo único a cada host en la red sin tener que contactar a la autoridad central.

INTERNIC otorga una de tres clases de direcciones IP (aunque existen cinco clases), de acuerdo al número de hosts que conforman a la red que se desea enlazar a Internet.

La figura 3.4 muestra las cinco formas que puede tener una dirección IP.

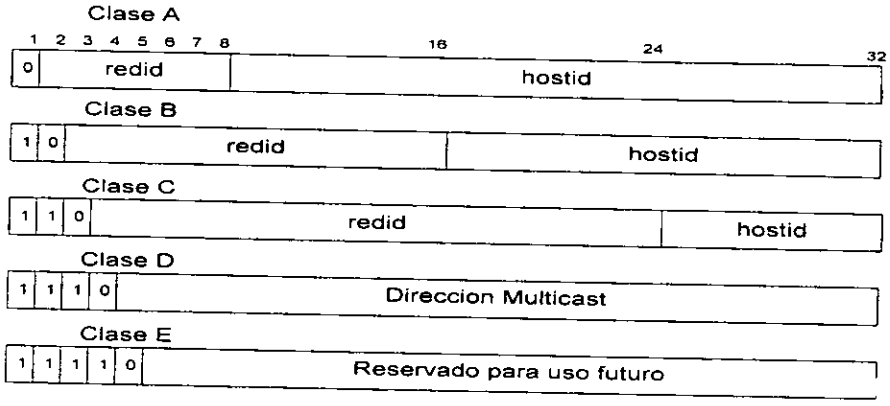


Figura 3.4 Las cinco formas de las direcciones IP

Si una red está constituida por más de 65,536 (2^{16}) hosts se le asigna una dirección Clase A, esto se deriva de lo siguiente: como cada dirección está constituida por 32 bits, se define que una dirección clase A tiene que utilizar el primer octeto para identificar a la red con el primer bit en 0 y los 3 octetos restantes para identificar a los hosts, por lo tanto, teóricamente se tendrían:

$(2^7) = 128$ redes con un máximo de

$(2^{24} - 2) = 16{,}777{,}216 - 2 = 16{,}777{,}214$ hosts cada una

Cabe aclarar que existen ciertas direcciones que tienen un significado especial y por lo tanto no se ocupan como direcciones validas para un host, tal es el caso cuando el hostid es 0, por convención un host nunca es asignado con todos sus bits en 0. Cuando en una dirección IP la parte que corresponde al hostid tiene ceros, su función es la de hacer referencia al numero de la red (número asignado por INTERNIC).

Otra dirección especial es aquella en la cual la parte correspondiente al hostid tiene solamente unos, este tipo de dirección nos sirve para enviar el mismo mensaje a todos los hosts de la red. De acuerdo con el estándar cualquier dirección IP con la porción correspondiente al hostid que contenga solo unos es reservada para difusión a todos los hosts de la red (también conocido como broadcast).

Tomando en consideración los dos aspectos anteriores, se justifica el -2 que aparece en las operación arriba mencionada.

Continuando con las direcciones clase B éstas son asignadas a las redes consideradas de tamaño mediano, es decir, aquellas que tienen entre 2^8 = 256 y 2^{16}= 65,536 hosts, permitiendo 14 bits para la identificación de la red y 16 bits para la identificación de los hosts. Entonces se tendrían:

(2^{14}) = 16,384 redes con un máximo de

$(2^{16}-2)$ = 65,536-2 = 65,534 hosts cada una

Finalmente las direcciones clase C son asignadas a las redes consideradas pequeñas,

y son aquellas que tienen un numero de hosts menor a 2^8 = 256, pero por otro lado permite tener un mayor número de redes, ya que define 21 bits para identificar a la red. Asi, se tendrían:

(2^{21}) = 2,097,152 redes con un máximo de

$(2^8 -2)$ = 256-2 =254 hosts cada una

Hay que notar que las direcciones IP han sido definidas de tal forma que es posible extraer las porciones hostid o redid rápidamente. Los ruteadores, quienes usan la porción redid de una dirección IP para reenviar un paquete, sacan provecho de esta característica para enrutar los paquetes con gran rapidez.

3.4.1 LAS DIRECCIONES IP ESPECIFICAN CONEXIONES A LA RED

Una dirección IP no puede considerarse estrictamente un medio para identificar un dispositivo dentro de la red, ya que, por ejemplo los ruteadores que se enlazan a dos o más redes, no podrían ser identificados por medio de una sola dirección. Los ruteadores requieren de varias direcciones IP, donde cada dirección corresponde a cada una de las conexiones con cada una de las redes.

Concluyendo, debido a que una dirección IP identifica tanto a una red como a un host o ruteador dentro de ella, no especifica a un dispositivo, sino una conexión a la red. Por lo tanto un ruteador conectando n redes tendrá n distintas direcciones IP, una para cada conexión de red.

3.4.2 REPRESENTACIÓN DECIMAL DE LAS DIRECCIONES IP

Para cualquier usuario el utilizar o hacer referencia a direcciones IP en modo binario es muy engorroso, por lo tanto, se estableció una representación más compacta y practica para las direcciones IP. Representándolas mediante cuatro números decimales enteros separados por medio de puntos, donde cada entero equivale a un octeto de la dirección IP. La notación decimal se denomina en ocasiones Notación Cuadrática con Punto. Por ejemplo, considérese la siguiente dirección IP en su forma binaria.

10010011 00001010 00001101 00011100 en notación cuadrática se escribiría

147 . 10. 13 . 28

Tomando como referencia la figura 3.4, se observa que los tres primeros bits de la dirección IP determinan la clase de ésta. Por lo cual, la dirección anterior corresponde a una clase B y como las redes de este tipo toman dos octetos para identificar a la red, entonces los octetos en representación decimal 147.10 definen el número de la red y los dos octetos restantes identifican al host dentro de esta red, en este ejemplo, el numero 13.28

La mayoría del software TCP/IP que despliega o solicita al usuario una dirección IP usa la notación decimal con punto. Por ejemplo los programas de aplicación como Telnet y FTP utilizan este tipo de notación.

La siguiente tabla muestra el rango de valores validos de direcciones de red para cada clase en notación decimal con punto.

CLASE	DIRECCIÓN MÁS BAJA	DIRECCIÓN MÁS ALTA
A	0.1.0.0	16.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

De la tabla anterior se deduce que no todas las direcciones posibles de red han sido asignadas a una clase. Por ejemplo, la dirección 127.0.0.0 un valor que correspondería a la clase A, esta reservada para usarse en el diagnostico de TCP/IP así como para procesos de comunicación internos de la máquina, por lo tanto no se utiliza como dirección valida de red.

3.5 LA NECESIDAD DE MAPEAR LAS DIRECCIONES IP

Hasta ahora se ha descrito el esquema de direccionamiento TCP/IP en el cual cada host es asignado con una dirección única de 32 bits, con el fin de distinguirlo entre los hosts que se encuentran en las demás redes, y poder llevar a cabo una correcta comunicación. También se ha explicado que Internet es una red virtual, gracias a los ruteadores y al esquema de direccionamiento que permiten el envío y recepción de paquetes de información a través de varias redes físicas, pero a la vez dando la ilusión de ser una sola red.

Por otro lado, se tiene qué, para que dos computadoras en cualquier red física puedan entablar una comunicación (comunicación al más bajo nivel) requieren conocer cada una de ellas la dirección física de la tarjeta de red de la otra. No hay que olvidar que finalmente lo que circula en el medio físico así como en la circuitería de las tarjetas de red son señales eléctricas.

De lo anterior se concluye que, para la entrega de un paquete a un nodo determinado de la red por parte de un ruteador o host, la dirección IP no es suficiente, debido a que no está asociada con la dirección física de la interface de red a la cual se desea enviar paquetes.

Como consecuencia se presenta la siguiente situación: Cómo tendrían que mapear[2] ya sea un host o un ruteador la dirección IP a una dirección física, para el envío de un paquete de un host a otro a través del medio físico?.

Antes de resolver la pregunta anterior se analizará con cierto detalle la operación de la tecnología Ethernet[3], la cual proporcionará la base de conocimiento necesario para enfrentar esta problemática.

3.6 UN REPASO A LA TECNOLOGÍA ETHERNET

De la misma forma que una red implementada con TCP/IP requiere de direcciones únicas para identificar a los hosts de una red, Ethernet y en general cualquier otra tecnología de red requiere de un direccionamiento que permita la comunicación a nivel físico entre las tarjetas de red. Ethernet define sus propias direcciones, asignando a cada una de las tarjetas desde su fabricación una dirección. Los diseñadores de Ethernet con el fin de evitarle a los administradores de red asignar direcciones a las tarjetas, y que éstas se pudieran duplicar, establecieron una autoridad central que las administrará.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) de Estados Unidos se encarga del manejo en la asignación del espacio de direccionamiento. Así, los distintos fabricantes de tarjetas de red le solicitan bloques de direcciones al IEEE, las cuales son grabadas en secuencia en las tarjetas conforme van siendo manufacturadas. De esta manera se evita que dos tarjetas puedan tener la misma dirección, y por lo tanto, también se evita que pueda haber conflictos de comunicación.

Las direcciones Ethernet están compuestas de 48 bits y debido a que están incorporadas en el hardware, son llamadas direcciones de bajo nivel o direcciones físicas.

---

[2] Mapear, se refiere a la relación de correspondencia que tiene un conjunto de datos con otro conjunto de datos

[3] Aunque Internet se compone de redes de diversas tecnologías, Ethernet predomina , es por eso que es tomada como ejemplo en este capitulo, pero así mismo es necesario mencionar que los principios generales se aplican también a las demás tecnologías.

Contrario a las direcciones IP que son manejadas por el software y que se les conoce como direcciones de alto nivel.

En una red Ethernet cuando un host envia un paquete hacia otro host, en él se incluye un encabezado que proporciona información tal como la dirección física del nodo emisor, así como la dirección física del nodo destino. El paquete viaja a través del medio físico, y cada una de las tarjetas de las maquinas en la red lo examinan si la dirección destino del paquete coincide con la dirección de la tarjeta de red entonces éste es tomado y pasado a la computadora. De la misma forma, todos los hosts de la red también procesan los paquetes que tienen una dirección comodín destino, llamada dirección "broadcast" (dirección de difusión).

Como se puede deducir del párrafo anterior, en la comunicación a más bajo nivel (señales eléctricas o bits en el cable) los paquetes de información (datos del usuario) requieren ser suministrados de información extra para que puedan ser tomados por las tarjetas de red. En esta información extra conocida como frame se "montan" los datos para su transporte en el medio físico, obviamente debe existir un estándar que defina como debe estar conformado el frame para que tenga el mismo significado en todas las tarjetas de red.

3.6.1 FORMATO DEL FRAME ETHERNET

En una red Ethernet el formato del paquete o frame que circula en el medio físico y el cual tiene significado para las tarjetas de red tiene la siguiente forma.

Preambulo	direccion destino	direccion fuente	tipo del frame	area de datos	CRC
8 octetos	6 octetos	6 octetos	2 octetos	64-1500 octetos	4 octetos

Figura 3.5 Formato del frame Ethernet

Además de la identificación del nodo fuente y del nodo destino, cada frame transmitido consta de un preámbulo compuesto de 64 bits de 0s y 1s alternados y que sirven para la sincronización de los hosts. El campo Tipo, formado de 16 bits identifica el tipo de los datos que están siendo acarreados por el frame. Cuando un paquete llega a una máquina destino, el Sistema Operativo usa el campo Tipo del frame para determinar

cual protocolo debe procesar el frame. La ventaja principal del uso del campo Tipo del frame Ethernet es que se permite el uso de múltiples protocolos en una red, así pueden convivir familias de protocolos como TCP/IP, DECNET, Xerox NS, etc.; al mismo tiempo sin interferencia.

El campo Datos corresponde al paquete de datos o información, de un usuario o de un programa de aplicación y el cual puede tener una longitud de 64 a 1500 octetos.

Al final del frame aparece el campo CRC (Cyclic Redundancy Check) por medio del cual se detectan errores en los paquetes transmitidos. El host emisor calcula un valor en función del campo de datos del frame y lo incluye en el campo CRC, en el host destino cuando llega el frame se vuelve a efectuar la misma operación calculando un nuevo valor; si éste valor empata con el del nodo emisor quiere decir que los datos no sufrieron daño en la transmisión, de otra manera si los valores no cuadran, quiere decir que los datos sufrieron algún daño y por lo tanto se desechará el paquete.

3.7 DOS CONJUNTOS DE DIRECCIONES INDEPENDIENTES

Después de haber analizado la operación de la tecnología Ethernet, y retomando la pregunta del apartado 3.5 se puede concluir que no existe una relación directa entre las direcciones IP y las direcciones Ethernet.

Por lo tanto para resolver tal situación, la meta fue idear un software que "escondiera" las direcciones físicas, pero que permitiera a los programas de alto nivel (aplicaciones) trabajar sólo con las direcciones de alto nivel IP.

Supóngase por ejemplo, que se tiene una red Ethernet como la que se muestra en la figura 3.6, y que la máquina A quiere enviar un paquete a la máquina B a través de la red a la cual ambas máquinas están enlazadas, pero A sólo conoce la dirección IP de B. La máquina A por lo tanto, tiene que mapear o traducir la dirección IP de B a su correspondiente dirección física, una vez obtenida la dirección física de la tarjeta de red de B, el paquete se monta en el campo de datos de un frame y en el campo dirección destino se coloca la dirección física de B, acto seguido se envía el frame por el medio físico. Cuando la máquina B observa que el frame tiene en su dirección destino la misma dirección que su tarjeta de red, entonces lo toma.

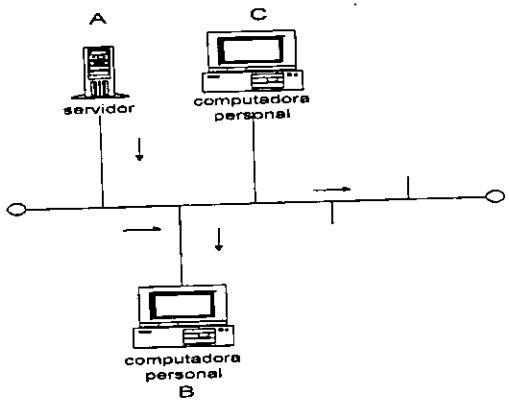


Figura 3.6 Comunicación entre computadoras en una red Ethernet

El problema de mapear direcciones de alto nivel a direcciones físicas se conoce como el 'Problema de resolución de direcciones'

3.8 EL PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES (ARP)

Los diseñadores de los protocolos TCP/IP encontraron una solución creativa para el problema de la resolución de direcciones para redes que tienen capacidad de difusión (broadcast) como Ethernet. Mediante la utilización de un protocolo de bajo nivel se logró mapear las direcciones IP a direcciones físicas, de una forma dinámica.

El protocolo ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones) provee un mecanismo de mapeo que es razonablemente eficiente y fácil de mantener dentro de una red física.

La traducción de una dirección IP a su correspondiente dirección física, se lleva a cabo mediante el uso de una tabla. La tabla, llamada tabla o cache ARP, es almacenada en la memoria de cada host y contiene un renglón por cada computadora instalada en la red. Se forma por una columna de direcciones IP con su correspondiente columna de direcciones Ethernet (escritas en el formato de 6 números en notación hexadecimal separados por dos puntos), como se muestra en el siguiente ejemplo:

Dirección IP	Dirección Ethernet
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

Así, antes de transmitirse un paquete IP (que al igual que Ethernet, también tiene una dirección fuente y una dirección destino) de un nodo a otro, se extrae la dirección destino IP del paquete y se busca en el cache ARP del host. Si se encuentra la dirección entonces el paquete de datos se monta (proceso conocido como encapsulacion) en el campo de Datos de un frame, colocándole a éste en su campo de Dirección Destino la dirección física asociada con la dirección IP encontrada, y finalmente se transmite a través del medio físico.

Por otro lado sino se encuentra la dirección IP en la tabla (por ejemplo, que se haya agregado una computadora nueva a la red), entonces, se difunde un frame especial en toda la red (un paquete de difusión o broadcast), en el cual se solicita al host con la dirección IP responda con su dirección física asociada.

Cada una de las interfaces de red procesan el frame de difusión en el cual va encapsulada la solicitud ARP. Examinan el campo Tipo del frame, si tiene el numero (0806_{16}) el cual corresponde a una petición ARP, entonces el paquete se pasa al modulo ARP. La petición ARP dice "Si tu dirección IP empata esta dirección IP destino, entonces, por favor dime tu dirección Ethernet". Una solicitud ARP se vería así:

Dirección IP del nodo fuente	223.1.2.1
Dirección Ethernet del nodo fuente	08:00:39:00:2f:c3
Dirección IP del nodo destino	223.1.2.2
Dirección Ethernet del nodo destino	

Cada modulo ARP compara la dirección destino IP del paquete de petición, con su dirección IP, si empatan las direcciones entonces se envía la dirección Ethernet del nodo destino directamente a la dirección fuente Ethernet. El paquete ARP de respuesta diría: "Si, ésta dirección destino IP es mía, permíteme darte mi dirección Ethernet". En una respuesta ARP las direcciones fuente y destino se intercambian con relación al mensaje de solicitud, como se muestra a continuación.

Dirección IP del nodo fuente	223.1.2.2
Dirección Ethernet del nodo fuente	08:00:1a:35:4d:07
Dirección IP del nodo destino	223.1.2.1
Dirección Ethernet del nodo destino	08:00:39:00:2f:c3

La respuesta es recibida por la computadora fuente original. El driver (manejador) Ethernet de la computadora fuente observa el campo Tipo en el frame Ethernet de respuesta, si es de tipo ARP, entonces lo pasa a éste modulo. El modulo ARP examina la respuesta y agrega tanto la dirección IP como la dirección Ethernet a su tabla, actualizándola.

3.8.1 REFINAMIENTOS EN EL PROTOCOLO ARP

Existe una razón muy importante por la cual se utiliza un tabla en la resolución de direcciones por parte del protocolo ARP, y es el costo de la comunicación.

Se podría pensar que para el envío de paquetes por parte de cualquier máquina en la red, la sola difusión o broadcast de los mismos seria suficiente, ya que, como este tipo de paquetes todas las maquinas de la red los procesan, a final de cuentas se encontraría la máquina con la dirección IP destino, y ésta los tomaría.

Pero la situación no es tan fácil; la difusión es demasiada costosa para ser usada cada vez que una máquina necesita transmitir un paquete. Debido a que, como se requiere que todas las maquinas en la red procesen todos los paquetes, entonces se desperdiciaría procesamiento de cómputo. De igual forma, como consecuencia de la difusión se generaría una gran cantidad de tráfico en la red lo que tendría un serio impacto en el rendimiento de la misma.

Las máquinas que utilizán ARP mantienen un cache de las direcciones recientemente mapeadas, de esta forma no tienen porque utilizar repetidamente la resolución para una misma dirección.

Un refinamiento en el protocolo ARP lo constituye el aprovechamiento de una solicitud de resolución por parte de los todos nodos. Como se mencionó una solicitud de resolución (la cual incluye las direcciones IP y física del nodo solicitante) es procesada por todas las máquinas de la red, por lo tanto, aunque no sean el destino de la resolución aprovechan para tomar los datos de la dirección IP y dirección física de la máquina fuente (la que está solicitando la resolución) y guardarlos en sus tablas.

Con este tipo de resolución, el sistema se puede adecuar en forma dinámica a direcciones físicas cambiantes (por ejemplo cuando se daña una interface y se tiene que reemplazar por una nueva) y a nuevas adiciones de hosts en la red.

3.8.2 RELACIÓN DE ARP CON OTRAS TECNOLOGÍAS

El protocolo ARP puede ser utilizado por cualquier tecnología de red (Ethernet, Token Ring , FDDI, etc.), ya que sus paquetes son encapsulados en el área de datos del frame particular de la tecnología utilizada.

Así, de esta forma ARP impone un esquema nuevo de direccionamiento por encima de cualquier mecanismo de direccionamiento de bajo nivel (físico) que el hardware utilice. La idea puede ser sintetizada de la siguiente manera:

ARP es un protocolo de bajo nivel que esconde el direccionamiento físico de la red, permitiendo a la aplicaciones trabajar con direcciones de alto nivel (en el caso de TCP/IP, direcciones IP) en la transmisión de paquetes de información de un host hacia otro.

Se debe pensar en ARP como una parte del sistema físico de la red, por lo mismo está disponible a las diferentes tecnologías.

3.8.3 FORMATO DEL PAQUETE ARP

Como se mencionó en el apartado anterior el protocolo ARP puede ser utilizado por diversas tecnologías de red, por lo cual la longitud de los campos que contienen direcciones en el paquete ARP dependen del tipo de tecnología de la red. Sin embargo, para hacer posible la interpretación de un mensaje ARP, el encabezado del paquete incluye campos fijos cerca del inicio de donde se especifica direcciones. En realidad, el formato del mensaje ARP es lo suficientemente general para permitirle ser usado con direcciones físicas arbitrarias y también direcciones de protocolo arbitrarias.

La figura 3.7 muestra los 28 octetos del mensaje ARP utilizado en una red Ethernet, es decir, este paquete se coloca en el campo de datos de un frame Ethernet, y se hace circular por el medio físico.

Figura. 3.7 Formato del mensaje ARP

Las direcciones físicas de la interface del emisor y el destino, etiquetadas como EMISOR HA y DESTINO HA, ocupan 6 octetos (48 bits) contiguos, de tal forma que ocupa dos líneas en el diagrama. Las direcciones de alto nivel del emisor y el destino, etiquetadas como EMISOR IP y DESTINO IP ocupan 4 octetos.

El campo TIPO DE HARDWARE especifica el tipo de la interface de hardware contiene el valor de 1 para Ethernet. De la misma forma el campo TIPO DE PROTOCOLO especifica el tipo de la dirección de protocolo de alto nivel, contiene el valor 0800_{16} para direcciones IP. El campo OPERACIÓN especifica uno de cuatro valores posibles Petición ARP (1), Respuesta ARP (2), Petición RARP (3), o Respuesta RARP (4) [4]. Los campos HLEN y PLEN le permiten a ARP ser utilizado como ya se dijo por diferentes tecnologías de redes, ya que especifican la longitud de las direcciones físicas y la longitud de las direcciones de los protocolos de alto nivel.

3.9 SISTEMA DE NOMBRES DE DOMINIO

La sección anterior menciono que Internet asigna a cada host un valor numérico único llamado dirección IP. Estas direcciones en su formato binario son utilizadas por el software para el envío y recepción de paquetes entre los nodos de la red.

[4] RARP (Reverse Address Resolution Protocol, Protocolo Inverso de Resolución de Direcciones), una máquina difunde una solicitud que contiene la dirección física de su interface y un servidor responde enviándole una dirección IP. Por lo general se utiliza en máquinas que no tienen disco duro

Aunque la notación cuadrática con punto provee una representación conveniente y compacta de las direcciones (con respecto a los 32 bits), para especificar la fuente y el destino de los paquetes a través de Internet, los usuarios prefieren hacer referencia a un host o red mediante un nombre descriptivo y no mediante una serie de números factibles de olvidar o escribirlos incorrectamente. Internet permite el uso de nombres alfabéticos para hacer referencia a los hosts y redes.

Considerando que los usuarios pueden hacer referencia a un host por medio de un nombre, y por otro lado que la comunicación entre los host se lleva a cabo mediante el uso de direcciones IP; entonces se requiere de un mecanismo que traduzca los nombres descriptivos de los hosts a sus correspondientes direcciones IP.

Internet ofrece un servicio que traduce nombres de máquinas a direcciones IP automáticamente. Los nombres descritos son conocidos como nombres de dominio, y el software que traduce o mapea un nombre de dominio a una dirección IP es llamado Sistema de Nombres de Dominio (DNS, por sus siglas en inglés).

3.9.1 UN ESPACIO DE NOMBRES PLANOS

En la sección 2.4.5.1 del capitulo anterior se explica como es que en los inicios de Internet cada uno de los hosts de la red era identificado por medio de un nombre simple asociándolo con una dirección IP, agrupando todos estos nombres en un archivo denominado hosts.txt.

Así los administradores de las redes identificaban a los hosts con nombres de sitios geográficos, personajes de películas, actores, colores, planetas, etc.; por ejemplo se tenían nombres como: Mercurio, Venus, Púrpura, América, etc.

Cuando Internet estaba formada por algunas decenas de maquinas, elegir el nombre para una máquina nueva era relativamente fácil, ya que el uso de un nombre simple era suficiente. Como consecuencia, todo el conjunto de nombres de máquina y sus direcciones IP asociadas dentro de Internet formo un espacio de nombres planos, es decir, nombres con una secuencia de caracteres sin estructura alguna. El NIC como autoridad central se encargaba de administrar la lista de los nombres, determinaba si un nombre nuevo era apropiado, prohibiendo nombres obscenos o nombres que se

repitieran con los existentes, además, se encargaba de la distribución de la lista de nombres hosts.txt a cada uno de los nodos de la red.

Con el crecimiento de la red ya no fue tan fácil encontrarle nombre a una máquina, además de que el esquema centralizado junto con el uso de un archivo para englobar todos los nombres presento varias desventajas (ver sección 2.4.5.1). Por lo cual se requirió de una nueva estructura de nombramiento para los hosts.

3.9.2 NOMBRES DE DOMINIO INTERNET

Los diseñadores de Internet idearon agregar una estructura a los nombres de las maquinas y emplear un sistema descentralizado.

La sintaxis de los nombres ahora seguiría un modelo jerárquico, es decir, los nombres estarían formados por una serie de cadenas o etiquetas alfabéticas separadas por puntos, denominados "Nombres de dominio".

Esta sintaxis jerárquica refleja así mismo una delegación de autoridad en la asignación del nombre. La cadena ubicada a la derecha tendrá mayor jerarquía con respecto a la(s) cadena(s) ubicadas a la izquierda, por ejemplo el nombre de dominio: .

condor.dgsca.unam.mx

contiene cuatro etiquetas: condor, dgsca, unam y mx. Cualquier sufijo de una etiqueta en un nombre de dominio es también llamado un dominio. El nombre de dominio de más bajo nivel es *condor.dgsca.unam.mx* (la computadora llamada condor de la Dirección General de Servicios de Cómputo Académico de la Unam en México), el segundo nivel del dominio es *dgsca.unam.mx* (el nombre de dominio para la DGSCA), el tercer nivel del dominio es *unam.mx* (el nombre de dominio para la UNAM) y el nivel más alto es *mx* (el nombre de dominio para todas las organizaciones ubicadas en México).

El mecanismo que implementa nombres de máquina jerárquicos para Internet es conocido como el Sistema de Nombres de Dominio (DNS). El DNS tiene dos aspectos conceptualmente independientes. El primero como ya se vio es abstracto y es el que se refiere a la sintaxis de los nombres y las reglas para delegar autoridad sobre los nombres.

El segundo es concreto debido a que especifica la implementación de un sistema distribuido que mapea eficientemente nombres a direcciones.

3.9.3 NOMBRES DE DOMINIO OFICIALES DE INTERNET

Internet define explícitamente el nombre de los dominios de más alto nivel (los que se ubican a la extrema derecha), sobre los cuales mantiene control. A partir de estos dominios se derivan los nombres, agregándose tantos subdominios como sea necesario para identificar a un host. Como se ilustra en la figura 3.8 en este esquema se pueden acomodar una gran variedad de instituciones, ya que permite a cualquier grupo elegir como dominios de alto nivel, jerarquías de nombres geográficos u organizacionales.

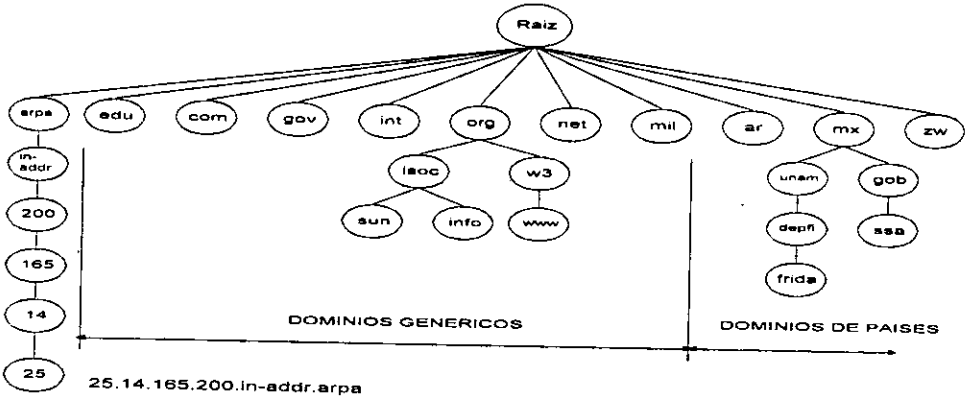


Figura 3.8 Nombres de dominio de más alto nivel dentro de Internet

Los dominios de más alto nivel del tipo organizacional (genéricos) están formados por etiquetas de tres caracteres y los de tipo geográfico (países) por etiquetas de dos caracteres que representan los códigos de los países según documento de la ISO (Organización Internacional para la Estandarizacion).

Los dominios de más alto nivel definidos por Internet son los siguientes:

NOMBRE DE DOMINIO	SIGNIFICADO
.com	Organizaciones comerciales
.edu	Instituciones educativas
.gov	Instituciones gubernamentales
.mil	Instituciones militares
.net	Organizaciones de manejo de redes
.org	Organizaciones que no caen en las arriba mencionadas
.arpa	Dominio temporal para ARPANET (obsoleto)
.int	Organizaciones internacionales
Código de país	Definido por el documento 3166 de la ISO

3.9.4 NOMBRES DE DOMINIO Y DELEGACIÓN DE AUTORIDAD

Los nombres de dominio implícitamente muestran una delegación de autoridad, para entender mejor lo anterior se muestra el siguiente ejemplo: una máquina llamada frida del Departamento de Física de la UNAM tiene el nombre de dominio **frida.depfi.unam.mx**. Esto implica que el nombre fue aprobado y registrado por el administrador de la red en el departamento de física. El administrador del departamento obtuvo previamente autorización para manejar el subdominio depfi.unam.mx, de parte de la UNAM, quien a su vez obtuvo permiso para manejar el subdominio unam.mx por parte de la autoridad Internet.

Así como Internet mantiene el control sobre el dominio com, por lo cual si nuevas organizaciones comerciales desean incorporarse a Internet, sólo podrán hacerlo mediante su autorización. Similarmente , el administrador de la red en la UNAM posee autoridad sobre el subdominio unam.mx, de tal forma que un dominio de tercer nivel nuevo puede ser agregado sólo con su autorización.

3.9.5 MAPEANDO NOMBRES DE DOMINIO A DIRECCIONES IP

Además de las reglas de sintaxis para los nombres y la delegación de autoridad, el esquema de nombres de dominio incluye un eficiente, confiable y de propósito general sistema distribuido para mapear nombres a direcciones. El sistema es distribuido en el sentido técnico ya que un conjunto de servidores operan en muchos sitios de Internet resolviendo el problema del mapeo. Es eficiente en el sentido que la mayoría de los nombres pueden ser mapeados localmente, sólo pocos requieren tráfico internet. Es de

propósito general ya que su uso no está restringido sólo a resolver nombres de máquinas, y es confiable debido a que la falla de una máquina no evita que el sistema siga operando correctamente.

El mecanismo de traducción sigue el modelo cliente/servidor, ya que consiste de un sistema cooperativo independiente, formado por servidores de nombres y clientes que solicitan la resolución de nombres. Un servidor de nombres, es un programa que proporciona mapeo de nombres de dominio a direcciones IP. El software cliente llamado resolvedor de nombres, usa uno o más servidores de nombres cuando traduce un nombre.

Para el mapeo de un nombre de dominio un cliente debe saber como contactar al menos un servidor de nombres (el servidor local[5]). Para asegurarse que un servidor de nombres pueda contactar a su vez a otros servidores, el DNS establece que cada servidor de nombres debe conocer la dirección de por lo menos un servidor de la raíz., además de poder conocer la dirección de un servidor para el dominio inmediato superior al de él, conocido como dominio padre.

Para entender mejor la operación considérese el siguiente ejemplo. Supóngase que un usuario en México necesita comunicarse con la computadora llamada Eifel localizada en la compañía ABC en Francia, cuyo nombre de dominio es el siguiente: **eifel.abc.fr**. Antes que cualquier programa de aplicación ejecutado en México pueda establecer comunicación con la computadora eifel, se requiere obtener la dirección IP de ésta. Para conocer la dirección IP, la aplicación utiliza el DNS. El proceso que se lleva a cabo es el siguiente.

- La aplicación en la computadora en México coloca el nombre eifel.abc.fr en un mensaje y lo envía al servidor de nombres local en México (en este caso podría ser al servidor que administra todos los subdominios por debajo del dominio raíz mx). Como este servidor no tiene autoridad sobre el dominio fr teóricamente no podrá resolver el nombre de dominio (más adelante se explica la forma en la cual se puede superar esta situación).

[5] Un servidor local de nombres de dominio es aquel que se encuentra dentro de la misma subdivisión del espacio de nombres en el que se encuentra la máquina que solicita la traducción

- Como los servidores de nombres deben conocer las direcciones de los servidores de la raíz, entonces el servidor de nombres de dominio mx tiene que contactar al servidor de nombres fr en Francia (generándose tráfico internet) el cual a su vez contacta el servidor de nombres de la compañía ABC.

- El servidor de nombres de la compañía ABC responde enviando la dirección IP de la máquina eifel, hacia el servidor de nombres en México.

- El servidor local en México finalmente envía la respuesta (la dirección IP) a la máquina solicitante.

Aunque el sistema DNS puede enviar varios mensajes a través de Internet la obtención de una respuesta no toma mucho tiempo. En muchos casos, una respuesta toma menos de un segundo. La velocidad es importante ya que la resolución ocurre en tiempo real cuando un usuario ejecuta una aplicación con un nombre de dominio. La aplicación debe esperar mientras el sistema DNS encuentra la dirección IP de la computadora, tan rápido el sistema DNS responde, el programa de aplicación podrá empezar a enviar paquetes directamente a la computadora referenciada.

3.9.6 REFINAMIENTO EN EL SISTEMA DNS

El costo de la resolución de nombres que no pueden ser mapeados por el servidor local puede ser extremadamente alto si los resolvedores (clientes) envían cada solicitud al servidor raíz, debido a que se genera una gran cantidad de tráfico en la red bajando su desempeño. Por lo tanto, para mejorar el desempeño general de un sistema de nombres, es necesario bajar el costo en la resolución para nombres no locales.

Los servidores de nombres en Internet lo logran usando un cache de nombres. Cada servidor mantiene un cache en el cual conserva los nombres resueltos más recientes, así como un registro de donde fue obtenida la información de mapeo para tales nombres.

Cuando un cliente solicita al servidor resolver un nombre, el servidor primero checa si tiene autoridad sobre el nombre de acuerdo al procedimiento estándar, sino, el

servidor revisa su cache para ver si el nombre ha sido resuelto recientemente. Los servidores cuando reportan la información almacenada en sus caches a los clientes, la marcan como no certificada, y proporcionan adicionalmente el nombre de dominio del servidor a partir del cual se obtuvo el mapeo. Por lo tanto, los clientes reciben respuestas rápidas, aunque la información podría ser obsoleta. Si la eficiencia es importante, el cliente aceptará la respuesta y procederá. Por el contrario si la exactitud es importante, el cliente elegirá contactar el servidor respectivo y verificar que el par nombre/dirección siga siendo valido.

El uso de un cache funciona bien en el DNS ya que los pares nombre/dirección no cambian frecuentemente, pero sin embargo lo hacen, por lo cual si los servidores almacenan información en su cache por mucho tiempo se tiene el inconveniente de que se vuelva obsoleta. Para mantener el cache correcto los servidores temporizan cada mapeo, borrándolos cada vez que se excede el tiempo establecido. Por lo tanto, si se requiere nuevamente el par nombre de máquina/dirección IP, se tiene que contactar nuevamente al servidor responsable del nombre para obtener la información de mapeo.

Mediante este refinamiento la mayoría de los nombres pueden ser resueltos por el servidor local, reduciendo el tráfico internet y aumentando el desempeño de la red.

3.9.7 MAPEO INVERSO

Como se mencionó en el apartado 3.9.5, el DNS puede proveer otros mapeos diferentes al de nombres de dominio a direcciones IP. El DNS puede también mapear una dirección IP a un nombre de dominio, situación conocida como mapeo inverso.

El DNS soporta un dominio especial y una forma especial de pregunta llamada pregunta apuntadora. En una pregunta apuntadora, la pregunta presentada a un servidor de nombres de dominio especifica una dirección IP codificada como una cadena de texto en la forma de nombre de dominio. La pregunta apuntadora le solicita al servidor de nombres le regrese el nombre de dominio correcto para la máquina con la dirección IP especificada.

Las preguntas apuntadoras no son difíciles de generar. Considerando que una dirección IP escrita en forma decimal con punto, tiene el siguiente formato: aaa.bbb.ccc.ddd. Para formar una pregunta apuntadora, el cliente reacomoda la

representación decimal con punto a una cadena de la siguiente forma: **ddd.ccc.bbb.aaa.in-addr.arpa**.

La nueva forma es un nombre en el dominio especial in-addr.arpa[6] (ver figura 3.8). Debido a que el servidor de nombres local no puede ser la autoridad tanto para el dominio arpa como para el dominio in-addr.arpa, se necesita contactar a otros servidores de nombres para completar la resolución. Para hacer la resolución de las preguntas apuntadoras en forma eficiente, los servidores de dominio raíz mantienen una base de datos valida de direcciones IP con información acerca de los servidores de nombres de dominio que pueden resolver estas direcciones.

3.9.8 FORMATO DEL MENSAJE DE UN SERVIDOR DE DOMINIO

La figura 3.9 muestra el formato del mensaje utilizado por el servidor de nombres de dominio para las preguntas como para las respuestas en la resolución de nombres. Las respuestas también contienen información acerca de los servidores que son autoridad proporcionando su dirección IP. Cada mensaje empieza con un encabezado fijo, el cual contiene un campo de IDENTIFICACIÓN que el cliente usa para empatar las respuestas con las preguntas, un campo PARÁMETRO que especifica la operación solicitada y un código de respuesta.

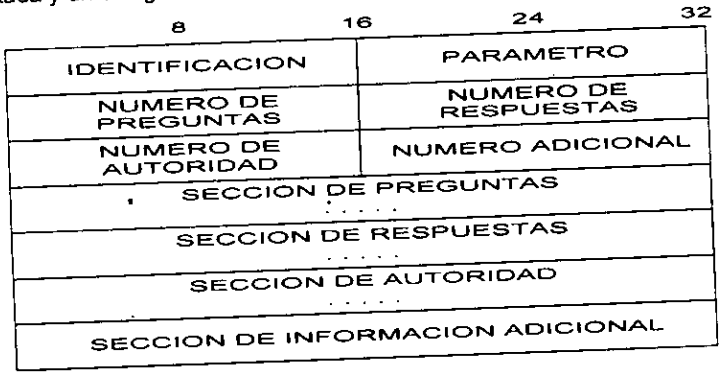


Figura 3.9 Formato del mensaje DNS

A continuación se da la interpretación de los bits en el campo PARÁMETRO.

[6] Con fines de consistencia para el DNS, los octetos de la dirección IP deben ser escritos en forma inversa cuando se forme una pregunta apuntadora, ya que las direcciones IP tienen los octetos mas significativos al inicio, mientras que los nombres de dominio los tienen al final.

Bit del campo PARÁMETRO	Significado
0	Operación:
	0 Pregunta
	1 Respuesta
1-4	Tipo de Pregunta
	0 Estándar
	1 Inversa
	2 Complemento 1 (ahora obsoleto)
	3 Complemento 2 (ahora obsoleto)
5	Establece si la respuesta es certificada
6	Establece si el mensaje es truncado
7	Establece si se desea recursion[7]
8	Establece si la recursion está disponible
9-11	Reservado
12-15	Tipo de Respuesta:
	0 No hay error
	1 Error de formato en la pregunta
	2 Falla en el servidor
	3 El nombre no existe

Los campos nombrados NUMERO DE, cada uno dan una cuenta de las entradas en las secciones correspondientes que aparecen más abajo en el mensaje. Por ejemplo, el campo NUMERO DE PREGUNTAS da la cuenta de entradas que aparecen en la SECCIÓN PREGUNTAS del mensaje.

Los siguientes campos son de longitud variable: la SECCIÓN DE PREGUNTAS contiene preguntas para las cuales se busca una resolución. El cliente llena sólo la sección de preguntas; el servidor regresa las preguntas y respuestas en su mensaje de contestación. Cada pregunta consiste de una PREGUNTA DE NOMBRE DE DOMINIO seguida por los campos TIPO DE PREGUNTA y CLASE DE PREGUNTA como muestra la figura 3.10

[7] Si el cliente solicita una traducción completa (resolución recursiva, en terminología de nombres de dominio), el servidor inicial contacta a uno o varios servidores hasta que se resuelva el nombre y regresa la respuesta al cliente. Si el cliente no solicita una resolución recursiva (resolución iterativa), el servidor inicial de nombres no podrá proporcionar una respuesta. Sólo generará un mensaje que especifica el nombre del siguiente servidor que el cliente debe contactar para resolver el nombre.

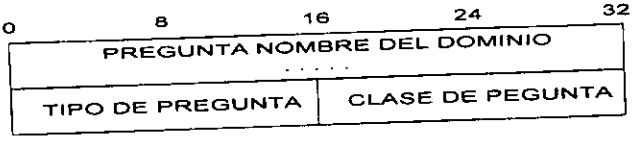


Figura 3.10 Formato de la sección de preguntas dentro del mensaje DNS

El TIPO DE PREGUNTA codifica el tipo de la pregunta (por ejemplo, si la pregunta se refiere a un nombre de máquina o una dirección) . Cabe hacer la aclaración que aunque la figura 3.10 sigue la convención de mostrar los formatos de los encabezados en múltiplos de 32 bits, el campo PREGUNTA DE NOMBRE DE DOMINIO puede contener un número arbitrario de octetos.

En lo que respecta al mensaje de respuesta de un servidor de nombres, cada una de los campos SECCIÓN DE RESPUESTAS, SECCIÓN DE AUTORIDAD y SECCIÓN DE INFORMACIÓN ADICIONAL consiste de un conjunto de registros de recursos que describen los nombres de dominio y los mapeos. Cada registro de recursos describe un nombre. La figura 3.11 muestra el formato del mensaje.

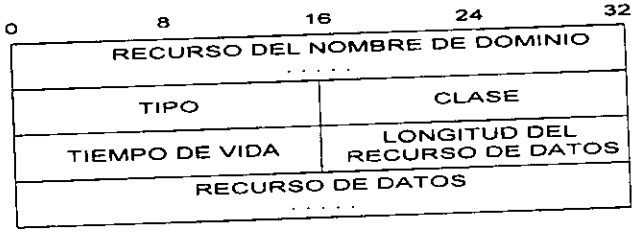


Figura 3.11 Formato de los registros de recursos regresados por los servidores de nombres de dominio

El campo RECURSO DEL NOMBRE DE DOMINIO contiene el nombre de dominio al cual este registro de recurso se refiere. Puede ser de longitud variable. El campo TIPO especifica el tipo de los datos incluido en el registro de recurso; el campo CLASE especifica la clase de los datos. El campo TIEMPO DE VIDA contiene un valor numérico que especifica el numero de segundos en los cuales la información es valida dentro del cache del registro de recurso. Los últimos dos campos contienen los resultados del mapeo, con el campo LONGITUD DEL RECURSO DE DATOS especificando la cuenta de los octetos en el campo RECURSO DE DATOS.

Se puede recapitular todo el proceso de direccionamiento y mapeo llevado a cabo en Internet mediante un ejemplo. Cuando un programa de aplicación, para su ejecución es provisto con un nombre de dominio, como: **telnet nic.merit.edu** ; el programa de aplicación en este caso telnet, hace una llamada al DNS para mapear el nombre de dominio (nic.merit.edu) a su dirección IP equivalente. Una vez obtenida la dirección IP, ésta es utilizada por el software en todo el proceso de comunicación. Cabe hacer la aclaración de que si una aplicación se ejecuta con la dirección IP en notación cuadrática del host destino, obviamente se ahorra este mapeo, por ejemplo, la dirección IP del dominio nic.merit.edu es 35.1.1.48, entonces, se tendría la siguiente alternativa: **telnet 35.1.1.48**

Un segundo mapeo se efectúa para la entrega de los datos al host destino, mediante la traducción de la dirección IP a la dirección física de la tarjeta de red; mediante el uso del protocolo ARP.

3.10 TCP/IP = PILA DE PROTOCOLOS

Como se ha podido observar a lo largo de este capitulo, los sistemas complejos de comunicación de datos no utilizan un protocolo único para manejar todas las tareas de comunicación. En su lugar, hacen uso de un conjunto cooperativo de protocolos llamados familia de protocolos o suite de protocolos.

El término genérico "TCP/IP" usualmente significa cualquier cosa y todo lo relacionado con los protocolos TCP e IP. Incluye otros protocolos, aplicaciones y aún el medio físico de la red. Una muestra de estos protocolos son ARP (visto en secciones anteriores), UDP, ICMP, etc., (protocolos que se verán en secciones posteriores). Como una muestra de las aplicaciones o servicios se tiene: Telnet, FTP, Correo electrónico, etc.

Para resolver el problema de la comunicación de datos de una máquina a otra a través de un internet, éste es dividido en "subproblemas" .

Conceptualmente la división equivaldría a tener una apilados módulos de protocolos en cada máquina. Así de esta forma cada modulo o capa manejaría un subproblema de la comunicación.

Desde el punto de vista de la transmisión, el envío de un mensaje desde un programa de aplicación en una máquina a un programa de aplicación en otra dentro de

una red, equivaldría a hacer pasar el mensaje a través de la pila de protocolos en sentido descendente en la máquina emisora, a medida que el mensaje pasa por cada una de las capas se le agrega un encabezado (como si al pasar por una capar el mensaje se introdujera en un sobre, al pasar a la siguiente capa se introdujera en un sobre mayor y así sucesivamente); se hace transferir el mensaje a través de la red y finalmente en la máquina receptora el mensaje circulando en forma ascendente a través de la pila de protocolos va removiendo por cada capa su encabezado correspondiente, hasta que los datos llegan al modulo correspondiente al programa de aplicación, como muestra la figura 3.12.

