110
24.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

"CAMPUS ARAGON"

ANALISIS DE CONECTIVIDAD A INTERNET, DESDE UNA PC STANDALONE

T E S I S

QUE PARA OBTENER EL TITULO DE :
INGENIERO MECANICO ELECTRICO
P R E S E N T A :

JOSE ADRIAN ZÚÑIGA GUZMÁN

ASESOR: ING. DAVID ESTOPIER BERMUDEZ

MEXICO **1997**

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
CAMPUS ARAGON

UNIDAD ACADEMICA

LIC. ROSA MARIA VALENCIA GRANADOS
Jefe de Carrera de Derecho,
P R E S E N T E .

En atención a su solicitud de fecha 10 de diciembre del año próximo pasado, por la que se comunica que el alumno JOSE ADRIAN ZUÑIGA GUZMAN, de la carrera de INGENIERO MECANICO ELECTRICO, ha concluído su trabajo de investigación intitulado "ANALISIS DE CONECTIVIDAD A INTERNET DESDE UNA PC STANDALONE", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión, así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, le reitero las seguridades de mi atenta consideración.

ATENTAMENTE
"POR MI RAZA HABLARA EL ESPIRITU"
San Juan de Aragón, Edo. de Méx. Enero 6 de 1997.
EL JEFE DE LA UNIDAD

LIC. ALBERTO [illegible] ROSAS

c.c.p. Asesor de Tesis.
c.c.p. Interesado

AIR*unac.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCIÓN

JOSÉ ADRIÁN ZUÑICA GUZMAN
P R E S E N T E .

En contestación a su solicitud de fecha 3 de septiembre del año en curso, relativa a la autorización que se le debe conceder para que el señor profesor, Ing. DAVID ESTOPIER BERMÚDEZ pueda dirigirle el trabajo de Tesis denominado "ANÁLISIS DE CONECTIVIDAD A INTERNET DESDE UNA PC STANDALONE", con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

ATENTAMENTE
"POR MI RAZA HABLARA EL ESPÍRITU"
San Juan de Aragón, México., 9 de septiembre de 1996.
EL DIRECTOR

M en I CLAUDIO C. MERRIFIELD CASTRO

c c p Jefe de la Unidad Académica.
c c p Jefatura de Carrera de Ingeniería Mecánica Eléctrica.
c c p Asesor de Tesis.

CCMC'AIR'lla.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO CAMPUS "ARAGON"

JEFATURA DE CARRERA DE INGENIERIA MECANICA ELECTRICA

Secretaría Técnica

ING. DAVID B. ESTOPIER BERMUDEZ (ASESOR)
ING. RAUL BARRON VERA
ING. SILVIA VEGA MUYTOY
ING. JUAN GASTALDI PEREZ
ING. ERNERTO ESCARCEGA CALZADA

ASUNTO: Revisión previa de Tesis, ante de autorizar su impresión.

En forma anexa le hago entrega de un ejemplar del proyecto de Tesis titulado: **"ANALISI: DE CONECTIVIDAD A INTERNET DESDE UNA PC STANDALONE"**, del alumn (a) : **JOSE ADRIAN ZUÑIGA GUZMAN**, con número de cuenta: **8504685-4**.

Esto con el fin de que sea revisada por Usted, y que nos de su evaluación y comentarios pc escrito, mismo que le pido me haga llegar a la brevedad posible.

Agradezco de antemano su colaboración y aprovecho la oportunidad para enviarle un cordi saludo.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
San Juan de Aragón, Edo. de Mexico, 16 de octubre de 1996

EL SECRETARIO TECNICO

ING. MIGUEL ANGEL MALDONADO MUÑOZ

c.c.p. Expediente
Alumno (a)

Introducción:

Este trabajo pretende ser una guía ó manual conciso para el manejo y utilización de la suite de Protocolos TCP/IP la cual es la base principal de muchos de los equipos que están interconectados actualmente ya que, a su vez, muchos ó la gran mayoría de usuarios están adecuando sus nuevas implementaciones para poder soportar TCP/IP, puesto que es un conjunto de protocolo que ha proporcionado una buena interoperatividad.

Antes de entrar de lleno a explicar cada uno de los puntos a tratar es bueno y conveniente dar la justificación a manera de contestación a la cuestión de la utilización de una PC sola (ó Standalone) para conectarse a una Red de servicios como Internet. Suena impactante: "Conectarse a una Red pública INTERNACIONAL" como lo es Internet, y más aún, !desde mi propia casa!. La idea pareciera ser para personas que tienen que tratar negocios Internacionales, altos ejecutivos ó políticos. Otro de los mitos que se tienen es que es una red complicadísima que solamente los que la desarrollaron ó en su defecto investigadores pueden accesar a ella. Si bien es cierto que el lenguaje UNIX en el que se basa TCP/IP no es muy digestible, tampoco es cosa del otro mundo, además hoy en día las interfaces de usuario, (entendiéndose por estas las que permiten interactuar entre las personas y las máquinas) son lo bastante "amigables" ó entendibles para que cualquiera pueda utilizarlas. Así entonces surgen las justificaciones a partir de las necesidades de cada persona. Una de las más importantes es la de tener comunicación y/o información disponible en todo momento, con la ventaja de no tener que desplazarse grandes distancias y sobre todo para gente que acostumbra llevar trabajo a casa.

Otro punto importante, por ejemplo, es la posibilidad de estar enterado de la información más reciente, a través de bancos de datos, sirviendo así para satisfacer nuestra necesidad de competitividad. Y por último es la cuestión del costo de la implementación, la cual resulta ser una opción bastante justificable, ya que se utiliza la línea telefónica convencional, una computadora que de preferencia sea con procesador 486, pero se puede utilizar una 386, un módem de al menos 9600 baud de velocidad y un software de comunicación que en la mayoría de los casos se puede conseguir con el vendedor de la cuenta de acceso a la Red Internet. Cabe hacer la aclaración de que sin alguno de estos dispositivos indispensables, la conexión no se pueda realizar.

Dentro de los primeros temas está el análisis de la utilización de la suite TCP/IP para establecer la comunicación; Aquí se contestan las primeras preguntas que surgen al leer el título de este trabajo, ¿Por que se utiliza TCP/IP para entrar a Internet?, ¿Qué es TCP/IP?, etc. Se dará una breve explicación de los términos, nomenclatura, los "modismos" utilizados y se comentarán los comandos que se pueden utilizar, su función, sus opciones y restricciones. Básicamente se realizará un comentario rápido de los comando de TCP/IP, pero a su vez dando las referencias necesarias para poder encontrar la información completa (mucha de la cual se encuentra dentro de la Internet).

Para el segundo capítulo se discutirá el medio de transmisión de la información, la cual es la línea pública telefónica, se verá porque se escogió este medio, lo que resultará bastante obvio, además de dar los estándares necesarios para poder tener una buena comunicación, esto dará pie a poder explicar como se realiza la comunicación entre PC, módem y línea telefónica, lo cual nos introduce a uno de los primeros puntos técnicos del tema que es la encapsulación de la información en paquetes ó frames tipo TCP/IP, es decir la forma como se acomoda la información (ya sea de control propio de los dispositivos y la de usuario ó datos) para poder usar un cable dedicado a transmitir voz. Todo esto sin olvidar la encapsulación última que se realiza en nuestro módem que es la de SLIP ó en su mejor caso PPP. Se verán más técnicamente las características de nuestro equipo, cuales son los

puntos importantes para adquirir un módem, sus características, configuraciones, comandos, etc. Se comentaran otros medios de enlace físico, solo como referencia.

Para el tercer capítulo abarcaremos de forma general el trabajo del software de acceso y "navegación" de la Internet; explicaremos su forma de interactuar con nuestra PC, como es posible poder trabajar en línea con equipos que se encuentra en otros lugares y como es posible que podamos obtener información aún no teniendo el software especialmente desarrollado para esto. Por último, se abarcará lo que es la entrada en la red Internet con diferentes utilerías, de acuerdo a las características de enlace que se tenga (tanto en el software, equipo al que se conecta y la cuenta de acceso). Aquí es bueno recordar el objetivo de este trabajo, el cual no pretende ser una guía de acceso, sino más bien una guía para entender la Red Internet, lo que sucede en el momento de estar conectados, las posibles fallas, y tal vez soluciones, que se nos pueden presentar al momento de intentar conectarnos ó al estar enlazado, más no una lista de lugares para viajar, ni la comparación exhaustiva de las interfaces de usuario ó "navegadores" y mucho menos sus características más recónditas.