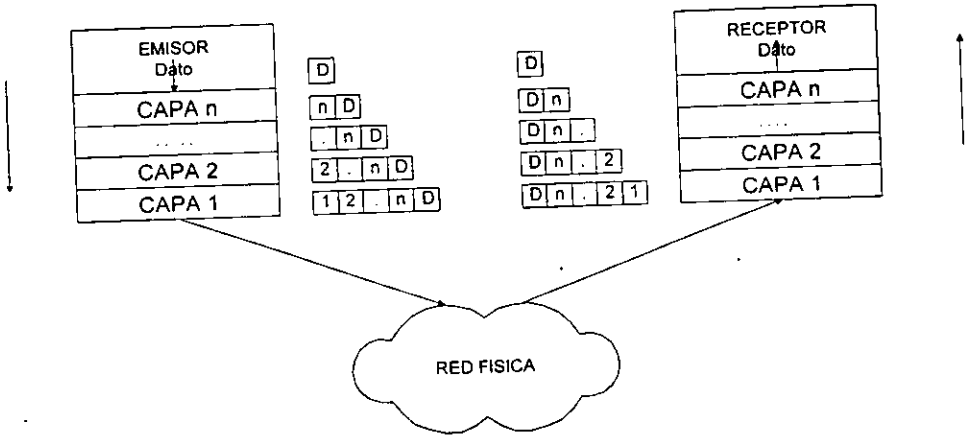


Figura 3.12 Organización conceptual de las capas de protocolos

Este modelo manejado en una sola red puede ser generalizado en un internet. Por ejemplo la figura 3.13 muestra las capas de protocolos usadas por un paquete que atraviesa tres redes.

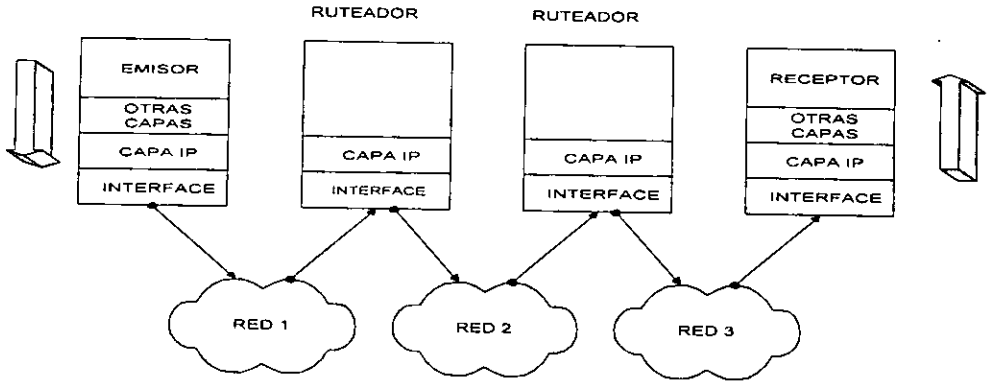


Figura 3.13 Ruta que siguen los paquetes desde el emisor, pasando por dos ruteadores hasta llegar al receptor, en un internet.

El diagrama muestra sólo la capa de interface de red y la capa del Protocolo Internet en los ruteadores debido a que sólo estas capas intervienen en la recepción, envío y ruteo de paquetes.

3.10.1 EL MODELO DE CAPAS DE TCP/IP

Hablando ampliamente, el software TCP/IP esta organizado en cuatro capas o estratos conceptuales, construidas sobre una quinta capa que es el nivel de hardware. La figura 3.14 muestra las capas conceptuales, así como la forma de los datos de acuerdo a como van siendo pasados entre ellas.

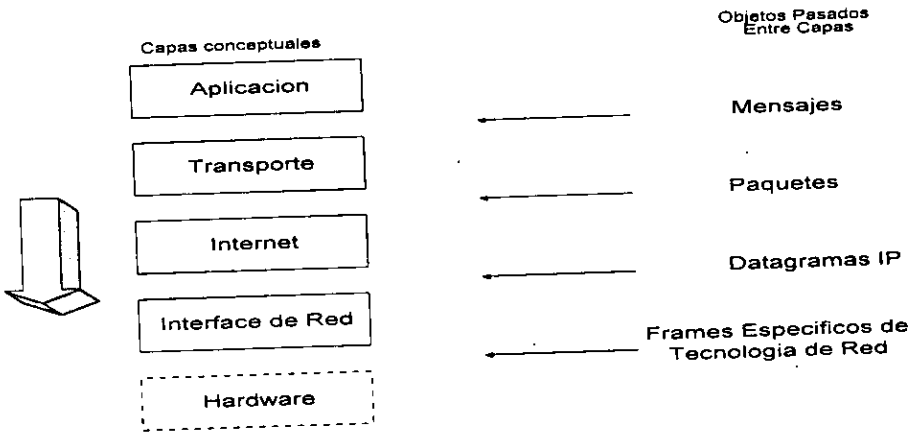


Figura 3.14 Las cuatro capas conceptuales del software TCP/IP y la forma de los objetos pasados entre las capas.

- **Capa de Aplicación**. Al nivel más alto, los usuarios invocan los programas de aplicación que accesan a los servicios disponibles a través de un internet TCP/IP. Una aplicación interactua con uno de los protocolos de la capa de transporte para enviar y recibir datos. Cada programa de aplicación elige el estilo de transporte necesario, el cual puede ser ya sea una secuencia de mensajes individuales o una corriente continua de bytes. El programa de aplicación pasa los datos en la forma requerida a la capa de transporte para su entrega.

Aunque la figura 3.14, usa un bloque sencillo para representar la capa de aplicación, una computadora de propósito general puede tener múltiples programas de aplicación accesando el internet a la vez.

- **Capa de Transporte**. El objetivo primario de la capa de transporte es proveer comunicación de un programa de aplicación a otro. Tal comunicación es frecuentemente llamada de extremo-a-extremo. La capa de transporte puede regular el flujo de la información. Puede también proveer un transporte confiable, asegurando que los datos lleguen sin error y en secuencia. Para hacer esto, el protocolo de transporte implementa que el lado receptor envíe de regreso al lado emisor acuses de recibo de los paquetes recibidos, y que a su vez el lado emisor retransmita paquetes en el caso de que se pierdan. El software de transporte divide la corriente de datos a ser transmitidos en

paquetes o fragmentos y los pasa con su dirección de destino a la siguiente capa para su transmisión.

La capa de transporte debe aceptar datos desde varios programas de aplicación y enviarlos a la siguiente capa inferior. Para hacer esto, le agrega información adicional a cada paquete (encabezado), incluyendo códigos que identifican cual programa de aplicación debe recibirlo, así como información para verificación de errores (checksum). La máquina receptora usa el checksum para verificar que el paquete haya llegado intacto, y utiliza el código de destino (puerto) para identificar el programa de aplicación al cual debe ser entregado.

- **Capa Internet.** La capa Internet se encarga del manejo de la comunicación de una máquina a otra. Acepta una solicitud para enviar un paquete de la capa de transporte con una identificación de la máquina a la cual el paquete debe ser enviado. Encapsula el paquete en un datagrama IP, llena el encabezado del datagrama, usa el algoritmo de ruteo para determinar si entrega el datagrama directamente (la misma red) o lo envía a un ruteador (hacia un nodo remoto, al internet), y finalmente pasa el datagrama a la interface de red apropiada del ruteador para su transmisión. La capa Internet también maneja el arribo de paquetes, checando su validez, y usando el algoritmo de ruteo para decidir si el datagrama debe ser procesado localmente o ser lanzado hacia otra red. Para datagramas direccionados a una máquina local, el software en la capa Internet de la máquina destino remueve el encabezado IP, y elige de entre algunos protocolos de transporte el que va a manejar al paquete. Finalmente, la capa Internet envía mensajes de error y de control conforme sea necesario mediante el uso de otro protocolo llamado ICMP.

- **Capa de Interface de Red.** El nivel más bajo del software TCP/IP comprende una capa de interface de red, responsable de aceptar datagramas IP y transmitirlos sobre una red física determinada. Una interface de red puede consistir de un manejador de dispositivo (por ejemplo, cuando la máquina se enlaza directamente a una red local) o un subsistema complejo que utiliza su propio protocolo de enlace de datos.

Hasta este momento, se ha explicado implícitamente como funciona la capa de interface de red para la tecnología Ethernet. Más adelante en este capitulo se explican

con mayor detalle las capas de Transporte e Internet de la suite de protocolos TCP/IP y en el siguiente capitulo se habla sobre la capa de aplicaciones.

3.10.2 EL PRINCIPIO DE LA ESTRATIFICACIÓN DE PROTOCOLOS

Independientemente del esquema particular de estratificación usado, o de las funciones de las capas, la operación está basada en una idea fundamental llamada el principio de estratificación que dice: "La estratificación de los protocolos está diseñada de tal forma, que el estrato **n** en la máquina receptora recibe exactamente el mismo objeto enviado en el estrato n por parte de la máquina emisora".

La idea de la estratificación es fundamental debido a que provee un marco conceptual para el diseño de los protocolos. Permite al diseñador de protocolos enfocar su atención en una capa a la vez, sin preocuparse acerca del desempeño de las demás capas. El diseñador asume que un host recibe (hablando de una capa en particular) exactamente la misma información, de la correspondiente capa en la máquina emisora.

La figura 3.15 ilustra como funciona el principio de estratificación para una sola red.

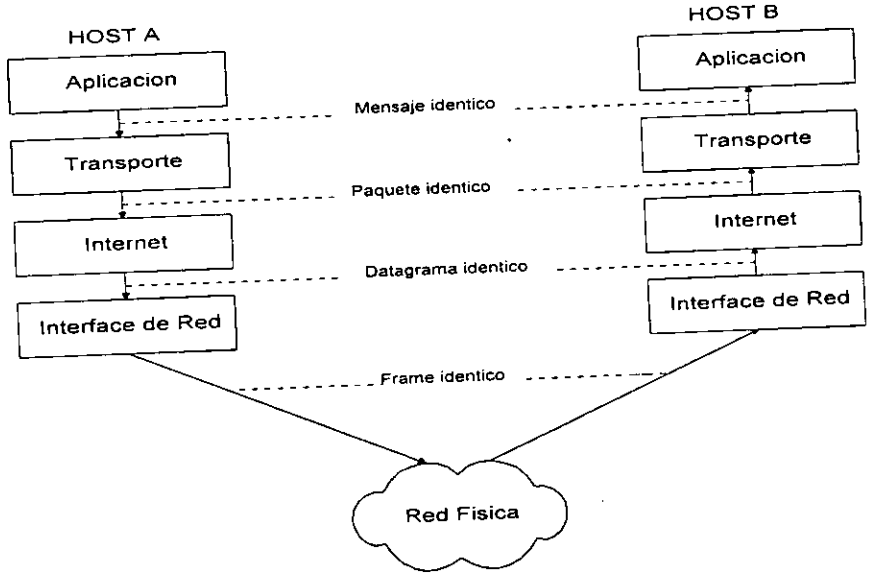


Figura 3.15 Principio de estratificación en TCP/IP en una red física

Trasladando el principio de estratificación a un ambiente Internet TCP/IP, la figura 3.15 quedaría de la siguiente manera:

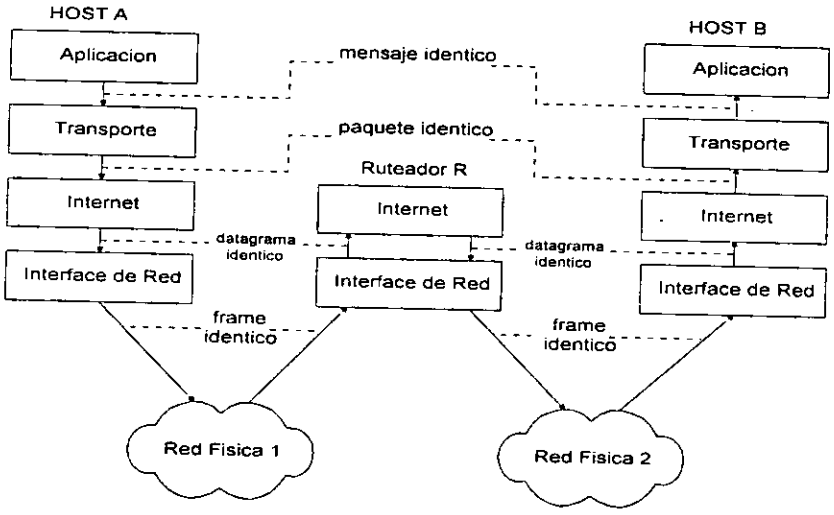
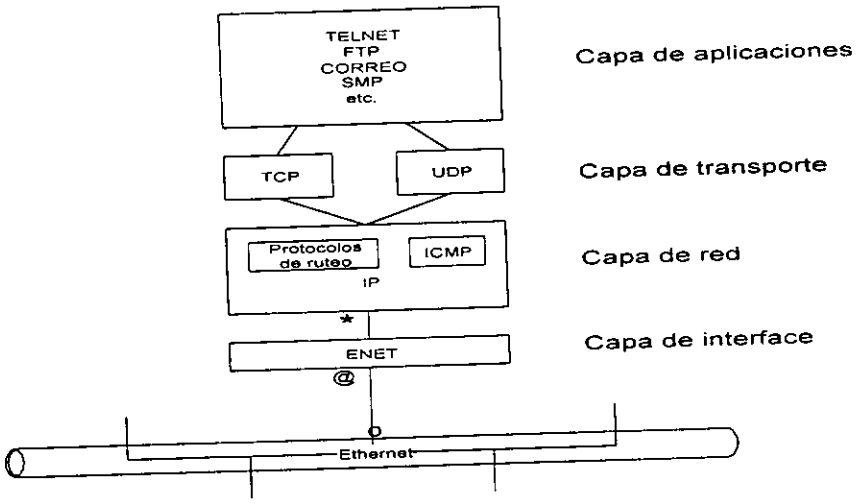


Figura 3.16 Principio de estratificación aplicado a un ambiente Internet

3.10.3 ESTRATIFICACIÓN DE LOS PROTOCOLOS EN UN MEDIO INTERNET

La figura 3.17 muestra la estructura lógica de la pila de protocolos dentro de una máquina en Internet.



3.17 Estructura lógica de los protocolos TCP/IP en un host

Es esta estructura lógica la que determina el comportamiento de la computadora dentro de la red.

En la figura las cajas representan procesamiento de datos conforme éstos pasan a través de la pila, y las líneas conectando las cajas muestran la ruta de los datos. La línea horizontal en la parte inferior representa el cable Ethernet; la "Ò" es el transceptor[8], el * es la dirección IP y la @ es la dirección Ethernet.

3.10.3.1 TERMINOLOGÍA

El nombre que toma una unidad de datos que fluye a través de un internet depende de donde este colocada en la pila de protocolos, ver figura 3.14. Si está en un Ethernet es llamado un frame Ethernet, si está entre el manejador[9] Ethernet y el modulo[10] IP es llamado un datagrama IP; si está entre el modulo IP y el modulo UDP es llamado un segmento UDP; si está entre el modulo IP y el modulo TCP es llamado un segmento o paquete TCP (más generalmente a la unidad de datos ubicada entre la capa IP y la capa superior, se le conoce como mensaje de transporte) y por último si está

[8] Transceptor es un dispositivo que conecta físicamente a la tarjeta de red con el medio físico, sirven para censar colisiones de los paquetes.
[9] Un manejador es software que se comunica directamente con la interface de red.
[10] Un modulo es software que se comunica con un manejador, con aplicaciones u otros módulos.

entre la capa de aplicación y la capa de transporte se le conoce como mensaje de aplicación.

3.10.3.2 FLUJO DE DATOS

Siguiendo el camino que toman los datos a través de la pila de protocolos se puede observar (figura 3.17) como un programa de aplicación puede utilizar como protocolo de transporte a TCP o a UDP (se ven más adelante en este capitulo), un ejemplo de aplicación típica que utiliza TCP es el Protocolo de Transferencia de Archivos (FTP) y su pila de protocolos seria FTP/TCP/IP/ENET. Una aplicación que utiliza como protocolo de transporte UDP es el Protocolo Simple de Administración de Red (Simple Network Management Protocol, SNMP) y su pila de protocolos seria SNMP/UDP/IP/ENET.

Los módulos en la capa de transporte en el envío de información se comportan como multiplexores. Al igual que los multiplexores físicos conmutan muchas entradas a una salida. En la recepción de información se comportan como demultiplexores, es decir, conmutan una entrada a muchas salidas, seleccionando una de estas de acuerdo al valor que contenga el campo Tipo en el encabezado del paquete.

Si un frame Ethernet es recibido por una máquina, el paquete puede ser enviado ya sea al modulo ARP o al modulo IP. El valor que contenga el campo Tipo en el frame Ethernet determina si es pasado ya sea al modulo ARP o al modulo IP.

Si un paquete IP llega al modulo IP, la unidad de datos es pasada ya sea a TCP o UDP, de acuerdo al valor del campo Protocolo en el encabezado IP. Si el datagrama UDP, llega a la capa de aplicación, es tomado por una aplicación de acuerdo al valor del campo Puerto en el encabezado UDP. Si el mensaje viene del modulo TCP, el mensaje es pasado hacia la capa de aplicación basado en el valor del campo Puerto en el encabezado TCP.

El multiplexaje en el envío de un paquete es sencillo de ejecutar debido a que desde cualquier punto de inicio hay sólo una ruta, cada capa de protocolo agrega su encabezado de información, de está forma cuando el paquete llega al host destino conforme va subiendo por la pila de protocolos cada capa va removiendo su encabezado correspondiente permitiendo demultiplexar el paquete.

3.11 EL PROTOCOLO INTERNET (IP)

El Protocolo Internet (IP) es el protocolo que implementa a la capa de red dentro del modelo de cuatro capas de TCP/IP. Define un mecanismo de entrega de paquetes sin conexión y no confiable. El servicio que proporciona el protocolo IP es denominado sin conexión ya que cada paquete transmitido en la red es manejado en forma independiente de los demás paquetes. Es considerado como no confiable, debido a que la entrega de un paquete no está garantizada; el paquete puede perderse, duplicarse, retrasarse, o entregarse en desorden; e IP no detectara tal condición así como tampoco informara al emisor o receptor.

El Protocolo Internet provee de tres importantes definiciones:

- El Protocolo Internet define la unidad básica de transferencia de datos usada a través de un internet TCP/IP. De está forma el protocolo especifica el formato exacto de todos los datos que circulan en la red.

- El software IP ejecuta la función de ruteo, eligiendo una ruta a través de la cual los datos serán enviados.

- IP incluye un conjunto de reglas que incorporan la idea de un sistema de entrega de paquetes no confiables. Las reglas definen, como deben tanto los hosts como los ruteadores procesar los paquetes; como y cuando los mensajes de error deben ser generados, y las condiciones bajo las cuales los paquetes deben ser descartados.

El Protocolo Internet es una parte tan fundamental del diseño de Internet que es llamado en ocasiones la tecnología IP.

3.11.1 EL DATAGRAMA INTERNET

La analogía entre una red física y un internet TCP/IP es fuerte. En una red física, la unidad de transferencia es un frame que contiene un encabezado y datos, donde el

encabezado da información tal como las direcciones físicas del host emisor y receptor (direcciones físicas o Ethernet).

En un internet la unidad básica de transferencia es denominada: datagrama internet, conocido también como datagrama IP o simplemente datagrama.

Al igual que un frame físico, un datagrama está dividido en un encabezado y una área de datos; el encabezado contiene una dirección fuente y destino, así como un campo de tipo que identifica el contenido de los datos del datagrama. La diferencia por supuesto, es que el encabezado del datagrama contiene direcciones IP y el encabezado del frame contiene direcciones físicas. La figura 3.19 muestra el formato general de un datagrama.

Figura 3.19 Formato general de un datagrama IP

3.11.2 FORMATO DEL DATAGRAMA IP

La figura 3.20 muestra la estructura de los campos que conforman a un datagrama IP. El procesamiento de los datagramas se hace por parte del software, por lo tanto el contenido y formato de los datagramas no está dictado por algún hardware particular.

Figura 3.20 Formato del datagrama IP

- **Número de Versión**. Es un campo de 4 bits que contiene el número de versión del protocolo que fue usado para crear el datagrama. Es utilizado para verificar que tanto el emisor, receptor y cualquiera de los ruteadores que intervengan estén de acuerdo en el formato del datagrama. A todo el software IP se le requiere que cheque el campo de versión antes de procesar un datagrama, para asegurarse que cumpla con el formato que el software espera recibir. Los dispositivos rechazaran datagramas con versiones de protocolos diferentes a las que estén manejando, previniendo una mala interpretación en el contenido del datagrama. La versión actual del protocolo IP es la 4.

- **Longitud del Encabezado.** Este es un campo también de 4 bits y refleja la longitud total del encabezado IP, medido en palabras de 32 bits. El encabezado más corto es de cinco palabras, pero el empleo de campos opcionales puede aumentar el tamaño. Para descifrar correctamente el encabezado IP se debe saber donde termina el encabezado y donde empiezan los datos, razón por lo cual se incluye este campo (no hay marcador de principio de datos.)

- **Tipo de Servicio.** Este es un campo de 8 bits que especifica como debe ser manejado el datagrama. Está subdividido en cinco subcampos como se muestra en la figura 3.21

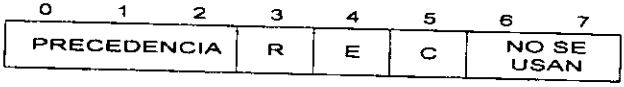


Figura 3.21 Los ocho bits del campo Tipo de Servicio de un datagrama

Los tres primeros bits especifican la precedencia del datagrama, con valores que van desde 0 indicando precedencia normal hasta el valor de 7 que indica control de red. Estos valores permiten al emisor indicar la importancia de cada datagrama. La mayor parte de las implementaciones de TCP/IP y prácticamente todo el hardware que utiliza TCP/IP ignoran este campo, y tratan a todos lo datagramas con el mismo grado de prioridad.

Las tres banderas siguientes de 1 bit controlan el Retraso, el Rendimiento y la Confiabilidad del datagrama; la combinación de estos tres bits especifican el tipo de transporte que el datagrama desea. Cuando se establece en 1, el bit R se solicita un retraso bajo, en el bit rEndimiento se solicita un alto desempeño, y en el bit C se solicita una alta confiabilidad. Por supuesto, no puede ser posible para un internet garantizar el tipo de transporte solicitado (por ejemplo, pudiera ser que ninguna ruta al destino final tuviera las propiedades solicitadas). Por lo tanto se debe pensar en estos tres bits como una pista para los algoritmos de ruteo y no como una demanda. Si un ruteador conoce más de una ruta posible a un destino dado, puede utilizar el campo de Tipo de Servicio para seleccionar una con las características más cercanas a las solicitadas.

Los últimos dos bits del campo Tipo de Servicio no se utilizan.

- **Longitud del Datagrama.** Este campo de 16 bits da la longitud del datagrama IP medido en octectos, incluye los octectos del encabezado y los datos. A partir del valor de este campo se puede determinar el tamaño del área de datos, restándole la longitud del encabezado. Debido a que maneja 16 bits de longitud, el tamaño máximo posible de un datagrama IP es de 2^{16} = 65,535 octetos.

Con el fin de entender mejor la operación de los campos Identificación, Banderas y Desplazamiento de Fragmento; se presenta la siguiente explicación.

Como ya se ha mencionado en secciones anteriores un paquete o datagrama es "acarreado" o encapsulado en un frame. El hardware no reconoce el formato del

datagrama, así como no entiende la dirección IP destino (en general, la información contenida en el campo de datos de un frame). En un caso ideal, se desea que un datagrama IP siempre quepa en un frame físico, haciendo la transmisión a través de la red muy eficiente. Pero en la realidad con un Internet constituida por redes de diferentes tecnologías y por lo tanto con frames de diferentes tamaños esta idea no es factible.

Para entender más claramente esta situación, hay que tener en cuenta que cada tecnología de conmutación de paquetes establece un limite máximo en la cantidad de datos que pueden transferir en un frame físico. Por ejemplo, la tecnologia Ethernet limita el tamaño del frame a 1500 octetos de datos, mientras que FDDI permite aproximadamente 4470 octetos de datos por frame. A estos valores se les conoce Unidades Máximas de Transferencia (MTU, por sus siglas en inglés).

Limitar a los datagramas a llenar el MTU más pequeño posible en el internet hace la transferencia ineficiente, por ejemplo, cuando tienen que pasar a través de redes que puede acarrear en sus frames datos de mayor longitud (de una red Ethernet a una red FDDI) se provoca un desperdicio en el ancho de banda. Sin embargo, si se permite que los datagramas sean más grandes que el MTU más pequeño en un internet significa que un datagrama no siempre va a caber en un frame físico, por ejemplo cuando se pasa de una red FDDI a una red Ethernet.

Por otro lado se ha mencionado que en un internet ningún aspecto está dictado por el hardware, entonces en lugar de diseñar datagramas que se adhieran a la tecnología física de la redes, el software TCP/IP eligió un tamaño conveniente inicial para el datagrama e ideo una forma de dividir datagramas grandes en pequeñas piezas cuando el datagrama necesite cruzar una red que tenga un MTU más pequeño. Las piezas pequeñas en las cuales un datagrama es dividido se les llama fragmentos.

El tamaño de los fragmentos es elegido de tal forma que cada fragmento puede ser acarreado a través del medio en un frame. Debido a que IP representa el desplazamiento de los fragmentos en múltiplos de 8 octetos, el tamaño del fragmento debe ser elegido como un múltiplo de ocho. Por supuesto, al elegir como múltiplo de ocho octetos más cercano al MTU de una red no divide usualmente al datagrama en fragmentos iguales; la ultima pieza es por lo general más pequeña que las otras.

Cada fragmento contiene un encabezado que duplica en su mayoria al encabezado del datagrama original (excepto por un bit en el campo Banderas que

muestra que es un fragmento), seguido por tantos datos como puedan ser acarreados en el fragmento mientras se mantenga la longitud total menor al MTU de la red a través de la cual debe viajar.

Los fragmentos deben ser reensamblados para producir una copia completa del datagrama original antes de que pueda ser procesado. Una vez que un datagrama ha sido fragmentado, los fragmentos viajan como datagramas separados todo el camino hasta el destino final donde deben ser reensamblados mediante el uso del campo desplazamiento de los fragmentos.

Con la presente explicación en mente se procede a explicar los siguientes campos del datagrama IP.

- **Identificación.** Contiene un número único que identifica al datagrama. Cuando un datagrama es fragmentado este numero es copiado en los fragmentos. Su propósito primario es permitir al sitio destino conocer cuales fragmentos pertenecen a cuales datagramas, es decir, asegurar que los fragmentos de un mensaje no se mezclen con los de otros mensajes.

- **Banderas.** El campo de banderas es un campo de tres bits, el primero de los cuales no se utiliza. Los dos bits restantes se dedican a banderas conocidas como NF (no fragmentar) y MF (más fragmentos), las cuales controlan el manejo de los datagramas cuando la fragmentacion resulta deseable.

Si la bandera NF tiene un 1, el datagrama no se puede fragmentar bajo ninguna circunstancia. Si el nodo no puede enviar el datagrama sin fragmentarlo, y este bit está en 1, el datagrama será descartado y se enviará un mensaje de error al dispositivo emisor.

Si la bandera MF está en 1 indica que el paquete será seguido por más fragmentos. El último fragmento, que se envía como parte de un datagrama, tiene su bandera MF en 0, esto para indicar que el dispositivo receptor sepa cuándo detener la espera de datagramas. Debido a que el orden de la llegada de los fragmentos tal vez no corresponda al orden en el cual se enviaron, la bandera MF se utiliza en conjunción con el campo de Desplazamiento del Fragmento para indicarle al dispositivo receptor la extensión total del mensaje.

- **Desplazamiento del Fragmento.** Este es un campo de 13 bits que especifica el desplazamiento dentro del datagrama original de los datos que están siendo acarreados en un fragmento, medido en unidades de 8 octetos, comenzando con el desplazamiento 0. Este campo sirve para reensamblar el datagrama, el sitio destino debe obtener todos los fragmentos empezando con el fragmento que tiene el desplazamiento 0 hasta el fragmento que tiene el desplazamiento más alto.

- **Tiempo de Vida.** Este campo especifica cuanto tiempo en segundos puede permanecer un datagrama en el internet antes de descartarse. Los ruteadores y hosts que procesen datagramas deben decrementar este campo conforme el tiempo pase y remover el datagrama del internet cuando el tiempo expire, además de notificar mediante un mensaje de error al sitio fuente.

Cada ruteador a lo largo de la ruta desde la fuente hasta el destino se le requiere que decremente el campo de Tiempo de Vida en 1 cuando procese un datagrama. Además, para manejar los casos de sobrecarga en los ruteadores que introducen largos retardos, cada ruteador graba el tiempo local de arribo del datagrama, y decrementa el valor del campo el número de segundos que el datagrama permanece dentro del ruteador esperando servicio. La idea de mantener un temporizador para los datagramas es interesante debido a que garantiza que los datagramas no podrán viajar alrededor de un internet por siempre, aun si las tablas de ruteo se corrompen y los ruteadores envían los datagramas entre los ruteadores en un ciclo infinito.

- **Protocolo.** El campo protocolo es análogo al campo Tipo de un frame físico. El valor en el campo Protocolo especifica cual protocolo de transporte fue utilizado para manejar el mensaje que está siendo acarreado en el área de datos de un datagrama. El mapeo entre el protocolo de transporte y el valor entero utilizado en el campo Protocolo debe ser administrado por una autoridad central para garantizar un acuerdo común a través de todo el internet.

- **Suma De Verificación Del Encabezado.** Asegura la integridad de los valores del encabezado. El valor de verificación se forma tomando el complemento a uno de la

suma de 16 bits de todas las palabras de 16 bits. Para propósitos del calculo del valor de verificación, el campo de Suma de Verificación se considera que contiene cero.

Es importante notar que el calculo del valor de verificación no incluye a los datos. El tener sumas de verificación por separado de los encabezados y los datos, tiene ventajas y desventajas. Debido a que el encabezado usualmente ocupa menos octetos que los datos, teniendo una verificación de éste por separado reduce el tiempo de procesamiento en los ruteadores, los cuales sólo necesitan calcular el valor de verificación de los encabezados. La separación también permite a los protocolos de alto nivel elegir sus propios formatos de verificación para los datos. La principal desventaja es que los protocolos de alto nivel están forzados a agregar un esquema de verificación de datos, o se corre el riesgo de tener información dañada sin detectar.

- **Direcciones IP del Emisor y el Destino.** Estos campos contienen las direcciones IP de 32 bits de los hosts emisor y destino. Estos campos se establecen al crearse el datagrama, y aunque el datagrama puede ser enrutado a través de muchos ruteadores intermedios, los valores de estos campos nunca cambian.

- **Opciones.** El campo Opciones no es requerido en cada datagrama; las opciones son incluidas principalmente para prueba y depuración de la red.. Este campo se compone de 24 bits divididos de la siguiente manera, un octeto para identificar un código, el cual puede estar seguido por un octeto que indica longitud y un octeto comodín.

La longitud del campo Opciones varia dependiendo de cuales opciones son seleccionadas. Algunas opciones son de un octeto de longitud; consisten solamente del código y otras son de longitud variable.

El octeto de código está a su vez dividido en tres campos: una bandera de **copia** de 1 bit, una **clase de opción** de 2 bits y un **numero de opción** de 5 bits. La bandera de copia se utiliza para estipular cómo será manejada la opción cuando sea necesaria la fragmentacion en un ruteador. Cuando el bit se establece en uno, especifica que la opción debe ser copiada en todos los fragmentos. Cuando se establece en cero, significa que la opción debe ser sólo copiada al primer fragmento.

La combinación de la clase de opción y el número de opción especifican la clase general de la opción y la opción especifica dentro de dicha clase. Las diferentes clases que existen son:

Clase de Opción	Significado
0	Control de red o datagrama
1	Reservado para uso futuro
2	Depuración y medición
3	Reservado para uso futuro

A continuación se muestran las posibles combinaciones validas entre la clase de opción y el número de opción:

Clase de opción	Número de opción	Longitud	Descripción
0	0	-	Fin de la lista de opciones.
0	1	-	Ninguna operación (usado para alinear octetos en una lista de opciones)
0	2	11	Opciones de seguridad (para fines militares únicamente)
0	3	variable	Enrutamiento de fuente libre. Usado para enrutar un datagrama a través de una ruta especifica
0	7	variable	Graba ruta. Usado para especificar una ruta
0	8	4	Obsoleto
0	9	variable	Enrutamiento de fuente estricto. Usado para enrutar un datagrama a través de una ruta especificada.
2	4	variable	Marcado de tiempo activo. Usado para grabar las marcas de tiempo a través de la ruta

La opción Graba Ruta permite al host emisor crear una lista vacia (contenida dentro del datagrama) de direcciones IP e implementar que cada ruteador por el cual pase el datagrama rumbo al host destino, agregue su dirección IP a la lista. Como se puede ver

esta opción se utiliza para obtener un registro del paso del datagrama a través de un internet, lo que puede resultar útil para efectos de diagnóstico.

Otra idea que los diseñadores encontraron interesante es la opción de Enrutamiento de fuente. Provee una forma para el emisor de dictar una ruta a través del internet. Por ejemplo, para probar el desempeño a través de una red física particular, R, los administradores del sistema pueden usar el enrutamiento de fuente para forzar que los datagramas IP atraviesen la red R aún si los ruteadores normalmente eligen otra ruta para ese destino.

IP soporta dos formas del enrutamiento de fuente. Una forma, llamada Enrutamiento de Fuente Estricto, especifica la ruta exacta que los datagramas deben seguir para llegar a su destino por medio de una secuencia de direcciones IP. La ruta entre dos direcciones sucesivas en la lista debe consistir de una red física; un error resulta si un ruteador no puede seguir la ruta. La otra forma, llamada Enrutamiento de Fuente Libre, también incluye una secuencia de direcciones IP. Especifica que el datagrama debe seguir la secuencia de direcciones IP pero permite múltiples "saltos" a otras redes entre dos direcciones sucesivas en la lista.

La opción de Marca de Tiempo trabaja como la opción Grabar Ruta en el sentido que contienen una lista inicial vacía, y cada ruteador a lo largo de la ruta desde la fuente hasta el destino llenan un renglón en la lista. La opción Marca de Tiempo tiene dos campos de 32 bits, la dirección IP del ruteador que está dando la entrada, y una marca de tiempo.

Las marcas de tiempo dan la hora y la fecha en la cual el ruteador manejo el datagrama, expresada en milisegundos desde la media noche, Tiempo Universal. Desafortunadamente, como la mayor parte de los sistemas tienen parámetros de tiempos muy distintos, aun cuando corregidos a tiempo universal, las marcas de tiempo se deberán tratar con cierta reserva.

- **Relleno.** Su contenido depende de las opciones seleccionadas. Por lo general el relleno se utiliza con bits en cero para asegurarse de que el encabezado del datagrama se extiende a un múltiplo exacto de 32 bits.

- **Datos.** El campo marcado como Datos en la figura 3.20 muestra el inicio del área de datos del datagrama. Su longitud incluyendo el encabezado depende, por su puesto, de la MTU de la tecnología de red que está manejando al datagrama.

3.12 EL PROTOCOLO INTERNET DE CONTROL DE MENSAJES (ICMP)

Considerando que pueden existir problemas en la transmisión de los datragramas en un internet, tales como fallas en las líneas de comunicación y las computadoras, la terminación del tiempo de vida de un datagrama, los datagramas fragmentados tal vez no lleguen con todos los segmentos intactos, un mal enrutamiento, etc. Entonces se presenta, la necesidad de establecer un mecanismo que le haga saber al dispositivo emisor cuando existan problemas con el manejo de los datagramas.

Para permitir a los ruteadores en un internet reportar errores o proporcionar información acerca de circunstancias inesperadas, los diseñadores agregaron un mecanismo de mensajes de propósito especial para los protocolos TCP/IP. El mecanismo conocido como el Protocolo Internet de Control de Mensajes (ICMP), es una parte integral del protocolo IP y debe incluirse en cualquier implementacion.

Los mensajes ICMP viajan a través del internet en la porción de datos de los datagramas IP. El ultimo destino de un mensaje ICMP no es un programa de aplicación o un usuario en la máquina destino, sino el software IP en tal máquina, es decir, ICMP provee comunicación entre el software IP de dos máquinas. Por supuesto, si ICMP determina que un protocolo de alto nivel o programa de aplicación ha causado el problema, informará al modulo apropiado.

Inicialmente diseñado para permitir a los ruteadores reportar la causa de errores de entrega a los hosts, ICMP no está restringido a sólo ruteadores. Así, un host puede usar ICMP para comunicarse con un ruteador u otro host

3.12.1 REPORTANDO CONDICIONES DE ERROR AL HOST EMISOR

Técnicamente hablando, ICMP es un mecanismo que reporta condiciones de error. Provee una forma para los ruteadores que encuentran un error reportarlo al host emisor, aunque la especificación del protocolo sugiere posibles acciones a ser tomadas en respuesta a reporte de errores, ICMP no especifica totalmente la acción a ser tomada

por cada error posible. ICMP restringe la comunicación con la fuente original debido a que, como se menciono en secciones anteriores los datagramas sólo contienen las direcciones IP fuente y destino, de esta forma si se presenta un error en un ruteador intermedio, se emite un mensaje al host original aunque no sepa cual ruteador causo el problema.

Debido al sistema de ruteo que sigue un internet, cuando un datagrama llega a un ruteador después de haber recorrido varias redes o aun después de haber atravesado una sola red, le es imposible conocer la ruta que ha seguido el datagrama para llegar hasta él. El datagrama no contiene un registro completo de su viaje a través del internet. La excepción es cuando se establece el enrutamiento de fuente (fijar una ruta a seguir), pero esto sólo se hace con propósitos de diagnostico o depuración para la red. De esta manera si el ruteador detecta un problema, como no puede saber el conjunto de máquinas intermedias que procesaron el datagrama, el ruteador usa ICMP para informar a la fuente original que un problema ha ocurrido, y confía que los administradores de las redes cooperaran entre si para localizar y reparar el problema.

3.12.2 ENCAPSULACION DE UN MENSAJE ICMP

Los mensajes ICMP requieren de dos niveles de encapsulacion como lo muestra la figura 3.22 . Cada mensaje ICMP viaja a través del internet en la porción de datos de un datagrama IP, el cual como puede pasar a través de redes de diferentes tecnologías en su camino al nodo emisor, es encapsulado en la porción de datos del frame que caracteriza a cada una de las redes por las cuales va pasando.

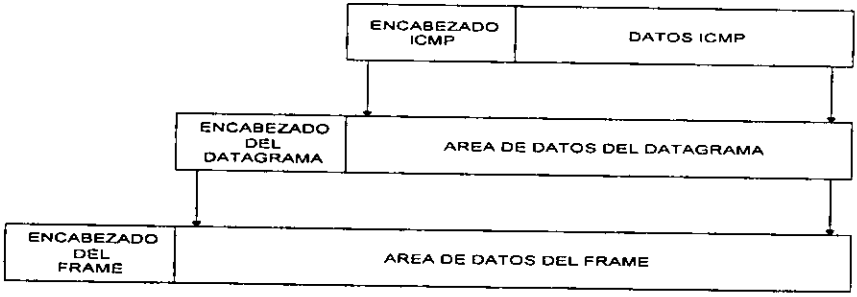


Figura 3.22 Encapsulacion de un mensaje ICMP

Los datagramas que llevan un mensaje ICMP son enrutados exactamente como los datagramas que llevan información de los programas de aplicación; no hay consideraciones especiales. Por lo tanto los mensajes pueden perderse, desecharse, o generar errores. Con el fin de evitar mensajes de error de datagramas que llevan mensajes de error, ICMP establece que solamente en esta condición no se generen tales mensajes.

Es importante mantener en mente que aunque los mensajes ICMP son encapsulados por IP, ICMP no es considerado un protocolo de capa superior, que en este caso correspondería a la capa de transporte (ver figura 3.17). Es considerado como una parte requerida del protocolo IP. Reiterando, la razón de usar IP para entregar mensajes ICMP es debido a la que necesidad que tienen de viajar a través de redes físicas de diferentes tecnologías para llegar a su destino final que en este caso es el nodo emisor.

3.12.3 FORMATO DEL MENSAJE ICMP

Todos los mensajes ICMP tienen en común tres campos en sus encabezados, como muestra la figura 3.23, un campo Tipo de mensaje de 8 bits que identifica al mensaje, un campo Código de 8 bits que provee mayor información acerca del tipo del mensaje y un campo de 16 bits de Suma de Verificación (funciona igual que la suma de verificación de IP, pero la diferencia con ICMP es que éste sólo cubre el mensaje).

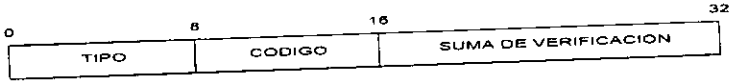


Figura 3.23 Los tres campos comunes dentro de los mensajes ICMP

Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama causante del problema. Los protocolos de alto nivel en la familia TCP/IP están diseñados de tal forma que información crucial está codificada en los primeros 64 bits.

La razón por la cual se regresa el encabezado más los primeros 64 bits del datagrama, es para permitir al receptor determinar de una más precisa cual protocolo(s) y cual programa de aplicación son los responsables del mismo.

El campo de Tipo de mensaje puede tener uno de los siguientes valores:

Tipo	Descripción del Mensaje
0	Respuesta de eco
3	Destino no alcanzable
4	Calmar la fuente
5	Solicitud de redireccion
8	Solicitud de eco
11	Tiempo de vida excedido
12	Problema de parámetro
13	Solicitud de marca de tiempo
14	Respuesta de marca de tiempo
15	Solicitud de información (obsoleto)
16	Respuesta de información (obsoleto)
17	Solicitud de mascara de dirección
18	Respuesta de mascara de dirección

- **Solicitud y respuesta de eco.** Estos mensajes se utilizan comúnmente para identificar y depurar problemas en la red. Un host o ruteador envía un mensaje ICMP de solicitud de eco a una máquina destino, cualquier máquina destino que recibe una solicitud de eco genera una respuesta de eco y la envía al host emisor. La solicitud contiene una área de datos opcional; y la respuesta debe regresar una copia de los datos enviados en la solicitud. La solicitud de eco y su respuesta asociada pueden ser usadas para probar si un host destino dado es alcanzable y responde. Estos pares de solicitud-respuesta resultan útiles para la identificación de problemas de enrutamiento, ruteadores con fallas o problemas de cableado. Debido a que tanto la solicitud como la respuesta viajan en datagramas IP, la recepción exitosa de un mensaje de respuesta verifica que las piezas mayores del sistema de transporte trabajan correctamente. Primero, el software IP en la computadora fuente debe enrutar el datagrama. Segundo, los ruteadores intermedios, entre la fuente y el destino deben estar operando y deben enrutar los datagramas correctamente. Tercero, la máquina destino debe estar funcionando, y tanto el software ICMP e IP deben estar trabajando. Finalmente, todos los ruteadores a lo largo de la ruta de regreso deben tener rutas correctas. Un sistema de solicitud-respuesta de uso común es el comando **ping**. El comando ping envía una serie de solicitudes y espera

las respuestas correspondientes. La figura 3.24 muestra el formato del mensaje de solicitud de eco (tipo 8) y respuesta de eco (tipo 9). Los campos Identificador y Numero de Secuencia son utilizados por el emisor para empatar las respuestas con las solicitudes.

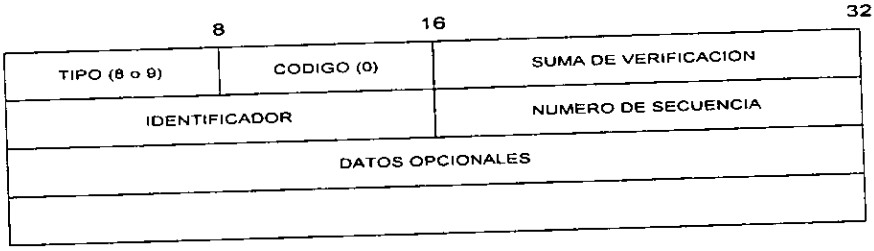


Figura 3.24 Formato del mensaje ICMP de solicitud-respuesta de eco

- **Destino no alcanzable.** Cuando un ruteador no puede enviar o entregar un datagrama IP, envía un mensaje de Destino no alcanzable al nodo emisor original y desecha el datagrama. La figura 3.25 muestra el formato del mensaje de destino no alcanzable.

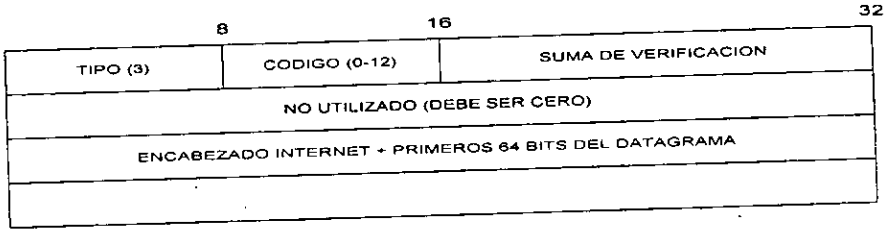


Figura 3.25 Formato del mensaje ICMP de Destino no Alcanzable

El campo Código de un mensaje de Destino no alcanzable contiene un valor que describe con mayor detalle el problema. Los posibles valores de campo Código del mensaje Destino no alcanzable son:

Tipo	Código	Significado
3	0	Red no alcanzable
	1	Host no alcanzable
	2	Protocolo no alcanzable
	3	Puerto no alcanzable
	4	Se requiere fragmentacion y la bandera NF está activa
	5	Fallo el enrutamiento fuente
	6	Red destino desconocida
	7	Host destino desconocido
	8	Host fuente aislado
	9	Comunicación con la red destino prohibida administrativamente
	10	Comunicación con el host destino prohibido administrativamente
	11	Red no alcanzable para tipo de servicio solicitado
	12	Host no alcanzable para tipo de servicio solicitado

Los errores de red no alcanzable usualmente implican fallas en el ruteo; así como fallas en la entrega por parte del ruteador final al host destino. Debido a que los mensajes ICMP contienen un pequeño prefijo del datagrama que causo el problema, la fuente conocerá exactamente la dirección no alcanzable.

Los destinos pueden ser no alcanzables debido a que los dispositivos estén temporalmente fuera de servicio, a que el emisor especifico una dirección destino no existente, o por que el ruteador no tiene una ruta a la red destino.

El significado de los mensajes Protocolo y Puerto no alcanzable se aclararan más adelante cuando se vean como los protocolos de alto nivel usan puntos de destino llamados puertos. La mayoría de los mensajes restantes se explican por sí mismos.