Capitulo 1

1.1.- Descripción.

" Nuevas comunidades se están empezando a crear hoy en día. No puede verlas, excepto en una pantalla de computadora. No puede visitarlas, excepto a través de su teclado. Su autopista son cables y fibra óptica; el lenguaje es una serie de unos y ceros."

Con una computadora y un módem, podrá estar en disposición para conectarse a la Red Internet, la red de computadoras más grande del mundo. La línea telefónica que usted tiene como línea de voz y que utilizamos para comunicarnos, puede ser una buena opción; solamente recuerde que si tiene una extensión, no podrá utilizarla para llamadas de voz mientras esta conectado a la Red.

Un módem es un tipo de traductor entre la computadora y el sistema telefónico. Esto es necesario puesto que la computadora y el sistema telefónico procesan y transmiten datos ó información en dos formas diferentes e incompatibles. Por un lado, las computadoras "hablan" digitalmente, esto es, almacenan y procesan la información en una serie de números discretos. La red telefónica realiza esta función en señales analógicas, las cuales en un osciloscopio se podrian ver como una serie de formas de onda. Cuando su computadora está lista para pasar datos a otra computadora sobre la línea telefónica, su módem convierte los números de su computadora en esas formas de onda (las cuales, si pudiéramos escucharlas sonarian como un chillido), esto es las "modulan". A su vez, cuando las formas de onda de información entran en su módem, este las convierte en números para que su computadora las pueda procesar, "demodulandolas".

En forma incremental, las computadoras vienen con módem ya instalado. Si la suya no lo tiene y desea uno, deberá decidir de entre otros factores, que velocidad de módem escogerá. Las velocidades de los módem son determinadas en "relación de bps" ó bits por segundo. Un bps significa que un módem puede transferir alrededor de un bit por segundo; entre más grande sea la relación bps, más rápidamente un módem puede enviar y recibir información. Una letra ó un carácter esta constituido de al menos 1 byte.

Puede comprar un módem de 14400 bps relativamente a bajo costo y muchos ahora viene con la habilidad de manejar también mensajes de fax. Un precio que ahora se comienza a manejar es de alrededor de $ 100 US, puede comprar un módem que puede transferir datos a 14,400 bps (y frecuentemente aún más rápidos, usando técnicas especiales de compresión). Si piensa utilizar la Red para transferencia de un gran número de archivos, un módem rápido (de unos 28,800 bps, por ejemplo) es siempre el valor del precio que pague. Este puede reducir ventajosamente la cantidad de tiempo que su módem y su computadora estén enlazado transfiriendo archivos y si estará pagando por el acceso a la Red por hora, puede salvarle de bastantes tiempo en la cuenta de acceso y en la línea telefónica.

Al igual que la computadora a la cual está conectada, un módem es inútil sin el software que le diga como funcionar. Muchos módem hoy en día vienen con software fácil de instalar. Se recomienda intente la conexión con el programa proporcionado en la compra del módem. Si encuentra dificultad para usarlo ó entenderlo, considere buscar un software más entendible.

Por otro lado, puede gastar varios cientos de dólares en un programa de comunicación, pero a menos de que tenga necesidades muy especializadas, esto puede ser una desperdicio de dinero, ya que existen programas disponibles, que pueden ser tomado de la misma Internet de forma gratuita

(Freeware) hasta otro que se consiguen con precios de varios cientos de dólares. La cantidad de funciones básicas que usted quiera tener son un tema de decisión al escoger entre diferentes "protocolos" para la transferencia de archivos a y desde la red y la habilidad de estos para escribir archivos de "script" ó "command" que le permitirán automatizar algunos pasos como son el entrar ó "logging" al sistema del host, entre otras opciones ó facilidades.

Cuando usted compre un módem y el software, pregunte a su vendedor como instalarlo y usarlo. Si es posible sacarlo y verificarlo en alguna máquina ó checar que tenga algún tipo de instructivo. Si el vendedor no puede ayudarlo, busque otro vendedor, puede no solamente salvarse de una frustración, sino también habrá practicado la primer directiva de Internet: "Pregunte. La gente sabe."

Para tomar ventaja completamente sobre la red, deberá gastar unos minutos en leer los manuales ó la documentación que viene con el software. Estas son de las pocas cosas en las que debe poner especial atención: cargado y descargado de archivos; pantalla de captura (también algunas veces llamada "pantalla de descargado"); "logging" ó acceso a un host; selección de emulación de terminal y como cambiar de protocolos, para evitar la frustración de que después de tener horas bajando un archivo, este no pueda ser ejecutado. Es también esencial el conocer como convertir archivos creados con un programa procesador de palabras en formato "ASCII" ó "de texto" el cual le permite compartirlos con otros usuarios a través de la Red ó para cambiar alguna configuración de nuestro equipo.

La actualización es el proceso de enviar un archivo de su computadora a un sistema en la Red. El descargado es la recuperación de un archivo de algún lado de la Red a su computadora. En general, los términos en el mundo del espacio cibernético se definen como "subir" a la red y "bajar" hacia usted.

Las ventajas en su software surgen con la opción de escoger de entre varios "protocolos" a usar en la transferencia. Estos protocolos son sistemas designados para asegurar que el ruido de línea ó estáticos no causan errores que podrían corromper cualquier información que este tratando de accesar.

Esencialmente, cuando se usa un protocolo para la transferencia de un archivo, este se divide en una serie de piezas. Después de que cada pieza es enviada ó recibida, su computadora y el sistema de Red comparan estas piezas. Si las dos piezas no coinciden exactamente, esta transferencia es repetida, hasta que estén de acuerdo en que la información que ambos tienen es idéntica. Si después de varios intentos, la información no logra cruzar, podría aparecer un mensaje de error ó su pantalla podría congelarse. En este caso, se recomienda intentar otra vez. Si después de algunos intentos, aún se encuentra trabada, lo más seguro es que algo está mal con:

a) el archivo
b) la línea telefónica
c) el sistema al cual está conectado ó
d) su propia computadora.

De vez en cuando, usted probablemente verá mensajes en la Red que le gustaría salvar para un vistazo posterior: una ayuda en forma de tip, una marca particularmente ingeniosa, etc., lo que sea; simplemente tener esa información y no perder tiempo (y dinero) en memorizarla ó apuntarla. Aquí es donde la pantalla puede ser capturada.

Cuando usted le dice a su software de comunicación que capture una pantalla, este abre un archivo en su computadora (usualmente en el mismo directorio ó folder usado por el software) y "deposita" una imagen de todo lo que pasa por su pantalla a la vez que lo muestra.

Existen otros comandos de captura que trabajan en bit de manera diferente. Cuando emite el comando, le está diciendo al software que abra un archivo (otra vez, usualmente en el mismo directorio ó folder usado por el software) y entonces le da a este un nombre. Luego, hasta que usted apague ó quite el comando, todo lo que se despliega en su pantalla es copiado en el archivo, ordenado de forma igual que una grabación de vídeo. Esto es útil para el capturado de documentos largos que salen en varias paginas, usando una pantalla de captura, tendrá que repetir el mismo comando para cada nueva pantalla.

La emulación de terminal es una forma de que su computadora haga mímica ó emule la forma en que otras computadoras ponen la información en la pantalla y acepten comandos desde un teclado. En general, muchos equipos en la red utilizan un sistema llamado VT100. Afortunadamente, casi todos los programas de comunicaciones de ahora soportan también este sistema, asegúrese de que el suyo lo hace.

Usted también tiene que conocer un poco sobre protocolos. Estas son las diversas formas, todas ellas diferentes, en que la computadora puede transmitir caracteres. Afortunadamente, estos se pueden dividir básicamente en solamente dos tipos que usted utiliza para corre el acceso: 8-1-N (el cual es estándar "8 bits, 1 stop bit, no parity") y 7-1-E (7 bits, 1 stop bit, even parity).

En general, los sistemas basados en Unix utilizan 7-1-E, mientras que sistemas basados en MS-DOS usan 8-1-N. ¿Qué debe hacer si no conoce a que tipo de sistema está conectándose? Intente uno de los seleccionados. Si usted obtiene algo que se ve como garabatos cuando se conecta, puede que en realidad necesite del otro seleccionado. Si es así, puede tanto cambiar el seleccionado mientras se conecta ó suspender e intenta otra vez con el otro seleccionado. También es posible que su módem y el módem del otro extremo final no puedan estar de acuerdo en la relación de bps correcta. Si pese al cambio de protocolo, no se nota una mejoría, intente usar otra relación de bps (pero no más rápido de los que están listados en su módem).

Para usuarios nuevos es importante hacer de su conocimiento que no tienen por que preocuparse, y que recordarles que no pueden "romper" nada!. Si algo se ve mal, es que probablemente este mal. Cambie su seleccionado e intente otra vez. Nada se aprende sin prueba, error y esfuerzo.

¡Esto es lo básico. Ahora a la red!

1.2.-Entrando a la Red.

Hoy en día, un número siempre creciente de sistemas de "acceso público" provee acceso para cualquiera que se quiera conectar a la Red Internet. Existen dos tipos básicos de esos sistemas. El más común es conocido como un sitio UUCP (UUCP empieza una forma común de transferir una cantidad de información de computadoras usando el sistema operativo Unix) y ofrece acceso a un correo electrónico internacional y conferencias.

Sin embargo, años recientes han visto el crecimiento de sitios más poderosos que le permiten sentir un completo poder en la red. Estos sitos Internet no solamente dan acceso a correo electrónico y

conferencias sino también a servicios como bases de datos, librerías e inmensidad de archivos además de colección de programas alrededor del mundo. Estos son además rápidos, tan pronto como usted termine de escribir el mensaje, este tiende a mandarlo a su destino. Algunos de estos accesos públicos, host ó sistemas son libres de cambiar. Otros cambian mensualmente ó anualmente alimentándose para acceso ilimitado.

El costo debe ser considerado al escoger un sistema de host, especialmente si usted vive en una área con más de un proveedor. Muchos sistemas no proveen usuarios de interface en todos sus sistemas: cuando usted se conecte, está descargando derechos dentro de un sistema operativo Unix. Si está familiarizado con Unix, ó quiere aprender como utilizar este, el sistema le ofrece un poder fenomenal, en adición al acceso a la red, muchos también le permiten tocar dentro del poder de Unix para hacer cualquier cosa, desde compilar sus propios programa hasta juegos en línea. Pero si usted no quiere tener que aprender Unix, hay otros sistemas de acceso público que trabajan a través de menúes (tal como en un restaurante en el cual le muestran una lista a escoger y después hace usted la selección de lo que quiere), ó quienes proveen una "interfaz de usuario" que es fácil de manejar fuera de la encriptación de Unix.

Si no quiere ó no necesita accesar al rango completo de los servicios de Internet, un sitio UUCP puede tener un buen sentido financiero para ser seleccionado. Estos tienden a "cargar" menos de lo que la Internet comercial provee. Algunos sistemas también tienen sus servicios locales propios y únicos, los cuales pueden estar en el rango que van desde conferencias extensivas hasta largas librerías de archivos.

1.3.- Accesando a un sistema público.

Cuando usted tiene su programa de comunicación marcando alguno de esos host de sistemas, una ó dos cosas le pueden pasar cuando se conecte. Puede ver un conjunto de garabatos en su pantalla; si ve garabatos, es la oportunidad de cambiar sus parámetros de software. Póngase en marcha, haga los cambios y después marque otra vez.
Por otro lado, cuando este conectado, probablemente verá algo como esto:

```
Welcome to THE WORLD
        Public Access UNIX for the '90s
        Login as 'new' if you do not have an account

        login:
```

La última línea es un prompt preguntándole si desea hacer algo. Puesto que esta es su primera llamada, teclee:

```
new
```

y presione Enter. Frecuentemente, cuando se le pregunta para teclear algo para un sistema host, puede ser que se lo pidan entre comillas (por ejemplo 'new'). No incluya las comillas. Lo que verá después depende del sistema, pero generalmente consiste de información sobre los costos y los servicios (usted puede querer encender sus funciones de captura de pantalla de su software de comunicación, para guardar esta información). Probablemente le será preguntado si quiere establecer una cuenta ahora ó simplemente echar un vistazo al sistema.

Otra posibilidad es que le sea preguntado el "user name". Este no es su nombre, sino un nombre de una palabra que quiera usar mientras está en línea, por lo general se tiene una cuenta de uso general llamada "anonymous". Para el nombre, este puede ser cualquier combinación de letras ó números, todos en minúsculas (recuerde que está manejando Unix). Mucha gente utiliza su primer inicial y su apellido(por ejemplo "jgarcia"); su nombre y la primera letra de su apellido (por ejemplo "joseg"); ó sus iniciales ("jgl"). Otros usan un apodo ó nombre corto. Puede que quiera pensar sobre esto por uno segundos, puesto que este nombre de usuario se convertirá en parte de su dirección de correo electrónico. Una excepción son los diversos sistemas Free-Net, de los cuales a todos le asignan un nombre de usuario que consiste de una secuencia arbitraria de letras y números.

Usted está ahora en la red. Checando el sistema. Aquí va un buen consejo: Vea si hay algún archivo de ayuda que pueda leer. Si este es un sistema de host basado en menúes, escoja varias opciones simplemente para ver que es lo que pasa. Recuerde: "No puede romper nada". Entre más juegue, más cómodo estará en la Red. La gran mayoría de sitios ofrecen correo electrónico internacional y Usenet (conferencias internacionales). En adición, algunos ofrecen:

FTP: File-transfer protocol--acceso a cientos de librerías de archivos (de todo, desde software de computadoras hasta documentación histórica pasando por letras de canciones y más cosas). Estará en disposición para transferir estos archivos desde la Red hasta su propia computadora.

Telnet: Acceso a base de datos, tarjetas de catálogos de librerías computarizadas, reportes de clima y otros servicios de información, así como "en vivo": juegos en línea en los que compite con jugadores de alrededor de todo el mundo. También permite comunicar dos P.C. como terminales asíncronas.

Servicios adicionales que pueden ser ofrecidos incluyen:

WAIS: Servidor de información de área amplia, un programa que puede buscar docenas de bases de datos en una sola búsqueda.

Gopher: Un programa que le da un acceso fácil a docenas de otras bases de datos en línea y servicios haciendo la selección desde un menú. Estará disponible de usar estos para copiar archivos de texto y algunos programas a su buzón.

IRC: Internet Relay Chart, un simulador CB que le permite tener en vivo cartas de teclado con gente de alrededor del mundo. Un sistema de intercambio de información y mensajes cortos "en línea".

Sin embargo, aún en sistemas que no proveen estos servicios directamente, puede estar en disposición para usar un gran número de estos a través de telnet.

1.4.- ¿Qué es TCP/IP?

TCP/IP es una puesta de protocolo usada para interconectar computadoras en red y para rutear tráfico en equipos muy diferentes. "TCP" significa Transmission Control Protocol, por su parte "IP" significa Internet Protocol. Los protocolos son estándares los cuales describen formatos permitidos, manejo de errores, etc. El paso de mensajes y estándar de comunicaciones en los sistemas de computadoras, los cuales los conforman los protocolos de comunicaciones tales como TCP/IP, se utilizan para hablar un lenguaje común. Estos los habilita para trasmitir mensajes con precisión y para el destino correcto, no importando las principales diferencias en el hardware y software de las máquinas.

Muchas redes grandes han sido implementadas con estos protocolos, incluyendo la DARPA Internet (Defence Advanced Research Projects Agency Internet). Una gran variedad de Universidades, agencias del gobierno y firmas de computadoras están conectadas a una interred ó "internetwork" la cual sigue el protocolo TCP/IP, además de las miles de máquinas individuales que están conectadas a Internet. Una máquina en la Internet puede comunicarse con cualquier otra. El término "Internerworking" se utiliza para referirse a la acción de unir dos ó más redes en una sola. El resultado puede ser descrito como una red de redes, la cual es llamada una "Internet". A las máquinas conectadas en la Internet son referidas como "host" ó "nodos".

TCP/IP provee las bases de muchos servicios útiles, incluyendo correo electrónico, transferencia de archivos y login remotos. El correo electrónico se refiere para transferencia de archivos de texto cortos. Los programas de aplicación de transferencia de archivos pueden transmitir archivos muy largos conteniendo programas ó datos. Estos también pueden proveer chequeo de seguridad controlando la transferencia de archivos. Login Remoto permite a los usuarios en una computadora el acceso (log in) en una máquina remota y transportar una sesión activa.