- **Calmar la fuente.** Se utiliza para controlar la velocidad a la cual se transmiten los datagramas , aunque ésta es una forma muy rudimentaria de control de flujo. Generalmente cuando los datagramas llegan demasiado rápido a un host o ruteador, tanto para que estos no los puedan procesar, entonces se almacenan temporalmente en memoria. Si los datagramas son parte de una ráfaga pequeña, tal almacenamiento resuelve el problema. Si el tráfico continua, el host o ruteador agotaran eventualmente su área de memoria (se congestionaran) y desecharan como consecuencia los datagramas

que sigan llegando. Una máquina usa el mensaje ICMP de Calmar la fuente para reportar problemas de congestión al host fuente. Un mensaje de calmar la fuente es una solicitud al nodo emisor original para que reduzca su tasa de transmisión de datagramas. Usualmente, los ruteadores congestionados envían un mensaje de calmar la fuente por cada datagrama desechado. Algunos monitorean el tráfico que les llega y envían mensajes de calmar la fuente a los hosts que tienen las tasas más altas de transmisión. Otros intentan evitar la congestión enviando mensajes de calmar la fuente en la medida que sus áreas de memoria se empiezan a llenar, pero sin llegar a la saturación.

Cuando el host emisor deja de recibir mensajes de calmar la fuente; entonces gradualmente incrementa la tasa de transmisión de datagramas mientras no se vuelvan a recibir nuevamente mensajes de calmar la fuente. La figura 3.26 muestra el formato del mensaje ICMP calmar la fuente.

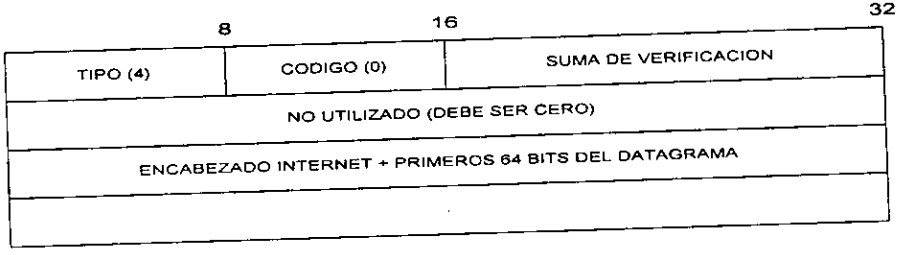


Figura 3.26 Formato del mensaje ICMP Calmar la Fuente

- **Solicitud de redireccion.** Si la topología de una red cambia, las tablas de enrutamiento en un ruteador pueden quedar incorrectas. Un cambio puede ser temporal por ejemplo, cuando el hardware necesita ser reparado; o puede ser permanente por ejemplo, cuando una red nueva se agrega al internet. Como se verá más adelante, los ruteadores intercambian información de enrutamiento periódicamente para acomodar los cambios de la red y mantener sus rutas actualizadas. Un caso especial se tiene cuando un ruteador detecta que otro ruteador está utilizando una ruta no optima, entonces le envía un mensaje ICMP, llamado Solicitud de redireccionamiento para que la actualice. Los mensajes de redireccion se envían a un ruteador en la trayectoria cuando está disponible una ruta mejor. Por ejemplo, si un ruteador acaba de recibir un datagrama de

otro ruteador, pero encuentra otra ruta mejor al verificar sus archivos de datos, regresará el mensaje de redireccion a dicho ruteador, con la dirección IP de la mejor ruta.

Cada mensaje de redireccion contiene además un campo de 32 bits llamado Dirección Internet del Ruteador y un campo Encabezado Internet como muestra la figura 3.27.

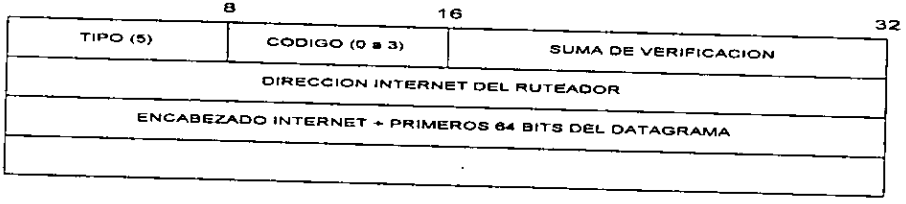


Figura 3.27 Formato del mensaje ICMP de Solicitud de Redirección

El campo dirección internet del ruteador contiene la dirección del ruteador que se tiene que utilizar para alcanzar el destino mencionado en el encabezado del datagrama. El campo Encabezado Internet contiene el encabezado IP además de los 64 primeros bits del datagrama que disparo el mensaje. El campo código de un mensaje de redireccion ICMP da más datos de como interpretar la dirección de destino, basado en los siguientes valores:

Tipo	Código	Significado
5	0	Redirecciona datagramas para la red (ahora obsoleto)
	1	Redirecciona datagramas para el host
	2	Redirecciona datagramas para el Tipo de Servicio y Red
	3	Redirecciona datagramas para el Tipo de Servicio y Host

- **Tiempo de vida excedido**. Los errores en las tablas de enrutamiento pueden producir que los datagramas sigan un ciclo infinito en su enrutamiento. Un ciclo puede consistir de dos o más ruteadores, en los cuales sus rutas para llegar a un determinado destino, se apuntan entre si formando un circuito (loop). Como se mencionó previamente, para prevenir que los datagramas circulen por siempre en un internet TCP/IP , cada datagrama contiene un contador de tiempo de vida a veces llamado "contador de brincos". Un ruteador decrementa el contador tiempo de vida cuando procesa un datagrama y lo desecha cuando el contador alcanza el valor de cero.

En cualquier momento que un ruteador desecha un datagrama debido a que su contador de brincos ha alcanzado el valor de cero o por que finaliza el tiempo mientras se está esperando por la totalidad de los fragmentos de un datagrama, se envía un mensaje ICMP de Tiempo excedido de regreso al host emisor, utilizando el formato que se muestra en la figura 3.28.

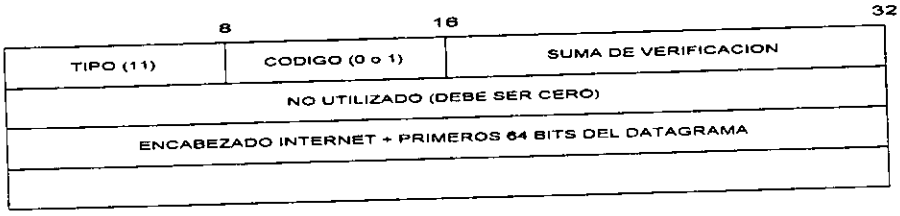


Figura 3.28 Formato del mensaje ICMP de Tiempo de Vida Excedido

El campo Código explica la naturaleza del Tiempo excedido.

Tipo	Código	Significado
11	0	Contador de Tiempo de vida excedido
	1	Tiempo de reensamble de fragmentos excedido

- **Problema de Parámetro.** El mensaje de problema de parámetro se utiliza siempre que se encuentra un error semántico o sintáctico en el encabezado IP. Esto puede ocurrir cuando se utilizan opciones con argumentos incorrectos. El formato del mensaje se muestra en la figura 3.29.

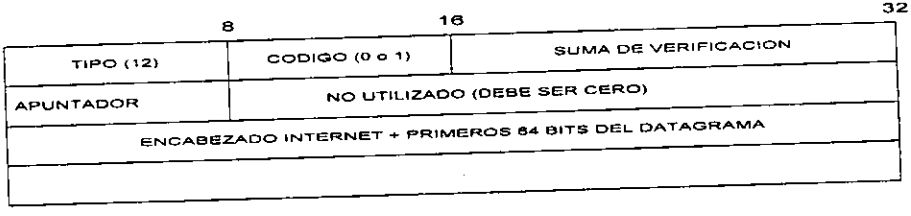


Figura 3.29 Formato del mensaje ICMP de Problema de Parámetro

Para no hacer el mensaje ambiguo, el emisor usa el campo Apuntador en el encabezado del mensaje para identificar el octeto en el datagrama que causo el problema. El código 1 es utilizado para reportar que una opción requerida está faltando, por ejemplo, una opción

de seguridad en la comunidad militar. El campo de Apuntador no se utiliza para el código 1.

- **Solicitud y Respuesta de marca de tiempo.** Aunque las máquinas en un internet pueden comunicarse, usualmente operan en forma independiente, cada máquina mantiene su propia noción del tiempo. Los protocolos TCP/IP incluyen varios protocolos que pueden ser utilizados para sincronizar los relojes. Una de las técnicas más simples usa un mensaje ICMP para obtener el tiempo de otra máquina. Una máquina solicitante envía un mensaje ICMP de Solicitud de Marca de Tiempo a otra máquina. Pidiendo que la segunda máquina regrese su valor de la hora del día. La máquina receptora de la solicitud regresa una Respuesta de Marca de Tiempo a la máquina solicitante. La figura 3.30 muestra el formato de los mensajes de solicitud y respuesta de marca de tiempo.

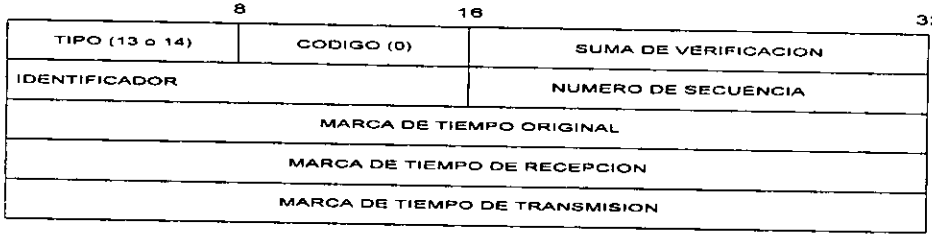


Figura 3.30 Formato del mensaje ICMP de Solicitud-Respuesta de marca de tiempo

El campo Tipo identifica el mensaje como una solicitud (13) o una respuesta (14); los campos Identificador y Numero de Secuencia son utilizados por el host fuente para asociar las respuestas con las solicitudes. Los campos restantes especifican tiempos, dados en milisegundos desde la media noche, es decir, tiempo universal. El campo de Marca de Tiempo de Origen es llenado por el host emisor justo antes de que el paquete sea transmitido, el campo de Marca de Tiempo Recibido es llenado inmediatamente después de la recepción de la solicitud, y el campo de Marca de Tiempo de Transmisión es llenado justo antes de que la respuesta sea transmitida.

Los hosts usan los tres campos anteriores para calcular estimaciones del retardo entre ellos y para sincronizar sus relojes. Cuando se combinan con un enrutamiento estricto, pueden ser muy útiles en la identificación de cuellos de botella en la red.

-Solicitud y Respuesta de dirección de máscara. Cuando los hosts usan un direccionamiento de subred dentro de una red; algunos bits en la porción de la identificación de la red en la dirección IP, son utilizados para identificar a un red física. Para participar en el direccionamiento de subred, un host necesita conocer cuales bits de la dirección internet de 32 bits corresponden a la red física y cuales corresponden al host. La información necesaria para interpretar la dirección es representada en una cantidad de 32 bits llamada máscara de subred.

Para aprender la máscara de subred utilizada por la red local una máquina puede enviar una solicitud de máscara de red a un ruteador y recibir una respuesta de mascara de red. La máquina que esté haciendo la solicitud puede ya sea enviar el mensaje directamente, si conoce la dirección del ruteador, o difundir el mensaje sino lo conoce. La figura 3.31 muestra el formato del mensaje.

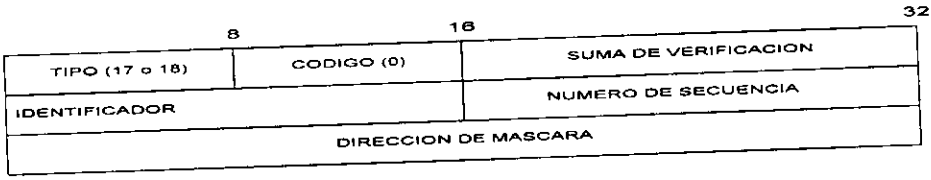


Figura 3.31 Formato del mensaje ICMP de Solicitud-Respuesta de Máscara

El campo Tipo en un mensaje de dirección de máscara especifica si el mensaje es una solicitud (17) o una respuesta (18). Una respuesta contiene la máscara de la dirección de subred en el campo Dirección de Máscara. Como es usual, los campos Identificador y Número de Secuencia le permiten a una máquina asociar las respuestas con las solicitudes.

3.13 EL PROTOCOLO INTERNET Y EL RUTEO

En una red de conmutación por paquetes, el ruteo o enrutamiento se refiere al proceso de elegir una ruta, a través de la cual se enviaran los paquetes en su camino hacia el host destino, y el dispositivo encargado de hacer tal conmutación se le conoce como ruteador.

Por parte del software, como se explico en el apartado 3.11, es el protocolo IP el que se encarga de la función de ruteo, eligiendo una ruta (por medio de un algoritmo de ruteo) a través de la cual los datos serán enviados.

En las siguiente secciones se explica con mayor detalle como se llevan a cabo las funciones de ruteo en Internet.

3.13.1 TIPOS DE RUTEO

Hablando ampliamente, el ruteo se divide en dos tipos: Ruteo Directo y Ruteo Indirecto. El ruteo directo, es la transmisión de un datagrama desde una máquina a través de una red física, directamente a otra máquina. Dos máquinas pueden establecer un ruteo directo sólo si ambas están directamente conectadas a la misma red física. El ruteo indirecto ocurre cuando la máquina destino no está directamente conectada a la red, forzando al emisor a pasar el datagrama a un ruteador para su entrega.

3.13.2 RUTEO DIRECTO

Como se ha explicado, dos máquinas conectadas a una misma red se comunica al nivel más bajo por medio de frames. Para transferir un datagrama IP, el emisor encapsula el datagrama dentro de un frame, mapea la dirección de destino del datagrama a una dirección física, y usa el hardware de red (medio físico) para transmitirlo.

Considérese el siguiente ejemplo, la figura 3.32 muestra una red Ethernet con 3 computadoras A, B y C. Cada computadora tiene la misma pila de protocolos TCP/IP como la que se muestra en la figura 3.17. La tarjeta de interface en cada una de las computadoras tiene su dirección Ethernet, el administrador de la red le ha asignado un numero IP a la red, y por lo tanto, cada computadora tiene también su dirección IP.

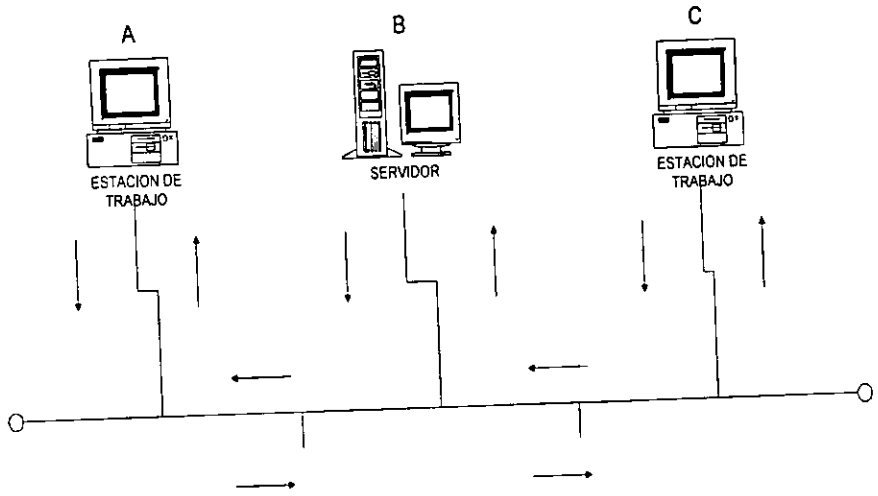


Figura 3.32 Ejemplo de una red con ruteo directo

Cuando A envia un datagrama a B, el encabezado del datagrama contiene la dirección IP de A como la dirección fuente, y el encabezado del frame que lo transporta contiene la dirección Ethernet de A como la dirección fuente Ethernet. También, el encabezado IP contiene la dirección IP de B como la dirección IP destino y el encabezado Ethernet contiene la dirección Ethernet de B como la dirección destino. Resumiendo las direcciones tanto del datagrama como las del frame se verían de la siguiente forma:

	Dirección Fuente	Dirección Destino
Encabezado IP	A	B
Encabezado Ethernet	A	B

Las direcciones IP como se sabe están compuestas por dos partes, una parte que representa el número de la red y otra que representa un host de dicha red. Para determinar si la máquina con la cual se quiere establecer comunicación reside físicamente en la misma red, el emisor es este caso A extrae la porción correspondiente al número de red de la dirección IP del host destino (de B) y la compara con la porción de red de su propia dirección IP. Si ambos coinciden, entonces se está hablando de la misma red, y por lo tanto el datagrama será enrutado en forma directa, es decir, se

encapsula el datagrama en un frame teniendo éste en su campo destino la dirección física del host B.

Desde la perspectiva de un internet, se puede ver al ruteo directo como el paso final en cualquier transmisión de datagramas, aun si el datagrama recorre varias redes y ruteadores intermedios, ya que el ruteador final que se conecta a la misma red física de la computadora destino, entregará el datagrama usando ruteo directo

3.13.3 RUTEO INDIRECTO

En el ruteo indirecto, el host emisor debe identificar un ruteador dentro de la red, al cual pueda enviar los datagramas, cuando el host destino está conectado físicamente en otra red. La función del ruteador es la de redirigir los datagramas rumbo a la red destino.

Para visualizar como trabaja el ruteo indirecto, imagínese un gran internet con muchas redes interconectadas por ruteadores pero con sólo dos hosts a los extremos. Cuando uno de los host quiere enviarle datagramas al otro, el host emisor compara la dirección IP del host destino con su dirección IP, al no coincidir los números de red, entonces no se podrá establecer un ruteo directo en la entrega. Acto seguido, el emisor tendrá que encapsular los datagramas en frames con destino al ruteador de la red, hablando con exactitud, sería hacia la interface[11] física en el ruteador, que comparte el mismo medio físico que el emisor.

Se sabe que puede alcanzar un ruteador, ya que todas las redes están físicamente interconectadas, por medio de estos dispositivos.

Una vez que los frames alcanzan el ruteador, el software IP extrae los datagramas encapsulados, y,como un ruteador tiene tantas direcciones IP como interfaces de red, el modulo IP del ruteador hace una comparación de la dirección destino con cada una de las direcciones IP de las redes que enlaza. Si existe una coincidencia entonces los datagramas son nuevamente encapsulados dentro de frames para ser transmitidos a través del medio físico (por otra interface) y entregarlos en forma directa al host destino. Sino existe coincidencia, entonces el software IP vuelve a encapsular los datagramas en frames dirigiéndolos a través de otra red física a un segundo ruteador, que pueda dirigir a los datagramas en su ruta hacia la red destino. Este proceso se repite sucesivamente

[11] Recuérdese que un ruteador físicamente tiene tantas tarjetas de interface como conexiones de red

hasta que los datagramas llegan a un ruteador, que pueda entregarlos en forma directa a la máquina destino.

La figura 3.33 muestra un pequeño internet compuesto de 3 redes Ethernet conectadas por un ruteador IP llamado D. Cada red IP tiene cuatro computadoras; cada computadora tiene su propia dirección IP y dirección Ethernet.

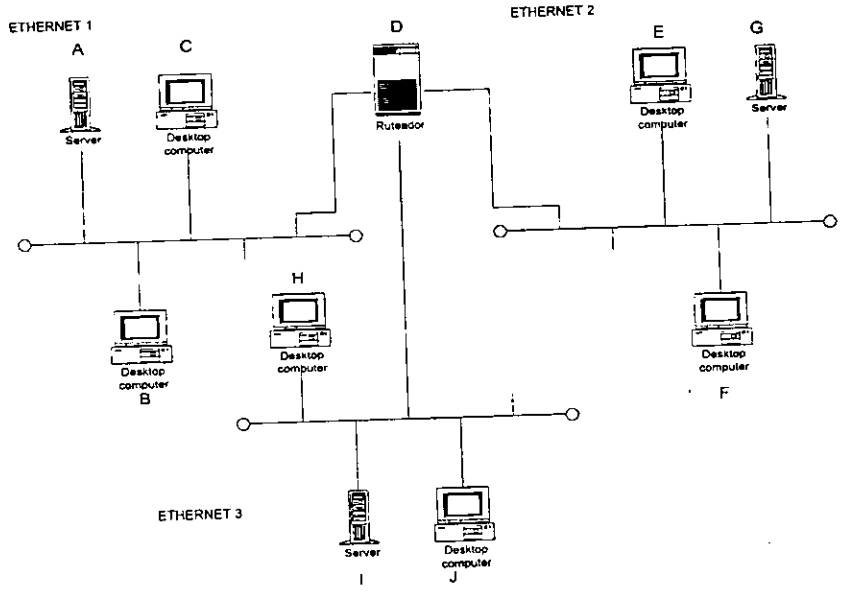


Figura 3.33 Ejemplo de un internet con ruteo indirecto

Excepto para D, cada computadora tiene una pila de protocolos TCP/IP como el de la figura 3.17. El ruteador está conectado a las tres redes y por lo tanto tiene 3 direcciones IP y 3 direcciones Ethernet, además posee un pila de protocolos como la que muestra la figura 3.16. Hay que hacer notar que los ruteadores tiene sólo un modulo IP como se muestra en la figura 3.34.

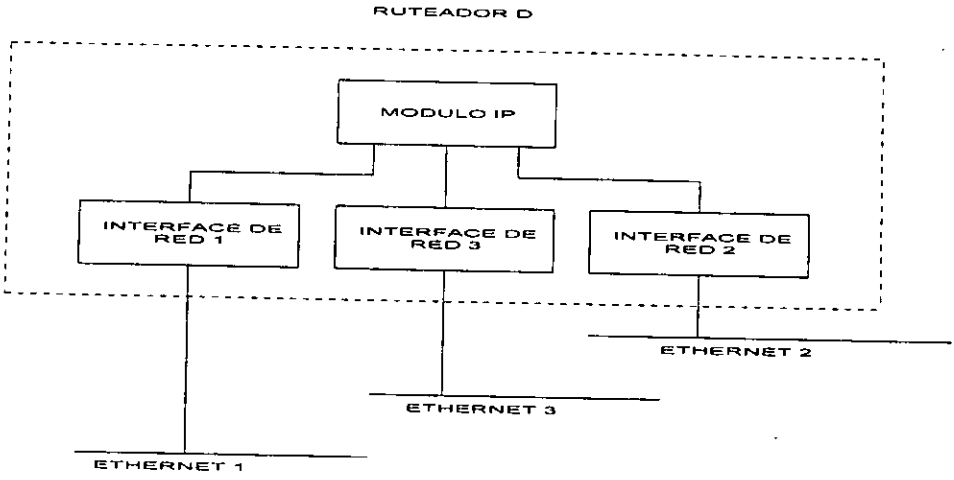


Figura 3.34 Esquema del ruteador de la figura 3.33

El administrador de la red ha asignado una dirección IP, a cada uno de los Ethernets. Los números IP de las redes no se muestran en la figura, sólo los nombres.

Cuando la computadora A envía un paquete IP a la computadora B, el proceso es idéntico al ejemplo del apartado anterior, es decir, un enrutamiento directo. Cualquier comunicación entre computadoras localizadas en una sola red cae dentro del ruteo directo discutido previamente, por ejemplo cuando D y A, D y E, ó D y H se comunican, se establece una comunicación directa. En forma general, cuando D se comunica con cualquier host del internet, se establece una comunicación directa, esto es debido a que, cualquier par de dispositivos Ruteador/Host se comunicaran sobre la misma red. Sin embargo, cuando la computadora A se comunica con cualquier computadora al otro extremo del ruteador, la comunicación ya no es directa. A debe usar a D para lanzar el paquete IP a la siguiente red. Esta comunicación se llama indirecta.

Si A envía un paquete IP a E, la dirección fuente IP en el datagrama y la dirección fuente del frame Ethernet son las de A. La dirección IP de destino es la de E, pero debido a que no existe una comunicación directa de A con E, el modulo IP de A enviara el paquete a D para su enrutamiento, la dirección Ethernet de destino será la de D, como se muestra a continuación.

	Dirección fuente	Dirección Destino
Encabezado IP	A	E
Encabezado Ethernet	A	D

El modulo IP de D recibe el paquete examina la dirección IP de destino y hace una comparación con las direcciones IP de las demás redes, al empatar la dirección de destino con la dirección del Ethernet 2, encapsula el datagrama en un frame colocándole en la dirección fuente la dirección física de D y en la dirección destino la dirección física de E; procediendo a hacer una entrega directa del datagrama.

	Dirección fuente	Dirección Destino
Encabezado IP	A	E
Encabezado Ethernet	D	E

Como se puede observar las direcciones IP de un datagrama no son modificadas en su paso por los ruteadores, únicamente las direcciones físicas en los frames que los transportan por las redes.

Resumiendo, para comunicaciones directas, tanto la dirección fuente IP como la dirección fuente Ethernet corresponden a las del emisor, y la dirección destino IP como la dirección destino Ethernet son las del host destino. Para comunicación indirecta, las direcciones IP y Ethernet no siguen este esquema.

Por lo tanto, se puede concluir que los ruteadores en un internet TCP/IP forman una estructura cooperativa interconectada, los datagramas pasan de ruteador en ruteador hasta que alcanzan uno que puede entregarlos en forma directa al host destino.

3.13.4 LA TABLA DE RUTEO IP

Llegando a este punto se presentan las siguientes preguntas: Cómo puede saber un ruteador en Internet a donde enviar un datagrama?, ó Cómo puede saber un host cual ruteador usar para un destino dado?. Las respuestas involucran el uso de una tabla que contiene direcciones IP. IP usa esta tabla para hacer todas las decisiones acerca del ruteo de un datagrama. El algoritmo de ruteo emplea la tabla de ruteo Internet (en ocasiones llamada tabla de ruteo IP), almacenada en cada máquina, ésta tabla contiene información acerca de posibles destinos y como alcanzarlos. En cualquier momento que

el software de ruteo IP en un host o ruteador necesita transmitir un datagrama, consulta la tabla para decidir a donde enviar el datagrama.

Las tablas IP con el fin de hacerlas compactas y más practicas para los ruteadores, son cargadas únicamente con la parte correspondiente al número de la red; de esta manera se hace el ruteo también más eficiente.

Típicamente, una tabla de ruteo contiene pares (N,R) donde N es la dirección IP de una red destino, y R es la dirección IP del siguiente ruteador a lo largo de la ruta, hacia la red N. El ruteador R es llamado el "siguiente brinco". Así, la tabla de enrutamiento en un ruteador sólo especifica un paso a lo largo de la ruta desde dicho ruteador hacia la red destino (el ruteador no conoce la ruta completa para llegar al host final). El formato general de una tabla de ruteo IP en un host o ruteador, es como el que se muestra en la figura 3.35.

Para alcanzar los hosts en la red (N)	Enrutar a la dirección (R)
128.10.0.0	Entrega directa
192.0.1.0	128.10.0.1
132.248.0.0	128.10.0.9

Figura 3.35 Tabla IP en un ruteador o host

Es importante entender que cada renglón en una tabla de enrutamiento apunta hacia un ruteador que puede ser alcanzado a través de una red física. Esto es, que todos los ruteadores listados en la tabla de enrutamiento de una máquina R deben residir en redes a las cuales R se conecta directamente. Cuando un datagrama está listo para dejar R el software IP localiza la dirección IP destino y extrae la porción correspondiente de red, R entonces usa la porción de red para hacer una decisión de ruteo, seleccionando un ruteador que pueda ser accesado directamente.

Los dos siguiente apartados ejemplifican el uso de la tabla de ruteo IP en conjunto con los dos tipos de ruteo analizados

3.13.5 DETALLES DEL RUTEO DIRECTO

Más específicamente la tabla de ruteo IP se compone de una columna con el número de IP de la red, una bandera de ruteo directo/indirecto, la dirección IP de la interface en el ruteador, y el número de la interface de red.

Para explicar como es utilizada esta tabla, se presenta con detalle un ejemplo del ruteo directo y algunos aspectos mencionados a lo largo de este capitulo. La figura 3.36 muestra una parte de una red Ethernet.

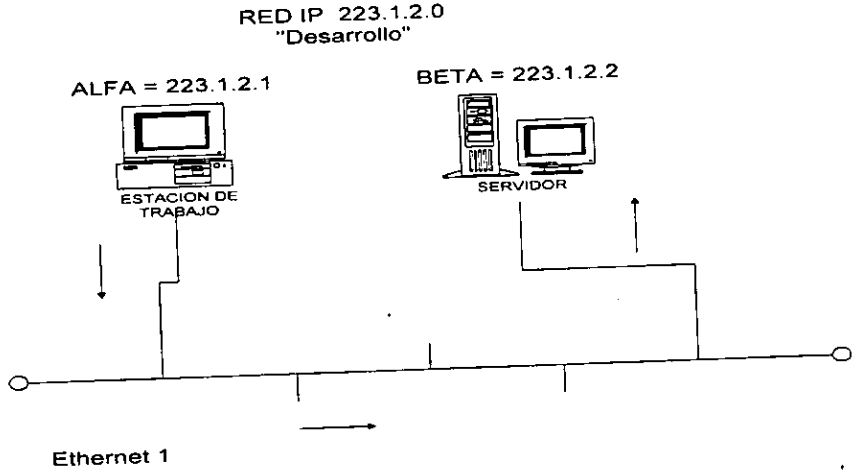


Figura 3.36 Acercamiento de una red IP llamada "Desarrollo"

La tabla de enrutamiento en la máquina denominada Alfa sería:

Nombre de la red	Bandera directo/indirecto	Ruteador	Número de interface
desarrollo	directo	< blanco>	1

Para fines de discusión, la tabla es mostrada otra vez pero ahora con su equivalente numérico.

Nombre de la red	Bandera directo/indirecto	Ruteador	Número de interface
223.1.2.0	directo	< blanco>	1

Considérese el envío de un datagrama de alfa a beta, el paquete está en el modulo IP de alfa y la dirección IP de destino de beta es 223.1.2.2. El software IP extrae la porción de red (clase C) de la dirección IP de beta (223.1.2) y busca en la primera columna de su tabla de ruteo por una coincidencia. Al encontrarse una coincidencia, la demás información en el renglón indica que las computadoras en ésta red pueden ser alcanzadas directamente a través de la interface número 1. Una traducción ARP se realiza de la dirección IP de beta y después el frame Ethernet es enviado directamente a beta vía la interface número 1.

Si una aplicación trata de enviar datos a un dirección IP que no esté en la red de desarrollo, IP será incapaz de encontrar una coincidencia en la tabla de ruteo. IP entonces desechará el paquete. Algunas computadoras proveen un mensaje de error "Red no alcanzable".

3.13.6 DETALLES DEL RUTEO INDIRECTO

Ahora, se analizara con mayor detalle un escenario más complicado de ruteo examinado previamente en el apartado 3.13.3. En la figura 3.37 se muestra un internet con tres redes Ethernet, con su nombre y dirección IP.

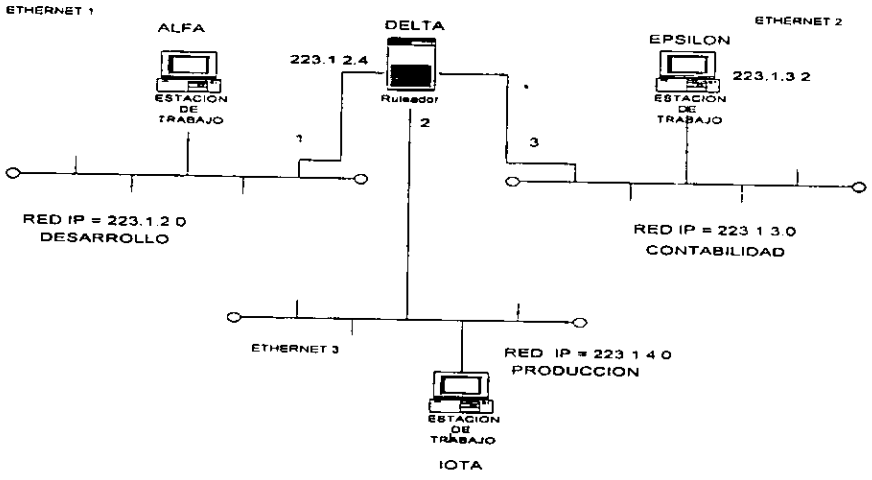


Figura 3.37 internet con ruteo indirecto

La tabla de ruteo en alfa sería:

Nombre de la red	Bandera directo/indirecto	Ruteador	Número de interface
desarrollo	directo	< blanco>	1
contabilidad	indirecto	delta	1
producción	indirecto	delta	1

En forma numérica sería:

Nombre de la red	Bandera directo/indirecto	Ruteador	Número de interface
223.1.2.0	directo	< blanco>	1
223.1.3.0	indirecto	223.1.2.4	1
223.1.4.0	indirecto	223.1.2.4	1

El ruteador en la tabla de alfa es la dirección IP de la conexión de delta para la red de "Desarrollo".

Considérese que alfa le envía un datagrama a épsilon. El datagrama está en el modulo IP de alfa y la dirección IP de destino de épsilon es 223.1.3.2. IP extrae la porción de red de esta dirección (223.1.3) y busca en la primera columna dentro de su tabla por una coincidencia con este número.

Esta entrada dentro de la tabla indica que las computadoras en la red 223.1.3 pueden ser alcanzadas a través del ruteador delta. El modulo IP de alfa entonces hace una traducción ARP para la dirección IP de delta y envía el paquete IP directamente al ruteador a través de la interface de alfa (número 1). El paquete IP sigue teniendo la dirección de destino de épsilon.

El paquete IP llega a la interface de red en delta, correspondiente a la red de Desarrollo y es pasado al modulo IP de delta. El modulo IP de delta extrae la porción de red de la dirección IP de destino (223.1.3) y busca en su tabla por una coincidencia con este número. La tabla de ruteo IP en el ruteador delta sería:

Nombre de la red	Bandera directo/indirecto	Ruteador	Número de interface
desarrollo	directo	< blanco>	1
contabilidad	directo	<blanco>	3
producción	directo	<blanco>	2

En su forma numérica sería:

Nombre de la red	Bandera directo/indirecto	Ruteador	Número de interface
223.1.2.0	directo	< blanco>	1
223.1.3.0	directo	<blanco>	3
223.1.4.0	directo	<blanco>	2

La coincidencia es encontrada en el segundo renglón. Se hace una traducción ARP de la dirección de destino e IP entonces envía el paquete directamente a épsilon a través de la interface número 3. EL paquete IP contiene la dirección IP de destino de épsilon y la dirección Ethernet de destino de épsilon.

El paquete IP llega a épsilon y es pasado al modulo IP de éste. La dirección IP de destino es examinada, encontrándose que empata con la dirección IP de la máquina, entonces el paquete es pasado a la capa de protocolo superior para su procesamiento.

3.14 PROTOCOLOS DE RUTEO

En apartados anteriores se ha mencionado que un ruteador se enlaza a dos o más redes y transmite datagramas IP entre ellas. Con excepción de la comunicación entre máquinas conectadas directamente a la misma red, los hosts pasan todo el tráfico IP a los ruteadores, los cuales reenvían los datagramas sucesivamente hacia otros ruteadores, hasta que son entregados a la máquina destino. También, se ha mencionado que el algoritmo de ruteo que utilizan los ruteadores, hace uso de una tabla para la toma de decisiones de hacia donde se dirigirán los datagramas. Cada renglón en la tabla de rutas especifica la parte correspondiente a la porción red de una dirección IP (red destino) y da la dirección del siguiente ruteador que se encargará de reenviar el datagrama en su camino hacia tal red.

Pero ahora se presenta otra situación: con qué direcciones deben ser cargadas las tablas de los ruteadores en Internet para una correcta coordinación y distribución de los paquetes a través de la red?. La solución se presenta en este y los siguientes apartados.

Una vez que una tabla inicial ha sido construida un ruteador debe actualizar todos los cambios en las rutas dentro de la red. Es decir, si hay modificaciones en la topología de la red, como la adición de máquinas nuevas, bajas temporales (debido a reparación o mantenimiento) o bajas permanentes, los ruteadores tienen que registrar estos cambios en sus tablas.

En un internet pequeño y poco cambiante, los administradores pueden establecer y actualizar las rutas manualmente. Pero en una red tan grande y tan cambiante como Internet es imposible efectuar los cambios en las tablas manualmente. Por otro lado la actualización manual es propensa a errores.

Los errores en las tablas de ruteo pueden bloquear la comunicación en la red en formas que son extremadamente difíciles de diagnosticar, por lo tanto, se hace necesario el uso de métodos automáticos en la actualización de las tablas de los ruteadores de la red. Esta actualización se lleva a cabo mediante una comunicación activa, dinámica y permanente entre todos los ruteadores de la red, intercambiando información de sus tablas.

La obtención de la información de ruteo para los ruteadores tiene que tomar en cuenta dos aspectos: que valores deben ser colocados en las tablas, y como deben obtenerse estos valores. Ambos aspectos dependen de la complejidad de la estructura de la red, del tamaño, así como de políticas administrativas.

Cada ruteador debe establecer un conjunto inicial de rutas cuando se enlaza a la red y debe actualizar su tabla conforme las rutas cambien. Este último aspectos es llevado a cabo mediante la utilización de protocolos por parte de los ruteadores. Los protocolos conocidos como **protocolos de ruteo**, son utilizados por los ruteadores para el intercambio de información de ruteo en la actualización de sus tablas.

3.15 EVOLUCIÓN DE LOS PROTOCOLOS DE RUTEO

Mucho del conocimiento que se tiene actualmente del enrutamiento y de los protocolos de propagación de rutas se ha derivado a partir de la experiencia y evolución de Internet..

Los diseñadores de Internet escogieron una arquitectura de ruteo consistente de un conjunto pequeño centralizado de ruteadores que mantenían una información completa para alcanzar todos los destinos posibles dentro de la red, y de un gran conjunto de ruteadores, constituido por cada uno de los ruteadores en los sitios participantes y los cuales mantenían información parcial[12] de ruteo.

[12] Muchos hosts tienen sólo dos rutas en sus tablas de ruteo, una ruta para la red local y una ruta de default para un ruteador cercano.

Mediante este esquema y adecuando las rutas por default en cada sitio remoto para que apunten a uno de los ruteadores centrales los paquetes alcanzarían invariablemente su destino. La ventaja de usar información parcial en los sitios remotos es que permite a los administradores locales manejar cambios en la estructura local sin afectar otras partes de Internet. La desventaja es que introduce la posibilidad de inconsistencias, las cuales en el peor de los casos, pueden hacer que los ruteadores distantes de una red no sea accesibles.

3.15.1 UNA ARQUITECTURA CENTRALIZADA

Los primeros ruteadores en Internet se agruparon en dos conjuntos, como lo indica el apartado anterior, un conjunto pequeño de ruteadores centrales (core routers) controlados por INOC, y un gran conjunto de ruteadores descentralizados controlados por los sitios participantes. El sistema central fue diseñado para proporcionar rutas confiables y consistentes para todos los destinos; fue el elemento que mantuvo a Internet enlazado e hizo la interconexión universal posible. Cada sitio asignado con una dirección de red de Internet tenía que anunciarla al sistema central. Los ruteadores centrales se comunicaban entre ellos, así que podían garantizar que la información que compartían era consistente. Debido a que una autoridad central monitoreaba y controlaba los ruteadores centrales, éstos eran altamente confiables.

La naturaleza centralizada del sistema se deriva del hecho de que Internet evolucionó de una red ya establecida llamada ARPANET y que funcionaba como un troncal principal, y a la cual se le iban agregando cada vez más redes. Así, que una gran parte de la motivación para el sistema central de ruteo vino del deseo de conectar redes a ARPANET. La figura 3.38 ilustra la idea.

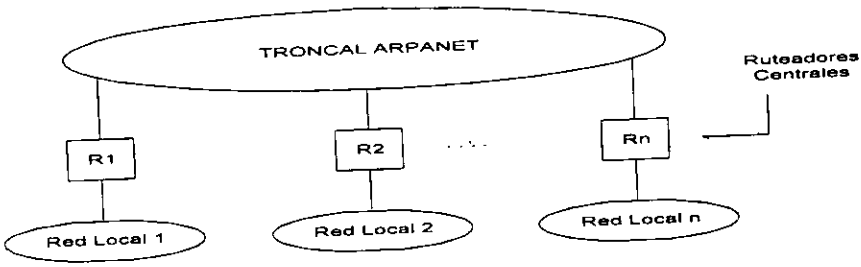


Figura 3.38 El sistema central de ruteadores de Internet visto como un conjunto de ruteadores que conectan las redes de área local a ARPANET. Los hosts en las redes locales pasan todo el tráfico no local al ruteador central más cercano.

Los diseñadores de Internet establecieron que todos los ruteadores centrales intercambiaran información de ruteo, de tal forma que cada uno de ellos tuviera una información completa acerca de las rutas más optimas para todos los destinos de la red.

Una vez que cada ruteador conoce las rutas a todos los destinos posibles, no necesita una ruta por default para enviar el tráfico que no pueda manejar. Si la dirección destino de un datagrama no se encuentra en la tabla de ruteo de un ruteador central, el ruteador generará un mensaje ICMP de destino no alcanzable y desechará el datagrama.

Con el paso del tiempo este modelo se volvió impractico por tres razones. Primero, Internet fue sobrepasado como troncal central. La topología comenzó a ser más compleja y los protocolos necesarios para mantener una consistencia entre los ruteadores centrales ya no fue tan trivial. Segundo no cualquier lugar podía tener un ruteador central conectado al troncal, así que se necesitaba de una estructura adicional de ruteo así como de protocolos. Tercero, debido a que los ruteadores centrales interactuaban para asegurar una información de ruteo consistente, la arquitectura central no podía crecer a un gran tamaño. La solución a ésta problemática se presenta más adelante después de analizar los algoritmos de ruteo.

3.16 ALGORITMOS DE RUTEO

Parecería que los mecanismos automáticos de propagación de rutas no son necesarios, especialmente en internets pequeños, sin embargo, los internets no son estáticos. Las conexiones fallan y son posteriormente reemplazadas o se agregan

nuevas. Las redes pueden en un momento dado estar congestionadas y subutilizadas en el siguiente. El propósito de los mecanismos de propagación de rutas no es meramente encontrar un conjunto de rutas, sino continuamente actualizar la información en las tablas de los ruteadores. El ser humano simplemente no puede responder a los cambios en la topología de la red lo suficientemente rápido; por lo cual se deben utilizar métodos automatizados. Así, en la propagación de rutas, es importante considerar el comportamiento dinámico de los protocolos y algoritmos.

Es importante no confundir información de ruteo que contiene direcciones, topología y detalles de retrasos en el enrutamiento con los algoritmos utilizados para elaborar la información de enrutamiento. Por lo general, los algoritmos de ruteo están fijos en cada ruteador y no se modifican. Naturalmente, conforme varia la información de ruteo, el algoritmo adaptará las rutas escogidas para reflejar la nueva información.

Existen básicamente dos tipos de algoritmos que siguen los protocolos de ruteo para el procesamiento y propagación de rutas entre los ruteadores. A continuación se describen cada uno de ellos.

3.16.1 ALGORITMO VECTOR-DISTANCIA O SALTOS MÍNIMOS

El término vector-distancia también llamado Bellman-Ford, en honor de los investigadores que publicaron la idea, se refiere a una clase de algoritmo que los ruteadores usan para propagar su información de ruteo.

El ruteador mantiene una tabla de todas las rutas que conoce, inicializandola con un renglón por cada red conectada directamente a él. Cada renglón dentro de la tabla identifica una red destino y la distancia a tal red, usualmente medida en saltos. Donde el número de saltos o cuenta de saltos a lo largo de una ruta, se refiere al número de ruteadores que un datagrama tiene que cruzar para llegar a la red destino desde la red fuente. De esta manera, la red destino se define que está a cero saltos si el ruteador está conectado directamente a la red (entrega directa), a un salto si hace uso de un ruteador para llegar a la red destino, dos saltos si hace uso de dos ruteadores y así sucesivamente.

Periódicamente cada ruteador envía una copia de su tabla a cualquier ruteador que pueda alcanzar directamente. Por ejemplo, cuando un reporte llega al ruteador K

desde el ruteador J, K examina el conjunto de destinos reportados y la distancia a cada uno de ellos. Si J conoce un camino más corto para llegar a un destino, o si J contiene un destino que K actualmente no tiene en su tabla, o si K actualmente enruta a un destino a través de J y la distancia de J a tal lugar cambia, K reemplaza o actualiza dicho renglón.

La Figura 3.39 muestra la tabla de un ruteador K, y un mensaje enviado por el ruteador J. Los renglones señalados con flechas serán utilizados para actualizar las entradas existentes o para agregar nuevas a la tabla del ruteador K, el mensaje enviado por J muestran las situaciones señaladas en el párrafo anterior.

Destino	Distancia	Ruta
Red 1	0	Directa
Red 2	0	Directa
Red 4	8	Ruteador L
Red 17	5	Ruteador M
Red 24	6	Ruteador J
Red 30	2	Ruteador Q
Red 42	2	Ruteador J

(a)

	Destino	Distancia
→	Red 1	2
	Red 4	3
→	Red 17	6
	Red 21	4
	Red 24	5
	Red 30	10
→	Red 42	3

(b)

Figura 3.39 (a) Tabla de enrutamiento para el ruteador K, y (b) un mensaje de actualización proveniente del ruteador J.

Hay que notar que si J reporta una distancia N, una entrada actualizada en K tendrá una distancia de N+1 (la distancia reportada por J más la distancia para alcanzar a J), por supuesto, la tabla de ruteo contiene una tercera columna que especifica el ruteador a donde se lanzaran los datagramas. Cuando un ruteador K agrega o actualiza un renglón en respuesta a un mensaje desde el ruteador J, este asigna en la tercera columna la dirección del ruteador J.

El termino vector-distancia se deriva de la información enviada de los mensajes periódicos. Un mensaje contiene una lista de pares (V,D), donde V identifica un destino (llamado vector), y D es la distancia a tal destino.

En este diseño, todos los ruteadores deben participar en el intercambio de pares V-D para que las rutas sean eficientes y consistentes.

Aunque los algoritmos vector-distancia son fáciles de implementar tienen ciertas desventajas. Una se refiere, cuando las rutas cambian rápidamente, el tiempo que tarda

en difundirse toda la información a través de la red puede provocar inestabilidad en los ruteadores. Cuando una ruta cambia, por ejemplo, cuando un conexión nueva aparece o cuando se presenta la falla de otra, la información se propaga lentamente de un ruteador a otro. Esta situación provoca que en un momento dado algunos ruteadores (los que no ha sido actualizados aun) tengan información incorrecta.

Otra desventaja, es con respecto al número de saltos para llegar a un destino, es obvio que usar el número de saltos para calcular la ruta más corta no siempre produce los resultados más óptimos. Por ejemplo, una ruta que cruza tres redes locales y por lo tanto con una cuenta de tres saltos, puede ser substancialmente más rápida, que una ruta con una cuenta de dos saltos que cruza dos redes de área amplia.

El sistema original de ruteadores centrales (figura 3.38) en ARPANET utilizaron una implementacion del algoritmo vector-distancia, por medio del protocolo conocido como Gateway Gateway Protocol (GGP) para el intercambio de información de ruteo. Actualmente GGP está en desuso.

3.16.2 ALGORITMO ESTADO DE ENLACE O SPF

El segundo tipo de algoritmo de ruteo que se tiene es, el algoritmo de Estado de Enlace o SPF (Shortest Path First, La Ruta Más Corta), el término SPF es un tanto equivoco en su designación ya que la mayoría de los protocolos de ruteo producen en su particular forma de trabajar las rutas más cortas. En este tipo de algoritmo se requiere que cada ruteador participante tenga una información topologica completa. La forma más fácil de pensar en la información topologica es imaginar que cada ruteador tiene un mapa que muestra todos los ruteadores y redes que se le conectan. En términos abstractos, los ruteadores corresponden a los nodos en una gráfica y las redes que se conectan a los ruteadores corresponden a los enlaces. Hay un enlace entre dos nodos si y sólo si los correspondientes ruteadores pueden comunicarse directamente.

En lugar de enviar mensajes que contengan listas de destinos, un ruteador participando en un algoritmo SPF ejecuta dos tareas. Primero, activamente prueba el estado de todos sus ruteadores vecinos. En términos de la gráfica, dos ruteadores son vecinos si comparte un enlace; en términos de la red, dos vecinos se conectan a una red común. Segundo, periódicamente propagan el Estado del Enlace a otros ruteadores.

Para checar el estado de un vecino directamente conectado, un ruteador periódicamente intercambia mensajes pequeños, que preguntan si el vecino (enlace) está "vivo" y alcanzable.

Para informar a los demás ruteadores, cada ruteador periódicamente difunde un mensaje que lista el estado de cada uno de los enlaces. El mensaje de estado no especifica rutas, simplemente reporta si la comunicación es posible entre un par de ruteadores. El software del protocolo en los ruteadores se las arregla para entregar una copia de cada mensaje de estado de enlace a todos los ruteadores participantes.

En cualquier momento que un mensaje de estado de enlace llega a un ruteador, éste usa la información para actualizar su mapa internet. Cuando un enlace cambia, el ruteador recalcula las rutas para todos los destinos desde un sitio fuente.

3.17 LA NECESIDAD DE UN NUEVO ESQUEMA DE RUTEO

Como se mencionó en el apartado 3.15.1, la arquitectura centralizada de ARPANET propició varios inconvenientes para el ruteo, a medida que crecía y se volvia más compleja su topología.

Tomando en cuenta que en los inicios de Internet, cada sitio conectaba sólo una red al backbone central, figura 3.38, con el paso del tiempo, los sitios participantes no se limitaron a tener una sola red en sus instalaciones, sino que, establecieron más redes interconectandolas, un ejemplo se muestra en la figura 3.40, pero con el esquema centralizado establecido no era posible conectarlas al backbone, a menos que se enlazaran individualmente por medio de ruteadores centrales. Situación que no era factible, ya qué, se tenia la restricción de que la estructura central de ruteadores no podía crecer a gran escala.

De esta forma se presento la necesidad de implementar un mecanismo nuevo de ruteo que permitiera al sistema central conocer no sólo una red, sino todas las redes de un sitio (todas las redes escondidas por debajo de la red que se conecta con la red troncal); es decir, un mecanismo que permitiera a los ruteadores no centrales difundir al sistema central todos las rutas existentes incluyendo las de las redes escondidas.

Este nuevo mecanismo también tendría que permitir a cada sitio, modificar en forma independiente el ruteo y acceso a todas las redes bajo su administración, sin afectar el resto del internet.

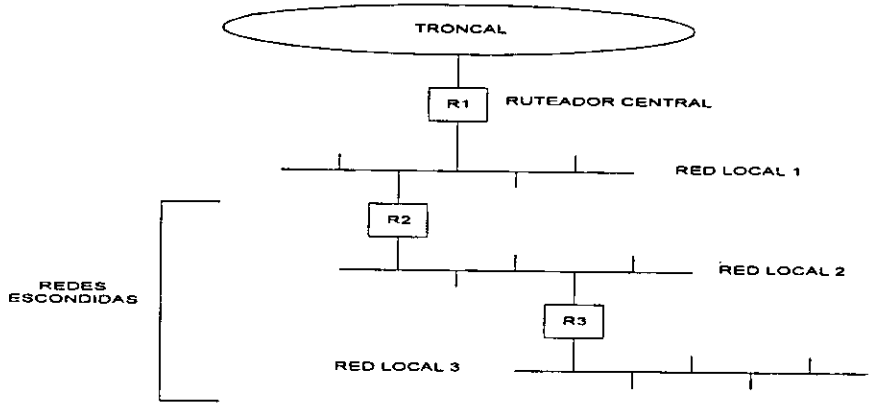


Figura 3.40 Ejemplo de múltiples redes instaladas en un sitio, que provocan un nuevo esquema de ruteo, ya que el troncal sólo ve las rutas de la red local 1.

3.18 EL CONCEPTO DE SISTEMAS AUTÓNOMOS

Partiendo del hecho de que todas las redes y ruteadores de una corporación están bajo el control de una autoridad administrativa, entonces es ésta autoridad la que puede garantizar que las rutas internas de sus redes sean consistentes y viables. Esto implica que cada sitio tenga la libertad de escoger cualquier arquitectura interna de ruteo, permitiendo que pueda escoger uno de sus ruteadores para que sirva como la máquina que anunciará al mundo exterior la accesibilidad a sus redes.

Para propósitos de ruteo, un grupo de redes y ruteadores controlados por una autoridad administrativa se denomina un Sistema Autónomo. Los ruteadores dentro de un sistema autónomo son libres de elegir sus propios mecanismos para descubrir, propagar, validar y checar la consistencia de las rutas. Bajo esta definición el sistema central de ruteadores por si mismo forma un sistema autónomo. La figura 3.41 muestra un ejemplo de un sistema autónomo.

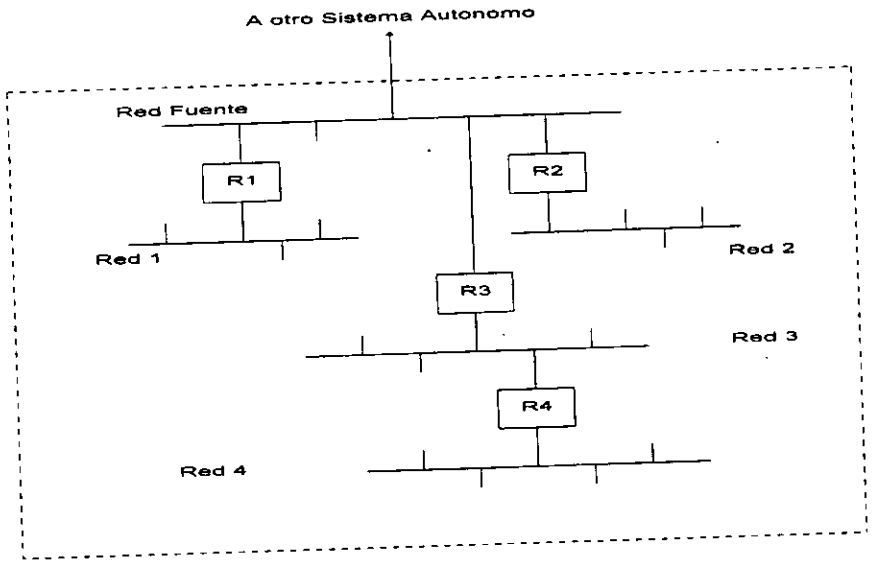


Figura 3.41 Ejemplo de un Sistema Autónomo

Conceptualmente, la idea de un sistema autónomo es una generalización del esquema original de ruteo, como lo ilustra la figura 3.42, reemplazando las redes locales de la figura 3.38 por sistemas autónomos.

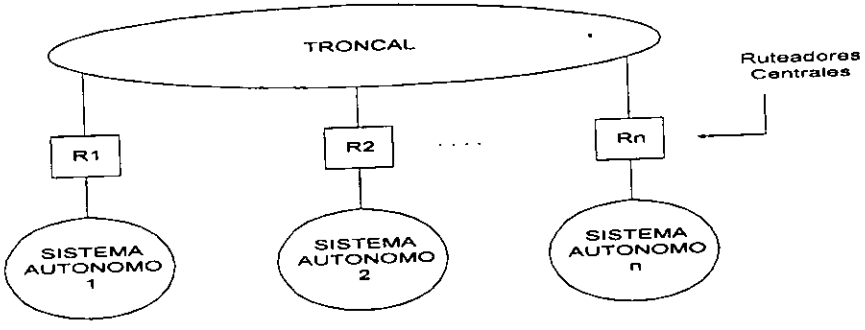


Figura 3.42 Arquitectura de un internet con sistemas autónomos conectados a una red troncal. Cada sistema autónomo consiste de múltiples redes y ruteadores bajo una autoridad administrativa.

Para hacer accesibles a través de Internet las redes que están escondidas dentro de los sistemas autónomos, cada sistema autónomo debe estar de acuerdo en anunciar sus rutas a otros sistemas autónomos y principalmente al sistema central. Usualmente, un ruteador en un sistema autónomo toma la responsabilidad de anunciar las rutas e interactuar directamente con uno de los ruteadores centrales.

Para hacer posible a los algoritmos de ruteo distinguir entre los diferentes sistemas autónomos, cada uno de estos es asignado con un número por parte de INTERNIC, la misma autoridad central que asigna todas las direcciones IP de la red.

Finalmente, cabe hacer mención que dos ruteadores que intercambian información, se denominan vecinos exteriores si pertenecen a dos sistemas autónomos diferentes y vecinos interiores si pertenecen al mismo sistema autónomo.

3.19 PROTOCOLOS DE COMPUERTA EXTERIOR

El apartado anterior hizo referencia a la interacción que dos ruteadores de sistemas autónomos (vecinos exteriores) pueden llevar a cabo para el intercambio de información de ruteo. Este intercambio es posible gracias a los protocolos conocidos como de compuerta exterior[13], y es precisamente el nombre que toma el protocolo que se describe a continuación.

3.19.1 EL PROTOCOLO DE COMPUERTA EXTERIOR (EGP)

El protocolo de compuerta exterior o EGP (Exterior Gateway Protocol), implementa al algoritmo vector-distancia, es utilizado por ruteadores vecinos exteriores (entendiéndose por vecino al ruteador que desea compartir información con otro, no habiendo implicación de una proximidad geográfica) para anunciar información de accesibilidad de sus respectivos sistemas autónomos. La figura 3.43 muestra a dos ruteadores exteriores intercambiando información de ruteo

[13] Los diseñadores originalmente utilizaron el término compuerta IP en lugar de ruteador

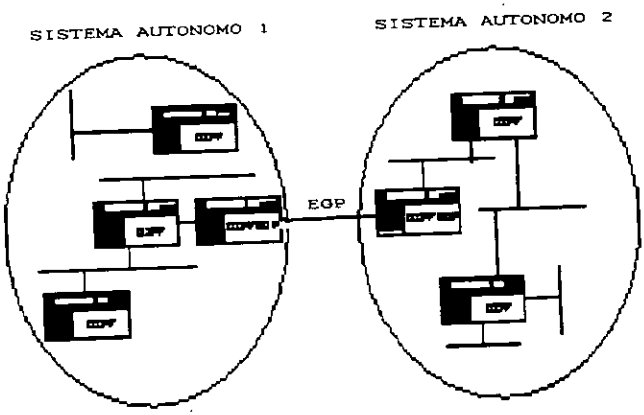


Figura 3.43 Dos ruteadores exteriores intercambiando información, usando EGP para anunciar las rutas de sus respectivos sistemas autónomos

EGP fue originalmente diseñado para comunicar accesibilidad a y desde los ruteadores centrales de la red ARPANET. La información era pasada desde cualquier sistema autónomo hasta los ruteadores centrales, los cuales circulaban la información a través del backbone hasta que podían entregarla a la red destino dentro de otro sistema autónomo.

EGP tiene tres funciones principales. Primero, soporta un mecanismo de adquisición de vecino que permite que un ruteador le solicite a otro que esté de acuerdo en que los dos intercambien información de accesibilidad. Segundo, un ruteador continuamente checa si sus vecinos están respondiendo. Tercero, los ruteadores EGP envian mensajes de actualización conteniendo información acerca de la accesibilidad de las redes dentro de sus sistemas autónomos. La figura 3.44 muestra el formato del paquete EGP.

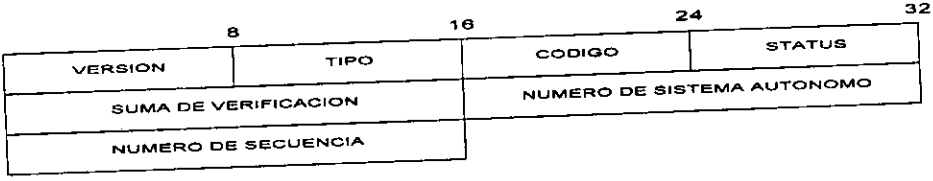


Figura 3.44 Formato fijo que precede a cada mensaje EGP

El campo **Número de versión** EGP contiene un entero que identifica la versión de EGP. Los receptores checan el número de versión para verificar que sus protocolos están usando la misma versión de software. Para acomodar las tres funciones básicas arriba mencionadas, EGP define diez tipos de mensajes:

Tipo de mensaje EGP	Descripción
Solicitud de adquisición	Solicita el ruteador convertirse en un vecino
Confirmación de adquisición	Respuesta positiva a la solicitud de adquisición
Negación de adquisición	Respuesta negativa a la solicitud de adquisición
Terminación de solicitud	Solicita la terminación de la relación de vecindad
Terminación de confirmación	Respuesta de confirmación a la solicitud de terminación
Hola	Solicita al vecino que responda si está vivo
Te escucho	Respuesta a los mensajes hola
Solicitud de sondeo	Solicita actualización de la información de ruteo
Actualización de ruteo	Información de accesibilidad de red
Error	Respuesta a mensajes incorrectos

El campo **Tipo** identifica el tipo del mensaje, en conjunto con el campo **Código** se usa para distinguir entre diversos subtipos. El campo de **Status** contiene mensajes que dependen del estado de la información. El campo de **Verificación** se usa para detectar posibles daños al paquete que pudieran efectuarse durante su transmisión. Para calcular el valor del campo de verificación, el mensaje EGP es tratado como una secuencia de enteros de 16 bits, tomando el complemento a uno de la suma de los complementos a uno. El campo de **Número de Sistema Autónomo**, identifica al Sistema Autónomo al cual el ruteador emisor pertenece. El campo de **Número de Secuencia** contiene un valor que el emisor usa para asociar las respuestas con los mensajes enviados, un ruteador establece un valor inicial de secuencia cuando adquiere un vecino e incrementa el número de secuencia cada vez que envía un mensaje. El vecino responde con el último número de secuencia que recibió, permitiendo al emisor empatar respuestas con el envío de los mensajes.

Campos adicionales siguen al encabezado EGP, el contenido de estos campos varían dependiendo del tipo de mensaje.

3.19.1.1 TIPOS DE MENSAJES EGP

-Mensaje de adquisición de vecino. Un ruteador envía un mensaje de adquisición de vecino para establecer comunicación EGP con otro ruteador. Hay que notar que EGP no especifica por que o como un ruteador elige a otro ruteador como su vecino. Se asume que tales elecciones son realizadas por la organización responsable de administrar los ruteadores y no por el protocolo.

Además del encabezado estándar el mensaje de adquisición de vecino incluye un campo llamado Intervalo Hola, que especifica el periodo del intervalo para probar si los vecinos están "vivos". También hace uso de un campo llamado Intervalo de Sondeo, el cual controla la máxima frecuencia de las actualizaciones de ruteo. El emisor suministra un intervalo de sondeo de n para especificar que el receptor no debe sondear más que cada n segundos, en la practica , la mayoría de las implementaciones usan el intervalo de sondeo como la frecuencia exacta a la cual deben enviar solicitudes de sondeo. La figura 3.45 muestra el formato del mensaje de adquisición.

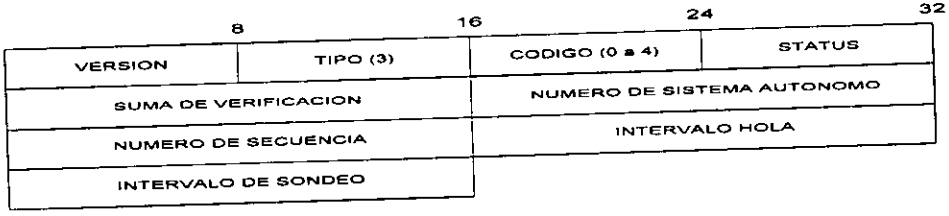


Figura 3.45 Formato del mensaje EGP de adquisición de vecino

El campo Código identifica el mensaje especifico como muestra la siguiente tabla:

Tipo	Código	Significado
(3) Adquisición	0	Solicitud de adquisición
	1	Confirmación de adquisición
	2	Negación de adquisición
	3	Terminación de solicitud
	4	Terminación de confirmación

- Mensaje de accesibilidad de vecino. Este mensaje no agrega campos extra al encabezado EGP. EGP permite dos formas de probar si un vecino esta vivo. En modo activo, los ruteadores prueban a sus vecinos enviándoles periódicamente mensajes Hola con mensajes de sondeo y esperando las respuestas. En modo pasivo, un ruteador depende de su vecino para periódicamente enviar mensajes Hola o de sondeo. Un ruteador operando en modo pasivo usa la información del campo de Status de un mensaje de accesibilidad para deducir si la comunicación entre vecinos esta viva.

La separación de las funciones de accesibilidad de las funciones de actualización de ruteo reduce el tráfico de la red. Debido a que la información de ruteo no cambia tan frecuentemente como el estado de la comunicación entre dos vecinos, ésta no necesitar ser pasada frecuentemente. Además, los mensajes de accesibilidad son pequeños y requieren de poco procesamiento de computo, mientras que los mensajes de actualización de ruteo son grandes y requieren de mucho procesamiento. La figura 3.46 muestra el formato del mensaje de accesibilidad de vecino, el código 0 especifica un mensaje Hola, mientras que el código 1 especifica una respuesta Te escucho.

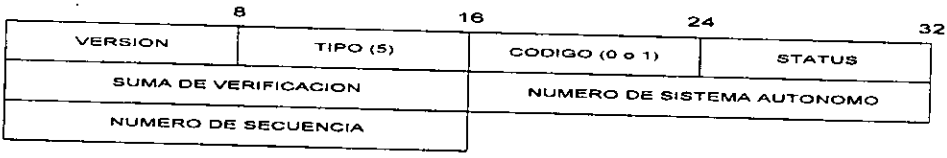


Figura 3.46 Formato del mensaje EGP de accesibilidad de vecino

Debido a que es posible que los mensajes Hola o Te escucho se pierdan en una transmisión, EGP usa una forma de la regla *k-fuera de-n* para determinar si la comunicación entre vecinos ha cambiado de 'arriba' a 'abajo'. Es decir, por lo menos k de los últimos n intercambios de mensajes deben fallar para que el ruteador declare a su vecino abajo, y al menos j deben suceder para que el ruteador declare que su vecino está arriba, una vez que ha sido declarado abajo.

-Mensaje EGP de sondeo. Los mensajes de solicitud y respuesta de sondeo le permiten a un ruteador obtener información de accesibilidad de la red. La figura 3.47 muestra el formato del mensaje, el campo etiquetado Red Fuente IP especifica una red

común a los sistemas autónomos a los cuales ambos ruteadores se enlazan. La respuesta contendrá rutas que tienen distancias medidas con respecto a los ruteadores en la red fuente IP especificada.

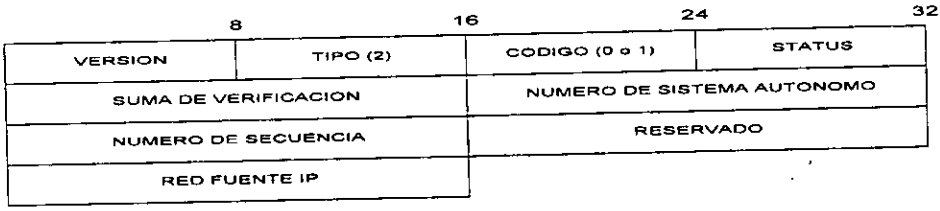


Figura 3.47 Formato del mensaje EGP de sondeo

Hay dos razones por las cuales EGP elige hacer una solicitud de sondeo especifica a una red fuente. Primero, un ruteador se conecta a dos o más redes físicas. Si una aplicación en el ruteador implementa EGP, éste no puede saber sobre cual interface está llegando la solicitud EGP. Por lo tanto, no puede saber a que red se refiere una solicitud. Segundo, los ruteadores que corren EGP frecuentemente coleccionan información de un sistema autónomo completo. Cuando anuncian accesibilidad de red, el ruteador exterior envía a los vecinos un conjunto de pares que cada uno especifica una red destino en el sistema autónomo y el ruteador utilizado para alcanzar tal destino. Por supuesto, el ruteador utilizado para alcanzar un destino depende en donde entra el tráfico al sistema autónomo. La red fuente mencionada en la solicitud de sondeo especifica el punto en el cual los paquetes entraran al sistema autónomo.

- **Mensajes EGP de actualización de ruteo.** Los mensajes de actualización de ruteo proveen una forma para los ruteadores EGP de indicar las ubicaciones de las redes dentro de sus sistemas autónomos. Además del encabezado común, estos mensajes incluyen muchos campos adicionales. El campo Número de compuertas interiores indica el número de compuertas interiores que aparecen en el mensaje. El campo Número de compuertas exteriores indica el número de compuertas exteriores que aparecen en el mensaje. El campo Red Fuente IP provee la dirección IP de la red desde la cual está siendo medida la accesibilidad. Siguiendo a este campo están una serie de bloques de compuertas. Cada bloque de compuertas provee la dirección IP de una compuerta y una

lista de redes y distancias asociadas para alcanzar estas redes. Para cada distancia, hay una cuenta de redes a la distancia seguida por la lista de direcciones de red. Después de la lista de todas las redes a una distancia dada, el patrón es repetido para todos los valores de distancias.

3.19.1.2 LAS LIMITACIONES DE EGP

EGP no interpreta las distancias métricas que están contenidas dentro de los mensajes de actualización de rutas. En esencia, EGP usa el campo de distancia para indicar si una ruta existe, el valor de distancia sólo puede ser usado para comparar rutas si existen completamente dentro de un sistema autónomo particular. Por esta razón, EGP es más un protocolo que anuncia accesibilidad que un protocolo de ruteo.

Anunciar accesibilidad con EGP es equivalente a decir "Mi sistema autónomo provee la ruta a la red X". EGP si conoce dos rutas diferentes a una misma red, no pueda saber cual es la más corta. Estas restricciones también establecen limitaciones topologicas en la estructura de Internet, específicamente, una porción EGP debe seguir una estructura de árbol, en el cual el sistema central de ruteadores forma la raíz, y no deben existir ciclos (loops) entre otros sistemas autónomos conectados a éste.

Estas restricciones son las limitaciones primarias de EGP, y provocan un ímpetu para su gradual reemplazo por otro y más capaz protocolo de compuerta exterior. Como el primer protocolo de compuerta exterior, EGP ha servido con un propósito muy valioso. Desafortunadamente, sus debilidades han sido más aparentes conforme Internet ha crecido y madurado. Como consecuencia de sus debilidades EGP actualmente está siendo desplazado de Internet, y está siendo reemplazado por otro protocolo de compuerta exterior llamado Protocolo de Compuerta de Frontera (Border Gateway Protocol. BGP).

3.19.2 PROTOCOLO DE COMPUERTA DE FRONTERA (BGP)

El Protocolo de Compuerta de Frontera (BGP) representa un intento para solucionar los problemas más serios de EGP. BGP es un protocolo de compuerta exterior creado para usarse en Internet y puede ser pensado como la siguiente generación de los protocolos de compuerta exterior que están lentamente reemplazando a EGP en Internet.

Aunque BGP fue diseñado como un protocolo de compuerta exterior cuya función principal es el intercambio de información de ruteo con otros sistemas BGP, puede ser utilizado también como un protocolo de compuerta interior. La información de ruteo que BGP maneja incluye la ruta completa de Sistemas Autónomos (SA), que el tráfico debe seguir para alcanzar las redes dentro de otro SA. Esta información es suficiente para construir una gráfica de la conectividad de los sistemas autónomos.
Dos vecinos BGP que requieran comunicarse deben residir en la misma red física. Los ruteadores BGP dentro de un mismo sistema autónomo, se comunican para asegurarse que tienen una vista consistente del sistema y determinar cual ruteador dentro del sistema servirá como el punto de conexión a o desde ciertos sistemas autónomos externos.

Algunos sistemas autónomos sirven meramente de canales de paso para el tráfico de la red. Esto es, algunos sistemas autónomos transportan el tráfico de la red que no se originó dentro del sistema autónomo y que tampoco está destinado para él . BGP debe interactuar con cualquier protocolo de compuerta interior que exista dentro de estos canales de paso.

Los mensajes BGP de actualización consisten de pares **numero de red/sistema autónomo**. La ruta de sistemas autónomos contiene la cadena de sistemas a través de los cuales la red especificada puede ser alcanzada. Estos mensajes son enviados a través del Protocolo de Control de Transmisión TCP (el cual se verá en la última sección de este capitulo), un mecanismo de transporte que asegura la confiabilidad en la entrega de la información.

Los datos iniciales de intercambio entre dos ruteadores, son las tablas enteras de ruteo BGP. Actualizaciones increméntales son enviadas conforme las tablas de ruteo cambian. A diferencia de algunos otros protocolos de ruteo, BGP no requiere un refresco periódico de la tabla total de ruteo. En su lugar, los ruteadores corriendo BGP retienen la última versión de cada par en la tabla. Aunque BGP mantiene una tabla de ruteo con todas las rutas posibles a una red particular, éste anuncia sólo la ruta más optima en sus mensajes de actualización.

La métrica utilizada por BGP es una unidad numérica arbitraria que especifica el grado de preferencia de un ruta particular. Estos valores están típicamente asignados por el administrador de la red a través de archivos de configuración. El grado de preferencia

puede estar basado en cualquier criterio, incluyendo cuenta de sistemas autónomos (rutas con el menor numero son generalmente las mejores), tipo de enlace (si es estable, rápido, confiable) y otros factores.

3.19.2.1 FORMATO DEL ENCABEZADO BGP

Todos los mensajes BGP tiene un encabezado de 19 octetos fijos, y pueden tener o no una porción de datos después de éste encabezado, dependiendo del tipo de mensaje. El formato del encabezado EGP es como el que se muestra en la figura 3.48

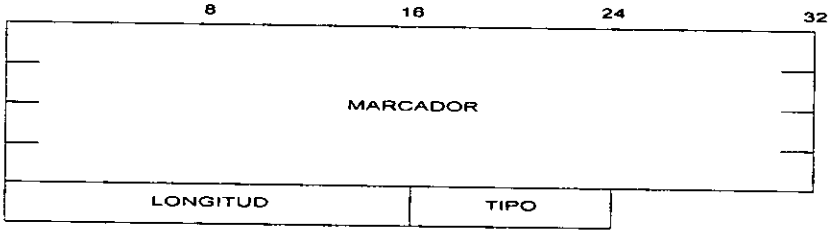


Figura 3.48 Formato del encabezado BGP

El **Marcador** es un campo de 16 octetos que el receptor del mensaje puede predecir de acuerdo al tipo de mensaje que se este manejando. El marcador puede ser utilizado para detectar la perdida de sincronización entre un par de ruteadores BGP, y para autenticar los mensajes BGP.

El campo **Longitud** de 2 octetos contiene el total de la longitud del mensaje medido en octetos, incluyendo el encabezado. El valor debe ser siempre al menos de 19 octetos (longitud del encabezado) y no mayor a 4096 octetos.

El campo **Tipo** de 1 octeto indica el tipo del mensaje. Los siguientes tipos están definidos: 1 Apertura, 2 Actualización, 3 Notificación y 4 Sigue_vivo.

3.19.2.2 MENSAJES BGP

- **Mensaje de apertura.** Después de que una conexión TCP es establecida, el primer mensaje enviado por cada lado es un mensaje de apertura. Si el mensaje de apertura es aceptado por el receptor, un mensaje Sigue_vivo confirmando el mensaje de

apertura se envía de regreso. Después de la confirmación exitosa de un mensaje de apertura, mensajes de actualizaciones, Sigue_vivo y notificaciones pueden se intercambiados.

Además del encabezado fijo BGP, el mensaje de apertura contiene los siguientes campos, figura 3.49

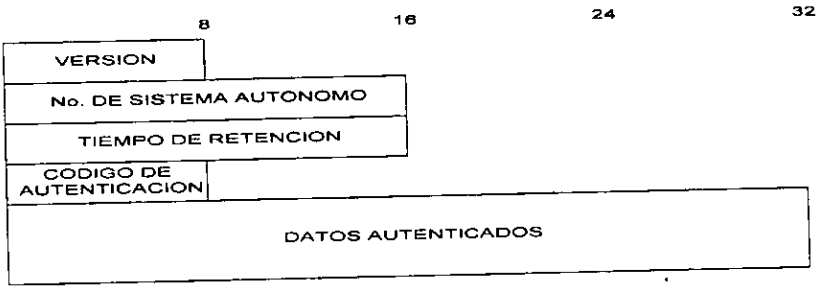


Figura 3.49 Formato del mensaje BGP de apertura

El campo **versión** de 1 octeto indica el numero de versión del protocolo BGP, y le permite al receptor checar si está corriendo la misma versión que el emisor. El campo **Numero de sistema autónomo** de 2 octetos proporciona el numero del sistema autónomo emisor. El campo **Tiempo de retención** de 2 octetos indica el numero máximo de segundos que pueden emplearse sin la recepción de un mensaje antes de que el transmisor se asuma como muerto. El campo **Código de autenticación** de 2 octetos indica el tipo de autenticación que está siendo utilizado (si se está manejando). El campo de **Datos autenticados** es de longitud variable y depende del campo Código de autenticación.

- **Mensaje de actualización.** Los mensajes de actualización son usados para transferir información de ruteo entre dos ruteadores BGP. La información en estos mensajes es utilizada para construir una gráfica describiendo la relación de varios sistemas autónomos. Además del encabezado fijo BGP, los mensajes de actualización tienen varios campos adicionales. Estos campos proveen información de ruteo listando los atributos de ruta correspondientes a cada red dentro del sistema autónomo.

BGP actualmente define cinco atributos:

- *Origen.* Puede tomar uno de tres valores: IGP, EGP, o incompleto. El atributo IGP significa que la red es parte del sistema autónomo. El atributo EGP significa que la información fue originalmente aprendida a partir de EGP. Las implementaciones BGP deberían inclinarse a preferir rutas IGP sobre las rutas EGP debido a que EGP falla en la presencia de ciclos infinitos de ruteo (loops). El atributo incompleto es usado para indicar que la red es conocida vía otros medios.
- *Ruta SA.* Provee la lista actual de Sistemas Autónomos en la ruta al destino final.
- *Siguiente brinco.* Proporciona la dirección IP del ruteador que deberá ser usado como el siguiente brinco a las redes listadas en el mensaje de actualización.
- *No alcanzable.* Si se presenta, indica que una ruta ya no es valida.
- *Métrica Inter-SA.* Proporciona una forma para un ruteador BGP de anunciar información de ruteo dentro de su propio sistema autónomo. Esta información puede ser usada por los ruteadores exteriores al sistema autónomo del emisor para seleccionar una ruta optima dentro del sistema autónomo para un destino particular.

- **Mensaje de notificación.** Los mensajes de notificación son enviados cuando una condición de error ha sido detectada, y un ruteador desea decir a otro porque está cerrando la conexión entre ellos. Aparte del encabezado común BGP, los mensajes de notificación tiene un campo de código de error, un campo de subcodigo de error , y un campo datos error. El campo de código de error indica el tipo de error, y puede ser un de los siguientes:
- *Error en el encabezado del mensaje.* Indica un problema con el encabezado del mensaje tal como una longitud no valida, un valor de marcador no aceptable, o un tipo de mensaje no aceptable.
- *Error en la apertura.* Indica un problema con un mensaje de apertura tal como un numero de versión no soportada, un numero de sistema autónomo no valido o dirección IP.
- *Error en un mensaje de actualización.* Indica un problema con un mensaje de actualización. Ejemplos incluye una lista de atributos mal formada, un error en la lista de atributos, y un siguiente brinco invalido.
- *Tiempo de retención terminado.* Indica la terminación del tiempo de retención, después del cual un nodo BGP será declarado "muerto".

- **Mensaje Seguir_vivo.** Estos mensajes consisten de sólo el encabezado y por lo tanto tiene una longitud de 19 octetos. Los mensajes son intercambiados entre los ruteadores BGP con la suficiente frecuencia para evitar que el tiempo de retención expire. Un tiempo máximo razonable entre los mensajes Seguir_vivo debería ser de un tercio del tiempo de retención.

3.20 EL ENRUTAMIENTO DENTRO DE UN SISTEMA AUTÓNOMO

A los ruteadores que están dentro de un sistema autónomo se les conoce como ruteadores internos, por ejemplo, dos ruteadores centrales del backbone de Internet son interiores uno del otro ya que el sistema central forma un sistema autónomo.

Para automatizar la tarea del mantenimiento de la información de accesibilidad de un sistema autónomo, los ruteadores interiores usualmente se comunican unos con otros intercambiando ya sea información de accesibilidad o información de ruteo (a partir de la cual se puede deducir la accesibilidad). Una vez que la información de accesibilidad para un sistema autónomo ha sido ensamblada, uno de los ruteadores en el sistema puede anunciarla a otro sistema autónomo con un protocolo de compuerta exterior. Con este mecanismo más los descritos en las secciones anteriores se cubre todo el proceso de ruteo en todo el Internet.

A diferencia de la comunicación con los ruteadores exteriores, para los cuales EGP y BGP proveen un estándar muy aceptado, ningún protocolo ha emergido para ser utilizado dentro de un sistema autónomo. Parte de ésta situación viene de la diversidad de topologías y tecnologías usadas dentro de un sistema autónomo. Como resultado, un puñado de protocolos han surgido, la mayoría de los sistemas autónomos usan alguno de ellos exclusivamente para propagar información de ruteo en forma interna.

Un ruteador puede usar dos protocolos diferentes de ruteo simultáneamente, uno para comunicarse fuera de su sistema autónomo y otro para comunicarse dentro de él.

En particular, los ruteadores que corren EGP o BGP para anunciar accesibilidad, usualmente necesitan también correr un protocolo de compuerta interior para obtener información del interior de los sistemas autónomos.

3.21 PROTOCOLOS DE COMPUERTA INTERIOR

3.21.1 PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)

Uno de los protocolos de enrutamiento interno utilizados más ampliamente dentro de los sistemas autónomos en Internet es el Protocolo de Información de Enrutamiento (Routing Information Protocol, RIP). RIP originalmente fue diseñado por Xerox y utilizado en la suite de protocolos Xerox Network Systems (XNS). RIP se empezó a asociar con Unix y TCP/IP en 1982 cuando la versión Berkeley Software Distribution (BSD) de Unix empezó a distribuirse con una implementacion RIP conocida como routed

Routed se generalizo para cubrir múltiples familias de redes, como se menciona en el párrafo anterior fue diseñado en la Universidad de California en Berkerley, con el fin de proveer de información de accesibilidad y ruteo entre las máquinas de las redes locales de la universidad. Se basa en la difusión de mensajes (broadcast) en toda la red para hacer el intercambio de la información de ruteo más rápida.

En los años siguientes a 1982, las nuevas implementaciones se derivaron principalmente del código de Berkerley, con una interoperabilidad entre ellas limitada por el entendimiento del programador acerca de detalles no documentados y sutilezas. Hasta que en Junio de 1988 un documento RFC (1058) establecía el estándar para RIP.

El protocolo RIP es una implementacion directa del algoritmo vector-distancia, divide a las máquinas participantes en activas y pasivas (silenciosas). Los ruteadores activos anuncian sus rutas a otros y los ruteadores pasivos escuchan y actualizan sus rutas basadas en los anuncios pero no anuncian. Sólo un ruteador puede correr RIP en modo activo; un host debe usar modo pasivo. Un ruteador corriendo RIP en modo activo difunde un mensaje cada 30 segundos, el mensaje contiene información tomada de la tabla de ruteo del ruteador y cada uno contiene pares de datos, donde cada par contiene una dirección de red IP y un valor que indica la distancia a la red. RIP usa una cuenta métrica basada en saltos para medir la ruta hacia una red. En la métrica usada por RIP, un ruteador tiene una cuenta de un salto para la red a la cual está directamente conectado, dos saltos para las redes que son accesibles a través de un ruteador más y así sucesivamente.

Tanto las máquinas activas como pasivas escuchan todos los mensajes y actualizan sus tablas de acuerdo al algoritmo vector-distancia descrito anteriormente. RIP mantiene sólo la mejor ruta a un destino, cuando nueva información proporciona una mejor ruta, esta información reemplaza a la ruta anterior. Cambios en la topología de la red puede provocar cambios a las rutas, provocando, por ejemplo, que una nueva ruta se convierta en la mejor ruta para un destino particular. Cuando ocurren cambios en la topología de la red, estos son reflejados en mensajes de actualización para las tablas. Por ejemplo, cuando un ruteador detecta una falla en un enlace o ruteador, recalcula sus rutas y envía mensajes de actualización de ruteo. Cada ruteador que recibe un mensaje de actualización que incluye un cambio lo registra en su tabla y propaga el cambio.

3.21.1.1 FORMATO DEL MENSAJE RIP

Los mensajes RIP pueden ser clasificados en dos tipos, mensajes de información de ruteo y mensajes usados para solicitar información; ambos utilizan el mismo formato el cual consiste de un encabezado fijo seguido por una lista opcional de redes y sus correspondientes distancias. La figura 3.50 muestra el formato del mensaje RIP para implementaciones IP[14].

[14] Como se menciono RIP cubre diversas familias de protocolos, la figura 3.50 muestra el formato RIP usado por redes IP en Internet. Algunas otras variaciones de RIP hacen ligeras modificaciones al formato y/o a los nombres de los campos, pero el algoritmo básico de ruteo es funcionalmente el mismo.

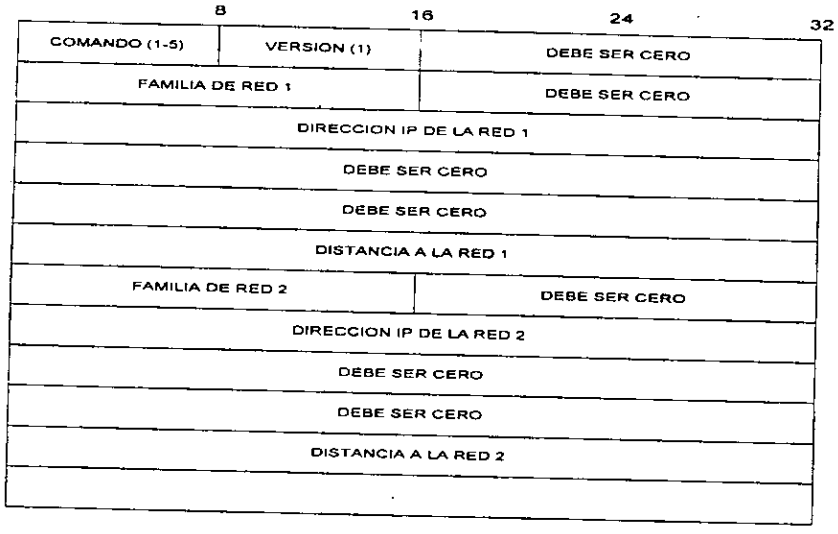


Figura 3.50 Formato de un mensaje RIP. Después del encabezado de 32 bits, el mensaje contiene una secuencia de pares, donde cada par consiste de la dirección de red IP y la distancia a tal red.

El campo **Comando** especifica una operación de acuerdo a la siguiente tabla:

Comando	Significado
1	Solicitud de información total o parcial de enrutamiento
2	Respuesta conteniendo pares red-distancia desde la tabla de ruteo del emisor
3	Encendido del modo trazado (obsoleto)
4	Apagado del modo trazado (obsoleto)
5	Reservado para uso interno de Sun Microsystems

Un ruteador o host puede pedir a otro ruteador información de enrutamiento enviando un comando de Solicitud. Los ruteadores responden a las solicitudes usando el comando Respuesta. En la mayoría de los casos, sin embargo, los ruteadores difunden mensajes de Respuesta regularmente aunque estos no sean solicitados. El campo **Versión** contiene el número de la versión del protocolo (actualmente 1), y es usado por el receptor para verificar que se interprete el mensaje correctamente. El formato del campo

de direcciones no está limitado únicamente a ser utilizado por TCP/IP; puede ser utilizado con múltiples familias de protocolos. Como lo muestra la figura 3.50 cada dirección de red reportada por RIP puede tener un dirección de hasta 14 octetos. Las direcciones IP ocupan desde el tercer hasta el sexto octeto del campo de dirección para asegurar un alineamiento de 32 bits. El campo etiquetado **Familia de Red n** identifica la familia del protocolo bajo la cual la dirección de red debe ser interpretada. RIP usa valores asignados a las familias de direcciones bajo el sistema operativo 4BSD UNIX (las direcciones IP son asignadas con el valor 2).

El campo final de cada entrada en un mensaje RIP, es el campo **Distancia a la Red n**, contiene un valor entero de la distancia a la red especifica. Las distancias están medidas en saltos, pero los valores están limitados del rango de 1 a 16, con distancia 16 utilizada para indicar infinito (no existe ruta).

Así como otros protocolos de ruteo, RIP usa ciertos temporizadores para regular su desempeño . El temporizador de actualización de ruteo está generalmente establecido a 30 segundos, asegurando que cada ruteador enviará una copia completa de su tabla a todos sus vecinos cada 30 segundos. Cuando un ruteador instala una ruta en su tabla, establece un temporizador para tal ruta. El temporizador denominado de ruta invalida, debe ser restablecido en cualquier momento que el ruteador recibe otro mensaje RIP anunciando la ruta. La ruta se convierte en invalida si 180 segundos pasan sin que la ruta haya sido anunciada nuevamente. Cuando un ruteador es marcado invalido, sus vecinos son notificados de este acto. Esta notificación debe ocurrir antes de la expiración del temporizador de limpieza de ruta. Cuando el temporizador de limpieza de ruta expira, la ruta es removida de la tabla de ruteo. Un valor tipico para el temporizador de limpieza de ruta es de 270 segundos.

3.21.2 EL PROTOCOLO RUTA MÁS CORTA PRIMERO ABIERTO (OSPF)

El protocolo Ruta Más Corta Primero Abierto (Open Shortest Path First, OSPF), fue creado debido a que RIP a mediado de los ochentas estaba siendo incapaz se soportar a grandes redes heterogéneas.

Como lo indica su acronimo, OSPF tiene dos caracteristicas principales. La primera es que es abierto, es decir, que su especificación es de dominio publico. La

especificación está publicada como un documento RFC (rfc 1247). La segunda característica es que está basado en el algoritmo SPF.

OSPF es un protocolo de ruteo de *enlace de estado*, como tal llama por el envío de anuncios de estado de enlace a los demás ruteadores dentro de la misma área jerárquica. Como los ruteadores OSPF acumulan información del estado del enlace, usan el algoritmo SPF para calcular la ruta más corta a cada nodo.

A diferencia de RIP, OSPF puede operar dentro de una jerarquía. La entidad más grande dentro de la jerarquía es el sistema autónomo. Un sistema autónomo puede ser dividido en un numero de áreas, una área es un grupo de redes contiguas y ruteadores. Los ruteadores con múltiples interfaces pueden participar en múltiples áreas. Estos ruteadores, los cuales son llamados como ruteadores de frontera de área, mantienen bases de datos topologicas para cada área.

Una base de datos topologica es esencialmente una gráfica global de redes en relación a los ruteadores, contiene la colección de anuncios de estado de enlace recibidos desde todos los ruteadores en la misma área. Debido a que los ruteadores dentro de la misma área comparten la misma información, tienen bases topologicas idénticas.

El termino dominio es a veces usado para describir una porción de la red en la cual todos los ruteadores tienen bases topologicas idénticas. El termino Dominio es frecuentemente usado como sinónimo de Sistema Autónomo. La topología de una área es invisible a las entidades fuera de la área, al mantener áreas topologicas separadas, OSPF pasa menos tráfico de ruteo, en contraste con un Sistema Autónomo no particionado.

El particionamiento de un Sistema Autónomo en áreas crea dos diferentes tipos de ruteo OSPF, dependiendo si la fuente y el destino están en la misma área o en áreas diferentes. El ruteo intra-area ocurre cuando la fuente y el destino están en la misma área; el ruteo inter-area ocurre cuando están en áreas diferentes.

Un backbone OSPF es responsable de distribuir información de ruteo entre áreas. Consiste de todos los ruteadores de frontera de área, redes no contenidas totalmente en una área, y sus ruteadores, la figura 3.51 muestra un ejemplo de un internet con varias áreas.

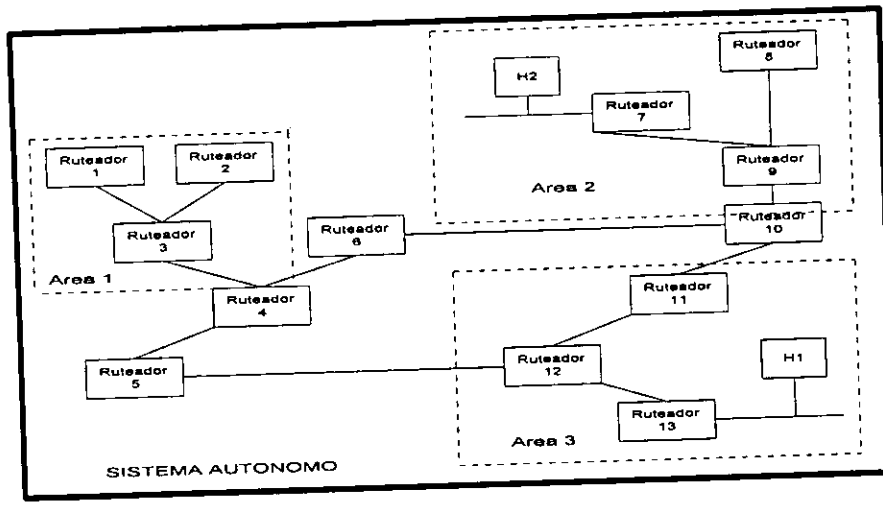


Figura 3.51 Un sistema autónomo dividido en varias áreas

En esta figura, los ruteadores 4,5,6,10,11 y 12 forman el backbone. Si el host H1 en el área 3 desea enviar un paquete al host H2 en el área 2, el paquete es enviado al ruteador 13, el cual lanza el paquete al ruteador 12, el cual a su vez lanza el paquete al ruteador 11. El ruteador 11 lanza el paquete a través del backbone al ruteador 10 de frontera de área, el cual envía el paquete a través de los ruteadores de intra-área (ruteadores 9 y 7) para entregar finalmente el paquete al host H2.