1.4.1.- El Protocolo Internet (Internet Protocol (IP))

El Internet Protocol, IP, define un envío de paquetes sin conexión. Este paquete entrega la conexión a una ó más redes de manejo de paquetes dentro de una Internet. El término "sin conexión" significa que la máquina enviadora y receptora no están conectadas por un circuito directo. En su lugar, los paquetes individuales de estructuras de datos (ó mejor conocidos como datagram) son ruteados a través de diferentes máquinas en la Internet para la red destino y el final en la máquina receptora. Así, un mensaje es dividido en varios datagram, los cuales son enviados separadamente. Note que el paquete sin conexión que es enviado, por si mismo, no es confiable. Los datagram individuales pueden ó no arribar y estos probablemente no podrán arribar en el orden en el cual fueron enviados. TCP añade esa confiabilidad.
Una datagram consiste de una información de cabecera y una área de datos. Esta información de cabecera es usada para rutear y procesar el "datagram". El "datagram" puede ser fragmentado dentro de pequeñas piezas, dependiendo de los requerimiento físicos de las redes que atraviesa. (Cuando un ruteador de mensajes ó "gateway" envía un "datagram" a una red la cual no puede acomodar dicho "datagram" en un paquete único, el "datagram" debe ser fragmentado en piezas que son lo suficientemente pequeñas para la transmisión.) El "datagram" fragmenta la cabecera conteniendo la información necesaria para reensamblar la fragmentación dentro del "datagram" completo. La fragmentación no necesariamente arriba en orden; el módulo de software implementando el protocolo IP en la máquina destino debe reensamblar los fragmentos dentro del "datagram" original. Si cualquier fragmento se pierde, el "datagram" que llego es descartado.

1.4.2.- El Protocolo de Control de Transmisión (Transmission Control Protocol (TCP))

El Transmission Control Protocol, TCP, trabaja con IP para proveer entregas de paquetes confiables. Este provee un método para asegurarse que los diversos datagram que se realizaron en un mensaje son reensamblados en el orden correcto en su destino final y que cualquier datagram olvidado ó perdido es enviado otra vez hasta que este es recibido correctamente.

El propósito primario de TCP es proveer una confiabilidad, seguridad y servicio de conexión de circuito virtual entre pares de procesos de comunicación en lo alto de paquetes de subred no confiables; cuando se pierden, se dañan, duplican , retardan ó desordenan, puesto que cualquiera de

estas cosas puede ocurrir. También, ofrece seguridad provisional tales como acceso limitado a usuarios para que solo ciertas máquinas puedan ser implementadas a través de TCP.

TCP concierne solamente para la total confiabilidad de los puntos finales. Esto hace pocas suposiciones sobre la posibilidad de obtener servicios de datagram confiables. Si un datagram es enviado a través de una Internet a un host remoto, la red interviniendo no garantiza la entrega de resultados. De igual forma, el envió de datagram no tiene forma de saber el camino de ruteado que usara para enviar el datagram. La confiabilidad de fuente-a-destino es provista por TCP; esto hace a TCP estar bien situado para una amplia variedad de aplicaciones de comunicación de máquinas múltiples.

La confiabilidad es archivada a través de un "checksum" (código de detección de errores), números de secuencia en la cabecera de TCP, reconocimiento positivo de datos recibidos y transmisión de datos reconocidos.

1.4.3.- ¿Como son ruteados los mensajes?

La siguiente sección explica direcciones de gateway y de red. Estos dos conceptos son la clave para entender como los datagram son ruteados a través de una Internet.

Gateways

Las diversas redes, las cuales componen una Internet están conectadas a través de máquinas gateway. Un gateway es una máquina que es conectada a dos ó más redes. Esta puede rutear datagram de una red a otra. El Gateway rutea un datagram basado en la red destino, ó mejor dicho, a la máquina individual (host) en esa red. Esto simplifica el algoritmo de ruteado. El gateway decide en cual red deberá estar el siguiente destino de un datagram dado. Si el host de destino del datagram está en la red, el datagram puede ser enviado directamente hacia el host. De otra forma, este continua pasando de gateway a gateway hasta que este encuentra a la red destino.

Network Address

Cada máquina host en una Internet TCP/IP tiene una dirección de red de 32.bit. La dirección incluye dos partes separadas: la id red y la id de host de máquina. Las máquinas que sirven como gateway de este modo tiene más de una dirección, puesto que estas están en más de una red. Las direcciones Internet son asignadas por el Network Information Center (NIC) localizado en SRI International en Menlo Park, California. El NIC asigna solamente id de redes; el administrador de red individual le asignará el id de máquina host para esa red.

Estas son las tres clases de direcciones de red, correspondiendo a redes pequeñas, medianas y largas. Entre más larga la red, más largo será el número de host en esa red; de igual forma, las redes pequeñas tienen pocos host. Así, cuando la dirección de red de 32 bit es dividida entre el id de red y el id de máquina de host, redes largas necesitarán un número largo de bits para únicamente especificar todo el host en la red. Las direcciones de red tienen así que estar divididas dentro de tres clases, identificadas como A, B y C. La siguiente tabla especifica las tres clases y sus formatos:

Clase	Configuración del tamaño de la red
Clase A	Permite id de 7-bit para red y id de 24-bit para host.
Clase B	Permite id de 14-bit para red y id de 16-bit para host.
Clase C	Permite id de 21-bit para red y id de 8-bit para host.

Todas las direcciones de red son de 32 bits. El primer bit de dirección de la Clase A es **0** (cero), para identificar la dirección como Clase A. Las direcciones Clase B comienzan con el dígito **10**, y las direcciones Clase C comienzan con **11**.

Este sistema de clases de direcciones de red provee una dirección única para las entradas estadísticas de distribución de tipos de redes que podrían ser una cantidad expectable de varias redes usando sus direcciones del sistema. Estas pueden ser un número muy pequeño de redes largas, teniendo muchos host (Clase A), un gran número de redes pequeñas, consistiendo de un número menor de host (Clase C) y un número medio de redes constituidas de un número medio de host (Clase B).

Las direcciones de red son frecuentemente escritas por cuatro decimales enteros separados por puntos (.), donde cada número decimal representa un octeto de la dirección de red de 32 bit. Por ejemplo, una máquina puede tener la dirección 128.12.3.5.

Puertos y Sockets

TCP también utiliza un número de 16 bit llamado el "puerto" para direccionar una conexión. El puerto especifica el destino particular del programa ó la utileria, tales como **ftp** (file transfer program). Un socket es una dirección que específicamente incluye un puerto de identificación, que es, la concatenación de una dirección Internet con un puerto TCP. Las conexión de puertos son desplegados en la Active Connections Display de **netstat** (TC).

Error ICMP y Mensajes de Control.

ICMP es el Internet Control Message Protocol, este define el error y el control de mensajes por IP. Los mensajes ICMP son enviados en datagram, como cualquier otro mensaje de red. Esos mensajes pueden ser mensajes de error, tales como destino irreconocible ó preguntas para información, tales como una dirección de red particular. Los mensajes ICMP son también usados para peticiones de tiempo de marca, la cual es utilizada cuando se sincroniza los relojes de varios hosts en una red.

Nivel de Protocolo.

El software de protocolo de comunicación es dividido en diferentes capas, donde la capa más baja es el hardware la cual transporta físicamente el dato, y la capa más alta es el programa de aplicación en la máquina host. Cada capa es muy compleja en sus propios derechos y ningún protocolo único puede abarcar todas las tareas de varias capas. Como lo mencionamos hace poco, el Internet Protocol maneja el ruteado de datagram, mientras que el Transmission Control Protocol, el cual es la capa de abajo de IP, provee transmisión confiable de mensajes los cuales han sido divididos dentro de los datagram. Los programas de aplicación en turno se confía en TCP para enviar información al host destino.

Para los programas de aplicación, TCP/IP aparece para proveer un circuito virtual "full-duplex" ó sea, tanto de transmisión como recepción, entre las máquinas. En la actualidad, toda la información

es dividida dentro de datagram, los cuales pueden ser más adelante fragmentados durante la transmisión. El modulo de software implementando IP reensambla los datagram individuales, mientras que el modulo implementando TCP asegura que los varios datagram son reensamblados en el orden en el cual ellos fueron enviados originalmente.

Estos son varios protocolos especializados de alto nivel para aplicaciones especificas tales como terminal traffic (**telnet**(TC)) y file transfer (**ftp**(TC)) y protocolos para otras funciones de red tales como monitoreo del estatús del ruteador (gateway-status monitoring). En varios lugares, sin embargo, usualmente estos no son referidos como protocolos, sino como programas ó servicios.