El backbone por si mismo es una área OSPF, así todos los ruteadores del backbone usan los mismo procedimientos y algoritmos para mantener la información de ruteo dentro del backbone como cualquier ruteador de área lo haría. La topología del backbone es invisible para todos los ruteadores de intra-área, como lo son las áreas topologicas individuales para el backbone.

Los ruteadores de frontera de un sistema autónomo que corren OSPF aprenden las rutas exteriores a través de los protocolos de compuerta exterior tales como EGP o BGP, o a través de información de configuración.

3.21.2.1 FORMATO DEL MENSAJE OSPF

Todos los paquetes OSPF empiezan con un encabezado de 24 octetos como lo muestra la figura 3.52

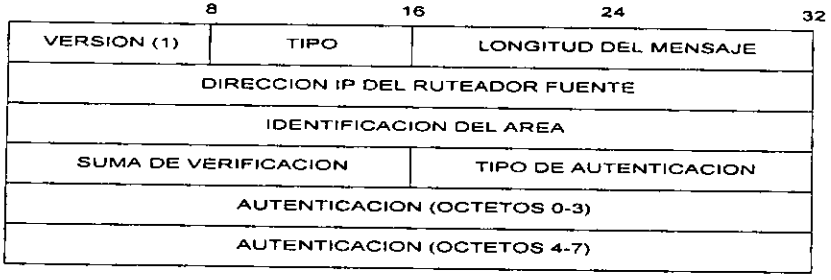


Figura 3.52 Formato del encabezado fijo de 24 octetos del mensaje OSPF

El campo **versión** especifica la versión del protocolo que está siendo utilizada. El campo **tipo** identifica el tipo del mensaje, los cuales son:

Tipo	Significado
1	Hola (usado para probar la accesibilidad)
2	Descripción de la base de datos (topología)
3	Solicitud del status del enlace
4	Actualización del status del enlace
5	Reconocimiento del status del enlace

El campo **longitud del mensaje**, especifica en octetos la longitud del mensaje incluyendo el encabezado. El campo **Dirección IP** del ruteador fuente, da la dirección del emisor. El campo **Identificación del área** da el numero de identificación de 32 bits del área. El campo **Suma de verificación**, checa el contenido del paquete entero por daños potenciales sufridos en la ruta. El campo tipo de **autenticación**, contiene un tipo de autenticación. "Un password simple" es un ejemplo de un tipo de autenticación. Todos los intercambios de los protocolos OSPF son autenticados. El tipo de autenticación es configurable en una base por áreas. Los campos autenticación, contienen información de autenticación formada por 64 bits de longitud.

3.21.2.2 MENSAJES OSPF

- Mensaje Hola OSPF. OSPF envía mensajes hola en cada enlace periódicamente para establecer y probar la accesibilidad a un vecino. La figura 3.53 muestra el formato del mensaje OSPF Hola.

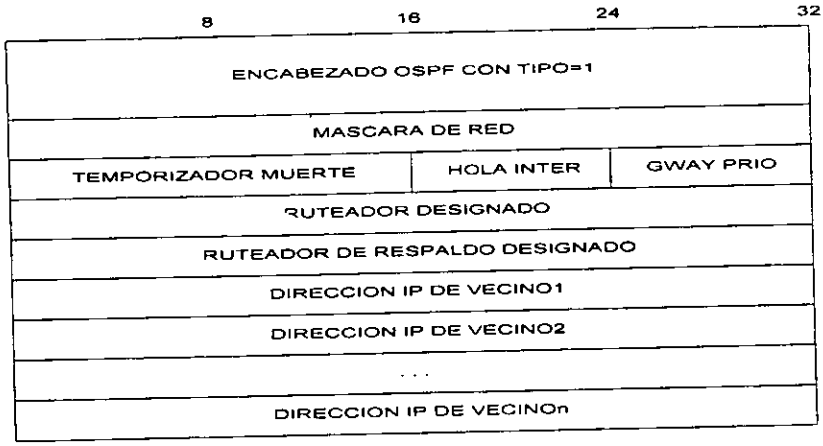


Figura 3.53 Formato del mensaje OSPF Hola.

El campo Mascara de red contiene una mascara para la red sobre la cual el mensaje ha sido enviado. El campo Temporizador muerte da el tiempo en segundos después del cual un ruteador que no responda se considera "muerto". El campo Hola inter es el periodo normal en segundos entre los mensajes hola. El campo Gway prio es un numero entero que da la prioridad del ruteador, y es usado en la selección de un ruteador de respaldo. El campo Ruteador designado y Ruteador respaldo designado contiene la dirección IP que se da desde el punto de vista del emisor para el ruteador designado y el ruteador de respaldo designado para la red sobre la cual el mensaje está siendo enviado. Finalmente los campos dirección IP del Vecino_n dan la dirección IP de todos los vecinos desde los cuales el emisor ha recibido recientemente mensajes hola.

- Mensaje OSPF de descripción de base de datos. Los ruteadores intercambian mensajes de descripción de base de datos para inicializar su base de datos topologica. En el intercambio, un ruteador sirve como maestro, mientras que el otro es un esclavo. El esclavo reconoce cada mensaje de descripción con una respuesta. La figura 3.54 muestra el formato.

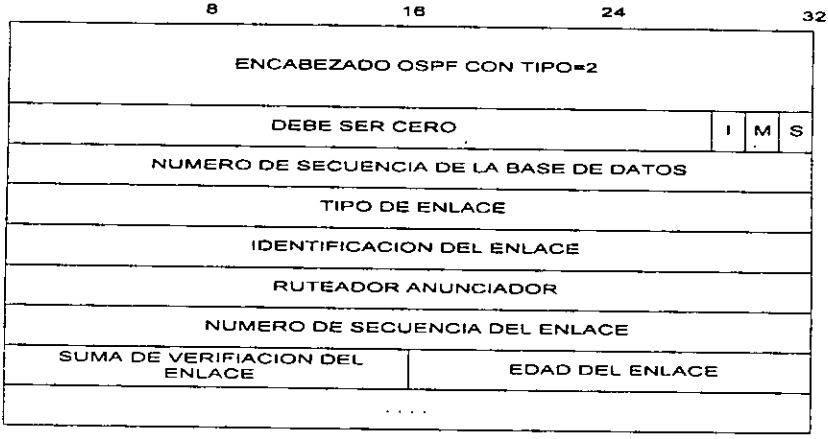


Figura 3.54 Formato del mensaje OSPF de Descripción de base de datos

Debido a que el mensaje puede ser grande, la base topologica puede ser dividida en varios mensajes usando los bits I y M. El bit I establecido en 1 en el mensaje inicial; el bit M es establecido en 1 si le siguen mensajes adicionales. El bit S indica si un mensaje fue enviado por un maestro (1) o por un esclavo (0). El campo Numero de secuencia base de datos, establece la secuencia de los números para los mensajes de tal forma que el receptor puede decir si falta alguno. Los campos desde Tipo de enlace hasta Edad del enlace describe un enlace en la topología de la red; están separados para cada enlace. El Tipo de enlace describe un enlace de acuerdo a la siguiente tabla.

Tipo de enlace	Significado
1	Enlace a ruteador
2	Enlace a red
3	Resumen de enlaces (red IP)
4	Resumen de enlaces (enlace a un ruteador de frontera)
5	Enlace externo (enlace a otro sitio)

El campo Identificación del enlace da una identificación para el enlace (el cual puede ser la dirección IP de un ruteador o una red, dependiendo del tipo de enlace).

El campo Ruteador anunciador especifica la dirección del ruteador que está anunciando el enlace. El campo Numero de secuencia del enlace contiene un entero generado por aquel ruteador que asegure que no hay mensajes faltantes o fuera de

orden. El campo Suma de verificación del enlace provee mayor seguridad de que la información de enlace no ha sido corrompida. Finalmente, el campo Edad del enlace también auxilia a ordenar los mensajes, da el tiempo en segundos desde que el enlace fue establecido.

- Mensaje Solicitud del status del enlace. Después del intercambio de mensajes de descripción con un vecino, un ruteador puede descubrir que partes de su base de datos están caducas. Para solicitar que el vecino proporcione información actualizada, el ruteador envía un mensaje de solicitud de status del enlace. El mensaje lista enlaces específicos como se muestra en la figura 3.55. El vecino responde con la información más actualizada que tiene acerca de dichos enlaces. Los tres campos mostrados son repetidos para cada enlace que está siendo solicitado.

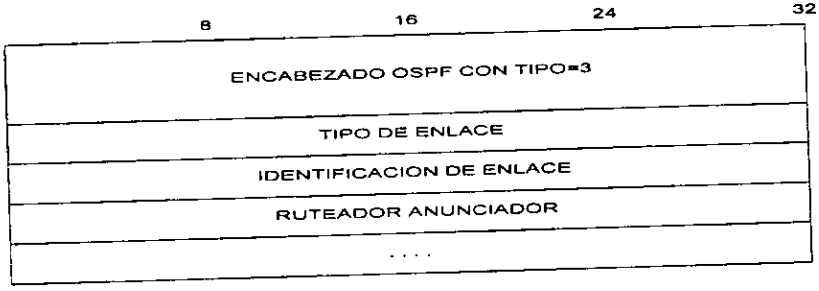


Figura 3.55 Formato del mensaje de Solicitud del status de enlace

- Mensaje de Actualización del status del enlace. Los ruteadores difunden (broadcast) el status de los enlaces con un mensaje de actualización. Cada actualización consiste de una lista de anuncios, como se muestra en la figura 3.56

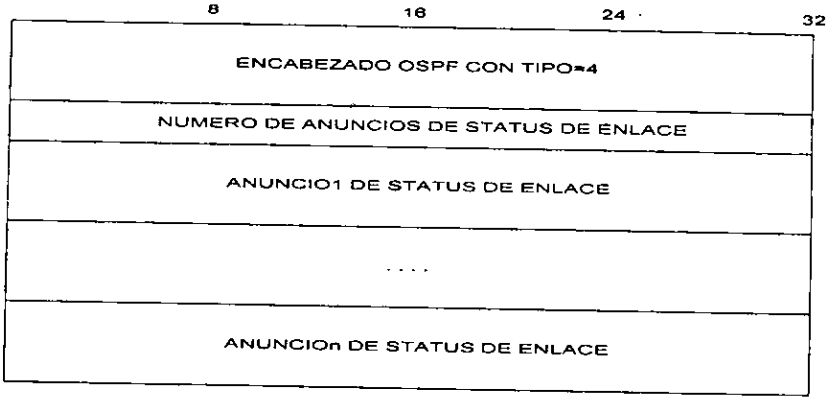


Figura 3.56 Formato del mensaje OSPF de Actualización del status del enlace

Cada anuncio de status de enlace tiene un encabezado como el que se muestra en la figura 3.57. Los valores utilizados en cada campo son los mismos que en el mensaje descripción de la base de datos.

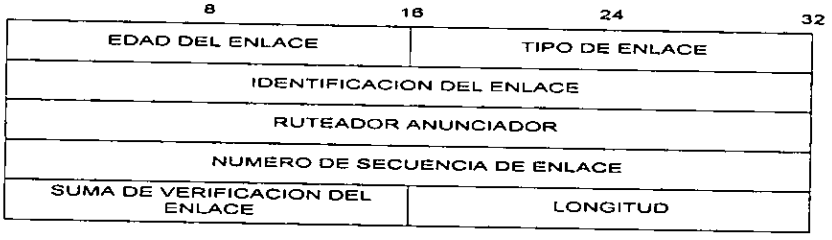


Figura 3.57 Formato del encabezado utilizado para todos los anuncios de status de enlace.

Siguiendo al encabezado vienen uno de cuatro posibles formatos para describir los enlaces desde un ruteador a una área dada, los enlaces desde un ruteador a una red especifica, los enlaces desde un ruteador a las redes físicas que comprenden una subred IP, o los enlaces desde un ruteador a las redes de otros sitios. En todos los casos, el campo Tipo de enlace en el encabezado especifica cuales de los formatos han sido especificados. De esta forma, un ruteador que recibe un mensaje de actualización del status del enlace sabe exactamente cual de los destinos descritos residen dentro del sitio y cuales son externos.

3.22 CAPA DE TRANSPORTE

Para finalizar este capitulo se explicaran los protocolos correspondientes a la capa superior del protocolo IP, es decir, los protocolos TCP y UDP ubicados en la capa de transporte del modelo TCP/IP (ver figura 3.14.)

3.23 EL PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

Como se muestra en la figura 3.14, TCP reside en la capa de transporte del modelo conceptual de cuatro capas del software TCP/IP. Está situado por arriba de la capa IP y por debajo de la capa de aplicaciones. Como se muestra también en la figura 3.16 TCP no se carga dentro de un ruteador. Está diseñado para residir en un host.

Debido a que IP es un protocolo sin conexión encargado entre otras cosas del enrutamiento de los datagramas, las tareas de confiabilidad, flujo de control, secuenciación de los paquetes, apertura y clausuras de transmisiones; están dadas a TCP. TCP es el responsable de romper el mensaje proveniente de la capa de aplicación en paquetes, reensamblarlos en el sitio destino, retransmitir paquetes perdidos, eliminar paquetes duplicados y colocarlos en el orden correcto.

TCP proporciona un numero considerable de servicios a la capa IP y capas superiores. Es un protocolo orientado a la conexión, este término se refiere al hecho de que TCP mantiene información del estado de cada corriente de datos de usuario que fluyen hacia dentro y fuera del modulo TCP. El término usado en este contexto también significa que TCP es responsable por la transferencia extremo-extremo de los datos a través de una red o múltiples redes para un par de aplicaciones (emisora-receptora). Refiriéndose a la figura 3.16, TCP debe asegurar que los datos sean transmitidos y recibidos entre los hosts ya se a través de una o más redes.

El aislamiento de estos servicios en una capa por separado permite que las aplicaciones se diseñen sin preocuparse del control de flujo o de la confiabilidad del mensaje. Sin la capa TCP, cada aplicación tendría que implementar estos servicios por sí misma, lo que resultaría en un desperdicio de recursos.

Debido a que TCP es un protocolo orientado a conexión, es el responsable de la transferencia confiable de cada uno de los caracteres (octetos) pasados desde un

aplicación en el host emisor a la aplicación en el host receptor. Consecuentemente para llevar a cabo está misión, usa números de secuencia y acuses de recibo por parte del host receptor de los paquetes recibidos.

El término asociado para estos aspectos de comunicación orientada a la conexión, se conoce como circuito virtual. Hacer una transferencia extremo-extremo es análoga a hacer una llamada telefónica, antes de que la comunicación pueda empezar, las aplicaciones en los extremos deben interactuar con sus respectivos sistemas operativos, informándoles del deseo de establecer una transferencia. Una vez establecida la conexión (circuito) la transferencia puede comenzar. Para las aplicaciones, la conexión es vista como un circuito de hardware dedicado, pero es una ilusión (virtual) provista por el servicio de entrega de datos, en este caso TCP.

Aunque muchas veces se presenta o se piensa a TCP como una parte inseparable de IP, éste es un protocolo independiente de propósito general que puede ser adaptado para ser usado con otros protocolos. Por ejemplo, TCP o algunas de sus partes se utilizan con FTP así como en el protocolo Simple de Transferencia de Correo (SMTP), ninguno de los cuales utiliza IP.

3.23.1 OPERACIÓN DE TCP

Con el fin de entender el papel de TCP dentro de Internet se presenta un ejemplo de su operación, abarcando los aspectos generales de éste para después revisar los aspectos particulares.

Un mensaje se origina a partir de una aplicación y se pasa a TCP desde una capa superior, a través de un protocolo conocido de capa superior. El mensaje se pasa como un flujo (una secuencia de caracteres individuales). TCP recibe el flujo de octetos y los agrupa en segmentos o paquetes TCP, añadiéndoles su encabezado. Cada segmento tiene calculada e incrustada una suma de verificación dentro del encabezado, así como un numero de secuencia si en el mensaje completo hay más de un segmento. La longitud del segmento por lo general es determinada por TCP o por un valor de sistema establecido por el administrador de la red.

Si se requiere comunicación de dos vías (como en el caso de Telnet o de FTP), se establece una conexión (circuito virtual) entre las máquinas emisora y receptora, antes

de pasar el segmento a IP para su enrutamiento. Este proceso se inicia en el software TCP emisor enviando una solicitud de conexión TCP a la máquina receptora. En el mensaje aparece un número único (conocido como número de socket) que identifica a la conexión de la máquina emisora. El software TCP de la máquina receptora asigna su propio número único de socket y lo devuelve a la máquina original. Estos dos números únicos definen entonces la conexión entre las dos máquinas hasta que se dé por terminado el circuito virtual.

Después de establecer el circuito virtual, TCP envía el segmento al software IP, el que a su vez envía el mensaje a la red como datagrama, una vez que haya recorrido el camino a través del internet, el modulo IP de la máquina receptora pasa el segmento recibido a la capa TCP, donde se procesa y se pasa a la capa superior (aplicación).

Si el mensaje tenía más de un segmento de largo, el software TCP receptor lo reensambla utilizando los números de secuencia contenidos en cada encabezado de segmento. Si algún segmento es erróneo o está corrompido, TCP devuelve un mensaje con el número de secuencia defectuoso. A continuación el software TCP emisor puede volver a enviar el segmento malo.

Si para todo el mensaje solamente se utiliza un segmento, después de comparar la suma de verificación del segmento con un valor recién calculado, el software TCP receptor puede generar ya sea un acuse de recibo positivo (ACK) o una solicitud de reenvío del segmento y enrutarlo de regreso a la máquina emisora.

3.23.2 PUERTOS Y SOCKETS

TCP permite a múltiples programas de aplicación en una máquina comunicarse concurrentemente, también demultiplexa el tráfico (en la máquina receptora) que fluye fuera del modulo TCP entre los programas de aplicación (ver apartado 3.10.3). TCP identifica a la aplicaciones mediante un número, denominado **número de puerto**. En otras palabras, el número de puerto identifica el tipo de servicio que un sistema TCP está solicitando a otro.

Cada circuito de comunicación dentro y fuera de la capa TCP se identifica en forma única mediante la combinación de dos números, los cuales en conjunto se conocen como **socket**. El socket se compone de la dirección IP de la máquina y del numero de

puerto utilizado por el software TCP. Hay un socket tanto en la máquina emisora como en la receptora. Debido a que la dirección IP es única a través de todo el internet y los números de puerto serán únicos para la máquina, los números de socket también resultaran únicos en todo el internet. Esto permite que un proceso se comunique con otro a través de la red basándose enteramente en el número de socket[15].

3.23.3 FORMATO DEL SEGMENTO TCP

La unidad de transferencia entre el software TCP en dos máquinas se llama paquete o segmento. El segmento está dividido en dos partes, un encabezado seguido por datos como se muestra en la Figura 3.58.

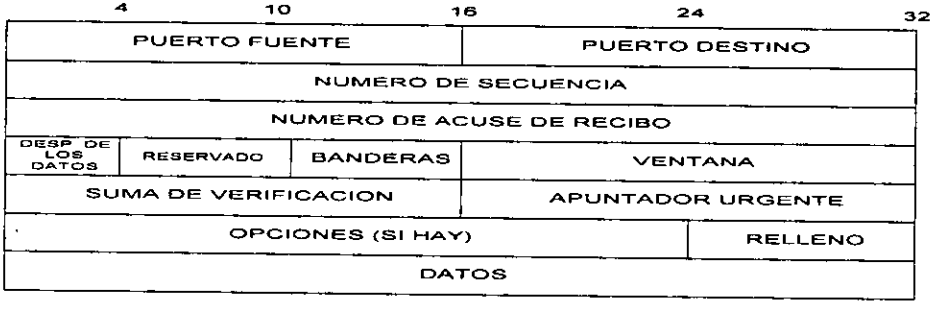


Figura 3.58 Formato del segmento TCP

Los primeros dos campos del encabezado del segmento son identificados como el *PUERTO FUENTE* y el *PUERTO DESTINO*. Estos campos de 16 bits identifican al programa de aplicación que están usando la conexión TCP.

El siguiente campo etiquetado como *NUMERO DE SECUENCIA*, es un número que indica la posición del bloque actual de datos dentro del mensaje total.

El número de secuencia también es utilizado durante una operación de conexión. Si una solicitud de conexión es utilizada entre dos entidades TCP, el numero de

[15] TCP utiliza la conexión como elemento fundamental. Una conexión completa tiene dos puntos extremos (sockets). Esto permite que un puerto de protocolo (aplicación) se utilice para varias conexiones al mismo tiempo.

secuencia especifica el numero de secuencia inicial que va a ser utilizado para la subsecuente numeración de los datos del usuario.

El *NUMERO DE ACUSE DE RECIBO*, el valor de este campo establece el numero de secuencia del siguiente octeto que se espera sea transmitido. De forma indirecta, también muestra el numero de secuencia del último dato que se recibió; siendo éste el del último número acusado menos 1.

El *DESPLAZAMIENTO DE LOS DATOS* especifica el numero de palabras de 32 bits alineadas que comprende el encabezado TCP. Este campo es usado para determinar donde empieza el campo de datos.

El campo *RESERVADO* consiste de 6 bits los cuales deben ser cero. Estos bits están reservados para uso futuro.

Algunos segmentos transportan sólo acuses de recibo, otros transportan datos, otros más; peticiones para solicitar el establecimiento o clausura de una conexión. TCP utiliza un campo de 6 bits etiquetado como *BANDERAS* para determinar el propósito y contenido de un segmento. Algunos de los bits determinan cómo interpretar a otros campos dentro del encabezado. Los seis bits son usados para cubrir la siguiente información.

- URG indica que es significativo el campo apuntador urgente
- ACK significa que el campo de acuse de es significativo
- PSH significa que el modulo va a ejercitar la función push o empuje
- RST indica que la conexión va a ser reinicializada
- SYN indica que los números de secuencia van a ser sincronizados. Esta bandera se utiliza al establecerse una conexión.
- FIN indica que el emisor no tiene más datos para enviar

El siguiente campo, etiquetado como *VENTANA*, se establece a un valor indicando cuantos octetos puede aceptar la máquina destino. El valor se anuncia en cada mensaje de acuse de recibo.

El campo *SUMA DE VERIFICACIÓN* se calcula tomando el complemento a uno de 16 bits de la suma de complementos a uno de las palabras de 16 bits. Incluye el

encabezado y los datos. El propósito de la suma de verificación es determinar si el segmento llega libre de errores.

El siguiente campo en el segmento es el, *APUNTADOR DE URGENTE* es utilizado sólo si la bandera URG está activa. Señala los datos dentro de un mensaje que son considerados como urgentes, mediante un desplazamiento en el número de secuencia del encabezado (el valor indicado por el apuntador especifica la posición donde terminan los datos urgentes). TCP no toma ninguna acción especifica en relación con datos urgentes; la acción queda determinada por la aplicación. Los datos urgentes son llamados también datos fuera de banda.

Aunque TCP es un protocolo orientado a un flujo de datos, en ocasiones es importante para el programa de aplicación al extremo de una conexión enviar datos fuera de banda (secuencia), sin que se tenga que esperar a que el programa de aplicación en el otro extremo consuma los octetos colocados en el flujo. Señales de interrupción o para abortar, son frecuentemente necesarias cuando un programa en una máquina remota falla en su operación. Por esta razón los datos fuera de banda deben ser procesados sin espera y sin importar su posición en el flujo de datos por el programa fallido, de otra forma no se podrían abortar los programas que detienen su entrada de datos.

El campo de *OPCIONES* está construido en una manera similar al campo de opciones del datagrama IP, en el que cada opción consiste de un octeto conteniendo un número de opción, un campo conteniendo la longitud de la opción, y finalmente la opción en sí misma. El campo de opciones tiene una función útil: especificar el tamaño máximo del búfer que una implementación TCP puede manejar. Debido a que no todos los segmentos a través de una conexión serán del mismo tamaño, TCP usa el campo de opciones para negociar con el modulo TCP del otro extremo de la conexión el tamaño máximo del segmento que van a transferir.

Actualmente el campo de opciones esta limitado en su uso, con sólo tres opciones definidas por el estándar TCP:

0 Fin de la lista de opciones

1 No operación

2 Tamaño máximo de segmento

El último campo en el encabezado es el *RELLENO* cuya función es la de completar a un múltiplo de 32 bits el encabezado.

3.23.4 ESTABLECIMIENTO DE UNA CONEXIÓN TCP

TCP tiene dos métodos para establecer una conexión: activo y pasivo. Un establecimiento de conexión activo ocurre cuando TCP emite una solicitud para una conexión, basado en una instrucción proveniente de un protocolo de nivel superior que proporciona el número de socket. Un método pasivo ocurre cuando el protocolo de nivel superior instruye a TCP que espere la llegada de solicitudes de conexión de un sistema remoto (una instrucción de apertura activa). Cuando TCP recibe esta solicitud, le asigna un número de puerto.

TCP tiene reglas estrictas en relación con la utilización de procesos de conexión pasivos y activos. Por lo general una apertura pasiva se ejecuta en una máquina, en tanto que la apertura activa se ejecutará en la otra con información especifica acerca del número del socket, precedencia (prioridad) y niveles de seguridad. Aunque la mayor parte de las comunicaciones TCP se establecen mediante una solicitud activa a un puerto pasivo, es posible abrir una conexión sin un puerto pasivo esperando.

Una conexión se puede establecer entre dos máquinas únicamente si ambas están de acuerdo en la conexión y si ambas máquinas tienen recursos TCP adecuados para darle servicio a la conexión. Si alguna de estas condiciones no se puede cumplir, la conexión no se efectuará. Cuando se establece una conexión, se le dan ciertas propiedades que se mantienen válidas hasta que se cierra la conexión. Típicamente, éstas consistirán en un valor de precedencia y un valor de seguridad.

En la mayor parte de los casos, dos aplicaciones esperan una conexión, por lo emiten solicitudes de apertura activas y pasivas. En la figura 3.59 se muestra el proceso para una conexión TCP.

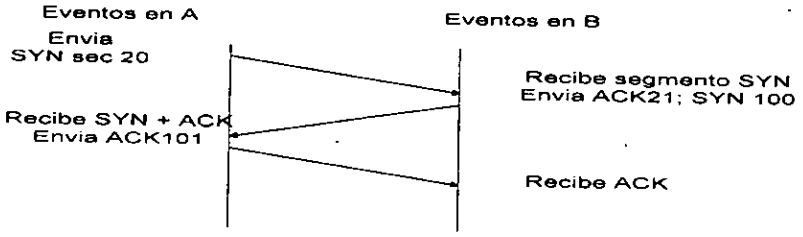


Figura 3.59 Secuencia de mensajes en una conexión TCP

El proceso empieza con el TCP de la máquina A recibiendo una solicitud de conexión de su protocolo de capa superior, el cual envía una solicitud de una apertura activa a la máquina B. El segmento que se construye tendrá la bandera SYN activa (en 1) y un numero de secuencia asignado. La figura muestra lo anterior con la notación SYN SEC 20 indicando que la bandera SYN está activa y el número de secuencia es 20 (cada máquina debe elegir un número inicial de secuencia en forma aleatoria que serán utilizados para identificar sus respectivos octetos).

La aplicación de la máquina en B previamente habrá emitido un instrucción de apertura pasiva a su TCP. Cuando recibe el segmento SYN SEC 20, el modulo TCP de la máquina B regresará un acuse de recibo a la máquina A, con el numero de secuencia 21. La máquina B también definirá un numero inicial de secuencia. La figura muestra el mensaje como ACK 21; SYN 100 indicando que el mensaje es un acuse de recibo con el numero de secuencia 21, tiene la bandera SYN activa y tiene un numero inicial de secuencia de 100.

Al recibirlo, la máquina A regresa su propio mensaje de acuse de recibo, con el numero de secuencia 101. Una vez que la conexión se ha establecido, los datos pueden fluir en ambas direcciones.

3.23.5 TRANSFERENCIA DE DATOS Y CONTROL DE FLUJO

La transferencia de información es sencilla, el emisor mantiene un registro de cada paquete enviado y espera por un acuse de recibo antes de enviar el siguiente paquete. El emisor también establece un temporizador cuando envía un paquete y retransmite el paquete si el temporizador expira antes de que llegue un acuse de recibo. La figura 3.60 muestra el procedimiento de transferencia entre dos maquinas.

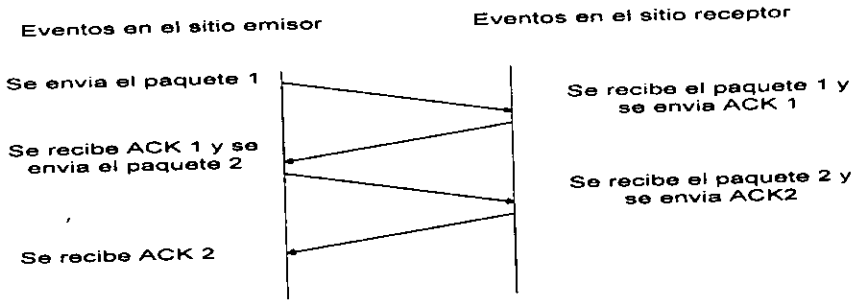


Figura 3.60 Secuencia en el envío y recepción de paquetes con TCP

En la figura 3.60, los eventos en el emisor y receptor están a la izquierda y derecha respectivamente. Cada diagonal muestra la transferencia de un mensaje a través de la red.

Si se siguiera el modelo anterior al pie de la letra entonces se provocaría un desperdicio en el ancho de banda de la red, debido a que los datos entre las máquinas sólo fluyen en una dirección en cualquier momento, y el desperdicio sería mayor si la red es capaz de soportar una comunicación simultánea en ambas direcciones. La red estaría completamente ociosa durante el tiempo que las máquinas retardaran sus respuestas.

TCP utiliza un mecanismo especializado conocido como "ventana deslizable" para aumentar la eficiencia de la transmisión y el control del flujo de la información. Los protocolos de ventana deslizable emplean mejor el ancho de banda debido a que le permiten al emisor transmitir múltiples paquetes antes de esperar un acuse de recibo. La forma más fácil de ver la operación de una ventana deslizable es pensar en una secuencia de paquetes a ser transmitidos como se muestra en la figura 3.61. El protocolo coloca una pequeña ventana de longitud fija en la secuencia y transmite todos los paquetes que quepan en la ventana.

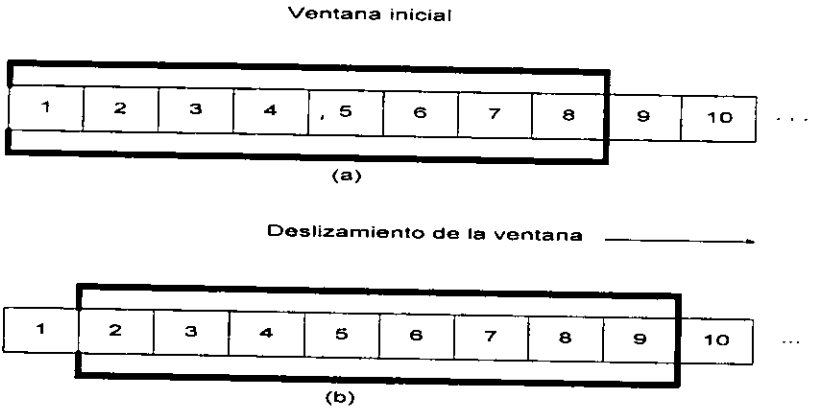


Figura 3.61 (a) Ventana deslizable con ocho paquetes, (b) la ventana se desliza al paquete 9 de tal manera que puede ser enviado cuando se recibe acuse de recibo para el paquete 1

Se dice que un paquete no ha sido acusado si ha sido transmitido pero no se ha reportado un acuse de recibo del mismo. Técnicamente, el número de paquetes que pueden estar sin acuse en cualquier momento está limitado por el tamaño de la ventana. Por ejemplo, un protocolo de ventana deslizable con un tamaño de 8, al emisor se le permite transmitir 8 paquetes antes de que reciba un acuse de recibo.

Como se muestra en la figura 3.61(b), una vez que el emisor recibe un acuse de recibo para el primer dentro de la ventana, este "desliza" la ventana y envía el siguiente paquete. La ventana continua deslizándose a medida que se reciban acuses de recibo. Así, la ventana divide la secuencia de los paquetes en tres conjuntos: aquellos paquetes a la izquierda de la ventana han sido exitosamente transmitidos, recibidos, y acusados; aquellos paquetes a la derecha que no han sido trasmitidos aún; y aquellos paquetes que residen dentro de la ventana y que están siendo transmitidos. Cabe mencionar que el lado receptor, mantiene una ventana análoga, aceptando y acusando de recibido los paquetes recibidos. De esta forma se incrementa el desempeño, ya que se mantiene a la red ocupada.

El mecanismo de ventana deslizable de TCP también resuelve el problema del control de flujo entremo-extremo, permitiendo al receptor restringir la transmisión hasta que su búfer de recepción tenga el suficiente espacio para acomodar más datos.

El mecanismo de ventana deslizable TCP opera a nivel de octetos, no al nivel de segmentos o paquetes. Los octetos del flujo son numerados secuencialmente, y el emisor mantiene tres apuntadores asociados con las posiciones de los octetos en la ventana (como se menciona líneas arriba).

Una variación que presenta el mecanismo de ventana deslizable TCP es que permite que el tamaño de la ventana varíe de acuerdo al tráfico existente en la red. Cada acuse de recibo, el cual especifica cuantos octetos han sido recibidos, también contiene una ventana de anuncio que especifica cuantos octetos adicionales de datos está preparado para aceptar el receptor. Se puede ver a la ventana de anuncio como el tamaño actual del búfer de recepción. En respuesta al incremento de la ventana de anuncio, el emisor incrementa el tamaño de su ventana deslizable y procede a enviar los octetos que no han sido acusados de recibo. En respuesta a un decremento de la ventana de anuncio el emisor decrementa el tamaño de su ventana y detiene el envío de octetos más allá del límite. TCP no debe contradecir los anuncios previos al encoger la ventana de posiciones previamente aceptadas en el flujo. En su lugar, anuncios pequeños acompañan a los acuses de recibo, de tal manera que el tamaño de la ventana cambia a la vez que se desliza.

La ventaja de usar un ventana de longitud variable es que proporciona control del flujo así como una transferencia confiable. Si el búfer del receptor empieza a llenarse, no podrá tolerar más paquetes, entonces envía una ventana de anuncio de longitud menor. En el caso extremo, el receptor anuncia una ventana de tamaño cero para detener la transmisión. Después, cuando el espacio del búfer se empiece a vaciar, el receptor emitirá otra ventana de anuncio diferente de cero para disparar el flujo de datos nuevamente.

Tener un mecanismo para controlar el flujo es esencial en un internet, donde las máquinas de varias velocidades y tamaños se comunican a través de redes y ruteadores de varias velocidades y capacidades.

3.23.6 LOS TEMPORIZADORES EN TCP

Uno de los aspectos más importantes y complejos en TCP está involucrado en la forma en que maneja los temporizadores y retransmisiones. Cada vez que se envía un

segmento TCP inicia un temporizador y espera por un acuse de recibo. Si el temporizador termina antes del arribo del acuse, TCP asume que el segmento se perdió o se corrompió y por lo tanto lo retransmite. En un medio internet donde un segmento viaja a través de muchas y diversas redes, es imposible conocer en forma exacta que tan rápido regresaran los acuses de recibo a la máquina emisora. Además, el retardo en cada ruteador depende del tráfico, así el tiempo total para que un segmento viaje al destino y regrese un acuse de recibo al emisor varia dramáticamente de un instante a otro.

TCP debe ajustar tanto las vastas diferencia en el tiempo requerido para llegar a los diferentes destinos, como los cambios en los tiempo para alcanzar un destino dado conforme el tráfico varía.

TCP acomoda los retrasos de un internet utilizando un algoritmo de retransmisión adaptativo. En esencia, TCP monitorea el desempeño de cada conexión y deduce valores razonables para los tiempos limite (timeout). Conforme el desempeño de una conexión cambia, TCP actualiza su valor limite (se adapta al cambio).

Para coleccionar los datos necesarios para un algoritmo adaptativo, TCP graba el tiempo en el cual cada segmento es enviado, y el tiempo en el cual un acuse de recibo llega. De los dos tiempos obtenidos TCP calcula el tiempo empleado conocido como Tiempo de viaje redondo. En cualquier momento que se obtiene un nuevo valor de tiempo de viaje redondo, TCP ajusta su noción del tiempo promedio para la conexión. Usualmente, TCP almacena el tiempo de viaje redondo, como un promedio y utiliza los valores de nuevas muestras para ajustarlo continuamente.

3.23.7 CERRANDO UNA CONEXIÓN TCP

Dos programas que usan TCP para comunicarse pueden terminar la conversación de una manera adecuada utilizando la operación cerrar. Cuando un programa de aplicación dice a TCP que no tiene más datos para enviar, TCP cerrará la conexión en una dirección. Para cerrar la mitad de la conexión, el modulo TCP emisor termina de transmitir el resto de los datos, espera a que el receptor los acuse de recibidos, y después envía un segmento con del bit de FIN activado. El modulo TCP receptor acusa el

segmento FIN e informa al programa de aplicación en su extremo que ya no hay más datos disponibles.

Una vez que una conexión ha sido cerrada en una dirección dada, TCP se rehusa en aceptar más datos, mientras tanto, los datos pueden seguir fluyendo en la dirección opuesta hasta que el emisor la cierra. Por su puesto, los acuses de recibo siguen fluyendo hacia el emisor aún después de que la conexión ha sido cerrada. Cuando ambas direcciones han sido cerradas, el software TCP en cada extremo borra el registro de la conexión. La figura 3.61 muestra el procedimiento que se efectúa en la clausura de una conexión.

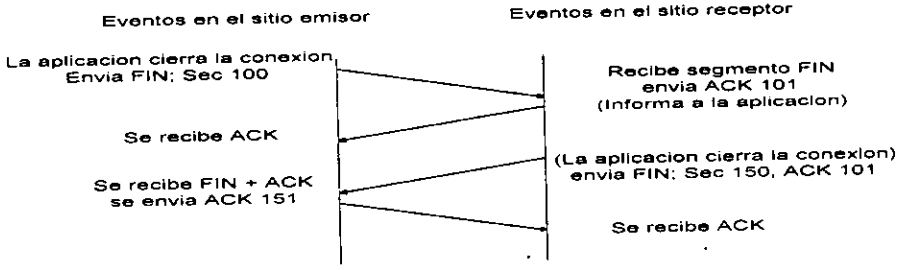


Figura 3.61 Secuencia de mensajes para la clausura de una conexión TCP

La diferencia con respecto al procedimiento para establecer una conexión ocurre después de que una máquina recibe el segmento inicial FIN. En lugar de generar un segundo segmento FIN inmediatamente, TCP envía un acuse de recibo y después informa a la aplicación de la solicitud de cierre. Informar al programa de aplicación de la solicitud y la obtención de una respuesta puede tomar un tiempo considerable (por ejemplo, puede involucrar interacción humana). Los acuse de recibo previenen la retransmisión del segmento inicial FIN durante la espera. Finalmente el programa de aplicación instruye a TCP que cierre la conexión completamente, TCP envía el segundo segmento FIN y el sitio original responde con un acuse de recibo.

3.23.8 NÚMEROS DE PUERTO BIEN CONOCIDOS TCP

Todas las aplicaciones de capa superior que utilizan TCP (o UDP) tienen un número de puerto que las identifica, esto permite que el número de puerto determine el

tipo de servicio que un sistema TCP está solicitando de otro. La mayor parte de los sistemas mantiene un archivo de los números de puerto y sus servicios correspondientes.

TCP define un conjunto de número de puertos bien conocidos para todo el Internet (para que no exista ambigüedad en la identificación de una aplicación) , para los programas de aplicación comúnmente utilizados, como por ejemplo el correo electrónico. De la misma manera deja más números de puertos disponibles para el sistema operativo, para alojar más programas como sea necesario. Aunque el estándar originalmente reserva números de puerto menores de 256 para ser utilizados como puertos bien conocidos, números por arriba de 1024 ahora han sido asignados. La siguiente lista muestra algunos de los números de puerto TCP, que actualmente han sido asignados

Número de puerto	Nombre del proceso	Descripción
1	TCPMUX	Multiplexor de servicio de puerto TCP
20	FTP-DATA	Protocolo de Transferencia de Archivos-Datos
21	FTP	Protocolo de Transferencia de Archivos-Control
23	TELNET	Telnet
25	SMTP	Protocolo Simple de Transferencia de Correo
53	DOMAIN	Servidor de nombres de dominio
79	FINGER	Finger
161	SNMP	SNMP
179	BGP	Protocolo de compuerta de frontera

3.24 EL PROTOCOLO DE DATAGRAMA DE USUARIO (UDP)

Como se explicó en la sección anterior TCP es un protocolo de transporte basado en conexión. Sin embargo la familia de protocolos TCP/IP posee un protocolo de transporte sin conexión, llamado UDP (User Datagram Protocol, Protocolo de Datagrama de Usuario). Un protocolo sin conexión no provee confiabilidad en la entrega (no hay indicación para el dispositivo emisor de que un mensaje se haya recibido correctamente), mecanismos de control de flujo ni tampoco tiene procedimientos de recuperación de errores (mismos que se deben ignorar o compensar en capas superiores o inferiores).

UDP es utilizado en las situaciones en las cuales la totalidad de los servicios de TCP no son necesarios. Por ejemplo, se tienen aplicaciones que generan mensajes que siempre caben en un datagrama, como en el caso del mapeo de un nombre a una dirección IP. Cuando un usuario intenta hacer una conexión a otro sistema, generalmente lo hace especificando el nombre del sistema, en lugar de la dirección Internet. Su sistema tiene que traducir el nombre a una dirección antes de que se pueda hacer cualquier cosa. Generalmente, sólo pocos sistemas tienen la base de datos utilizada para traducir los nombres en direcciones. Así el sistema del usuario tendrá que enviar una petición a uno de los sistemas que tenga la base de datos. La petición va a ser muy corta, la cual ciertamente cabrá en un datagrama, así como la respuesta; por lo que para su transporte no se necesita toda la complejidad de TCP para hacerlo. En esta situación se recomienda el uso de UDP, si no se obtiene una respuesta después de algunos segundos, simplemente se vuelve a enviar la petición.

Por lo tanto, UDP está diseñado para aplicaciones donde no se necesita colocar muchas secuencias de datagramas juntos.

UDP sirve como una simple interface para el protocolo IP, ya que principalmente funciona como multiplexor/demultiplexor para la recepción y envío de tráfico IP. UDP hace uso del concepto de puerto para direccionar los datagramas a la aplicación correcta de capa superior. Los paquetes UDP contienen un campo de puerto de destino y otro de puerto fuente. El numero de puerto de destino es utilizado por el modulo UDP para entregar el tráfico al recipiente correcto.

3.24.1 FORMATO DEL MENSAJE UDP

Cada mensaje UDP se conoce como datagrama de usuario. Conceptualmente, un datagrama de usuario contiene dos partes: un encabezado y área de datos. Como muestra la figura 3.62 el encabezado está dividido en cuatro campos de 16 bits que especifican el puerto fuente, el puerto destino, la longitud del mensaje y una suma de verificación.

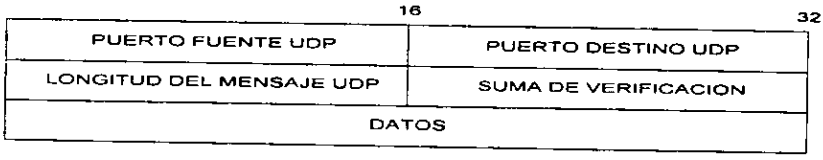


Figura 3.62 Formato del mensaje UDP

El puerto fuente y destino contienen los números de protocolo utilizados para demultiplexar los datagramas entre los procesos receptores. El puerto fuente es opcional, cuando se utiliza, especifica el puerto al cual las respuestas deben ser enviadas; sino se utiliza, debe ser cero.

El campo de longitud contiene una cuenta de los octetos en el datagrama UDP, incluyendo el encabezado y los datos. Así, el valor mínimo para la longitud es de ocho, equivalente a la longitud del encabezado.

La suma de verificación es opcional, un valor de cero en el campo suma de verificación significa que el valor no fue calculado.

3.24.2 NÚMEROS DE PUERTO UDP BIEN CONOCIDOS

Así como TCP, que tiene definidos los numero de puerto para un gran cantidad de aplicaciones, UDP sigue el mismo mecanismo. En general TCP y UDP siguen dos mecanismos para la asignación en el numero de los puertos. Un mecanismo utiliza una autoridad central - la IANA (The Internet Assigned Number Authority, La Autoridad Internet de Asignación de Números) - que asigna los números de puerto como sea necesario y publica una lista de las asignaciones. Este mecanismo es denominado a veces asignación universal y los números de puerto asignados por la autoridad central son denominados números de puerto bien conocidos.

El segundo mecanismo para la asignación de puertos utiliza una ligadura dinámica. En este mecanismo, los puertos no son conocidos globalmente, en su lugar en cualquier momento que un programa necesita un puerto, el software de red le asigna uno.

La familia de protocolos TCP/IP adopta un mecanismo híbrido que asigna algunos números de puerto por omisión, pero deja muchos disponibles para los sitios locales o

programas de aplicación. La siguiente lista muestra algunos de los puertos UDP actualmente asignados por la IANA.

Numero de puerto	Nombre del proceso	Descripción
7	ECHO	Eco
37	TIME	Tiempo
42	NAMESERVER	Servidor de nombres host
43	NICNAME	Quien es
53	DOMAIN	Servidor de nombres de dominio

CAPITULO IV

LOS PRINCIPALES SERVICIOS DE INTERNET

4.1 INTRODUCCIÓN

Este capitulo presenta los servicios de alto nivel mas representativos que una red implementada con los protocolos TCP/IP puede proporcionar a los usuarios. Estos servicios están soportados por protocolos y por lo tanto son una parte integral de TCP/IP.

La capa de aplicación o servicio en el modelo de capas de TCP/IP se ubica en el estrato más alto (ver figura 3.14). Estos servicios determinan como es percibida la red Internet y demuestra el poder de la tecnología. De la misma manera que un sistema operativo es valorado por la cantidad de aplicaciones diseñadas para él, así mismo Internet ha sido valorado ya que ofrece una gran variedad de servicios y usos que a final de cuenta es lo que le interesa a un usuario común y corriente.

En este capitulo se explica con detalle la operación de los servicios Telnet, FTP y Correo Electrónico, siendo éstos los primeros servicios que ofreció Internet, surgiendo inicialmente como una forma de satisfacer la comunicación interna entre sus diseñadores y posteriormente con el crecimiento de la red, ofrecidos al usuario convencional. También, en este capitulo se da una panorámica de algunos servicios adicionales que gracias al dinamismo de la red han y siguen surgiendo, se describe su aplicación particular y objetivos, sin llegar a un alto grado de detalle.

El hablar y detallar la gran gama de servicios que ofrece Internet equivaldria a tener el material para elaborar un libro y se saldria del ámbito de este trabajo, la descripción de estos servicios se hace con el fin de mostrar al lector las infinitas posibilidades que se pueden explotar de la red, indicándole las herramientas que están a su disposición. Mostrando que los protocolos de alto nivel están implementados mediante

programas de aplicación y que dependen de los servicios que proporcionan las demás capas descritas a lo largo de este trabajo.

4.2 TELNET

Uno de los servicios más sobresalientes dentro de Internet, es el servicio denominado Telnet. Telnet permite a un usuario en una computadora local obtener acceso a una computadora remota dentro de Internet.

Por lo general el acceso a una computadora dentro de la red está restringido, es decir, el usuario debe de tener una cuenta personal, con la cual se le otorga una contraseña de identificación para que pueda accesar el host remoto. A este proceso de identificación usualmente se le conoce como Login o Logon. Sin embargo, muchas computadoras dentro de Internet, tales como aquellas que ofrecen directorios de paginas blancas, servicios de búsqueda, etc., proporcionan servicios públicos que no le requieren al usuario una cuenta personal dentro de ellas.

El protocolo Telnet es uno de los protocolos más viejos en TCP/IP, como se menciona en el primer párrafo permite a una computadora local negociar un login remoto hacia otra computadora en Internet. Durante el proceso de negociación, las dos computadoras acuerdan los parámetros que gobernarán la sesión e incluye la capacidad de no aceptar un servicio que uno de los extremos de la conexión no pueda soportar. Una de las primeras cosas que establecen es el tipo de emulación de terminal que van a utilizar, por ejemplo una terminal Digital VT100 o VT220 muy comunes en los sistemas multiusuarios, así como un método para el intercambio de información entre las dos máquinas.

Una vez que la conexión se ha realizado, Telnet actúa como un intermediario entre la computadora local y remota. Telnet pasa directamente los caracteres capturados desde el teclado del usuario local a la computadora remota, como si hubieran sido capturados directamente en un teclado conectado a la máquina remota; así mismo, también acarrea de regreso los datos de la máquina remota a la computadora local.

El resultado es que el teclado y la pantalla local parecieran que están conectados directamente a la computadora remota.

4.2.1 EL LOGIN CONVENCIONAL

El login remoto de Internet es una extensión del login utilizado en una computadora multiusuario convencional de tiempo compartido. Por lo tanto para entender el login remoto, se debe entender el login convencional, el cual se describe a continuación.

A diferencia de las computadoras personales que están dedicadas usualmente a un individuo, un sistema multiusuario permite que muchas personas usen la computadora simultáneamente. Para dar servicio a múltiples usuarios una computadora necesita software sofisticado conocido como sistema de tiempo compartido. Un usuario normalmente interactua con una computadora de tiempo compartido a través de una terminal que incluye un teclado y monitor. Múltiples terminales se enlazan a un computadora de tiempo compartido, permitiendo una persona en cada terminal.

Desde el punto de vista del usuario, una computadora de tiempo compartido parece operar de la misma forma que una computadora personal, debido a que el software da la ilusión a cada usuario de tener un computadora independiente.

En realidad, muchos sistemas de tiempo compartido operan tan eficientemente que un usuario normalmente no sabe si otros usuarios están trabajando en la misma computadora hasta que intentan usar un recurso compartido simultáneamente (por ejemplo, el mismo registro en el uso de una base de datos, o una impresora).

Debido a que múltiples usuarios pueden interactuar con una computadora de tiempo compartido, el sistema le requiere a cada usuario que se identifique, con propósito de contabilizar los recursos que está utilizando (por ejemplo, cuanto espacio en disco están ocupando sus archivos), y con fines de seguridad (evitar el acceso a gente no autorizada). Antes de que una persona pueda usar el sistema, debe ser asignado con una cuenta. La cuenta tiene un nombre único denominado "login" que el sistema usa para identificar al usuario, además, cada usuario es asignado con una contraseña conocida como "password" que el usuario debe mantener en secreto para prevenir que otros utilicen su cuenta.

Antes de que un usuario empiece a interactuar con una computadora de tiempo compartido, el software del sistema solicita el login y el password. Después de un login exitoso, un usuario puede proporcionar comandos al sistema o invocar programas de

aplicación. Cuando el usuario termina de utilizar la computadora se lo informa al sistema mediante un comando (log out), inmediatamente después de que el sistema cierra la sesión del usuario, procede a desplegar la petición de login en la terminal en espera de que otro usuario ingrese al mismo.

4.2.2 EL LOGIN REMOTO

El login remoto sigue el modelo cliente/servidor. Cuando un usuario en la computadora local decide establecer una sesión con un sistema remoto, éste invoca un programa de aplicación local para el servicio de sesión, dando el nombre de la computadora remota a contactar. La aplicación se convierte en un cliente que utiliza TCP/IP para conectarse a través del Internet a un servidor en la computadora remota. El servidor envía exactamente el mismo mensaje de petición login utilizado por las terminales convencionales. La figura 4.1 ilustra la idea:

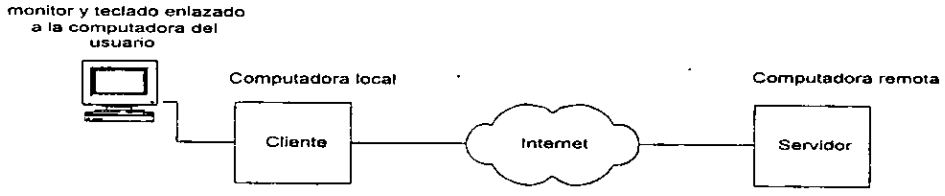


Figura 4.1 Login remoto a través de Internet

Una vez que la conexión ha sido establecida entre el cliente y el servidor, el software permite al usuario interactuar directamente con la computadora remota. Cuando el usuario presiona una tecla en el teclado, la aplicación cliente envía los datos a través de la conexión a la máquina remota. Cuando el programa de aplicación en la computadora remota produce datos de salida, el servidor los envía de regreso al cliente.

Después de que el usuario sale del sistema remoto, el control del teclado y monitor regresa a la computadora local.

4.2.2.1 LAS VENTAJAS DE UN LOGIN REMOTO

Una de las ventajas directas del uso del login remoto Telnet, es aquella en la cual un usuario puede accesar la computadora de su organización sin importar a donde se

traslade fisicamente, ya sea a otra ciudad, estado o inclusive otro país; ya que mediante Telnet, es como si trasladara fisicamente la computadora remota hacia donde se encuentra él, quedando limitado una vez conectado con la máquina remota, al nivel de acceso que tenga asignada su cuenta para poder disfrutar de los servicios que proporciona la máquina.

Este esquema de trabajo también está permitiendo que en algunos países desarrollados, ciertas empresas permitan que su personal que tiene que ver con computadoras labore desde su casa.

Otra de las ventajas que proporciona Telnet, radica en que provee acceso general a los programas en la computadora remota sin que estas requieran modificaciones. Una vez que el software Telnet ha sido instalado, los usuarios pueden correr aplicaciones convencionales (procesadores de texto, hojas de calculo, bases de datos, etc.) desde ubicaciones remotas.

Finalmente otra ventaja que proporciona Telnet, es que permite que equipos de diferentes fabricantes se puedan comunicar sin problema alguno, mediante la incrustación de las secuencias caracteristicas de terminal dentro del mismo protocolo.

4.2.3 OPERACIÓN DEL PROTOCOLO TELNET

El protocolo Telnet está construido sobre tres ideas principales:

Primero, considerando que dentro de Internet existe una amplia variedad de terminales y computadoras cada una con sus propios códigos de control y características de terminal, entonces Telnet define el concepto de "Terminal Virtual de Red " que provee una interface estándar entre ambos extremos de una conexión Telnet. Los programas cliente no tienen que entender los detalles de todos los sistemas remotos posibles; están diseñados para utilizar la interface estándar. Con este mecanismo Telnet trata ambos extremos de la conexión como si fueran terminales virtuales. Los dos programas en cada extremo administran la conversión de la terminal virtual a los dispositivos fisicos reales. El concepto de terminales virtuales permite a Telnet interconectarse con cualquier tipo de dispositivo, siempre y cuando haya mapeo disponible de los códigos virtuales al dispositivo fisico.

Segundo, Telnet incluye un mecanismo que permite al cliente y al servidor negociar al inicio de la sesión opciones adicionales al conjunto de opciones básicas estándar, con el fin de configurar el medio ambiente de operación de la sesión.

El principio de la negociación de opciones, toma conocimiento del hecho de que muchos hosts proporcionan servicios adicionales a las opciones básicas de terminal, y de que muchos usuarios tendrán terminales sofisticadas y desearan hacer uso de esos servicios.

Independientemente de las opciones estándar básicas, el protocolo Telnet soporta opciones adicionales que permiten a los extremos de la conexión acordar el uso de un conjunto de convenciones más elaboradas (o quizás diferentes) para la conexión Telnet. Tales opciones incluyen el cambio del conjunto de caracteres, si se establece un eco, modo de transmisión, etc.

La estrategia básica para establecer una opio, es tener de cualquier extremo la solicitud de que alguna opción se efectúe y que el otro extremo acepte o rechace la solicitud. Si la solicitud es aceptada la opción inmediatamente toma efecto; si es rechazada el aspecto asociado de la conexión permanece como fue especificado por la terminal virtual de red (opciones básicas).

Tercero, Telnet considera simétricos a ambos extremos de la conexión con relación al proceso de negociación de opciones. Muchas máquinas, especialmente las estaciones de trabajo UNIX, actúan simultáneamente como cliente y servidor, permitiendo que un usuario se conecte a otras máquinas de la red y otros usuarios se conecten a la máquina de este usuario. Por lo tanto, con Telnet cualquier extremo puede iniciar la negociación de opciones.

4.2.3.1 LA TERMINAL VIRTUAL DE RED

Dentro de Internet existe una gran diversidad de sistemas cuya forma de operación difiere entre ellos grandemente, ya que por ejemplo algunos requieren que sus líneas de texto finalicen con el carácter de control ASCII *regreso de carro* (CR), otros del carácter *alimentación de línea (LF)*, y otros más de una combinación de ambos CR-LF. Otro ejemplo se presenta en la secuencia de caracteres que requiere un sistema para la

interrupción de un programa o proceso que está corriendo, entre otras existen CTRL-C, CTRL-D, Esc, Break, etc.

Para acomodar tal diversidad, Telnet define como deben ser enviados los datos y los comandos a través de Internet. La definición es conocida como Terminal Virtual de Red, ilustrada en la figura 4.2.

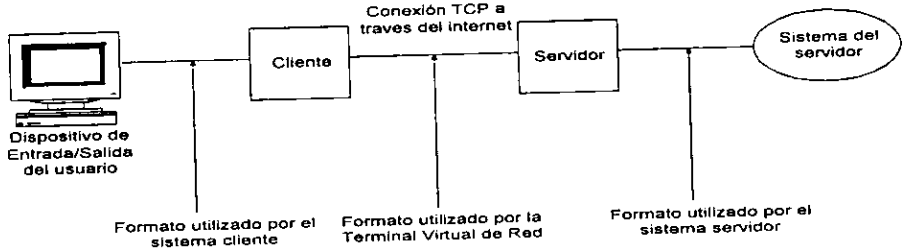


Figura 4.2 Terminal Virtual de Red utilizada por Telnet

Como se ilustra en la figura 4.2 el software del cliente traduce los caracteres generados y la secuencia de comandos del formato utilizado por la terminal del usuario dentro del formato de la terminal virtual de red y los envía al servidor. El software del servidor traduce los datos y comandos que le llegan de la terminal virtual al formato que su sistema utiliza. Para los datos de regreso, el servidor remoto traduce desde el formato de la máquina remota al formato de la terminal virtual, y el cliente local lo traduce del formato de la terminal virtual al formato de la máquina local.

La terminal virtual de red utiliza para todos los datos y comandos el conjunto de caracteres ASCII de 7 bits, formado por 95 caracteres visibles gráficos (letras, números, etc.), y 33 códigos de control; así mismo también define el código de terminación de las líneas como la secuencia de caracteres CR-LF. Cuando un usuario presiona la tecla que corresponde al fin de línea en la terminal local (ENTER o RETURN), el cliente Telnet debe mapearla a CR-LF para su transmisión a través de la terminal virtual. El servidor Telnet traduce CR-LF al carácter de fin de línea manejado por la máquina remota.

4.2.3.2 FUNCIONES DE CONTROL DE LA TERMINAL REMOTA

Aunque un cliente login usualmente pasa cada carácter generado a la computadora remota, el software del cliente debe proveer al usuario de una mecanismo que haga posible que se comunique con la computadora local. Para entender por que es necesaria tal característica, se deben entender dos situaciones

1. Durante un login remoto, dos programas corren simultáneamente, la aplicación en la computadora remota y el cliente en la computadora local.
2. Una de las teclas en el teclado puede ser utilizada para abortar un programa corriendo.

La interrupción de una aplicación no es una actividad normal, sin embargo, si una aplicación remota tiene un mal comportamiento o se "congela" debe abortarse y obtenerse nuevamente el control.

Telnet , para satisfacer estas necesidades, definió la representación estándar de cinco funciones para tener el control sobre la terminal virtual del sitio remoto.

Para pasar funciones de control a través de la conexión, Telnet los codifica usando una secuencia de escape. Una secuencia de escape utiliza un octeto reservado para indicar que lo que sigue en la corriente de caracteres es un código de control. En Telnet, el octeto reservado que inicia una secuencia de escape se conoce como *interpretar como comando* (Interpret As Command, *IAC*). Así primero se envía esta secuencia e inmediatamente después el comando o la función de control. A continuación se mencionan las funciones de control definidas para Telnet.

Interrumpir Proceso (IP). Muchos sistemas proveen una función que suspende, interrumpe, o aborta la operación de un programa corriendo. Esta función se usa frecuentemente cuando un usuario cree que su proceso esta en un ciclo infinito, o cuando un proceso no deseado ha sido inadvertidamente activado.

Abortar la Salida (AO). Muchos sistemas proveen una función con la cual se permite a un proceso que está generando salida correr hasta su terminación (o alcanzar el mismo punto de terminación como si hubiera corrido completamente) pero sin enviar la

salida a la terminal del usuario. Además, esta función típicamente limpia cualquier salida ya producida pero aún no impresa (o desplegada) en la terminal del usuario.

Está Usted Ahí (AYT). Muchos sistemas proveen una función la cual proporciona al usuario una evidencia visible de que la aplicación remota sigue funcionando. Esta función puede ser invocada por el usuario cuando el sistema está inexplicablemente "silencioso" por largo tiempo, debido a diferentes causas. A

Borrar Carácter (EC). Esta función borra el carácter previo de la corriente de datos que está siendo suministrada por el usuario. EC es típicamente utilizada para editar datos de entrada desde el teclado cuando se cometen errores.

Borrar Línea (EL). Esta función borra todos los datos en la línea actual de entrada.

Estas funciones están implementadas mediante el mapeo de un carácter o secuencia de caracteres ASCII con una función de control, de tal manera que cuando un usuario presiona la(s) tecla(s), el sistema operativo toma la acción apropiada en lugar de aceptar el carácter o caracteres como datos de entrada.

4.2.3.3 FUNCIONES ADICIONALES

Además de las funciones de control de terminal remota existen otras funciones de control Telnet, las cuales son generalmente utilizadas en el proceso de negociación inicial para la conexión, así como, durante el curso de la sesión en la cual se pueden modificar sus valores, esto siempre y cuando ambos extremos estén de acuerdo.

La figura 4.3 muestra los comandos posibles y su codificación decimal (se incluyen los comandos de control de terminal).

Comando	Codificación Decimal	Significado
IAC	255	Interpretar el siguiente octeto como comando
DON'T	254	Negación a la solicitud de ejecutar una opción especificada
DO	253	Aprobación para permitir la opción especificada
WON'T	252	Rehusarse a ejecutar la opción especificada
WILL	251	Acuerdo para ejecutar la opción especificada
SB	250	Subnegociación de una opción
GA	249	La señal "adelante", indica permiso para seguir adelante al utilizar comunicaciones half-duplex (sin eco)
EL	248	Borra una línea
EC	247	Borra un carácter
AYT	246	Consulta el otro extremo para asegurarse de que una aplicación esté funcionando
AO	245	Ejecuta el proceso hasta su terminación pero no envía la salida
IP	244	Interrumpe, suspende, aborta o da por terminado el proceso
BRK	243	Envía una instrucción de ruptura
DMARK	242	La porción de datos de un SYNCH (siempre acompañado por la notificación Urgente TCP)
NOP	241	No operación
SE	240	Fin de una subnegociación
EOR	239	Fin de registro

Figura 4.3 Comandos Telnet y su codificación. Los códigos sólo tienen significado si son precedidos por un carácter IAC.

Como se muestra en la figura 4.3, las señales generadas por las teclas conceptuales del teclado de una terminal virtual de red tendrán un comando correspondiente. Por ejemplo, para solicitar que el servidor interrumpa el programa remoto en ejecución, el cliente debe enviar la secuencia IAC IP (255 seguido por 244). Comandos adicionales permiten al cliente y servidor negociar cuales opciones usaran, así como sincronizar la comunicación.

4.2.3.4 LA SEÑAL SYNCH DE TELNET

La mayoría de los sistemas de tiempo compartido locales proveen de un mecanismo con el cual se permite a un usuario en una terminal recuperar el control sobre ésta cuando una aplicación presenta un comportamiento anormal. Las funciones IP y AO descritas son ejemplos de estos mecanismos. Pero esto no es necesariamente cierto

cuando los sistema están conectados a través de una red. Los mecanismos de control de flujo de la red pueden provocar que las señales de control sean almacenadas en otra parte, por ejemplo en el host del usuario; o que el mal comportamiento de una aplicación remota inadvertidamente bloquee la corriente de datos (deteniendo la lectura de datos hacia la aplicación remota) evitando así que las funciones de control lleguen a la aplicación.

Para resolver este problema, el mecanismo "Synch" de Telnet es introducido. Una señal Synch consiste de un segmento de notificación Urgente TCP (ver BANDERAS del encabezado TCP, apartado 3.23.3), acompañada con el comando Telnet Marca de Datos (DMARK).

La notificación Urgente, supera el flujo de datos perteneciente a la conexión Telnet en el sitio remoto, arribando inmediatamente a la aplicación (esto lo hace mediante la lectura y desecho de todos los datos almacenados en el búfer, hasta el limite indicado por el apuntador de urgencia). Acto seguido la corriente de datos es inmediatamente revisada por alguna señal como IP, AO, AYT, u otros comandos Telnet, ejecutándose. Por ultimo mediante el comando DMARK (la marca de sincronización en la corriente de datos), se indica que cualquier señal especial ya se presentó y que el receptor puede regresar al procesamiento normal de la corriente de datos (sale del modo de urgencia).

4.2.3.5 LA NEGOCIACION DE OPCIONES

Como se mencionó Telnet es simétrico con respecto a la negociación de las opciones de un conexión, es decir, cualquiera de los extremos pueden emitir una solicitud (no hay explícitamente un cliente y un servidor). El protocolo Telnet utiliza cuatro comandos en la negociación de las opciones: WILL X es enviado por cualquier extremo, para indicar que se desea (ofrece) empezar a ejecutar la opción X, DO X y DON'T X son los acuses de recibo positivo y negativo; similarmente DO X es enviado para indicar el deseo (solicitud) de que el otro extremo empiece a ejecutar la opción X, WILL X y WON'T son los acuses de recibo positivo y negativo. Debido a que la Terminal Virtual de Red (opciones estándar básicas) es lo que queda cuando no se habilita ninguna opción, los comandos DON'T y WON'T garantizan dejar la conexión en un estado en el cual ambos

extremos pueden manejar. De esta forma, todos los hosts pueden implementar sus procesos Telnet para que estén totalmente ignorantes de las opciones que no soportan, regresando simplemente una negación a cualquier solicitud que no entiendan. La figura 4.4 lista las opciones más comunes implementadas por Telnet.

Nombre	Código	Significado
Transmisión binaria	0	Cambia la transmisión a 8 bits
Eco	1	Permite hacer eco de los datos recibidos
Suprimir adelante	3	Suprime (ya no se envía) la señal Adelante, después de los datos
Status	5	Solicita el Status de una opción Telnet del sitio remoto
Marca de tiempo	6	Solicita una marca de tiempo a ser insertada en la corriente de datos de regreso para sincronizar los extremos de la conexión
Tipo de terminal	24	Intercambia información acerca de la marca y modelo de la terminal que está siendo usada
Fin de registro	25	Termina los datos enviados con código de Fin de Registro
Modo de línea	34	Utiliza edición local y envía líneas completas en lugar de caracteres individuales

Figura 4.4 Opciones Telnet usadas comúnmente

Si se hace referencia al listado de códigos anterior y la tabla de comandos, para activar por ejemplo, el Eco (instruir a la otra terminal que empiece a regresar los caracteres que reciba), un extremo tendría que emitir el comando WILL ECHO (255 251 1). Una respuesta afirmativa seria DO ECHO (255 253 1) y la respuesta negativa DON'T ECHO (255 254 1).

4.2.4 SESIÓN TELNET

Para iniciar Telnet, se debe proporcionar el nombre o dirección IP de la máquina a la cual se desea conectarse. Solamente se puede utilizar el nombre si el sistema tiene algún método para convertir el nombre a su dirección IP, como en el caso del Sistema de Nombres de Dominio. Si no se especifica nombre o dirección, Telnet introducirá su modo de comando y esperará instrucciones especificas. Cuando se establezca la conexión, se solicitará identificación de usuario y contraseña. En cualquier momento se puede entrar al modo de comando Telnet, usualmente por medio de la combinación de teclas Ctrl +]. Si al entrar en modo de comando está conectado en una sesión activa, Telnet esperará a

que se emita un comando, lo ejecutará, y a continuación retornará automáticamente a la sesión. El modo de comando permite introducir comandos relacionados con la máquina local.

Una vez que se establezca con éxito la conexión a la máquina remota, todas las instrucciones serán relativas al servidor.

4.2.5 TIPOS DE SERVICIO TELNET

Los servicios Telnet pueden ser divididos en dos grandes tipos: Cuenta Telnet Invitado (pública) y Cuenta Telnet Totalmente Privilegiada o Privada.

Muchos usuarios en Internet tiene cuentas privadas Telnet. Por ejemplo, aquellos usuarios que pertenecen a una gran organización con varias computadoras dentro de la red, y a las cuales son accesadas por medio de un login y contraseña especiales proporcionados por los administradores de esas computadoras.

Pero más importante es el hecho de que Internet al ser una estructura cooperativa, en la cual se da la ayuda a los usuarios en forma desinteresada o sin fines de lucro, permite que muchas computadoras de la red sean accesadas sin restricción alguna, otorgando una gran diversidad de servicios públicos como catálogos de librerías en línea, programas de correo, consulta a bases de datos, rastreadores de información, etc. En el apéndice B se presenta algunas servicios de interés proporcionados a través de Telnet.

Resumiendo, las características que diferencia a cada una de las cuentas son las siguientes:

- Cuenta Invitado Telnet (o Acceso Público)
  - Permite login anónimo sin contraseñas
  - Permite acceso a servicios sin cargo
- Cuenta Telnet Totalmente Privilegiada (o Acceso Privado)
  - Requiere un login y contraseña
  - Los servicios son otorgados por una organización hacia sus usuarios o son proporcionados por alguna empresa comercial.
  - Las empresas comerciales hacen generalmente un cargo por los servicios proporcionados

Se proporcionan más servicios de los que usualmente otorga una servicio público.

4.3 PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP)

El Protocolo de Transferencia de Archivos, conocido simplemente como FTP (File Transfer Protocol) forma parte de la familia de protocolos TCP/IP, hace posible la transferencia de archivos desde una computadora en Internet a otra computadora. Hay muchas implementaciones diseñadas sobre la especificación del protocolo FTP (existen versiones FTP para DOS, UNIX, Windows, etc.). Por lo tanto, proporciona un medio estándar para la transferencia de información entre dos computadoras de la red, sin importar sus plataformas (por ejemplo, entre un servidor UNIX y una PC tal como una Apple Mac o una IBM PC) .

El usuario de un programa FTP debe identificarse (con su login y password) en ambos hosts para poder transferir un archivo de una máquina a otra. Sin embargo, los usuarios de Internet pueden sacar ventaja de la riqueza de información disponible de los miles de sitios que soportan acceso público, utilizando una cuenta de propósito general llamada "FTP anónimo".

4.3.1 FTP Y EL MODELO CLIENTE/SERVIDOR

Como la mayoría de las aplicaciones Internet, FTP utiliza el modelo cliente/servidor. Un usuario invoca un programa FTP en la computadora local (cliente), instruyéndola contactar una computadora remota (servidor), el sistema remoto requiere al cliente tanto el login como el password, para autorizar el acceso a su sistema. El servidor niega el acceso a los clientes que no puedan suministrar un login y password validos.

Si la identificación resulta ser exitosa, entonces se puede enviar comandos de usuario al cliente FTP para que solicite la transferencia de archivos al servidor, todo esto utilizando TCP. El servidor FTP toma las solicitudes y envía el archivo o archivos que el cliente le está solicitando. Conforme el cliente recibe datos, por parte del servidor, éste los escribe en un archivo en el disco duro del sistema local.

Cabe aclarar que FTP está diseñado para soportar la operación inversa, es decir, permite a un usuario o cliente transferir la copia de un archivo local a una computadora

remota o servidor. Después de que la transferencia se ha completado, los programas cliente y servidor terminan la conexión TCP utilizada para la transferencia.

4.3.2 EL FORMATO DE LOS ARCHIVOS

Aunque existen diversos formatos para almacenar los archivos de computadoras, FTP sólo entiende dos formatos básicos. Clasifica cada archivo ya sea como archivo de texto o archivo binario. Un archivo de texto contiene una secuencia de caracteres agrupadas en líneas. Aunque la mayoría de las computadoras usan el código ASCII para los archivos de texto, FTP incluye comandos para convertir entre ASCII y otros formatos de codificación (por ejemplo para traducir entre ASCII y EBCDIC). De esta forma, es posible transferir un archivo de texto entre una computadora que usa ASCII y otra que utiliza otro código.

FTP utiliza el término de archivo binario para todos los archivos que no son de texto. En general se deben identificar como archivos binarios a los siguientes: archivos ejecutables, archivos de audio, gráficos o imágenes de vídeo, hojas de cálculo, documentos de un procesador de texto, archivos comprimidos (archivo que ha sido procesado para reducir su tamaño), etc.

Los sitios que ofrecen servicios FTP frecuentemente comprimen los archivos para reducir la cantidad total de espacio en disco que el archivo ocupa, además, para que el tiempo que tarde en transmitirse sea menor.

Antes de la transferencia de un archivo, el usuario debe decir a FTP si el archivo a ser transferido es de texto o binario. Se debe proporcionar el comando *binary* para prepara a FTP a transmitir un archivo que no es de texto, o el comando *ascii* para preparar a FTP a transferir un archivo de texto.

4.3.3 LA IMPORTANCIA DE ELEGIR UN FORMATO CORRECTO

Es importante elegir el formato correcto del archivo que se va a transferir debido a que FTP no entiende el contenido del archivo. Usualmente los programas FTP asumen que los archivos usan solamente 7 bits por byte, la norma para los archivos codificados en ASCII, y aunque se transmitan en octetos al estar bien coordinado el sitio receptor con respecto al tipo de transferencia seleccionada, entonces el archivo será convertido

correctamente. La trasferencia binaria toma los 8 bits de un byte para un archivo que no es de texto, y así los transmite al sitio receptor. Como se puede ver si se elige un formato diferente los resultados pueden ser impredecibles.

Si un usuario solicita a FTP que ejecute una transferencia utilizando un tipo incorrecto, la copia del archivo resultante puede deformarse. Por ejemplo, si se transfiere una hoja de cálculo en modo ascii (texto) a una computadora remota, muy probablemente cuando se cargue el archivo (la hoja) en la aplicación éste será rechazado, ya que no se reconocerá su formato. Algunos programas FTP generan mensajes de precaución cuando el tipo de archivo parece no checar con el modo de transferencia solicitado. Sin embargo, no se debe depender en el envío de mensajes por parte de los hosts para cambiar el tipo de transferencia.

4.3.4 TIPOS DE PROGRAMAS (CLIENTES) FTP

Hay un gran número de programas clientes FTP. Algunos de estos operan en línea de comando, los cuales requieren que se escriban comandos especiales para la transferencia de archivos. Otros programas FTP, sin embargo, pueden tener una interface gráfica permitiendo que los archivos y botones sean elegibles mediante el uso de un dispositivo apuntador (ratón). En este caso no se necesita recordar ningún comando FTP.

También, FTP está frecuentemente integrado dentro de otros programas incluyendo los navegadores (hojeadores) de paginas Web tales como Netscape y Lynx. Estos navegadores esconden el establecimiento de la conexión a los usuarios.

El cliente FTP más famoso es la utileria UNIX llamada *ftp*. Este programa trabaja en línea de comando y casi todos los demás clientes se derivan a partir de él. Los programas cliente basados en línea de comando establecen muy pocos requerimientos, solamente ocupan una conexión orientada a texto. En contraste los clientes gráficos requieren de más recursos (interface gráfica, ratón, etc.), pero son normalmente más fáciles e intuitivos (la mayoría de los comandos están representados por botones) de utilizar.

Los clientes FTP integrados en los navegadores de paginas Web son también fáciles de manejar, esconden todos los comandos FTP al usuario, permitiendo "navegar" a través de las conexiones utilizando ligas de hipertexto. Aunque simples, estos clientes

FTP tienen algunas limitaciones: le es imposible seleccionar múltiples archivos y así se está forzado a transferir un archivo a la vez. Tienden a ser ineficientes ya que los navegadores normalmente no mantienen la conexión abierta para toda la sesión, (sólo el tiempo que dura la transferencia), y por lo tanto cada vez que se transmite un archivo o se lista el contenido de un directorio, el navegador está forzado a establecer una nueva conexión con el servidor FTP.

4.3.5 FTP ANÓNIMO

Internet provee acceso a una vasta cantidad de recursos de información. Algunos de estos son proporcionados con un costo, pero muchos están disponibles libres de cargo. Cientos de organizaciones proveen libre de cargo el acceso a sus sistemas de archivos o librerías. Estos archivos son accesibles vía una técnica conocida como FTP anónimo. Para utilizar un FTP anónimo un usuario da como login **anonymous** y como password **guest** o su dirección de correo electrónico. Las sesiones FTP anónimas restringen el acceso sólo a archivos públicos. Así, aun si la computadora contiene muchos directorios y archivos, un usuario FTP anónimo puede accesar y transferir sólo aquellos archivos que el administrador del sistema ha elegido hacer disponibles.

Dentro de los tipos de archivos que los sitios FTP anónimos permiten "bajar" se incluyen: software para la mayoría de las plataformas, programas manejadores de dispositivos, documentos cubriendo casi todos los tópicos imaginables tales como el texto completo de libros, revistas electrónicas, material audio/visual incluyendo música, gráficas y archivos de vídeo.

A los usuarios en una sesión FTP anónima usualmente no se les permite transferir archivos hacia el sitio remoto (servidor).

4.3.6 ACCESO CONCURRENTE A LOS SERVIDORES

Como otros servidores, la mayoría de las implementaciones FTP servidoras permiten acceso concurrente por parte de múltiples clientes. Los clientes FTP usan TCP para conectarse a un servidor. Típicamente, los programas servidores tienen dos partes: un programa maestro que es responsable de aceptar peticiones nuevas, y un conjunto de

esclavos que son responsables del manejo de cada una de las solicitudes. El servidor maestro ejecuta los cinco pasos siguientes:

Apertura del puerto

El maestro abre el puerto en el cual puede ser contactado.

Espera por un cliente

El maestro espera por un cliente nuevo que le envíe una solicitud.

Elige un puerto

Si es necesario, el maestro asigna un puerto local de protocolo nuevo para esta solicitud y se lo informa al cliente (este paso es innecesario con TCP).

Inicia un esclavo

El maestro comienza un esclavo concurrente e independiente para manejar la solicitud del cliente. Hay que notar que los esclavos manejan una solicitud y después terminan, los esclavos no esperan por solicitudes de otros clientes.

Continua

El maestro regresa al paso de *espera* y continua aceptando solicitudes nuevas mientras que los esclavos creados recientemente manejan las solicitudes previas concurrentemente.

4.3.7 OPERACIÓN DE FTP

4.3.7.1 ESTABLECIMIENTO DE UNA CONEXIÓN FTP

Como se describe en el apartado anterior, un servidor maestro espera hacer conexiones con múltiples clientes y crear un proceso esclavo que maneje cada conexión. En FTP a diferencia de la mayoría de los servidores, el proceso esclavo no desempeña la mayoría del trabajo. En su lugar, el esclavo acepta y maneja la conexión de control del cliente, y utiliza un proceso adicional para manejar una conexión separada, para la transferencia de los datos. La conexión de control acarrea los comandos que le indican al servidor cual archivo transferir, y la conexión de transferencia se encarga del acarreo de los datos.

En el contexto de Internet la conexión de control esta establecida sobre una sesión Telnet (la cual está a su vez sobre una sesión TCP). La conexión de transferencia de

datos corre directamente sobre TCP. FTP sigue el modelo que se presenta en la figura 4.5

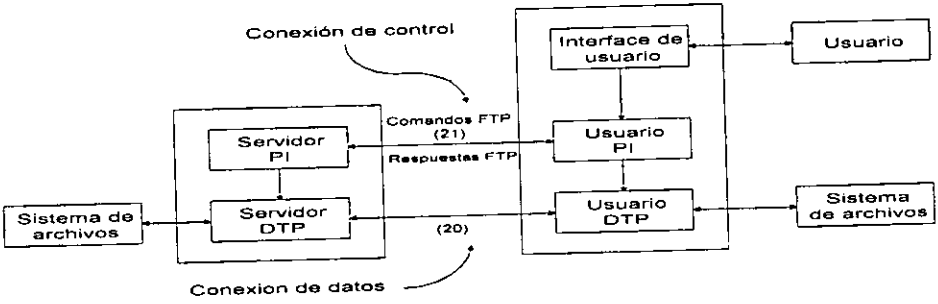


Figura 4.5 Un servidor y cliente FTP con una conexión de control TCP entre ellos y un conexión TCP separada entre sus procesos de transferencia de datos asociados.

La Interface de Usuario. Como su nombre lo indica proporciona un medio para que un usuario interactue con el sistema, además de que maneja el interprete de protocolo del cliente.

El Cliente PI (Process Interpreter). Este es el Interprete de Protocolo del Cliente. Edita comandos al interprete de protocolo del servidor remoto y también maneja el proceso de transferencia de datos del cliente.

El Servidor PI. Este es el Interprete de Protocolo del Servidor, el cual responde a los comandos editados por el interprete de protocolo del cliente y maneja el proceso de transferencia de datos del cliente.

El Cliente DTP (Data Transfer Process). Este es el proceso de transferencia de datos del cliente responsable de comunicarse con el proceso de transferencia de datos del servidor y el sistema local de archivos.

El Servidor DTP. Este es proceso de transferencia de datos del servidor responsable de comunicarse con el proceso de transferencia de datos del cliente y el sistema remoto de archivos.

Como se mencionó, durante la sesión FTP habrá dos conexiones separadas una entre los PI y otra entre los DTP. La conexión entre los PI es la conexión de control y la conexión entre los DTP es la conexión de datos.

Cuando un cliente PI ejecuta una conexión inicial a un servidor, el cliente utiliza un número de puerto aleatorio, asignado localmente, y contacta al servidor PI en el puerto bien conocido TCP número 21. Una vez establecida la conexión de control, el cliente PI obtiene otro número de puerto de su máquina, y utiliza la conexión de control para contactar el proceso de transferencia de datos en el servidor. El proceso de transferencia de datos en el servidor utiliza el número de puerto bien conocido TCP para la identificar a la función transferencia de datos, la cual corresponde al número 20. Para asegurarse que el proceso de transferencia de datos en el servidor conecta con el proceso de transferencia de datos correcto en la máquina cliente, el lado servidor no debe aceptar conexiones de un proceso arbitrario. Por tal motivo cuando recibe una solicitud de apertura (conexión), solicita tanto el puerto que será utilizado en la máquina cliente así como el puerto local[1].

En general, además de permitir el paso de los comandos de usuario al servidor, FTP utiliza la conexión de control para permitir a los procesos de control del cliente y el servidor coordinar su uso en la asignación dinámica de puertos TCP y la creación de procesos de transferencia de datos que usan tales puertos.

4.3.7.2 COMANDOS INTERNOS FTP

Como se menciona en apartados más arriba la conexión de control FTP toma la forma de una sesión Telnet. A diferencia del protocolo Telnet que negocia varias opciones, los comandos internos de FTP únicamente utilizan la definición básica de la Terminal Virtual de Red (ver Telnet). De esta forma, el manejo de una conexión de control FTP es mucho más simple que el manejo de una conexión Telnet estándar.

Los comandos del protocolo interno FTP son secuencias de tres o cuatro letras mayúsculas terminados por CR/LF (retorno de carro/alimentación de línea). Algunos de los comandos requieren argumentos opcionales. Una ventaja primordial en el uso de caracteres ASCII para comandos, es que un usuario puede observar el flujo de comandos y comprenderlos fácilmente. Esto ayuda en forma considerable durante el proceso de

[1] Aunque la mayor parte de las comunicaciones TCP se establecen mediante una solicitud activa a un puerto pasivo, es posible abrir una conexion sin un puerto pasivo esperando. En este caso, el TCP que envia la solicitud de conexion incluira tanto el numero de puerto local como el numero del puerto remoto. Si el TCP receptor se configura para permitir la solicitud la conexion se podra abrir.

depuración. La figura 4.6 presentan los comandos internos FTP que utiliza el protocolo. Figuran los comandos de proceso de conexión, verificación de contraseña y transferencia de archivos. Hay que dejar bien claro que no se deben de confundir con los comandos para el usuario.

Comando	Descripción
ABOR	Abortar el comando anterior y cualquier transferencia de datos asociada
ACCT	Identificación de la cuenta del usuario
ALLO	Asignar almacenamiento para la operación que sigue
APPE	Agregar datos que se están recibiendo a un archivo existente
CDUP	Cambiar a directorio padre
CWD	Cambiar directorio de trabajo
DELE	Borrar archivo
HELP	Presenta información de ayuda del servidor
LIST	Envía una lista de archivos del directorio actual en el sistema remoto
MODE	Definir modo de transferencia
NLST	Envía un listado completo de los directorios en el directorio actual
NOOP	No hay operación
PASS	Contraseña del usuario
PASV	Solicitar una apertura pasiva
PORT	Especifica el número de puerto del cliente en el cual el proceso de transferencia de datos está "escuchando" por una solicitud de conexión
PWD	Muestra el nombre del directorio actual
QUIT	Logout o romper la conexión
REIN	Terminar y reiniciar una conexión
REST	Reiniciar la transferencia
RETR	Obtener archivo del sistema remoto
RMD	Eliminar directorio
RNFR	Especifica la ruta (path name) antigua de archivo a ser renombrado. Sigue con el comando RNTO
RNTO	Especifica la nueva ruta del archivo a ser renombrado
SMNT	Monta un sistema de archivo
STAT	Muestra información de estado
STOR	Almacena archivo en el sitio remoto, sobre escribe el archivo si ya existe
STOU	Almacena bajo un nombre único. No sobre escribe archivos existentes
STRU	Especifica la estructura del archivo
SYST	Reporta el tipo del sistema operativo del sitio remoto
TYPE	Especifica el tipo de archivo
USER	Identificación del usuario

Figura 4.6 Comandos internos del protocolo FTP

4.3.7.3 RESPUESTAS A LOS COMANDOS FTP

Las respuestas a los comandos FTP son ideadas para asegurar la sincronización de las solicitudes y acciones en el proceso de la transferencia de un archivo, y garantizar que el proceso del usuario siempre conozca el estado del servidor. Cada comando debe generar al menos una respuesta, aunque puede haber más de una; en este caso, las múltiples respuestas deben ser fácilmente distinguibles. Además, algunos comandos también se presentan en grupos, tales como USER, PASS y ACCT, o RNFR y RNTO.

Una respuesta FTP consiste de tres dígitos numéricos, seguidos por algún texto. El número es para uso de la computadora con el fin de determinar en que estado se va a entrar; el texto es para entendimiento del usuario. En particular, el texto puede ser dependiente del servidor, así que hay probabilidad de que los textos varíen entre los sistemas para cada código de respuesta.

Como se mencionó, una respuesta está definida para contener un código de tres dígitos, seguido por un espacio, seguido por una línea de texto, terminado por un fin de línea Telnet (CR/LF). Habrá casos sin embargo, donde el texto sea más largo que una línea, por lo tanto se requerirá de un formato especial en la primera línea para indicar que más de una línea está llegando, y otro en la última línea para señalar que es la última. Al menos una de estas líneas debe contener el código de respuesta adecuado para indicar el estado de la operación. Para satisfacer todas estas situaciones, se decidió que el código de la primera línea como el de la última línea fuera el mismo.

Así, el formato para un respuesta que involucra varias líneas, es que la primera línea empezará con el código de respuesta requerido, seguido inmediatamente por un guión "-", seguido por texto. La última línea empezara con el mismo código, seguido inmediatamente por un espacio, opcionalmente algún texto, y el carácter de fin de línea Telnet. Por ejemplo,

123-Primera línea
Segunda línea
789 Una línea empezando con números
123 La última línea

El interprete de protocolo del usuario entonces simplemente necesita esperar por la segunda ocurrencia del mismo código de respuesta, seguido por un espacio al inicio de una línea e ignorar todas las líneas intermedias. Si una línea intermedia empieza con un número de tres dígitos, el servidor debe agregarle espacios en blanco al inicio para evitar confusión.

Cada uno de los tres dígitos de las respuestas tienen un significado especial. Están pensados para permitir desde respuestas sencillas hasta respuesta muy sofisticadas para el interprete de protocolo del usuario. El primer dígito denota si la respuesta es buena, mala o incompleta. Un proceso simple será capaz de determinar la siguiente acción (proceder como se planeo, rehacer, etc.) simplemente examinando este primer dígito. Un proceso de usuario que desea conocer aproximadamente que clase de error ocurrió (por ejemplo, error en el sistema de archivos, error de sintaxis al invocar un comando, etc.) puede examinar el segundo dígito, reservando el tercer dígito para una mayor explicación en la respuesta (por ejemplo, un comando RNTO sin un comando RNFR precedente).

Hay cinco valores para el primer dígito en el código de respuesta como se muestra en la figura 4.7

Tipo	Descripción
1yz	Respuesta positiva preliminar. Espera otra respuesta antes de enviar otro comando
2yz	Respuesta positiva complementaria. El último comando se ha completado exitosamente
3yz	Respuesta positiva intermedia. El comando ha sido aceptado, pero la acción solicitada está en espera de mayor información
4yz	Respuesta negativa pasajera. La acción solicitada no se efectúo pero puede ser reemitida
5yz	Respuesta negativa permanente. La acción solicitada no se efectúo, volver a emitir el comando dará como resultado el mismo error (no volver emitir)

Figura 4.7 Descripción del primer digito en las respuesta a los comandos FTP

Las siguientes funciones están agrupadas en el segundo dígito:

Tipo	Descripción
x0z	Sintaxis. Estas respuestas se refieren a errores de sintaxis
x1z	Información. Estas son respuestas a solicitudes de información, tales como status o ayuda
x2z	Conexiones. Respuesta que se refieren a las conexiones de control y datos
x3z	Autenticación y Cuentas. Respuestas para los procesos de identificación (login)
x4z	No especificado
x5z	Sistema de archivos. Estas respuestas indican el estado del sistema de archivos del servidor

Figura 4.8 Descripción del segundo digito en las respuesta a los comandos FTP

El tercer dígito da una información más detallada del significado de cada una de las funciones anteriores. En la figura 4.9 se dan algunos ejemplos de códigos de respuesta:

Número	Significado
120	Servicio listo en nnn minutos
125	Conexión de datos ya abierta, empieza la transferencia
200	Comando OK
220	Servicio listo para usuario nuevo
331	Nombre se usuario OK, necesita password
332	Necesita cuenta para ingresar al sistema
421	Servicio no disponible, cerrando la conexión de control.
425	No se puede abrir la conexión de datos
500	Error de sintaxis, comando no reconocido. Esto puede incluir errores tales como una línea con comandos demasiado larga
501	Error de sintaxis en parámetros o argumentos.

Figura 4.9 Ejemplos de algunos códigos de respuesta

4.3.8 EJEMPLO DE UNA SESIÓN FTP ANÓNIMA

4.3.8.1 ESTABLECIENDO UNA CONEXIÓN

El presente ejemplo muestra una sesión FTP interactiva, trabajando desde la línea de comando en UNIX, las palabras que aparecen después de **ftp>** son comandos de usuario. Por lo general, FTP se inicia con el nombre o con la dirección de la máquina destino. Igual que para Telnet, deberá ser posible convertir el nombre a una dirección IP. De esta forma el usuario da la siguiente instrucción para conectarse:

```
$ ftp ftp.uunet.ca
Connected to seraph.uunet.ca.
220 seraph FTP server (Version wu-2.4(1) Fri Aug 5 17:30:28 EDT 1994) ready.
```

Una vez realizada la conexión el sistema pregunta la identificación de usuario (login/password), como este sitio es un FTP anónimo, de login se proporciona "anonymous" y como password la dirección de correo electrónico.

```
Name (ftp.uunet.ca:pcgranados): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-Please read the file README
230-  it was last modified on Thu Aug 24 22:50:11 1995 - 627 days ago
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
```

4.3.8.2 NAVEGANDO POR EL SISTEMA REMOTO

Una vez registrado en la computadora remota, ya se tiene la capacidad de navegar a través del sistema de archivos con el fin de localizar el archivo que se desea transferir. Los comandos **dir** y **ls** son utilizados para listar el contenido del directorio actual, "ls" dará un listado breve de todos los archivos y directorios en el directorio actual, "dir" dará un listado más completo de estos archivos y directorios, también listando los permisos de los archivos sus fechas de creación etc. Los comandos **chdir** o **cd** se utilizan para cambiar de directorio. Si no se está seguro del nombre del directorio actual, el comando **pwd** lo mostrará.