1.4.4.- Comandos de Red de TCP/IP más comunes.

El comando TCP/IP son derivados de tanto el ambiente Berkeley UNIX y el ambiente de red ARPANET. (ARPA es un acrónimo de Defense Advanced Research Projects Agency.) Los comandos derivados de Berkeley UNIX pueden ser usados solamente con UNIX ó sistemas compatibles con UNIX. Los derivados de ARPA son designados para trabajar con cualquier sistema operativo. La principal diferencia entre estos dos tipos diferentes de comandos es que los comandos 4.3BSD (Berkeley UNIX) propagan permisos al estilo de UNIX a través de la red. Los comandos ARPANET no entienden los permisos estilo UNIX. Incluido en el comando TCP/IP está un seleccionado de comandos frecuentemente referidos para entrar en un ambiente UNIX Berkeley como el comando **r**. El **r** permanece para remotos. Esta selección incluye comandos tales como **rcp, rcmd** y **rlogin**. Estos comandos son similares a su contraparte de UNIX Berkeley. Estos comandos tipo 4.3BSD son designados para ser especificos de UNIX y son muy fácil de ser usados cuando usted está trabajando en un host tipo UNIX.

Comandos tales como **telnet** y **ftp** originarios de ARPANET, son designados para ser independientes del sistema operativo. El protocolo usado en esos comandos está acorde con las especificaciones de Internet del Department of Defense (DoD). Los comandos de red son listados alfabéticamente en la tabla de abajo con una breve descripción. No todos estos comandos son propuestos para usarse por los usuarios de red. Algunos proveen funciones administrativas de red.

Comandos de Red de TCP/IP

Comando	**Descripción**
ftp(TC)	programa de transferencia de archivos
ifconfig(ADMN)	parámetros de interface de configuración de red
logger(TC)	realizar una entrada al sistema
mkhosts(ADMN)	comando para dar un nombre a un nodo
netstat(TC)	mostrar el estatús de la red
remd(TC)	ejecución de comandos de la estructura remota
rcp(TC)	copiar archivos remotos
rlogin(TC)	acceso remoto
ruptime(TC)	desplegar el estatús de los nodos en la red local
rwho(TC)	quien está dentro de la red local via su nombre de nodo
slattach(ADMN)	conectarse a una linea serial como una interface de red
sldetach(ADMN)	desconectarse de una linea serial como una interface de red
talk(TC)	hablar con otro usuario

telnet(TC)	interface de usuario para el protocolo DARPA TELNET
trpt(ADMN)	imprimir el trazo del protocolo, sus rutas

1.5.- Comando de Red en UNIX

Una red UNIX es un grupo de máquinas UNIX ó compatibles con UNIX enlazadas conjuntamente, usualmente a través de Ethernet. Una internetwork UNIX son dos ó más de tales redes unidas conjuntamente por gateway para formar una gran red. El gateway internetwork es invisible al nivel de interface del comando, dando la apariencia de una red única. (Un Gateway es también referidos como routers ó bridge IP). UNIX es un sistema operativo orientado a comandos, aunque últimamente su tendencia es hacia la interface de usuario gráfica, y para que este haga uso de recursos remotos en un ambiente internetworking UNIX, ciertos comandos específicos de red están disponibles. Estos comandos son completamente integrados con UNIX y pueden ser invocados de la línea de comandos shell y shell scripts. Alternativamente, estos pueden ser ejecutados dentro del programas de usuario usando las llamadas del sistema **fork(S)** ó **exec(S)**, ó la rutina de biblioteca **system(S)**. Estos comandos están en el uso del proceso del sistema operativo, pero estos requieren del software de red para funcionar. En UNIX, el nombre del comando es el mismo que el nombre del archivo que contiene el programa procesado.

Algunas de las muchas cosas que se pueden hacer como usuario cuya máquina es conectada en una red UNIX son:

* Acceso remotamente a otra máquina en la cual se tenga una cuanta.
* Moverse lógicamente de una máquina remota a otra sin que introducir su password (si su administrador del sistema tiene "iguales" las máquinas ó si usted tiene creado un usuario equivalente para esa máquina).
* Ejecutar comandos en cualquier máquina en la red. Esto significa, por ejemplo, que puede ejecutar comandos desde donde quiera que el dato este localizado. La ventaja de esto es que no necesita mover archivos. Alternativamente, puede escoger ejecutar comandos donde el cargado es menor, más bajo, ó puede construir secuencias de comandos UNIX incluyendo entubaciones que mueven datos entre máquinas para procesamiento.
* Acceso a datos públicos desde todas las máquinas.
* Copiar ó transferir archivos desde una máquina a otra si tiene permisos para hacerlo (ver **chmod(C)**).
* Compartir dispositivos remotos tales como impresoras y dispositivos de cintas.
* Acceso a sistemas de correo electrónico que hayan sido implementados para la red.
* Correr aplicaciones residentes en otras máquinas.
* Acceso a otras máquinas UNIX que están corriendo el protocolo de comunicaciones apropiado

Note que estas son tres tipos de objetos UNIX networking:

* Comandos ejecutables y programas del servidor (algunas veces llamados daemons) soportando los comandos.
* Archivos de configuración.
* Bibliotecas y sistemas llamados para uso por programadores

1.5.1.- Comando de UNIX de uso imprescindible.

Si está conectado a la Red a través de un sistema UNIX, eventualmente tendrá que relacionarse con los términos de UNIX. Por fortuna ó desgracia, muchos sistemas UNIX no lo protegen contra sus trabajadores interiores -- si quiere copiar de un Usernet a un archivo, por ejemplo, tendría que usar algún comando de UNIX cada vez que quiera hacer algo con ese archivo. Tal como MS-DOS, UNIX es un sistema operativo--este le dice a la computadora como hacer las cosas. Ahora, mientras Unix puede tener un reputación de estar más completo que MS-DOS, en muchos casos, unos pocos comandos básicos y simples son todo lo que necesitara.

Si su computadora usa MS-DOS ó PC-DOS, el concepto básico será muy familiar --pero hay que tener cuidado con algunos comandos los cuales trabajan lo suficientemente diferente de su similar en DOS al grado de que puede provocar serios problemas. Así mismo, a diferencia de MS-DOS, Unix es sensitivo al tipo de carácter-- si teclea los comando ó los nombres de directorios en el tipo equivocado, puede tener un mensaje de error. Recuerde teclear todo con minúsculas. En general, estos son algunos de los comandos básicos para el manejo de un sistema en UNIX:

cat Equivalente al comando "type" de MS-DOS. Para detener al archivo por pantalla, se teclea:

cat file more

donde file es el nombre del archivo que se quiere ver. Presionando Ctrl-C se detiene el desplegado de la pantalla. Alternativamente se puede teclear:

more file

para obtener el mismo resultado, pero por páginas. También puede usar cat para escribir ó actualizar archivos de texto a su directorio hogar (de manera similar al comando "copy con" de MS-DOS). Si teclea:

cat>test

inicia un archivo llamado "test". Puede escribir desde algo simple (no podrá editar una vez que termine una línea y tendrá que presionar return en cada final de línea) ó sobreescribir algo dentro de su archivo usando su protocolo ASCII de software de comunicaciones. Para cerrar el archivo presione Ctrl-D.

cd El comando "cambio de directorio". Para cambiar de su presente directorio a otro, teclee:

cd directorio

y presione return. A diferencia de MS-DOS, el cual utiliza (\) para denotar subdirectorios (por ejemplo: \stuff\text), Unix utiliza una (/) (por ejemplo: /stuff/text). Así para cambiarse de su presente directorio al subdirectorio stuff/text, deberá teclear:

cd stuff/text

y luego presionar enter. Como en MS-DOS, no necesita la primera diagonal si el subdirectorio viene del directorio en el que se encuentra. Para moverse de regreso en el árbol de directorios puede teclear:

cd ..

seguido de enter. Note el espacio entre el cd y los dos puntos--aquí es donde los usuarios de MS-DOS toman la visión de Unix y MS-DOS.

cp Para copiar un archivo. La sintaxis es:

cp file1 file2

el cual copia un archivo file1 a file2 (o sobreescribe file2 con file1).

ls Este comando, cuando es seguido de enter, le dice lo que está en el directorio; es similar al comando dir de MS-DOS, excepto en el ordenamiento alfabético.

ls more

detiene el listado cada 24 lineas-- es útil si este es un lote de cosas en el directorio. El comando ls básico no lista archivos "escondidos", tales como el archivo .login el cual controla como su sistema interactua con Unix. Para ver estos archivos, teclee:

ls -a ó ls -a more

ls -l le dice el tamaño de cada archivo en bytes y también cuando fueron creados ó modificados.

mv Es similar al comando renombrar de MS-DOS.

mv file1 file2

el cual renombra al archivo file1 como file2. El comando puede ser utilizado también para mover archivos entre directorios.

mv file1 News

puede mover al archivo file1 al directorio News.

rm Borrar un archivo. Teclee:

rm filename

y presione enter (pero tenga cuidado antes de practicarlo).