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 96
drwx--x--x   2 0      0          512 Feb 22  1995 .domain
-rw-r--r--   1 91     91         607 Aug 25  1995 README
lrwxrwxrwx   1 0      0            7 Feb 15  1994 bin -> pub/bin
toronto.edu/ca-domain
drwxr-x--x   9 0      0          512 Sep  5  1996 distrib
drwxrwxr-x 190 0      91        5120 Apr 28 14:45 ftp
dr-xr-xr-x   2 0      0          512 Oct 21  1996 incoming
drwxr-xr-x   2 91     0          512 Apr 29  1996 lists
-rw-r--r--   1 91     91       31121 May 13 11:30 ls-lR.Z
drwxrwxr-x   6 0      10         512 Oct 16  1996 priv
drwxr-xr-x   9 0      0         1024 May 13 12:00 pub
drwxrwxrwt   2 0      0          512 Apr 29 11:50 tmp
drwxr-xr-x   4 100    0          512 Apr 19  1996 uucpmap
.net/uunet-info
```

```
226 Transfer complete.
ftp> pwd
257 "/" is current directory.
ftp> cd pub
250 CWD command successful.
ftp> pwd
257 "/pub" is current directory.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 408
ftp.uu.net/uunet-info/active
drwxr-xr-x   2 0      0          512 Jan 30  1994 bin
cs.toronto.edu/doc/ftp.sites
drwxr-xr-x   2 0      0          512 Apr 11  1995 info
drwxr-xr-x   2 0      0          512 Aug 16  1995 isi
lrwxrwxrwx   1 0      0           10 Feb 15  1994 ls-lR.Z -> ../ls-lR.Z
drwxr-xr-x   6 0      0          512 Apr  3 19:47 news
lrwxrwxrwx   1 0      0            1 Aug 29  1994 pub -> .
drwxr-xr-x   3 0      0         1024 Jan  8  1996 registry
-rw-r--r--   1 0      0       183969 May 13 06:59 routes
drwxr-xr-x  10 0      0         1024 Aug 15  1996 software
drwxr-xr-x   3 0      0          512 Apr  2 09:00 tmp
ftp/ftp.uu.net/uunet-info
226 Transfer complete.
ftp> cd software
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 18
drwxr-xr-x   2 0      0          512 Feb 19  1996 BSDI
drwxr-xr-x   6 0      0          512 Apr 11  1995 DOS
-rw-r--r--   3 0      0          898 Aug 15  1996 Macintoch
drwxr-xr-x   4 0      0          512 Apr 11  1995 Macintosh
drwxr-xr-x   2 0      0          512 May 18  1995 Novell
drwxr-xr-x   4 0      0          512 Apr 11  1995 OS2
drwxr-xr-x   7 0      0          512 Sep 13  1995 Unix
drwxr-xr-x   2 0      0          512 Feb 26 19:16 Win95
drwxr-xr-x   5 0      0         1024 Aug 15  1996 Windows
226 Transfer complete.
ftp> cd DOS
250 CWD command successful.
ftp> pwd
257 "/pub/software/DOS" is current directory.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 10
-rw-r--r--   1 0      0          121 Sep 12  1994 00_index.txt
drwxr-xr-x   2 0      0          512 Apr 11  1995 fossil
drwxr-xr-x   3 0      0          512 Apr 11  1995 ip
drwxr-xr-x   2 0      0          512 Apr 11  1995 utils
drwxr-xr-x   4 0      0          512 Apr 11  1995 uucp
```

```
226 Transfer complete.
ftp> cd utils
250 CWD command successful.
ftp> pwd
257 "/pub/software/DOS/utils" is current directory.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 792
-rw-r--r--   1 0      0         25335 Mar 11  1994 compress.exe
-rw-r--r--   1 0      0         56015 May  4  1992 dmp205.zip
-rw-r--r--   1 0      0        202624 Feb 13  1995 pk204g.exe
-rw-r--r--   1 0      0         79343 May 10  1994 tar.exe
-rw-r--r--   1 0      0         29888 Jun  1  1994 uucode.exe
226 Transfer complete.
```

4.3.8.3 TRANSFIRIENDO LOS ARCHIVOS

Supóngase que se quiere traer una copia del archivo pk204g.exe (listado en el ultimo directorio accesado). Como se menciono en secciones anteriores, antes de hacer la transferencia de un archivo se debe considerar el tipo de éste. Si el archivo es de texto la transferencia se debe establecer a este tipo por medio del comando **ascii**. Si el archivo no es de texto (como el archivo que se pretende transferir) la transferencia se debe de establecer a este tipo con el comando **binary**. Una vez establecido el tipo se puede obtener el archivo mediante el comando **get**.

```
ftp> bin
200 Type set to I.
ftp> get pk204g.exe
local: pk204g.exe remote: pk204g.exe
200 PORT command successful.
150 Opening BINARY mode data connection for pk204g.exe (202624 bytes).
226 Transfer complete.
202624 bytes received in 13 seconds (15 Kbytes/s)
```

Mientras se está haciendo la transferencia de un archivo, el sistema no indica si está trabajando o está "congelado", por lo que FTP proporciona un comando llamado **hash** que pone una marca (#) en la pantalla del usuario conforme se está haciendo la transferencia de un archivo. Una variante del comando get es el comando **mget** que permite la transferencia de dos o más archivos, y solicita la confirmación de cada archivo a ser transferido.

```
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
```

```
.ftp> mget pk204g.exe dmp205.zip
mget pk204g.exe? y
200 PORT command successful.
150 Opening BINARY mode data connection for pk204g.exe (202624 bytes).
##########################################################################
#######
####################################
226 Transfer complete.
202624 bytes received in 15 seconds (13 Kbytes/s)
mget dmp205.zip? y
200 PORT command successful.
150 Opening BINARY mode data connection for dmp205.zip (56015 bytes).
#####################################################
226 Transfer complete.
56015 bytes received in 5.2 seconds (11 Kbytes/s)
ftp> cd /
250 CWD command successful.
ftp> pwd
257 "/" is current directory.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 96
drwx--x--x   2 0      0           512 Feb 22  1995 .domain
-rw-r--r--   1 91     91          607 Aug 25  1995 README
lrwxrwxrwx   1 0      0             7 Feb 15  1994 bin -> pub/bin
toronto.edu/ca-domain
drwxr-x--x   9 0      0           512 Sep  5  1996 distrib
drwxrwxr-x 190 0      91         5120 Apr 28 14:45 ftp
dr-xr-xr-x   2 0      0          512 Oct 21  1996 incoming
drwxr-xr-x   2 91     0           512 Apr 29  1996 lists
-rw-r--r--   1 91     91        31121 May 13 11:30 ls-lR.Z
drwxrwxr-x   6 0      10          512 Oct 16  1996 priv
drwxr-xr-x   9 0      0          1024 May 13 12:00 pub
drwxrwxrwt   2 0      0           512 Apr 29 11:50 tmp
drwxr-xr-x   4 100    0           512 Apr 19  1996 uucpmap
.net/uunet-info
226 Transfer complete.
```

FTP permite ver el contenido de un archivo de texto, esta característica es importante ya que deja al usuario revisar o verificar el contenido de un archivo de texto antes de transferirlo está operación se realiza con el comando **get <nom_arch> "|more"**.

```
ftp> get README "|more"
local: |more remote: README
200 PORT command successful.
150 Opening BINARY mode data connection for README (607 bytes).

----------------------------------------------------------------------
Welcome to the UUNET Canada FTP archives.

 This file is /README
```

```
Get the file ~/pub/info/ls-lR.Z (or ~/ls-lR.Z); it contains a
complete list of the files in these archives.

----------------------------------------------------------------------
 UUNET Canada Inc.
 20 Bay Street          info@uunet.ca
 Suite 1910            +1 416 368 6621
 Toronto, Ontario       +1 800 463 8123 toll free
 Canada  M5J 2N8          +1 416 368 1350 fax
----------------------------------------------------------------------

#
226 Transfer complete.
607 bytes received in 0.37 seconds (1.6 Kbytes/s)
ftp> ascii
200 Type set to A.
ftp> get README
local: README remote: README
200 PORT command successful.
150 Opening ASCII mode data connection for README (607 bytes).
#
226 Transfer complete.
623 bytes received in 0.23 seconds (2.7 Kbytes/s)
```

4.3.8.4 TERMINANDO LA CONEXIÓN

Una vez que ya se transfirieron los archivos deseados, se debe de terminar la conexión. Si se desea cerrar la sesión actual se edita el comando **close**, el cual deja al usuario dentro del programa ftp, y le permite abrir otra sesión con el comando open. Si se desea salir totalmente del programa ftp se edita el comando **bye**, el cual cierra la sesión activa y da por terminado el programa ftp.

```
ftp> close
221 Goodbye.
ftp> bye
$
```

En este ejemplo la conexión ha sido terminada con el comando close, para después salir de ftp con el comando bye.

4.3.9 COMANDOS DE USUARIO FTP

En el ejemplo de la sesión FTP mostrado en la sección anterior, se pudo ver que el usuario interactua con el programa ftp por medio de un número de comandos puestos a su disposición. La figura 4.10 presenta los comandos utilizados con mayor frecuencia por un usuario en una sesión FTP.

Comando FTP	Descripción
ascii	Cambia a modo de transferencia ASCII
binary	Cambia a modo de transferencia binario
cd o chdir	Cambia de directorio en el servidor
close	Termina la conexión
del	Borra un archivo en el servidor
dir o ls	Despliega el contenido del directorio del servidor
get	Obtiene un archivo del servidor
hash	Despliega un carácter # por cada bloque transmitido
help	Despliega la ayuda
lcd	Cambia el directorio en el cliente
mget	Obtiene varios archivos del servidor
mput	Envía varios archivos al servidor
open	Conecta con un servidor
put	Envía un archivo al servidor
pwd	Despliega el nombre del directorio actual en el servidor
quote	Proporciona directamente un comando FTP
quit	Termina una sesión FTP

Figura 4.10 Comandos de usuario para una sesión FTP

4.4 CORREO ELECTRÓNICO

El correo electrónico fue originalmente diseñado para permitir que un par de usuarios se comunicaran vía la computadora. Los primero programas proporcionaron únicamente un servicio básico: permitir que una persona escribiera un mensaje en su computadora y pudiera enviarlo a través de Internet a otra.

Los sistemas actuales de correo electrónico proporcionan servicios que permiten una comunicación e interacción más compleja. Por ejemplo, el correo electrónico puede ser utilizado para:

- Enviar un mensaje a muchos destinatarios
- Enviar un mensaje que incluya texto, voz, vídeo, o gráficos
- Enviar un mensaje a un usuario en una red fuera de Internet
- Enviar un mensaje para el cual un programa de computadora responda

El correo electrónico es uno de los servicios más ampliamente utilizados en un medio ambiente de red e Internet no es la excepción. El correo electrónico es muy popular debido a que ofrece un método conveniente y rápido de transferir información puede acomodar desde notas pequeñas hasta documentos extensos con un mecanismo muy simple.

4.4.1 BUZONES

Para que un usuario pueda recibir correo, debe tener un buzón, es decir, una área de almacenamiento usualmente en disco en donde se graben los mensajes hasta que pueda ser leídos. Además, la computadora en la cual reside el buzón debe tener un programa que permita escribir y leer mensajes. Cuando llega un mensaje el software automáticamente lo almacena en el buzón del usuario.

Como los buzones postales, cada buzón de correo electrónico tiene una dirección. Para enviar un mensaje de correo a otro usuario, se debe conocer la dirección del buzón del destinatario. Un buzón electrónico es privado de la misma forma que los son los buzones postales: cualquier persona puede enviar un mensaje al buzón, pero sólo el dueño puede examinarlo.

4.4.2 ENVIÓ Y RECEPCIÓN DE UN MENSAJE DE CORREO ELECTRÓNICO

Para enviar un mensaje de correo electrónico a través de Internet, un usuario ejecuta una aplicación de correo electrónico en su computadora local. La aplicación opera de una forma similar a un procesador de texto, permite a un usuario editar un mensaje y especificar un destinatario dando una dirección. Una vez que el usuario termina de capturar el mensaje, el software de correo lo envia a través de Internet al buzón del destinatario.

Una vez que el mensaje llega al destinatario, un usuario puede extraer los mensajes de su buzón utilizando un programa de aplicación de correo. La aplicación permite a un usuario ver cada mensaje, y opcionalmente enviar una respuesta. Usualmente, cuando una aplicación de correo se ejecuta, le indica al usuario acerca de los mensajes que están esperando en el buzón. Le presenta un sumario conteniendo una línea por cada mensaje que ha llegado; la línea informa el nombre del emisor, la fecha y

hora de arribo y la longitud del mensaje. Después de examinar el sumario, un usuario puede seleccionar y ver los mensajes de la lista. Cada vez que un usuario selecciona un mensaje del sumario, el programa de correo despliega el contenido del mensaje. Después de la revisión del mensaje, el usuario puede enviar un mensaje de respuesta o contestación, dejar el mensaje en el buzón de tal manera que pueda ser revisado en una ocasión posterior, salvar una copia del mensaje en un archivo o borrarlo.

4.4.3 ESTÁNDARES TCP/IP PARA CORREO ELECTRÓNICO

A lo largo de todo este trabajo se ha mencionado que la meta de los protocolos TCP/IP es proveer los medios para que sea posible la interoperabilidad entre el rango más amplio de sistemas de computadoras y redes. Por lo tanto para extender la interoperabilidad del correo electrónico, TCP/IP divide sus estándares de correo en dos conjuntos. Un estándar especifica el formato de los mensajes (RFC 822) y el otro especifica los detalles del intercambio de correo entre dos computadoras (RFC 821). Manteniendo los dos estándares separados hace posible construir compuertas de correo o pasarelas que conectan internets TCP/IP con otros sistemas de entrega de correo que no siguen estos protocolos (como Compuserve, America Online, MCImail, etc.), pero así mismo permite la utilización del mismo formato de los mensaje, en ambos sistemas.

El estándar (RFC 822) especifica que cada mensaje debe ser transmitido en código ASCII (con CR/LF para delimitar las líneas). También describe la estructura general de un mensaje, como un conjunto de líneas de encabezado, después una línea en blanco, terminando con el cuerpo del mensaje propiamente. Finalmente, describe la sintaxis de las líneas del encabezado en detalle, las cuales generalmente consisten de una palabra clave seguida por dos puntos y después un valor

Algunas palabras claves son requeridas y otras son opcionales. Por ejemplo, el encabezado debe contener una línea que especifique el destino. La línea empieza con la palabra **To:** y contiene la dirección electrónica de correo del destinatario en el resto de la línea. Una línea que empieza con **From:** contiene la dirección electrónica del emisor. Opcionalmente , el emisor debe especificar una dirección a la cual las respuestas deban ser enviadas (se le permite al emisor que especifique una dirección diferente a la de su buzón, a la cual las contestaciones deban ser enviadas). Si se presenta, una línea que

empieza con la palabra **Reply-to:** especifica la dirección para las contestaciones. Si no existe tal línea, el destinatario usará la información de la línea From: como la dirección de regreso.

El formato del mensaje es elegido para facilitar el proceso y transporte a través de máquinas heterogéneas. Manteniendo un formato sencillo del encabezado se permite utilizarlo en un amplio rango de sistemas de correo. Además restringiendo los mensajes a un texto leíble, se evitan los problemas de seleccionar una representación estándar binaria y traducirla entre las representaciones locales correspondientes de cada máquina particular.

4.4.4 DIRECCIONES DE CORREO ELECTRÓNICO

Todas las direcciones de correo electrónico dentro de Internet tiene un formato estándar fácil de recordar como se presenta a continuación:

parte-local @ nombre-de-dominio

donde el nombre-de-dominio es el nombre de dominio de un destino de correo y al cual el mensaje debe ser entregado; y la parte-local es el nombre de un buzón en tal máquina.

Durante el envío de un mensaje por Internet, lo que al principio le interesa al sistema es determinar el nombre de la computadora (el dominio) que recoge el correo de la persona con la que se quiere comunicar. Es semejante a las máquinas clasificadoras de las oficinas de correo, que sólo prestan atención a los códigos postales. Así que, por ejemplo, si se envía un mensaje a *juanperez@estaempresa.com*, el sistema sólo se fija en *estaempresa.com.* Incluso si la primera parte de la dirección estuviera mal, si la parte local fuera en realidad *joseperez* , no *juanperez*, aún así llegaría el mensaje al dominio correcto. Pero cuando el dominio verificara la parte local y resultara que no coincide con ninguno de los nombres de entrada de ese dominio, entonces simplemente el mensaje se devolverá.

4.4.5 OPERACIÓN DEL CORREO ELECTRÓNICO

El sistema de correo electrónico sigue el modelo cliente/servidor: dos programas cooperan para transferir un mensaje de correo desde la computadora del emisor hasta el buzón del destinatario (la transferencia requiere dos programas debido a que una aplicación corriendo en una computadora no puede almacenar los datos directamente en un buzón en el disco de la otra computadora). Cuando un usuario envía un mensaje de correo, un programa en la computadora del emisor se convierte en un cliente. Éste contacta un programa servidor de correo (utilizando TCP) en la computadora del destinatario y transfiere una copia del mensaje. El servidor almacena el mensaje en el buzón del destinatario. La figura 4. 11 muestra el modelo que sigue el correo electrónico.

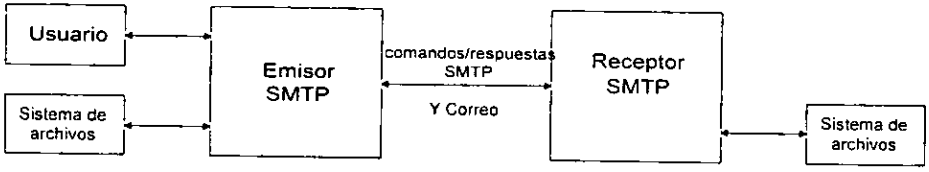


Figura 4.11 Esquema que representa la operación del correo electrónico

La interacción entre un cliente y un servidor es compleja debido a que en cualquier momento las computadoras en Internet pueden fallar. Para asegurar que el mensaje sea entregado de forma segura, el cliente mantiene una copia del mensaje durante la transferencia. Después de que el servidor informa al cliente que el mensaje ha sido recibido y almacenado en disco, el cliente borra su copia.

4.4.6 SEUDÓNIMOS

La mayoría de los programas manejadores de correo soportan la creación de seudónimos o alias, que permiten a un usuario definir un conjunto de abreviaciones para las direcciones de correo que se utilizan frecuentemente. Usualmente, los mecanismos de seudónimos requieren que el usuario prepare una lista pequeña de seudónimos, que el software utilizará. Por ejemplo, supóngase que un usuario envía correo a la dirección jcgutierrez@computadora1.algunacorporacion.com con mucha frecuencia.

El usuario puede definir un seudónimo para la dirección de correo de la forma:

julio = jcgutierrez@computadora1.algunacorporacion.com

Cuando se edita un mensaje de correo, el usuario puede dar julio en el campo To. El software de correo consultará automáticamente el alias del usuario y reemplazara la abreviación con la dirección completa. Así, aunque el usuario sólo escriba el seudónimo, el mensaje de correo contendrá la dirección completa del buzón.

4.4.7 ENVIANDO CORREO A MÚLTIPLES DESTINATARIOS

Aunque el correo electrónico fue originalmente diseñado como una forma de comunicación para dos personas, la mayoría de los sistemas de correo permiten a un usuario enviar un mensaje a múltiples destinatarios. Para hacer esto, el emisor especifica múltiples direcciones de correo en la línea To en el encabezado de un mensaje.

Otra alternativa para el envió de correo a varios destinatarios son las **listas de correo** las cuales son un extensión del mecanismo de seudónimos, es decir, un alias que especifica múltiples destinatarios. Cuando el sistema de correo expande un alias y encuentra múltiples destinatarios, le envía una copia de un mensaje a cada uno.

Informalmente, la gente se refiere a un alias que especifica múltiples destinatarios como un lista de correo. Por ejemplo, la siguiente definición crea una lista de correo llamada *amigos* que contiene tres direcciones de correo

amigos = luis@aragon.unam.mx, alex@iztacala.unam.mx, susana@acatlan.unam.mx

Una vez que tal alias ha sido creado, cualquier mensaje enviados a *amigos* será entregado a los tres destinatarios

Otra clase de lista de correo es el **reflector de correo.** Se trata de una especie de lista de correos pública: los mensajes que se envían a la dirección de un reflector se envían automáticamente a todos los miembros de la lista de correo del reflector. Constituye una forma muy cómoda de controlar en forma centralizada la lista de correos

que utiliza un grupo de personas (por ejemplo, el departamentos de ventas, de cobranza, etc.).

Un usuario normal no puede crear un reflector de correo; esto lo hace el administrador del sistema. Sin embargo, lo que sí puede hacer es solicitar que lo incluyan dentro de la lista, lo que generalmente se hace enviando un mensaje de correo al administrador de la lista, por ejemplo si se desea pertenecer a la lista *historia@unam.mx*, tiene que enviar el mensaje a *historia_postmaster@unam.mx*.

Una de las aplicaciones más comunes de los reflectores de correos es para los grupos de intercambio de ideas y opiniones sobre algún tema en particular (conocidos como grupos de noticias). Se envían mensajes al reflector y todos los miembros de la lista los leen y, si lo desean, los responden.

4.4.8 ACCESO A SERVICIOS VÍA CORREO ELECTRÓNICO

Debido a que una computadora puede ser programada para que responda automáticamente ("contestadora") a los mensajes de correo que le llegan, cualquier sistema de cómputo enlazado a Internet puede proveer acceso a cierto servicio vía correo electrónico.

Algunas de los servicios que se ofrecen dentro de Internet por medio del correo electrónico son servicios de información, envió de archivos, consultas a base de datos, etc. Por ejemplo, para obtener un documento RFC (Request For Coment, Solicitud Para Comentario) que son los papeles oficiales donde se especifican los estándares para los protocolos TCP/IP y los cuales están identificados por un número; se puede enviar mensajes a INTERNIC y muchos otros sitios donde operan servidores de información que responden a los mensajes de correo electrónico. Esto es, un usuario envía un mensaje a una dirección especial de correo, un programa de computadora lee el mensaje, consulta su base de datos de información, y regresa una respuesta usando el correo electrónico. La dirección de correo electrónico del servidor de información de INTERNIC es:

mailserv@ds.internic.net

Si se desea obtener una copia de algún documento RFC, simplemente se envía un mensaje a la dirección anterior con la siguiente línea

send rfcN.txt

donde N es el número del documento RFC que se desea.

4.4.9 PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO (SMTP)

Además de la especificación del formato de los mensajes de correo electrónico dada por el estándar RFC 822, la familia de protocolos TCP/IP especifica un estándar para el intercambio de mensajes de correo entre dos máquinas. Esto es, el estándar especifica el formato exacto de los mensajes que un cliente en una máquina debe utilizar para transferir correo a un servidor en otra máquina. Este estándar se conoce como el Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP), especificado en el documento RFC 821. El SMTP se enfoca especialmente en como debe el sistema de entrega pasar los mensajes a través de un enlace desde una máquina a otra.

El diseño de SMTP está basado en el siguiente modelo de comunicación: como resultado de una solicitud de correo por parte de un usuario, el emisor establece un canal de transmisión con un receptor o destinatario. La comunicación entre el emisor (cliente) y el destinatario (servidor) consiste de texto ASCII, de tal manera que el cliente le emite comandos al servidor y éste a su vez le envía respuestas al cliente como resultado de los comandos que procesa.

Una vez que el canal de transmisión está establecido, el cliente envía un comando MAIL indicando el emisor o remitente del correo. Si el servidor puede aceptar correo le responde al cliente con un OK. El cliente después envía un comando RCP identificando al destinatario del mensaje. Si el servidor puede aceptar correo para tal destinatario responde con un OK; si no, responde con una mensaje negativo. El cliente y el servidor pueden negociar varios destinatarios para el mismo mensaje. Cuando los destinatarios han sido negociados el cliente procede a enviar el mensaje, indicando su finalización mediante una secuencia de 5 caracteres: retorno de carro (CR), alimentación de línea

(LF), un punto y otro par CR/LF[2]. Si el servidor procesa exitosamente el mensaje responde con un OK.

El cliente puede solicitar al servidor que intercambien los roles de emisor y receptor de tal manera que los mensajes puedan fluir en dirección opuesta.

Los comandos y respuestas están compuestos de caracteres ASCII y tiene una sintaxis rígida, aunque esto no evita que un usuario pueda fácilmente leer una transcripción de las interacciones entre un cliente y un servidor. Las respuestas al igual que FTP también tienen un código numérico.

4.4.9.1 EJEMPLO DE LA OPERACIÓN INTERNA DE SMTP

Para dar una mayor idea acerca del proceso de transmisión de un mensaje de correo electrónico, considérese el siguiente ejemplo: El usuario gbenson en la computadora jazz.musica.com, desea enviar el mensaje que se presenta líneas más abajo a los usuarios cfisher y psanchez en el host fusion.unam.edu, sin saber que el usuario psanchez ya no está registrado en tal host.

Date: Sat, 27 Jun 87 13:26:31 EDT
From: gbenson@jazz.musica.com
To: cfisher@fusion.unam.edu, psanchez@fusion.unam.edu
Subject: Sesión de grabación

Reunión Lunes 29 a las 10 a.m. para empezar sesión de grabación

Como se puede ver el mensaje sigue el formato especificado por el estándar en cuestión del encabezado, línea en blanco, mensaje y terminación del mismo.

El cliente hace uso del sistema de nombres de dominio para traducir el nombre del servidor de correo electrónico, que en este caso se considera que es la máquina fusion.unam.edu correspondiendo al número 128.6.4.2. A continuación el cliente abre una conexión TCP al puerto 25 en 128.6.4.2 El puerto 25 es el número TCP bien conocido para recibir correo electrónico. Una vez que esta conexión esta establecida, el cliente

[2] Generalmente se indica la finalizacion de un mensaje por medio de una linea conteniendo unicamente un punto, si un punto es parte del mensaje entonces se tiene que escribir por duplicado.

empieza a mandarle comandos al servidor. Aquí está un conversación típica, cada línea esta etiquetada con un "c" o una "s" para identificar al cliente y servidor respectivamente

s: 220 FUSION.UNAM.EDU SMTP Service at 29 Jun 87 05:17:18 EDT
c: HELO jazz.musica.com
s: 250 FUSION.UNAM.EDU - Hello, JAZZ.MUSICA.COM
c: MAIL From: <gbenson@jazz.musica.com>
s: 250 MAIL accepted
c: RCPT To: <cfisher@fusion.unam.edu>
s: 250 Recipient accepted
c: RCPT To: <psanchez@fusion.unam.edu>
s: 250 No such user here

c: DATA
s: 354 Start mail input; end with <CRLF>.<CRLF>
c: Reunión Lunes 29 a las 10 a.m. para empezar sesión de grabación
c: <CRLF>.<CRLF>
s: 250 OK
c: QUIT
s: 221 FUSION.UNAM.EDU Service closing transmission chanel

En el ejemplo el servidor niega el destinatario *psanchez* debido a que no reconoce el nombre como un destino valido. El SMTP no especifica los detalles de como debe de manejar un cliente tales errores. Sin embargo como se puede observar todos los comandos usan texto normal (situación típica de los estándares en Internet como se ha podido constatar a lo largo de este capitulo) lo cual facilita la observación de lo que está sucediendo y diagnosticar problemas. Por ejemplo, el programa de correo mantiene una bitácora de cada conversación, si algo se presenta anormal, la bitácora puede ser simplemente enviada al postmaster[3]. Debido a que es texto normal puede ver que está sucediendo.

Todas las respuestas por parte del servidor empiezan con un código de tres dígitos, el resto de la respuesta es texto, el cual es normalmente para información del usuario y no tiene efecto alguno en la operación de los programas.

Generalmente, hay un patron para los números de respuesta. El protocolo define el conjunto especifico de respuestas que pueden ser enviadas como resultado a un

[3] Por convención, este es el alias para la persona que administra el sistema de correo electrónico en una computadora dada

comando dado. En general, respuestas que empiezan con 2 indican acciones exitosas. Aquellas que empiezan con 3 indican que alguna acción posterior es necesaria. 4 y 5 indican errores; 4 es un error "temporal", tal como un disco lleno y 5 es un error permanente, tal como un destinatario no existente. No existen códigos de respuesta que empiecen con 1.

4.4.9.2 COMANDOS INTERNOS SMTP

En el ejemplo anterior se pudo observar que SMTP tiene un conjunto sencillo de comandos internos, mediante el uso de estos elementos el correo electrónico se transfiere fácil y elegantemente. La figura 4.12 presenta una lista completa de los comandos internos del protocolo SMTP.

Comando	Descripción
DATA	El receptor trata las líneas que siguen al comando como el texto del mensaje
EXPN	Este comando pide al receptor que confirme que el argumento identifica a un lista de correo, y si es así, que regrese las direcciones de correo de sus miembros
HELO	Utilizado en el establecimiento de una conexión para cambiar identificadores
HELP	Solicitud de ayuda
MAIL	Este comando es utilizado para iniciar una transacción de correo en la cual se especifica la dirección del emisor
NOOP	No hay operación.
QUIT	Especifica que el receptor debe enviar una respuesta OK, y después cerrar el canal de transmisión
RCPT	Este comando es utilizado para identificar un destinatario del mensaje; múltiples destinatarios pueden ser especificados
RSET	Especifica que la transacción de correo actual va a ser abortada
SAML	Este comando es utilizado para iniciar una transacción de correo en el cual el mensaje es entregado a una o más terminales y buzones. Para cada destinatario el mensaje es entregado a la terminal del usuario si está activo en ella, y también se graba en su buzón
SEND	El mensaje es enviado a una o más terminales
SOML	El mensaje es enviado a una o más terminales o buzones. El mensaje es entregado al destinatario en su terminal si esta activo en ella, de otra forma se graba en su buzón
TURN	Modifica la dirección del emisor (invierte los papeles del emisor y receptor)
VRFY	Este comando verifica el nombre del usuario.

Figura 4.12 Comandos internos del protocolo SMTP

4.4.9.3 CÓDIGOS DE RESPUESTA SMTP

La figura 4.13 presenta una lista completa ordenada por número de los códigos de respuesta a los comandos internos SMTP.

Código	Descripción
211	Status del sistema, o respuesta de ayuda de sistema
214	Mensaje de ayuda
220	<dominio>Servicio listo
221	<dominio>Cerrando el canal de transmisión
250	Acción de correo solicitada OK, completada
251	El usuario no está en este host, el mensaje se enviara a <ruta>
354	Empieza la entrada del mensaje, termina con <CRLF>.<CRLF>
421	<dominio> servicio no disponible
450	Acción de correo solicitada no ejecutada: buzón no disponible
451	Acción solicitada abortada: error local en el procesamiento
452	Acción solicitada no tomada: insuficiente espacio
500	Error de sintaxis, comando no reconocido
501	Error de sintaxis en parámetros o argumentos
502	Comando no implementado
503	Secuencia de comandos errónea
504	Parámetro no implementado
550	Acción solicitada no tomada: buzón no disponible
551	Usuario no local
552	Acción de correo solicitada abortada: se excede la capacidad de almacenamiento
553	Acción solicitada no tomada: no se permite tal nombre para el buzón
554	Transacción fallida

Figura 4.13 Códigos de respuesta a los comandos internos SMTP

4.4.10 EXTENSIONES DE CORREO INTERNET DE MULTIPROPOSITO (MIME)

Como se menciono al inicio de esta sección, con el correo electrónico además de poder transmitirse mensajes de texto ASCII, también es posible transmitir archivos que no son de texto (por ejemplo de audio, vídeo, gráficos, etc.), mediante un estándar denominado Extensiones de Correo Internet de Multiproposito (Multipurpose Internet Mail Extensions, MIME). MIME no cambia a SMTP o lo reemplaza, más bien permite codificar

cualquier tipo de dato en ASCII y poder después transmitirlo en un mensaje estándar de correo.

Para acomodar tipos de datos y representaciones arbitrarias, cada mensaje MIME incluye información que le indica al destinatario el tipo de datos y la codificación utilizada. La información MIME reside en el encabezado del mensaje, especifica la versión MIME utilizada, el tipo de datos que están siendo enviados, y la codificación utilizada para convertir los datos en ASCII. Por ejemplo, el encabezado que se muestra a continuación ilustra un mensaje MIME que contiene una fotografía en la representación estándar GIF (Graphics Interchange Format, Formato de intercambio de gráficas). La imagen GIF ha sido convertida a una representación ASCII de 7 bits usando la codificación base64.

```
From: laura@college.edu
To: luis@empresa.com
MIME-Version: 1.0
Content-Type: image/gif
Content-Transfer-Encoding: base64

..... datos para la imagen .....
```

En el encabezado la línea MIME-Version: declara que el mensaje fue compuesto usando la versión 1.0 de MIME. La línea Content-Type: especifica que los datos son de una imagen GIF, y la línea Content-Transfer-Encoding: declara que la codificación base64 fue utilizada para convertir la imagen a ASCII. Para ver la imagen, el sistema del destinatario debe convertir primero de la codificación base64 a binario, y después correr una aplicación que despliegue una imagen GIF en la pantalla del usuario.

El estándar MIME especifica que una declaración Content-Type debe contener dos identificadores, el tipo del contenido y un subtipo, separado por una diagonal. La figura 4.14 muestra los tipos y subtipos definidos por MIME.

Tipo	Subtipo	Uso
Texto	Plain, html	Representa texto con y sin formato
Multiparte	mixed, digest, parallel, alternative	Combina varias partes, posiblemente de diferentes tipos de datos dentro de un mensaje
Mensaje	Partial, external-body	Un mensaje completo de correo o una referencia externa a un mensaje (por ejemplo, un servidor FTP y un nombre de archivo)
Aplicación	octetos, postscript, rtf, pdf, msword	Transmite datos en el formato especifico de una aplicación o datos binarios
Imagen	jpeg, gif, tiff, x-xbitmap	Imágenes estáticas, o imágenes generadas por computadora
Audio	Basic, wav	Para transmitir audio
Vídeo	mpeg	Para transmitir vídeo o imágenes con movimiento posiblemente con audio

Figura 4.14 Tipos y subtipos definidos para el estándar MIME

4.5 EJEMPLO DE OTROS SERVICIOS EN INTERNET

4.5.1 FINGER

Internet ofrece el servicio *finger* que permite contactar a un servidor remoto para obtener información acerca de un usuario especifico o todos los usuarios en tal máquina. Un usuario en Internet es conocido frecuentemente sólo por el nombre de su cuenta (login name), y por lo tanto, generalmente cuando un usuario invoca a finger lo hace utilizado este nombre, por ejemplo:

finger iden_usuario@nombre_de_computadora

Incluso puede introducir:

finger @nombre_de_computadora

sin ningún nombre, lo que permitirá ver una lista de todas las personas que este en ese momento en ese dominio.

La información que proporciona finger usualmente incluye el nombre real o completo del usuario, número telefónico, dirección de oficina, etc. Algunos sistemas finger pueden proveer información relacionada al status del acceso de un usuario al sistema, tal como la ultima vez que ingreso al sistema y si hay correo que no ha sido leído. Esta característica puede ser útil cuando un usuario necesita checar si el receptor ha recibido un mensaje importante enviado por él.

No siempre funciona el comando finger para todos los anfitriones, ya que muchos administradores consideran que da acceso a demasiada información y por lo tanto no habilitan el servicio.

4.5.2 INTERNET RELAY CHAT (IRC)

El servicio Internet Relay Chat (IRC) proporciona una forma de poder "platicar" entre muchos usuarios sobre un tópico dado en tiempo real. Cada platica ocurre en un "canal" separado. Un usuario puede crear un canal elegir un tópico y especificar si el canal está abierto a cualquier persona o restringido a un conjunto de personas especificadas. Cuando un usuario se conecta a un servidor IRC, puede solicitar una lista de los canales IRC que están actualmente en progreso, y puede elegir unirse a uno de ellos. Cuando un usuario se une a un cana IRC, toma un seudónimo para indentificarse con los otros usuarios.

Los participantes reciben cada una de las línea de texto que los demás escriben junto con su seudónimo correspondiente. Así, un participante que escribe una línea de texto sabe que todos los demás participantes recibirán una copia del texto en sus pantallas.

IRC permite a un usuario en Internet "oír a escondidas" la conversación de otras personas, cambiar de una platica a otra, además de invitar a otros para una conversación privada.

Para utilizar el servicio IRC, un usuario en Internet necesita tener un programa cliente que actúe como interface. Este cliente se conecta a un servidor IRC y a su vez todos los servidores IRC se conectan unos con otros, creando una red global de usuarios IRC en Internet.

4.5.3 GOPHER

Conforme Internet ha crecido, los usuarios han enfrentado dos problemas relacionados. Uno de ellos es la gran cantidad de información que existe en la red que en un momento dado es difícil localizarla en su totalidad y el otro es que existen diferentes maneras de obtener los diferentes recursos (Telnet, FTP, finger, etc.).

Gopher resuelve muy bien ambos problemas, es un sistema cliente/servidor que permite a un usuario en Internet accesar una gran variedad de recursos. El poder de Gopher es proporcionar un menú listando diversas entradas. Algunas de las entradas son archivos que Gopher puede desplegar, enviarlos por correo o copiarlos a la computadora; otras son entradas Telnet que inician una sesión para que un anfitrión proporcione determinado servicio. Algunas más son entradas de búsqueda que pedirán que se introduzca una cadena para localizar algún documento, o el nombre total o parcial del archivo que se busca, lo interesante de Gopher es que todos los resultados los presenta en forma de menús.

En otras palabras, Gopher proporciona una serie de menús a partir de los cuales un usuario puede accesar virtualmente cualquier tipo de información textual en Internet.

El Gopher original fue desarrollado en 1991 por el Departamento de Computación y Sistemas de Información, de la Universidad de Minnesota, para proveer una forma fácil de distribuir la información disponible del campus. Hoy en día, hay varios cientos de servidores Gopher, ubicados en muchas universidades y organizaciones.

4.5.4 ARCHIE

Cuando un usuario en Internet desea obtener un archivo de algún sitio utilizando FTP, se supone que debe de conocer el nombre de dominio de la máquina servidora, conectarse a ella mediante un cliente FTP y obtenerlo. Pero si se presenta la situación en la cual un usuario desea obtener un archivo del cual sólo conoce su nombre pero no sabe o no recuerda el sitio FTP en donde se ubica éste, es aquí en donde aparece el servicio *archie*[4].

Archie es un sistema que elabora índices de sitios FTP y lista todos los archivos que existen en cada uno de estos sitios, formando listas con varios millones de archivos, que comprenden más de un millar de sitios FTP alrededor del mundo. Archie es un medio increíblemente rápido para orientarse a donde ir para conseguir un archivo que sea de interés.

Archie está configurado según el sistema cliente/servidor. El servidor en Archie es una computadora que periódicamente realiza revisiones por todos los sitios FTP que hay

[4] Archie se deriva de archive = archivo

en el mundo y, con la información obtenida, construye una lista de todos los archivos que hay en existencia. Cada servidor construye su base de datos a partir de tales archivos. Un programa cliente Archie se comunica a cualquier servidor Archie y realiza búsquedas en su base de datos, la que le sirve de índice.

Como resultado final se presentan los lugares FTP anónimos, en donde se puede obtener el archivo solicitado. Acto seguido simplemente el usuario se conecta con alguno de los servidores de la lista para obtener una copia.

4.5.5 VERONICA

Otro servicio automático de búsqueda dentro de Internet lo constituye veronica un acronimo que aun traducido no dice gran cosa (Very Easy Rodent Orieted Net-wide Index to Computerized Archives, Índice de archivos computarizados, muy sencillo, orientado a los roedores, que abarca toda la red), pero todo hace indicar que se le dio este nombre con un sentido humoristico, ya que, si existía Archie faltaba Veronica (su novia).

Veronica busca menús gopher en la computadoras a través de Internet de forma análoga que archie busca por archivos disponibles vía FTP. La mayoría de los sistemas Gopher cuando presentan sus menús incluyen generalmente una opción correspondiente a veronica, al seleccionarla se solicita al usuario que de la palabra o palabras que desea localizar y veronica buscará las ocurrencias en todas las computadoras que tengan servidores Gopher.

La forma que veronica responde a la búsqueda solicitada es interesante: veronica despliega los resultados como un menú gopher, es decir, crea un menú extrayendo entradas individuales que contienen la palabra(s) buscada(s) de menús gopher en muchas máquinas distribuidas a lo largo de Internet integrándolas en un solo menú.

4.5.6 WAIS

El Servicio de Información de Área Amplia (Wide Area Information Service, WAIS) es un servicio que permite a un usuario buscar una gran cantidad de información de forma rápida a través de Internet. En otras palabras, WAIS es un sistema de búsqueda de texto distribuido. Permite a un usuario en Internet buscar en cualquiera de los cientos de

fuentes de información sobre una gran variedad de tópicos. Generalmente es utilizado para solicitar información bibliográfica.

Históricamente, WAIS creció de un proyecto iniciado por tres compañías: Apple, Thinking Machines y Dow Jones. Apple fabricante de computadoras personales con una interface gráfica de usuario fácil de usar, Thinking Machines diseñando supercomputadoras capaces de buscar grandes cantidades de datos en forma rápida; y Dow Jones corriendo un servicio que vendía servicios de noticias e información.

Una de las ideas ambiciosas detrás del desarrollo de WAIS fue proveer de una herramienta que permitiera a una computadora seguir la pista de una vasta cantidad de información, presentando a los usuarios sólo la información que es relevante para satisfacer sus necesidades.

Como muchos otros servicios dentro de Internet, WAIS opera bajo un esquema cliente/servidor y permite a un usuario buscar en cualquiera de los cientos de colecciones de datos. Cada una de estas colecciones es llamada una fuente de información, la cual es mantenida por un programa servidor WAIS. En operación, un usuario necesita tener un programa cliente WAIS para accesar a un servidor público WAIS en Internet. El uso de WAIS es razonablemente simple, cuando un usuario introduce un conjunto de palabras que describen lo que se busca, el cliente se conecta a un servidor que se encargara de buscar en las bibliotecas especificas los documentos solicitados. A diferencia de Archie y Veronica, WAIS busca dentro de los documentos y no sólo en los títulos. Esto requiere de mucho más trabajo por parte del servidor (es por eso que se involucra el uso de supercomputadoras para realizar este trabajo), pero por otro lado es más fácil de localizar el material necesario.

El servidor al encontrar la información solicitada entonces envía al usuario una lista de los artículos o citas que pueden ser apropiadas. Hay un limite al número de artículos que WAIS reporta, usualmente entre 15 y 50, dependiendo del cliente que el usuario esté utilizando.

WAIS también utiliza retroalimentacion, lo que significa que, dentro de la lista de los documentos encontrados se podrá identificar los archivos más adecuados a las necesidades del usuario y pedirle a WAIS que localice material adicional parecido.

4.5.7 TRACEROUTE

Un usuario interesado en la estructura de Internet puede correr el programa *traceroute*. Dando el nombre de dominio de una computadora remota después del comando, se imprimirá la lista de todo los ruteadores que seguirán los paquetes desde la computadora local hasta la computadora remota. Aunque traceroute fue pensado para utilizarse en la instalación y mantenimiento de las conexiones de los hosts a la red, es un programa muy practico e ilustrativo para visualizar cuantos ruteadores separan la computadora local de un destino dado.

4.5.8 WORLD WIDE WEB

El World Wide Web (WWW), Web o W3, es una herramienta muy popular utilizada para explorar los recursos y servicios de Internet. Con el Web se puede establecer una búsqueda WAIS, accesar menús Gopher, iniciar sesiones Telnet, hacer transferencias FTP, etc. El Web ofrece una interface gráfica fácil de usar, en lugar de la arcaica interface de línea de comando. Esta herramienta le permite a un usuario solicitar un documento formateado que puede contener texto, sonidos, gráficas , y/o video.

El Web está conformada de una colección de servidores y clientes que intercambian información. La mayoría de los clientes y servidores Web han sido diseñados para comunicarse utilizando TCP/IP. Tipicamente, cuando un servidor recibe un mensaje de solicitud de un cliente Web, éste envía el documento solicitado al cliente. El cliente despliega el documento en su pantalla. El programa cliente, también llamado hojeador o navegador, le permite a un usuario leer un documento, y seguir cualquier liga que sea seleccionada.

El protocolo que el cliente Web usa para comunicarse con el servidor Web es el Protocolo de Transmisión de Hipertexto (Hypertext Transmission Protocol, HTTP). Todos los clientes y servidores Web deben utilizar HTTP para enviar y recibir documentos hipermedia (una combinación de hipertexto y multimedia). El lenguaje estándar que el Web utiliza para crear y/o reconocer un documento hipermedia es el Hyper Text Markup Language (HTML). HTML es un lenguaje simple que hace posible incluir ligas de hipertexto y referencias a otros medias dentro de un documento. Un documento Web escrito en HTML tiene un formato de texto similar al de los documentos ASCII.

4.5..9 TELEFONÍA POR INTERNET

Este servicio ofrece llamadas de larga distancia a cualquier parte del mundo a través de Internet pagando sólo el costo de la llamada local. Sin embargo, es un servicio que inicia y que poco a poco va mejorando.

Se requiere obviamente de una cuenta de acceso a Internet, una computadora multimedia que cuente con micrófono, bocinas y tarjeta de sonido y el software. La otra persona debe tener los mismos requisitos anteriores. A diferencia de un teléfono real, las dos personas que se deseen comunicar deben estar conectados a Internet en ese momento y debido a una falta de estandarización deben de estar utilizando el mismo programa de software.

Antes de intentar llamar a alguien, el usuario debe conectarse con algún servidor, generalmente el de VocalTec (iphone.vocaltec.com), mismo que funcionará como central telefónica. Esto permitirá saber quienes son los otros usuarios conectados y a los cuales se puede contactar. Como se menciona arriba llamar a una persona en particular exige que ésta esté conectada al servidor.

Las conversaciones no son tan fluidas como el teléfono, pues debe seguirse un esquema de radio banda civil, en el que no es posible escuchar y transmitir al mismo tiempo. Primero se habla y enseguida se espera a que el interlocutor conteste.

Tal vez aún no sea la mejor manera de ahorrarse dinero en llamadas de larga distancia, habría que evaluar el precio de una llamada de este tipo contra lo que cuesta estar conectado al servidor todo el día para recibir llamadas por este medio.

Tampoco es la mejor manera de hablar por teléfono dada la calidad en general de la recepción/ transmisión, pero el servicio cada día se perfecciona más.

CONCLUSIONES

A raiz de la investigación realizada a través de la elaboración de este trabajo se puede concluir lo siguiente:

- Internet es una red internacional de redes de computadoras entrelazadas por medio de dispositivos especiales conocidos como ruteadores. Considerando que existen redes de diferentes tecnologías incompatibles entre si, es decir, que no existe posibilidad que puedan comunicarse al enlazarlas físicamente, entonces se requiere de un elemento que haga la función de interface común entre ellos que permita que se puedan comunicar. Este elemento que viene a servir de interface es el conjunto de protocolos TCP/IP.

- Una red de computadoras es un conjunto coordinado de elementos de hardware y software que interconectan computadoras aisladas y que tienen como finalidad compartir recursos y proporcionar servicios a los usuarios que las utilizan.

- Existen diferentes tecnologías de redes, las cuales están clasificadas por el área geográfica que cubren. Así, se tiene redes que abarcan una extensión pequeña conocidas como redes LAN o redes de área local, las redes MAN o redes metropolitanas que cubren la extensión equivalente a una ciudad y las redes WAN o de área amplia que abarcar grandes extensiones geográficas como Estados o países. Internet en una red WAN.

CONCLUSIONES

A raíz de la investigación realizada a través de la elaboración de este trabajo se puede concluir lo siguiente:

- Internet es una red internacional de redes de computadoras entrelazadas por medio de dispositivos especiales conocidos como ruteadores. Considerando que existen redes de diferentes tecnologías incompatibles entre si, es decir, que no existe posibilidad que puedan comunicarse al enlazarlas físicamente, entonces se requiere de un elemento que haga la función de interface común entre ellos que permita que se puedan comunicar. Este elemento que viene a servir de interface es el conjunto de protocolos TCP/IP.

- Una red de computadoras es un conjunto coordinado de elementos de hardware y software que interconectan computadoras aisladas y que tienen como finalidad compartir recursos y proporcionar servicios a los usuarios que las utilizan.

- Existen diferentes tecnologías de redes, las cuales están clasificadas por el área geográfica que cubren. Así, se tiene redes que abarcan una extensión pequeña conocidas como redes LAN o redes de área local, las redes MAN o redes metropolitanas que cubren la extensión equivalente a una ciudad y las redes WAN o de área amplia que abarcar grandes extensiones geográficas como Estados o países. Internet en una red WAN.

- Las redes también son identificadas por la forma que adquieren al ser enlazados los diversos nodos, dando origen a la topología de redes así tenemos; topología en bus, anillo, estrella y malla.

- Con el fin de evitar los sistemas propietarios se han establecido estándares. Un organismo muy involucrado en la elaboración de estándares para las redes de área local es el Instituto de Ingenieros Eléctricos y Electrónicos de E.U., principalmente con su proyecto 802.

- Algunos de los estándares derivados del proyecto 802 del IEEE son CSMA/CD 802.3, Token Bus 802.4 y Token Ring 802.5

- Dentro de la implementacion comercial de los estándares para las redes locales destaca principalmente la tecnología Ethernet, la cual cumple con la norma IEEE 802.3. De las diferentes tecnologías que existen para implementar una red de computadoras Ethernet es la más popular en todo el mundo.

- Una red de computadoras amplia el horizonte de posibilidades en relación a los recursos y servicios que le puede proporcionar a un usuario. Entre estos servicios destaca, el correo electrónico, servicios de impresión, comparición de archivos y aplicaciones, servicios de fax, acceso a servidores dè discos compactos, comunicación remota a computadoras remotas, etc.

- Internet ha pasado a lo largo de sus casi 30 años de existencia por diversas etapas de adaptación al crecimiento a que ha sido sometido, para convertirse en la red más grande del mundo.

- Ante el temor de una ataque nuclear por parte de la U.R.S.S hacia los E.U. durante la guerra fría, el gobierno estadounidense consideraba que un sistema de comunicación centralizado podía ser fácilmente destruido en un ataque y que las tecnologías tradicionales no trabajarían correctamente para comunicar las bases militares. Este

temor imprimió la necesidad en el gobierno de hacer algo diferente -- desarrollar un nuevo esquema de comunicación post-nuclear.

- El Internet que usamos hoy en día es una de las pocas herencias positivas de la paranoia de la guerra fría, proporcionando comunicaciones eficientes y económicas entre las personas de todo el mundo.

- Las raíces de lo que es ahora Internet vienen de ARPA (Advanced Research Proyect Agency, la Agencia de Proyectos Avanzados de Investigación), la cual en lugar de llevar a cabo sus propias investigaciones, regularmente auspicio proyectos de investigación relacionados a desarrollos tecnológicos o problemas militares. En los años 60's, ARPA se intereso en desarrollar una forma por medio de la cual las computadoras se pudieran comunicar y empezó a patrocinar programas en universidades y corporaciones. Pensaban que una red elevaría el desarrollo tecnológico americano y proporcionaría un comando seguro y control de la información durante una guerra. Para este fin, a mediados de los 60's empezó a apoyar la investigación para la construcción de tal red.

- La base del nuevo sistema se apoyaría en IMP's (Interfaces Procesadoras de Mensajes, predecesores de lo que ahora se conoce como ruteadores), los cuales utilizarían un tecnología llamada de conmutación de paquetes, para la entrega de la información a las computadoras destino.

- Para fines de 1969, 4 sitios eran enlazados dando origen a la red ARPANET, esta red utilizo un poco más adelante el protocolo NCP (Network Control Program).

- En 1972 ARPANET hizo su primera aparición pública en la Conferencia Internacional en Computadoras y Comunicaciones, en Washington D.C., muchas personas presenciaron una nueva revolución tecnológica, como el hecho de que el acceso remoto a archivos era posible. Después de esta presentación, muchas tecnologías para auxiliar al desarrollo de las redes de computadoras empezaron a brotar.

- Para 1973, un enlace satelital a Hawaii se establece, mientras la tecnología estaba creciendo rápidamente, el numero de hosts enlazados a ARPANET se movía lentamente. Entre 1969 y principios de 1977 ARPANET sólo tenia 107 hosts, aun así los diseñadores reconocieron que esta nueva red de comunicaciones estaba creciendo más rápido de lo que ellos se habían imaginado, por lo tanto necesitaban desarrollar un diseño apropiado para alojar una gran cantidad de hosts.

- Sabiendo que NCP no era apropiado para una afluencia masiva de hosts, los investigadores en DARPA empezaron a trabajar en un nuevo protocolo que fuera capaz de manejar grandes números de usuarios y TCP/IP nacía a mediados de los 70's. Esta tecnología más sofisticada era aceptada por el gobierno de los E.U. en 1978 y TCP/IP se convertía en la herramienta de red preferida.

- Una vez que los protocolos TCP/IP se establecieron mucho del software y los servicios que existen en Internet aparecieron. Los servicios básicos para conectividad remota y correo electrónico aparecieron en 1972 y el protocolo

- Muchas personas vieron como el día 1 de Enero de 1983 toda la red ARPANET era reemplazada de NCP a TCP, dando el inicio "oficial" de Internet.

- En 1983 ARPANET era dividida en dos partes una conservaba el mismo nombre y la otra tomaba el nombre de MILNET (Red Militar), el Departamento de Defensa continuo auspiciando ambas redes.

- En 1983 TCP/IP para su amplia difusión en incorporado en la versión UNIX 4.2 de Berkeley, la cual es licenciada a bajo costo e inclusive gratis a muchas universidades.

- A principio de los años 80's, surgieron muchas redes que no se basaban en la familia de protocolos TCP/IP, como CSNET, BITNET, y muchas más, las cuales posteriormente si se pudieron comunicar con ARPANET aunque de una manera parcial, utilizando gateways o compuertas para intercambiar correo electrónico.

- Para 1984 la red ya contaba con aproximadamente 1000 hosts.

- En 1986 la Fundación Nacional de la Ciencia (NSF) crea la NSFNET, una red TCP/IP que utilizaba líneas telefónicas de 56kbps, para conectar sus centros de supercomputo. Poco después con el fin de enlazar a la universidades que no tenían acceso a Internet, implementa un modelo de enlace tomando a NSFNET como backbone principal, al cual se conectaban redes regionales y finalmente a éstas se enlazaban las redes de las universidades.

- Aunque originalmente, la NSF deseo incorporar su red a ARPANET, pero debido a un numero de dificultades políticas y técnicas no lo pudo realizar, pasado un poco de tiempo después finalmente lo logra.

- Para 1987 a consecuencia de la gran cantidad de trafico circulante por la red, baja el desempeño del backbone NSFNET y se decide darle más poder. Para este fin, la NSF emite una convocatoria para aquellos que estuvieran interesados en establecer y operar un nuevo backbone. Otorgándose a una sociedad constituida por IBM, MCI, MERIT Network Inc., y el Estado de Michigan.

- En Julio de 1988 empieza a operar el segundo backbone NSFNET corriendo a una velocidad de 1.544 Mbps

- 1989 ve como crece exponencialmente la red, ya que de los 10,000 hosts instalados en 1987 para 1989 se tenia la cantidad de 100,000. En este año México se enlaza a la NSFNET y surge el primer prototipo del servicio World Wide Web.

- Junio de 1990, el backbone ARPANET dejaba de funcionar como tal, siendo rebasado en su servicio y reemplazado por el backbone NSFNET. En este año el gobierno de los E.U. decide ya no auspiciar a Internet y empieza una política de privatización y comercialización de la red.

- Atendiendo al llamado anterior IBM, MERIT y MCI forman una sociedad no lucrativa denominada ANS (Advanced Network and Services, Red Avanzada y Servicios) y toma a Internet, pero con la supervisión de NSF..

- En 1991 ANS actualiza a NSFNET con un velocidad de 45 Mbps y la denomina ANSNET.

- En 1992, Internet rompe la marca del millón de hosts instalados. NSF toma la decisión de regresar a cumplir con el objetivo para el cual fue creada, es decir, a su misión de apoyar las iniciativas de investigación y educación en E.U. para el desarrollo de tecnología de punta, y dejar su papel de patrocinador y operador de la red. Para lo cual emite otra convocatoria con el fin de encontrar a alguien que desarrollara un proyecto nacional de red, estableciendo una nueva arquitectura para Internet a través de redes comerciales.

- Los primeros años de la década de los 90's ha visto el crecimiento exponencial del numero de hosts en Internet, ya que para Marzo de 1995 se rompía la barrera de los 4,000,000 de hosts abarcado cerca de 150 paises.

- El 30 de Abril de 1995, el gobierno estadounidense y las organizaciones que habían construido a Internet desde el principio, lo abandonan, deja de operar ANSNET y el trafico Internet es manejado en una nueva estructura a través de redes comerciales.

- Internet es una red de conmutación de paquetes, esta tecnología divide grandes secciones de datos (mensajes) en pequeñas partes llamadas paquetes, cada uno etiquetado con una dirección de origen y destino. Así pueden ser enviados en cualquier orden y a través de diferentes rutas dentro de la red las cuales llevan al mismo destino. Llegando a la computadora de destino, los paquetes son reensamblados al mensaje original.

- Las direcciones utilizadas en Internet para identificar a cada uno de los host se denominan Direcciones IP, constituidas de 32 bits las cuales se escriben en un

formato de cuatro octetos codificados en decimal separados por puntos, para facilitar su interpretación por parte de los usuarios. Una autoridad central las administra. Existen 5 clases diferentes de direcciones IP, pero para identificar a un host de la red sólo se utilizan 3 de ellas. La dirección IP otorgada a una red se asigna de acuerdo al numero de computadoras que tiene dicha red.

- El software de red generalmente necesita una dirección IP de 32 bits para abrir una conexión o enviar un datagrama, sin embargo los usuarios prefieren tratar con nombres de computadoras en lugar de números. Así, existe una base de datos distribuida de nombres de computadoras dentro de Internet que permite que el software localice el nombre y como resultado se obtenga la dirección IP correspondiente. Este mecanismo se conoce como el Sistema de Nombres de Dominio (DNS), y es un método jerárquico distribuido de organización del espacio de nombres de Internet.

- Para poder llevar a cabo las complejas funciones de comunicación dentro de la red se requiere de un conjunto de protocolos, generalmente estos están conceptualmente uno encima del otro formando una pila, cada uno de estos protocolos tiene una función especial en la transmisión y recepción de los paquetes hacia el host destino. Internet se basa en el conjunto de protocolos TCP/IP (Protocolo Control de Transmisión/ Protocolo Internet) para llevar a cabo esta función.

- El término genérico TCP/IP usualmente significa todo y cualquier cosa relacionada con los protocolos TCP e IP. Incluye otros protocolos, aplicaciones, y aun el medio físico de red. Un ejemplo de estos protocolos son UDP, ARP, ICMP, etc. Como ejemplo de las aplicaciones se tiene a Telnet, FTP, correo electrónico, etc.

- El Protocolo Control de Transmisión (TCP) es el responsable de romper los mensajes en datagramas, reensamblandolos en el sitio destino, reenviando cualquier paquete que se haya perdido, y ordenándolos correctamente. TCP provee servicios de comunicación full-duplex, control de flujo y acuses de recibo para los protocolos de

aplicación. TCP es un protocolo de transporte orientado a la conexión, es decir, debe existir un circuito previo entre el emisor y receptor para poder enviar la información.

- El otro protocolo de transporte de la familia de protocolos TCP/IP es el Protocolo de Datagrama de Usuario (UDP). Es mucho más simple que el protocolo TCP y es útil en situaciones donde los mecanismos de confiabilidad de TCP no son necesarios. Es un protocolo sin conexión.

- EL Protocolo Internet (IP) define al datagrama como la unidad básica de transferencia de datos usada a través de un internet. El software IP es el responsable del enrutamiento de los datagramas y también define un conjunto de reglas que definen como deben tanto los hosts como los ruteadores procesar los paquetes; como y cuando se deben generar los mensajes de error, y las condiciones bajo las cuales los paquetes deben ser descartados.

- El Protocolo Internet de Control de Mensajes (ICMP), es una parte integral de protocolo IP y se encarga de manejar los mensajes de error y control. Específicamente, los ruteadores y hosts usan ICMP para enviar reportes de problemas (en el manejo de datagramas) de regreso a la fuente original que envío el datagrama.

- Las direcciones IP son asignadas independientemente de las direcciones físicas del hardware (tarjetas de interface). Para enviar un paquete a través de una red física de una computadora a otra, el software de red debe mapear la dirección IP (software) a una dirección física de interface de red y utilizar la dirección física para transmitir la información en un frame físico para que finalmente sea entregada al host destino. El Protocolo de Resolución de Direcciones (ARP) ejecuta la traducción o resolución dinámica de las direcciones IP a direcciones físicas, utilizando sólo el sistema de comunicación de bajo nivel de la red.

- El ruteo IP consiste en la toma de decisión de hacia donde se va a enviar un datagrama, basándose en la dirección IP de destino del datagrama. Un ruteo directo es posible si la máquina de destino reside en la red a la cual la máquina emisora

pertenece (paso final en la entrega de un datagrama al host destino). Si el emisor no puede alcanzar el destino directamente, éste debe entregar el datagrama a un ruteador. Los datagramas viajan a través de Internet de ruteador a ruteador hasta que puede ser entregado directamente a través de una red física.

- El algoritmo de ruteo Internet está basado en una tabla, que contiene sólo la porción identificadora de red de las direcciones IP. Mediante este mecanismo se mantienen pequeñas las tablas de ruteo.

- Para asegurarse que todas las redes permanezcan alcanzables con alta confiabilidad, un internet debe proveer un ruteo global consistente. El Internet resuelve el problema de ruteo utilizando una arquitectura central de ruteadores, los cuales contienen una información completa de todas las redes.

- Los ruteadores en forma continua y dinámica intercambian información de ruteo, permitiéndoles tener información actualizada y consistente de la topología de la red.

- Cuando los ruteadores intercambian información usualmente utilizan uno de dos algoritmos básicos: vector distancia o la ruta más corta primero. El término vector distancia se deriva de la información periódica enviada por parte de los ruteadores el cual consiste de una lista de pares (V,D), donde V identifica un destino de red y D es la distancia a tal destino (el número de ruteadores que se tienen que cruzar los paquetes para llegar al destino). El algoritmo la Ruta más corta primero ejecuta dos tareas principales, primero, activamente prueba el estado del enlace de todos los ruteadores vecinos y segundo periódicamente propagan el estado del enlace a otro ruteadores.

- El Internet está compuesto de un conjunto de sistemas autónomos, donde cada sistema autónomo consiste de ruteadores y redes bajo una autoridad administrativa. A los ruteadores que se ubican dentro de un sistema autónomo se les conoce como ruteadores internos.

- Con el fin de mantener una adecuada consistencia de las rutas de un sistema autónomo, los ruteadores internos utilizan protocolos conocidos como protocolos de compuerta interior para mantener actualizadas sus tablas. Los protocolos de compuerta interior que destacan principalmente son el RIP (El Protocolo de Enrutamiento de Información) y el protocolo OSPF (Abre la Ruta más corta Primero).

- De la misma forma que existen ruteadores internos, existen ruteadores exteriores los cuales se encargar de difundir las rutas de un sistema autónomo a otro.

- Un sistema autónomo utiliza el Protocolo de Compuerta Exterior (EGP) para anunciar sus rutas, a otros sistemas autónomos. Otro protocolo de compuerta exterior lo constituye el Protocolo de Compuerta de Frontera (BGP).

- Los servicios y aplicaciones dentro de Internet están implementados por medio de protocolos. Generalmente los servicios siguen un esquema cliente/servidor.

- Mucho de la rica funcionalidad asociada con TCP/IP resulta de una variedad de servicios de alto nivel suministrados por programas de aplicación. Entre los principales servicios destacan el correo electrónico, la transferencia de archivos y el login remoto.

APÉNDICE A

DIRECCIONES ELECTRÓNICAS DE INTERÉS

TELNET

Como se ha mencionado Telnet es un servicio que permite usar el poder de Internet para conectarse a bases de datos, catálogos de librerías y otros recursos de información alrededor del mundo. A continuación se presentan como ejemplo algunos de los servicios a los que se puede accesar en Internet por medio de Telnet.

Agricultura

telnet psupen.psu.edu
User name: PNOTPA

Mantenido por el Colegio de Ciencias Agrícolas de la Universidad Estatal de Pennsylvania, provee de un reporte semanal acerca del clima y las cosechas de diversos cultivos a nivel mundial. Estos reportes detallan todo desde el efecto del clima en las palmas en Malasia hasta el estado de la cosecha de trigo en Ucrania.

Sida

telnet callcat.med.miami.edu
Log in: library

La Universidad de Miami mantiene una base de datos de las clínicas especializadas en el tratamiento del Sida.

Arte

telnet ursus.maine.edu

Login: ursus

La Galería Nacional de Arte en Washington mantiene una base de datos de sus obras, las cuales se pueden buscar por artistas (Van Gogh, por ejemplo) o Estilo (acuarelas, óleos, etc.)

Calculadoras

telnet hpcvbbs.cv.hp.com
No requiere login

Hewlett-Packard mantiene un servicio gratuito con el cual se puede buscar ayuda acerca de su línea de calculadoras.

El Espacio

telnet spacelink.msfc.nasa.gov

La NASA Spacelink en Huntsville, Alabama, proporciona todos los reportes y datos acerca de la NASA, su historia y sus misiones. Se encuentran reportes detallados sobre cada viaje de exploración

telnet ipac.caltech.edu
Log in: ned

La base de datos NED-NASA/IPAC provee información de más de 100,000 galaxias, quazares y otros objetos que se ubican fuera de vía Láctea

Direcciones Telnet

telnet access.usask.ca
Log in hytelnet

Hytelnet, en la Universidad de Saskatchewan en Canadá, es una guía en línea de cientos de sitios Telnet alrededor del mundo

Localizando a Alguien en la Red

Aunque hay una variedad de servicios de directorios de "paginas blancas" disponibles en Internet, están lejos de ser completos. Pero por el momento existe un par de servicios de "paginas blancas" que pueden servir para localizar a alguien, o para entretenerse buscando gente famosa.

El directorio whois provee nombres, direcciones de correo electrónico, números telefónicos de las personas listadas en él. Para utilizarlo hay que escribir:

telnet internic.net
No necesita login

La forma más rápida de utilizarlo es escribir

whois nombre
donde "nombre" es el apellido o el nombre de la organización que se está buscando.

Otro servicio es el sistema "knowbot" accesible por Telnet

telnet nri.reston.va.us 185
No necesita login

Este servicio actualmente busca a través de una variedad de sistemas de "paginas blancas", incluyendo el directorio de usuarios de MCIMail. Para buscar por alguien se escribe

query nombre

"nombre" es el apellido de la persona que se está buscando.

SITIOS FTP ANÓNIMOS

Un sitio FTP anónimo es un servidor conectado a Internet, el cual contiene muchos archivos de dominio público así como software. Se pueden obtener imágenes, sonidos, documentos y muchas otras cosas. A continuación se muestra algunos sitios FTP muy populares dentro de Internet.

wuarchive.wustl.edu

Este es el sitio FTP más grande en América. Se pueden encontrar programas muy útiles para MS-DOS, Windows, Mac, y otros sistemas. Un gran directorio de juegos para MS-DOS esta disponible. Como este sitio es muy popular en ocasiones es difícil de accesar principalmente en horas pico.

oak.oakland.edu

Otro sitio con gran cantidad de software para MS-DOS

ftp.borland.com

Este es el sitio de la empresa de software Borland. Se pueden encontrar ejemplos, pequeños programas, documentos de texto.

sunsite.unc.edu

Este sitio reúne casi todos los archivos disponibles para Linux (un clon de UNIX para PC) y UNIX en general

step.polymtl.ca

Contiene el software PSPICE el cual es útil para algunos cursos de circuitos eléctricos. También se puede encontrar software antivirus de McAfee. Este sitio está muy completo con respecto a Linux.

mcafee.com

Una de las empresas mas grandes desarrolladoras de productos antivirus, pone a la disposición del publico Internet algunos de sus productos más populares.

nic.funet.fi

Este sitio ofrece varios archivos relacionados con el sistema operativo OS/2. También hay un gran cantidad de imágenes en formato jpeg.

ARCHIE

Archie, cuyo nombre viene del inglés "archive" que quiere decir archivo, permite buscar un archivo dentro de los índices que mantienen los servidores FTP anónimos. Se requiere que el usuario de exactamente el nombre y extensión del archivo que desea. Hay varios servidores archie dentro de la red que pueden ser accesados por los usuarios, ya sea mediante un programa cliente gráfico el cual facilita grandemente el trabajo de seleccionar un servidor, o mediante Telnet en línea de comando como UNIX que requiere la palabra "archie" en respuesta a la solicitud del login y no necesita password. A continuación se da una lista de servidores archie distribuidos en varias partes del mundo.

Nombre del servidor	Dirección de la computadora	País
archie.ac.il	132.65.20.254	Israel
archie.ans.net	147.225.1.10	Estados Unidos
archie.au	139.130.4.6	Australia
archie.doc.ic.ac.uk	146.169.11.3	Reino Unido
archie.edvz.uni-linz.ac.at	140.78.3.8	Austria
archie.funet.fi	128.214.6.102	Finlandia
archie.hensa.ac.uk	129.12.200.130	Reino Unido
archie.internic.net	198.49.45.10	Estados Unidos
archie.kr	128.134.1.1	Corea
archie.kuis.kyoto-u.ac.jp	130.54..20.1	Japón
archie.luth.se	130.240.18.4	Suecia
archie.ncu.edu.tw	140.115.19.24	Taiwan
archie.nz	130.195.9.4	Nueva Zelanda
archie.rediris.es	130.206.1.2	España
archie.rutgers.edu	128.6.18.15	Estados Unidos
archie.sogang.ac.kr	163.239.1.11	Corea
archie.sura.net	128.167.254.195	Estados Unidos
archie.switch.ch	130.59.1.40	Suiza
archie.th-darmstadt.de	130.83.22.60	Alemania
archie.unipi.it	131.114.21.10	Italia
archie.univie.ac.at	131.130.1.23	Austria
archie.unl.edu	129.93.1.14	Estados Unidos
archie.uqam.ca	132.208.250.10	Canadá
archie.wide.ad.jp	133.4.3.6	Japón

GOPHER

Gopher presenta una variedad extremadamente amplia de diversos tipos de información en una interface a base de menús fácil de manejar. Los servidores gopher reúnen información de todo el Internet de una manera transparente para el usuario. Algunos servidores gopher (principalmente basados en modo carácter) están disponibles vía Telnet, pero también existen aplicaciones cliente (gráficas) que se comunican directamente con el servidor. A continuación se da una lista de algunos servidores gopher.

Nombre del servidor	Perteneciente a:
gopher.micro.umn.edu	Universidad de Minesota
condor.dgsca.unam.mx	UNAM (Dirección General de Servicios de Cómputo Académico)
gopher.ccu.umich.mx	Universidad de Michoacán
gopher.dsi.uanl.mx	Universidad Autónoma de Nuevo León
tonatiuh.uam.mx	Universidad Autónoma Metropolitana
leo.uacj.mx	Universidad Autónoma de Ciudad Juárez
procesos.esiqie.ipn.mx	Instituto Politécnico Nacional
gopher.mty.itesm.mx	Instituto Tecnológico y De Estudios Superiores de Monterrey
gan.nnc.go.jp	Centro Nacional Contra el Cáncer (Japón)
tolten.puc.cl	Universidad Pontificia de Chile
info.anu.edu.au	Australia
panda.uiowa.edu	Universidad de Iowa
rs.internic.net	INTERNIC
gopher.uiuc.edu	Universidad de Illinois en Urbana Champain
gopher.unipi.it	Italia

VERONICA

Veronica es un sistema de búsqueda automático disponible a través de Gopher. Generalmente es incluido como una opción dentro de un menú gopher. Veronica permite buscar por una palabra, y regresa un menú gopher con los resultados obtenidos a partir de muchos servidores gopher consultados (generalmente la mayoría de los gophers están enlazados entre sí).

Cuando alguien utiliza el servicio y da una la palabra para su búsqueda, es equivalente a decirle a Veronica qué: "por favor localice todas las entradas (items) en los menús gopher que contengan la palabra solicitada".

Las búsquedas usualmente se hacen por medio de una sola palabra, pero también se pueden hacer búsquedas boleanas utilizando "and", "or" y "not". Por ejemplo, para buscar por la palabra *salud* relativa a la *mujer* o la *familia* se escribiría:

salud and (mujer or familia).

A continuación se da una lista de algunos sitios gopher que incluyen en su menú la opción de búsqueda Veronica.

- condor.dgsca.unam.mx
- gopher.dsi.uanl.mx
- consultant.micro.umn.edu
- gopher.micro.umn.edu
- gopher.uiuc.edu
- info.anu.edu.au
- veronica.scs.unr.edu
- nysernet.org
- gopher.unipi.it
- gopher.uib.no
- gopher.psi.com
- veronica.uni-koeln.de
- veronica.uib.no
- veronica.utdallas.edu
- gopher.cc.umanitoba.ca

WAIS

WAIS (Wide Area Information Server, Servidor de Información de Área Amplia) es un servicio de búsqueda automático de documentos. WAIS permite tanto palabras clave como frases completas para solicitar la búsqueda de un documento. La ventaja de WAIS radica en que busca tanto en el titulo o nombre de los archivos, como en el contenido de ellos. WAIS puede ser utilizado por medio de un programa cliente (generalmente gráfico), o en línea de comando mediante Telnet. La siguiente lista muestra algunos servidores WAIS dentro de Internet.

Nombre del servidor	Login (sólo en línea de comando)	País
info.funet.fi	wais	Finlandia
wais.nis.garr.it	wais	Italia
swais.cwis.uci.edu	swais	Estados Unidos
wais.com	wais	Estados Unidos
sunsite.unc.edu	swais	Estados Unidos
quake.think.com	wais	Estados Unidos
nctuccca.edu.tw	wais	Taiwan

que todos los datos lleguen al receptor en forma correcta (por eso el término confiable), para lo cual el emisor requiere de acuses de recibo de parte del receptor para cada uno de los segmentos que recibe.

Telnet: Protocolo Internet estándar para el servicio de conexión de terminal remota. Telnet permite a un usuario en un sitio, interactuar con un sistema remoto de tiempo compartido ubicado en otro sitio, como si la terminal estuviera conectada directamente a la computadora remota.

UDP: Protocolo de Datagrama de Usuario. Es uno de los dos protocolos de la capa de transporte de la familia de protocolos TCP/IP. UDP, como TCP, utiliza IP para la entrega de paquetes; sin embargo, a diferencia de TCP, UDP no prevé en la entrega de datagramas acuses de recibo por parte del receptor, y tampoco garantiza la de entrega de los mismos.

Veronica: Servicio automático de búsqueda disponible a través de gopher. Veronica permite a un usuario buscar a través de menús gopher por una cadena dada. Debido a que veronica ha sido integrado con gopher, un usuario puede usarlo para accesar veronica y desplegar los resultados de la búsqueda.

WAIS: Servidor de Información de Área Amplia. Servicio de búsqueda automático que permite a un usuario localizar documentos que contienen palabras clave o frases. WAIS a diferencia de gopher y veronica busca dentro de los documentos y no solamente en el nombre de los archivos.

World Wide Web (WWW): Servicio a gran escala en Internet que organiza la información utilizando hipertexto. Cada documento puede contener referencias a imágenes, audio, u otros documentos (razón por la cual ha surgido el término hipermedia, es decir, un documento tiene una combinación de hipertexto y elementos multimedia). Para seguir las referencias dentro del documento o página el usuario utiliza un programa denominado navegador como Mosaic, Netscape, Explorer, etc.

APÉNDICE B

GLOSARIO

Archie: Servicio de búsqueda automático disponible en Internet que encuentra todos los archivos con un nombre dado, ubicados en los sitios FTP anónimos. El nombre archie se deriva de archive=archivo.

ARP: Protocolo de Resolución de Direcciones. Protocolo utilizado para mapear dinámicamente direcciones IP a direcciones físicas (hardware) en redes de área local. Limitado a redes que soportan hardware de difusión (broadcast) como Ethernet.

ARPA: Agencia de Proyectos Avanzados de Investigación. Ahora denominada DARPA, agencia gubernamental de Estados Unidos que fundo ARPANET.

ARPANET: Red de conmutación de paquetes desarrollada a principios de los 70s. Se considera el "abuelo" de lo que es ahora Internet. ARPANET dejo de operar en Junio 1990.

ASCII: Código Estándar Americano para el Intercambio de Información. Código binario de 7 bits utilizado para representar 128 caracteres, incluye las letras del alfabeto (mayúsculas y minúsculas), los 10 dígitos numéricos, códigos de control no imprimibles y signos de puntuación. Los códigos de control no imprimibles sirven para controlar la operación de los dispositivos receptores.

ATM: Modo de Transferencia Asíncrona. Técnica de conmutación por paquetes de alta velocidad adecuada para redes de área metropolitana. ATM tiene la ventaja potencial de poder transmitir voz, vídeo y datos en el mismo canal.

Backbone: Termino utilizado para referirse a una red central que contiene muchos ruteadores, a los cuales se conectan redes más pequeñas. El backbone soporta la mayoría del trafico que circula por la red.

BBN: Bolt Beranek and Newman, Inc. La compañía responsable del desarrollo, operación y monitoreo de ARPANET, y después, del sistema central de ruteadores de Internet.

BGP: Protocolo de Compuerta de Frontera. Protocolo utilizado por el ruteador exterior de un sistema autónomo, para transmitir información de las direcciones IP de tal sistema, a un ruteador exterior en otro sistema autónomo.

Broadcast: Sistema de entrega de paquetes donde una copia de un paquete es dado a todos los hosts enlazados de la red, por ejemplo Ethernet.

Cliente/servidor: modelo de interacción en un sistema distribuido en el cual un programa en un sitio envía una solicitud de servicio a otro programa en otro sitio y espera una respuesta. El programa solicitante es denominado un cliente; el programa que responde a la solicitud es denominado servidor. Adviértase la diferencia con procesamiento centralizado, donde las terminales (sin poder de procesamiento) se conectan a una macrocomputadora (mainframe)

Compuerta: Dentro del contexto de Internet, es el término original para lo que ahora se conoce como ruteador o más precisamente, ruteador IP. En la actualidad, el termino compuerta (dispositivo físico) y "aplicación compuerta" se refiere a los sistemas que hacen traducción de un formato nativo a otro formato.

CSMA/CD: Portadora Sensa Múltiples Accesos/Detección de Colisión. El método de acceso utilizado por las tecnologías de redes de área local tales como Ethernet.

DARPA: Agencia de Proyectos Avanzados de Investigación de la Defensa de los Estados Unidos, ver ARPA.

Datagrama IP: Unidad fundamental de información pasada a través de Internet. Contiene las direcciones de los hosts fuente y destino, los datos de usuario y un número adicional de campos que definen la longitud del datagrama, la suma de verificación del encabezado para detectar errores, banderas, etc. Un datagrama IP es a un internet como lo es un paquete de hardware a una red física.

Dirección Internet o IP: Número de 32 bits que se asigna a cada computadora que participa en un internet TCP/IP. Las direcciones IP son la abstracción de las direcciones físicas de hardware, tal como un internet es una abstracción de redes físicas. Para hacer el enrutamiento más eficiente, cada dirección IP está constituida por dos partes, una parte que identifica el número de la red y otra que identifica un host dentro de ésta.

DNS: Sistema de Nombres de Dominio. Mecanismo distribuido de traducción de nombres de dominio a direcciones IP utilizado en Internet.

Dominio: Una parte de una jerarquía de nombres. Sintácticamente, un nombre de dominio Internet consiste de una secuencia de nombres (etiquetas) separados por puntos, por ejemplo, servidor.dgsca.unam.mx

EBCDIC: Código binario que está constituido por 8 bits y que admite 256 combinaciones de caracteres. Fue inventado por IBM y se emplea ampliamente en sus computadoras y en dispositivos compatibles con ellas. EBCDIC y ASCII son los principales métodos para la codificación de caracteres.

EGP: Protocolo de Compuerta Exterior. Protocolo de enrutamiento utilizado por un ruteador exterior en un sistema autónomo, para anunciar las direcciones IP de las redes de tal

sistema a un ruteador exterior en otro sistema autónomo.

Encapsulacion: Técnica utilizada por protocolos estratificados en la cual cada capa agrega información de encabezado a la unidad de datos proveniente de la capa superior. Esta agregación de información cabe aclarar que se hace en la transmisión de los datos, es decir, cuando circulan en forma descendente a través de la pila de protocolos.

Estándar: Criterio común establecido por acuerdo, regla, tradición o prueba de rendimiento. Sirve de modelo en la medición, elaboración de un producto o establecimiento de un procedimiento.

Ethernet: Tecnología de red de área local inventada por la Corporación Xerox. Un Ethernet consiste de un cable al cual se enlazan las computadoras. Cada computadora necesita de un elemento de hardware conocido como tarjeta de interface o red para poder conectarla al Ethernet. Ethernet implementa al estándar CSMA/CD y se transmite a 10 Mbits/seg.

Finger: Un servicio de Internet utilizado para determinar que usuario está en sesión en un sistema (computadora) dado, también se utiliza para buscar más información sobre un usuario en la red, por ejemplo, nombre completo, teléfono, dirección, etc.

Fragmentacion: Proceso en el cual un datagrama IP es dividido en pequeñas piezas para cumplir los requerimientos de una red física dada. El proceso contrario se denomina reensamblaje.

Frame: Grupo de bits que constituyen un bloque elemental de datos para su transmisión mediante ciertos protocolos. El término se deriva de los protocolos orientados a carácter, que agregan un carácter especial al inicio y al final de un paquete para su transmisión a través del medio físico. El término se emplea a lo largo de este trabajo para referirse a los objetos que las redes físicas ocupan para transportar los datos a través del medio físico.

FTP anónimo: Es un sistema que permite a un usuario de Internet tener acceso a archivos de determinados sitios FTP denominados "públicos". El usuario solamente requiere que de como nombre de entrada (login) en la computadora anfitriona la palabra anonymous (anónimo) y como password su clave de correo electrónico.

FTP : Protocolo de Transferencia de Archivos. Protocolo Internet (y programa) utilizado para transferir archivos entre hosts.

Gopher: Servicio de Internet, en el cual toda la información está organizada dentro de menús. Gopher despliega un menú en la pantalla del usuario y le permite seleccionar una entrada. La selección lleva al usuario ya sea a un archivo de información, a otro servicios como veronica o Telnet, o a otro menú.

Hipertexto: Sistema en el que los documentos cuentan con enlaces mediante los cuales el lector puede desplazarse a través de diversas áreas de la documentación respectiva, lo que permite hacer el seguimiento de un tema de interés a través de diversas rutas.

Host: Un sinónimo para computadora del usuario. Técnicamente, cada computadora

conectada a Internet está clasificada como un host o un ruteador.

IAB: Consejo de Actividades Internet. El cuerpo técnico que inspecciona el desarrollo de la familia de protocolos de Internet (comúnmente referida como TCP/IP). Tiene dos cuerpos (fuerzas) de trabajo (la IRTF y la IETF) cada una encargada de la investigación de una área particular.

ICMP: El Protocolo Internet de Control de Mensajes. Protocolo utilizado para manejar los errores y mensajes de control en la capa IP.

IEFT: Fuerza de Trabajo de Ingeniería Internet. Grupo de personas que trabajan en el diseño e ingeniería de TCP/IP e Internet. El IEFT está dividido en áreas, las cuales tienen un director. Las áreas están adicionalmente divididas en grupos de trabajo.

IGP: Protocolo de Compuerta Interior. Término genérico aplicado a cualquier protocolo utilizado para propagar información de accesibilidad a una red, así como información de enrutamiento; todo esto dentro de un sistema autónomo

Internet: Es la colección global de redes y ruteadores que usan la familia de protocolos TCP/IP, y que funcionan como una sola red cubriendo gran parte del mundo.

internet: Físicamente, es un conjunto de redes locales o de área amplia interconectadas por medio de ruteadores y que utilizan una serie de protocolos como TCP/IP, que les permite funcionar lógicamente como una sola red (es por eso, que también se denominan redes virtuales). Cuando se escribe con "I" se refiere específicamente a la red global que adoptó este término como nombre.

INTERNIC: Es la organización que provee información acercar de los servicios de Internet y los documentos que describen los protocolos. Además, maneja el registro de las direcciones IP y los nombres de dominio.

IP: Protocolo Internet. Protocolo correspondiente a la capa de red para la familia de protocolos Internet. Define al datagrama IP como la unidad de información que pasa a través de un internet y provee las bases para el servicio de entrega y enrutamiento de datagramas. Se incluye como una parte integral de IP, el protocolo de control y mensajes de error (ICMP).

IRTF: Fuerza de Trabajo de Investigación Internet. Grupo responsable de la investigación y desarrollo de la familia de protocolos Internet.

Mapear: Conjunto de datos que tiene que tiene una relación de correspondencia con otro conjunto de datos

MIME: Extensiones de Correo Internet de Multiproposito. Un estándar utilizado para codificar datos que no son de texto (binarios) tales como imágenes, archivos de audio, etc., en código ASCII (texto) para su transmisión a través de correo electrónico.

MTU: Unidad Máxima de Transferencia. Es la unidad de datos más grande posible que

puede ser enviada en un medio físico dado. Por ejemplo, el MTU de Ethernet es de 1500 bytes.

NIC: Centro de Información de la Red. Es una organización que proporciona a los usuarios de una red información relacionada con los servicios que ésta ofrece. Actualmente el centro de información de la red de internet se denomina INTERNIC.

NOC: Centro de Operaciones de la Red. Es la organización responsable del mantenimiento de la red.

Notación decimal con punto: Representación para una dirección IP de 32 bits, que consiste de cuatro números de 8 bits escritos en base 10 separados con puntos, por ejemplo, 192.67.67.20

NSF: Fundación Nacional para la Ciencia. Agencia gubernamental de Estados Unidos que fomento parte del desarrollo de Internet mediante el patrocinio de algunas investigaciones.

OSPF: Abrir la Ruta Más Corta Primero. Protocolo de compuerta interior, implementa al algoritmo de enrutamiento que tiene el mismo nombre.

Paquete: Término genérico empleado para referirse a los datos transferidos a través de una red. El término es utilizado con inexactitud. Mientras parte de la literatura de Internet lo utiliza para referirse específicamente a los datos enviados a través de una red física, otra parte que ve a Internet como una red de conmutación de paquetes describe a los datagramas IP como paquetes.

Protocolo: Descripción formal de las reglas que dos computadoras deben seguir para intercambiar mensajes. Un protocolo describe tanto el formato de los mensajes que pueden ser enviados así como la forma que una computadora debe responder a cada mensaje. Los protocolos pueden describir detalles de bajo nivel de interfaces máquina a máquina (por ejemplo, el orden en el cual los bits y bytes son enviados a través de un cable) o intercambios de alto nivel entre programas (por ejemplo, la forma en la cual dos programas transfieren un archivo a través de Internet)

Puerto de protocolo: Es la abstracción que los protocolos de transporte de TCP/IP usan para distinguir entre múltiples destinos (generalmente aplicaciones) dentro de la computadora destino. Los protocolos TCP/IP identifican los puertos mediante números enteros positivos. Usualmente el sistema operativo permite a un programa de aplicación especificar que puerto desea utilizar. Algunos puertos están reservados para servicios estándar como correo electrónico, FTP, Telnet, etc.

Red : Conjunto de dispositivos interconectados que se comunican a través de un medio como cables, líneas telefónicas, ondas de radio, etc., con el fin de compartir recursos entre ellos.

Red de área amplia (WAN): Red que cubre grandes distancias geográficas como estados y países. Las redes WAN usualmente operan a un velocidad más lenta y tiene retardos significativamente más altos que las redes que operan en distancias más cortas.

Red de área local (LAN): Cualquier tecnología de red física diseñada para cubrir pequeñas distancias (hasta algunos cientos de metros), como Ethernet y Token Ring.

Red de área metropolitana (MAN): Red que soporta altas velocidades (usualmente de los cientos de megabits por segundo hasta varios gigabits por segundo), y que cubre un área geográfica equivalente a una ciudad.

RFC: Documentos Solicitud de Comentario. Es el nombre que se le da a un serie de documentos que contienen especificaciones y estándares correspondientes a los protocolos TCP/IP. Los RFCs también se usan para proponer nuevos protocolos, presentar ideas, técnicas, experimentos, etc. Los RFCs están disponibles al usuario en varios sitios dentro de la red, por ejemplo, en el Centro de Información de la Red Internet (INTERNIC).

RIP: Protocolo de Información de Enrutamiento. Protocolo utilizado para propagar información de enrutamiento entre los ruteadores que están dentro de un sistema autónomo.

Ruteador exterior: Es el ruteador que se encarga de difundir las direcciones IP de las redes del sistema autónomo al cual se enlaza, a otro sistema autónomo.

Ruteador interior: Es el ruteador que se encarga de difundir información de enrutamiento a otros ruteadores ubicados dentro de su mismo sistema autónomo.

Ruteador : Dispositivo de propósito especial que enlaza dos o más redes y es el responsable de hacer decisiones sobre cual de varias rutas posibles dirigirá el trafico. Para hacer esto utiliza un protocolo de enrutamiento con el cual obtiene información acerca de la red y algoritmos para elegir la mejor ruta basado en varios criterios conocidos como "métricas de enrutamiento". Un ruteador utiliza la dirección de destino de un datagrama para elegir el siguiente ruteador que dirigirá el datagrama rumbo al host destino. Los investigadores originales utilizaron el termino *compuerta IP*.

Sistema Autónomo: Colección de redes y ruteadores controlados por una autoridad administrativa. El sistema por lo general utiliza un protocolo de compuerta interior común y difunde sus rutas a otros sistemas mediante un ruteador denominado exterior.

SMTP: Protocolo Simple de Transferencia de Correo. Protocolo estándar para transferir mensajes de correo electrónico de una máquina a otra. SMTP especifica como deben interactuar dos sistemas de correo, y también define el formato de los mensajes de control que deben intercambiar para poder transferir correo electrónico.

TCP: Protocolo de Control de Transmisión. Es el protocolo estándar de la capa de transporte de la familia de protocolos Internet, que provee de un servicio de flujo de datos confiable full-duplex (transmisión y recepción simultánea), del cual muchas aplicaciones dependen. TCP es un protocolo orientado a la conexión en el sentido que antes de transmitir datos los participantes (emisor y receptor) deben establecer una conexión o un "circuito". Todos los datos de la capa de aplicación viajan en segmentos TCP, los cuales a su vez viajan a través de Internet en un datagrama IP. TCP maneja la tarea de asegurar

que todos los datos lleguen al receptor en forma correcta (por eso el término confiable), para lo cual el emisor requiere de acuses de recibo de parte del receptor para cada uno de los segmentos que recibe.

Telnet: Protocolo Internet estándar para el servicio de conexión de terminal remota. Telnet permite a un usuario en un sitio, interactuar con un sistema remoto de tiempo compartido ubicado en otro sitio, como si la terminal estuviera conectada directamente a la computadora remota.

UDP: Protocolo de Datagrama de Usuario. Es uno de los dos protocolos de la capa de transporte de la familia de protocolos TCP/IP. UDP, como TCP, utiliza IP para la entrega de paquetes; sin embargo, a diferencia de TCP, UDP no prevé en la entrega de datagramas acuses de recibo por parte del receptor, y tampoco garantiza la de entrega de los mismos.

Veronica: Servicio automático de búsqueda disponible a través de gopher. Veronica permite a un usuario buscar a través de menús gopher por una cadena dada. Debido a que veronica ha sido integrado con gopher, un usuario puede usarlo para accesar veronica y desplegar los resultados de la búsqueda.

WAIS: Servidor de Información de Área Amplia. Servicio de búsqueda automático que permite a un usuario localizar documentos que contienen palabras clave o frases. WAIS a diferencia de gopher y veronica busca dentro de los documentos y no solamente en el nombre de los archivos.

World Wide Web (WWW): Servicio a gran escala en Internet que organiza la información utilizando hipertexto. Cada documento puede contener referencias a imágenes, audio, u otros documentos (razón por la cual ha surgido el término hipermedia, es decir, un documento tiene una combinación de hipertexto y elementos multimedia). Para seguir las referencias dentro del documento o página el usuario utiliza un programa denominado navegador como Mosaic, Netscape, Explorer, etc.