Comodines ó "Wildcards": Sirven cuando busca, copia ó borra archivos; puede usar los caracteres comodines, si no está seguro del nombre exacto del archivo.

*ls man**

podrá encontrar los siguientes archivos:

manual
manual.txt
man-o-man

Use el signo de interrogación cuando este seguro de que se trata de uno ó dos caracteres. Por ejemplo:

ls man?

podrá encontrar un archivo llamado mane, pero no encontrara a uno llamado manual.

Apéndice A

Conceptos sobre TCP/IP

TCP/IP (Protocolo de control de transmisión/Protocolo Internet) es un conocido conjunto de protocolos de conectividad estándar. Estos protocolos se utilizan para habilitar nodos diferentes en un entorno heterogéneo para que puedan comunicarse unos con otros.

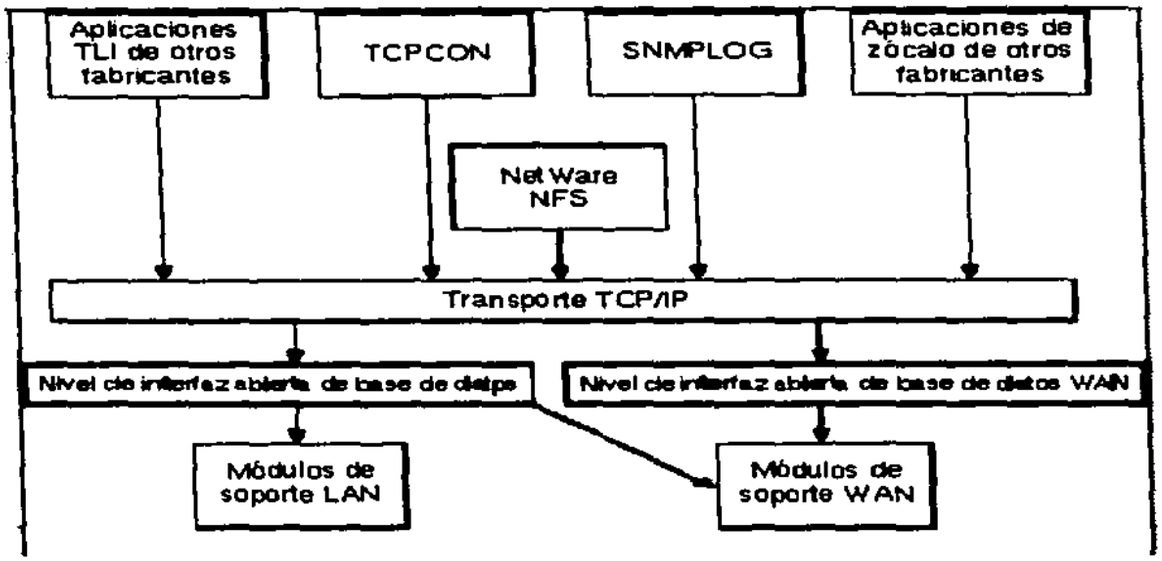
La idea general de conectar un red con computadoras diferentes partió de las investigaciones llevadas a cabo en la Defense Advanced Research Projects Agency (DARPA). En el marco de esta investigación, DARPA desarrolló el conjunto de protocolos TCP/IP para establecer comunicaciones entre redes e implantó una interred que recibió el nombre de ARPAnet, que más adelante conformó la Internet. El conjunto de protocolos TCP/IP define los formatos y normas utilizados en la transmisión y recepción de información con independencia de cualquier tipo de hardware determinado u organización de red. A pesar de que los protocolos se desarrollaron para la Internet, TCP/IP es, ahora, el estándar de facto, ya que muchas organizaciones públicas y privadas la utilizan para su conectividad.

Esta red, tal y como la concibió DARPA e implantada con el conjunto de protocolos TCP/IP, es una red de conmutación de paquetes. Las redes de conmutación de paquetes transmiten la información por la red en pequeños segmentos que reciben el nombre de paquetes. Por ejemplo, si un computador transmite un archivo de cierta longitud a otro computador, el archivo se dividirá en varios paquetes en el origen que volverán a unirse cuando lleguen al destino. Los protocolos TCP/IP definen el formato de estos paquetes. Esta definición incluye el origen, el destino, la longitud y el tipo de paquete, asi como el modo en que los computadores de la red van a recibir y retransmitir los paquetes.

Las posibilidades de encaminamiento de TCP/IP permiten el reenvio de paquetes IP de una red a otra. TCP/IP usa el Protocolo de Información de Encaminamiento (RIP), el Protocolo Gateway Externo (EGP) ó el protocolo Abrir la via más corta primero (OSPF) para comunicarse con otros ruteadores. De este modo, todos los ruteadores de la interred pueden conocer la configuración de la interred sin necesidad de la intervención humana.

Además de los servicios de encaminamiento, TCP/IP proporciona unas interfaces de transporte mediante las cuales es posible utilizar servicios de red de alto nivel. Estas interfaces la utiliza el sistema NFS y aplicaciones de otros fabricantes para su uso con 4.3BSD con la interfaz del zócalo UNIX® ó la Interfaz de la capa de transporte (TLI) STREAMSTM .

TCP/IP da soporte a redes Ethernet, Token Ring, FDDI y ARCNET a través de la especificación de Open Data-Link Interface TM (ODITM).



Características TCP/IP

El software TCP/IP incluye las características siguientes:

Soporte de aplicación TCP/IP

El soporte de aplicación TCP/IP proporciona una interfaz de transporte que permite la utilización de servicios de red de alto nivel. Esta interfaz la utiliza el sistema NFS y aplicaciones de otros fabricantes creadas para utilizarla con la interfaz de zócalo 4.3BSD UNIX ó con la Interfaz de la capa de transporte (TLI) STREAMS. La interfaz de transporte proporciona acceso a los servicios de transporte del Protocolo de control de transmisión (TCP) ó al Protocolo de datagram de usuario (UDP).

Encaminamiento IP

Las posibilidades de encaminamiento IP de TCP/IP permiten el reenvio de paquetes IP de una red a otra. Los routers de una interred TCP/IP intercambian información entre si. TCP/IP da soporte al estado del enlace, vector de distancia y encaminamiento estático.

RIP

El Protocolo de Información de Encaminamiento (RIP) usa el algoritmo del vector de distancia como base para efectuar operaciones y tomar decisiones de encaminamiento. RIP es un protocolo estándar que se basa en el algoritmo del vector de distancia. La mayoria de las empresas que utilicen TCP/IP usan RIP.

OSPF

La opción Abrir la via más corta primero (OSPF) usa el algoritmo de estado del enlace como base para efectuar operaciones y tomar decisiones. OSPF es un nuevo protocolo IGP que se basa en un

algoritmo de estado del enlace. OSPF está siendo muy bien aceptado en empresas públicas y privadas que usan redes extensas y complejas.

EGP (External Gateway Protocol)

El Protocolo de compuerta externo (EGP) se utiliza para intercambiar información de encaminamiento entre interredes IP que están bajo control administrativo diferente.

Encaminamiento estático

Las rutas estáticas están configuradas manualmente. Las rutas estáticas definen los caminos a utilizar para alcanzar el destino remoto. Los ruteadores pueden utilizar rutas estáticas en lugar, ó además de, las rutas indicadas por los protocolos de encaminamiento dinámico.

Descubrimiento del Ruteador

Los ruteadores utilizan el protocolo Descubrimiento del Ruteador para indicar su presencia en la red. Los Hosts pueden utilizar el protocolo descubrimiento del ruteador para saber los ruteadores que existen en la red.

Soporte de Subred

TCP/IP permite al usuario dividir las redes en subredes para facilitar la gestión y resolución de problemas.

Soporte de subred variable

Como se comento anteriormente, TCP/IP permite al usuario dividir las redes en subredes de tamaño variable para facilitar la gestión y la resolución de problemas. Normalmente, estas subredes tienen un tamaño uniforme y pueden utilizar el mismo número de hosts. Existe software que proporciona soporte adicional para subredes de tamaño diferente. Esto es posible, porque se permite el uso de máscaras de subred de longitud variable.

Subred cero

TCP/IP proporciona soporte para la subred cero si se utilizan los protocolos de encaminamiento OSPF ó RIP II. Estos protocolos de encaminamiento incluyen la máscara de subred y eliminan la ambigüedad entre la subred cero y la red natural.

Difusión general dirigida

La difusión general dirigida se envía a todos los hosts de una red ó subred IP determinada. Algunas aplicaciones utilizan difusión general dirigida para buscar ó anunciar servicios.

Reenvío de paquetes BOOTP

BOOTP es un protocolo utilizado por algunos hosts para obtener las direcciones IP. El host emite una difusión general de una petición BOOTP en la red local. Si el servidor BOOTP está conectado a la misma red que el host, recibirá la petición y responderá con un paquete que contendrá la dirección

del host. Si el servidor está en una red diferente, el remitente BOOTP debe dirigir la difusión general a un servidor BOOTP y reenviar la respuesta al host. El software TCP/IP proporciona el archivo que permite a la máquina reenviar los paquetes de petición/respuesta de BOOTP entre el servidor BOOTP y los clientes BOOTP.

Gestión de la red TCP/IP

Se puede monitorizar y resolver problemas en la interred con SNMP. Este es un protocolo de gestión de red más conocido del conjunto de protocolos TCP/IP. Permite que las estaciones de gestión de red basadas en TCP/IP acumulen información sobre la configuración y el estado de nodos de una interred basada en TCP/IP.

Utilidad de configuración de interconectividad

La utilidad de configuración de interconectividad es una utilidad dirigida por un menú que simplifica la tarea de configuración del LAN para operar con protocolos de red múltiples.

Conectividad de la LAN

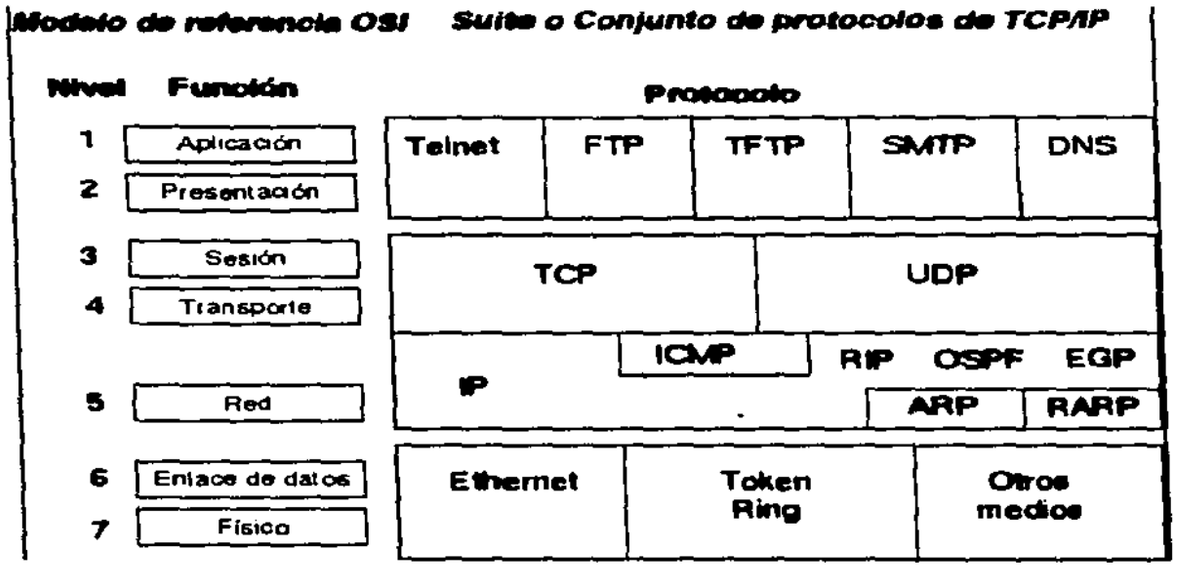
El software de TCP/IP proporciona conectividad para estaciones de trabajo y servidores conectados por medio de redes LAN y/o WAN, como por ejemplo Ethernet, FDDI, Token Ring y ARCNET.

Conexiones permanentes

Durante la inicialización del sistema pueden establecerse conexiones permanentes. Estas conexiones se mantienen continuamente. Si un error de enlace rompe la conexión, vuelve a intentarse automáticamente.

Conjunto de protocolos TCP/IP

En líneas generales, el conjunto de protocolos TCP/IP corresponde con el modelo de comunicaciones de red definido por la International Organization for Standardization (ISO). Este modelo se denomina modelo de referencia Interconexión de Sistemas Abiertos (OSI). El modelo OSI describe un sistema de redes ideal que permite establecer una comunicación entre procesos de capas distintas y fáciles de identificar. En el host, las capas prestan servicios a capas superiores y reciben servicios de capas inferiores. La figura muestra las siete capas del modelo de referencia OSI y su correspondencia general con las capas del conjunto de protocolos TCP/IP.



Modelo de referencia OSI y las capas de TCP/IP correspondientes

El sistema para determinar capas permite a los programadores concentrar sus esfuerzos en las funciones de una capa determinada. No es necesario que creen todo los mecanismos para enviar información a lo largo de la red. Sólo tienen que saber los servicios que el software debe proporcionar a la capa superior, los servicios que las capas inferiores pueden proporcionar al software y qué protocolos del conjunto proporcionan estos servicios.

La tabla enumera los protocolos más comunes del conjunto de protocolos TCP/IP y los servicios que proporcionan.

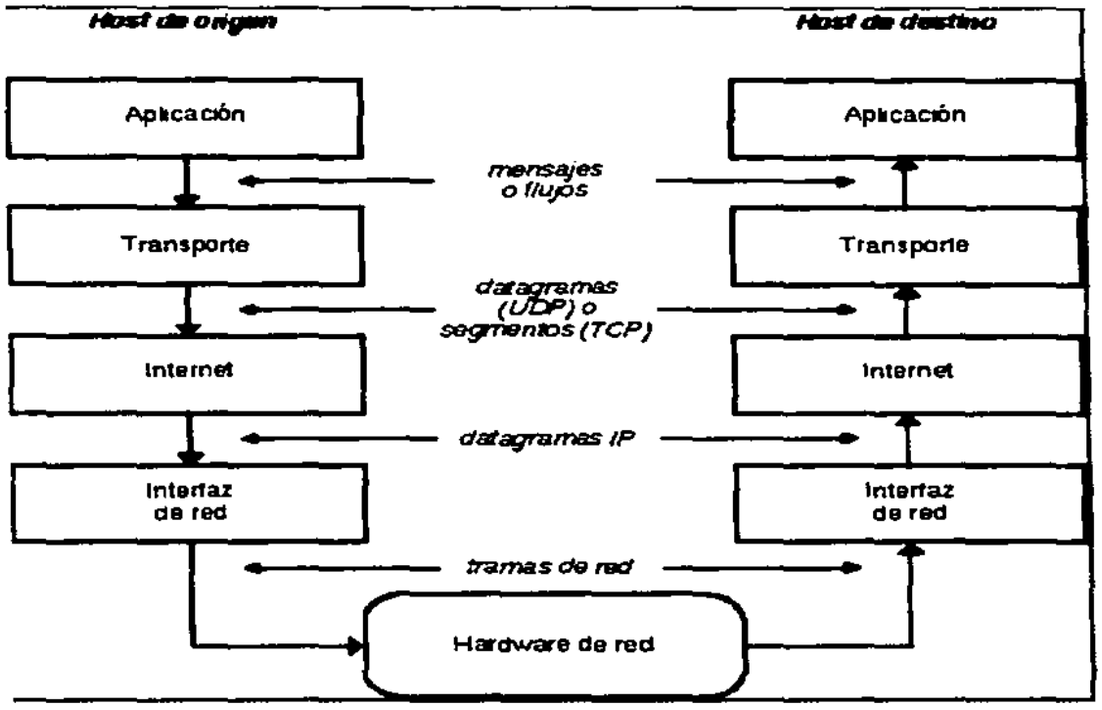
Protocolo	Servicio
Protocolo Internet (IP)	Proporciona servicios para la entrega de paquetes (encaminamiento) entre nodos
Protocolo de control de mensaje Internet (ICMP)	Regula la transmisión de mensajes de error y control entre los host y las gateways
Protocolo de resolución de direcciones (ARP)	Asigna direcciones Internet a direcciones físicas
Protocolo de resolución de direcciones invertidas (RARP)	Asigna direcciones físicas a direcciones Internet.
Protocolo de control de transmisión (TCP)	Proporciona servicios de envío de flujos fiables entre los clientes.
Protocolo de datagrama de usuario (UDP)	Proporciona servicio de entrega de datagramas no fiable entre clientes.
Protocolo de transferencia de archivos (FTP)	Proporciona servicios de nivel de aplicación para la transferencia de archivos
TELNET	Proporciona un método de emulación de terminal
Protocolo de información de encaminamiento (RIP)	Permite el intercambio de información de encaminamiento de vectores de distancia entre routers
Protocolo Abrir la vía más corta primero (OPSF)	Permite el intercambio de información de encaminamiento de estado del enlace entre routers
Protocolo Gateway externo (EGP)	Permite el intercambio de información de encaminamiento entre routers externos

Descripción general del uso de TCP/IP

Las aplicaciones que se desarrollan con TCP/IP, normalmente, usan varios protocolos del conjunto. La suma de las capas del conjunto de protocolos se conoce también como el stack de protocolo. Las aplicaciones definidas por el usuario se comunican con la capa superior del conjunto de protocolos. La capa de nivel superior del protocolo del computador de origen traspasa la información a las capas inferiores del stack, que a su vez la pasan a la red física. La red física traspasa la información al computador de destino. Las capas inferiores del stack de protocolo del computador de destino pasan la información a las capas superiores, que a su vez la pasan a la aplicación de destino.

Cada capa del conjunto de protocolos TCP/IP tiene varias funciones; estas funciones son independientes de las otras capas. No obstante, cada capa espera recibir determinados servicios de la capa inferior y cada capa proporciona ciertos servicios a la capa superior.

La figura muestra las diferentes capas del conjunto TCP/IP. Cada capa del stack de protocolo del computador de origen se comunica con la misma capa del computador de destino. Las capas que se encuentran al mismo nivel en el computador de origen y de destino son pares. Así mismo, la aplicación del computador de origen y la del destino también son pares. Desde el punto de vista del usuario ó programador, la transferencia de paquetes se efectúa directamente de una capa par a otra.



Capas de los protocolos TCP/IP

El proceso que utiliza una aplicación para transferir el contenido de un archivo es el siguiente:

1. La capa de la aplicación envía un flujo de bytes a la capa de transporte del computador de origen.

2. La capa de transporte divide el flujo en segmentos TCP, asigna un encabezado con un número de secuencia al segmento en cuestión y transmite este segmento a la capa de Internet (IP). Se calcula la suma de comprobación.

3. La capa de IP crea un paquete con parte de los datos que contiene el segmento TCP. La capa de IP añade al paquete un encabezados que indica las direcciones IP de origen y de destino. Esta capa también determina la dirección física del computador de destino ó los computadores que actúan como intermediarios hasta el host de destino. Entonces, envía el paquete y la dirección física a la capa de enlace de datos. Se vuelve a calcular la suma de comprobación.

4. La capa de enlace de datos transmite el paquete IP en la sección de datos de una trama de enlace de datos al computador destino. Si el computador destino actúa como intermediario, el paso 3 volverá a repetirse hasta que se alcance el destino final.

5. Cuando se alcanza el computador destino, la capa de enlace de datos descarta el encabezado del enlace y envía el paquete IP a la capa de IP.

6. La capa de IP verifica el encabezado del paquete. Si la suma de comprobación del encabezado no coincide con la calculada por dicha capa, el paquete se ignora.

7. Si las sumas coinciden, la capa IP descarta el encabezado y envía el segmento TCP a la capa TCP correspondiente. Esta capa comprueba el número de secuencia para determinar si el segmento, es el segmento correcto de la secuencia.

8. La capa TCP calcula una suma de comprobación para los datos y el encabezado TCP. Si la suma no coincide con la suma transmitida con el encabezado, la capa TCP descarta el segmento. Si la suma coincide y el segmento está en la secuencia correcta, la capa TCP envía un reconocimiento al computador de destino.

9. La capa TCP descarta el encabezado TCP y transfiere los bytes del segmento que acaba de recibir a la aplicación.

10. La aplicación que se encuentra en el computador de destino recibe un flujo de bytes como si estuviera conectado directamente a la aplicación del computador de origen.

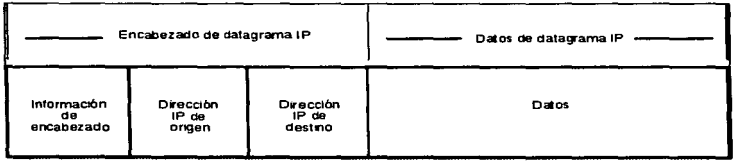
Las secciones siguientes describen estas operaciones interactivas con mayor detalle:

Protocolo Internet

En el conjunto de protocolos TCP/IP, todos los paquetes se entregan mediante el servicio de entrega de datagrams IP. Este servicio no garantiza la entrega de paquetes. Los paquetes pueden dirigirse a lugares a los que no corresponde, duplicarse ó perderse antes de llegar a su destino. Este servicio carece de conexión por lo cual tales paquetes se transmiten independientemente unos de otros. Esto puede contrastarse, por ejemplo, con una red telefónica en la que la conexión se mantiene una vez establecida.

Las aplicaciones TCP/IP que utilizan este servicio de entrega de datagram hacen un seguimiento del estado de la entrega esperando las respuestas desde el nodo destino ó utilizando uno de los protocolos de capa de transporte del conjunto TCP/IP.

IP define el formato que los paquetes deben tener y el modo de utilizarlos durante el envio y la recepción. El formato que toma el paquete se denomina datagram IP. Los datagram IP son análogos a las tramas físicas que se transmiten en una red. Los datagram tienen una sección de encabezado que incluye, entre otra información, las direcciones IP del receptor y del emisor y una sección de datos. La figura muestra el formato general de un datagram IP. Cada tipo de red transmite paquetes IP en la sección de datos de la trama física.



Estructura de datagram IP

Cuando un datagram IP se envía por una red, se encapsula en la porción de datos de la trama de la red física. Dado que la longitud de la trama de la red se define con independencia de IP, mediante requisitos técnicos de la red física, un datagram IP puede no ajustarse a una trama de red. Además, durante el camino que recorre hasta su destino, un datagram puede pasar a través de diferentes tipos de redes con diferentes longitudes de trama de red. Por lo tanto, puede suceder que un ruteador reciba datagram IP demasiado extensos para reenviarlos a la siguiente red.

Para solucionar este aspecto de la transmisión de paquetes, IP especifica un método para romper los datagram en fragmentos. Los fragmentos de un datagram IP vuelven a unirse cuando llegan al destino final. Cuando los fragmentos vuelven a unirse, se reconstruye el datagram por completo.

Encaminamiento

El término encaminamiento hace referencia a la transmisión de datagrams desde un nodo hacia otro en la misma u otra red diferente. La ruta hace referencia a las vías de acceso que se seleccionan para transmitir datagrams IP desde su origen hasta su destino, en base a direcciones IP que están contenidas en los datagrams.

En una red, los nodos que envían datagrams IP pueden llevar a cabo las acciones siguientes directamente:

* Consultar con los demás nodos de la red la dirección física que corresponde a una dirección IP

* Encapsular el datagram IP en una trama física que se encuentra en una dirección física.

* Enviar el datagram encapsulado directamente a la dirección física del nodo destino de la red.

Cuando se envía un datagram a un nodo que se encuentra en otra red, las secciones de la red de la dirección IP de origen y la dirección IP de destino son diferentes. El nodo emisor reconoce esta diferencia y envía el paquete al ruteador que conecta la red de origen con otras redes. Sólo es posible conectar dos redes si un ruteador está conectado a ambas redes y puede transferir datos en un formato compatible con ambas redes.

El nodo emisor contiene una tabla con direcciones IP de uno ó varios computadores de la red que actúan como ruteador para otras redes. Busca la dirección IP de un ruteador en la tabla y efectúa una difusión general de una petición ARP solicitando al ruteador su dirección física. Una vez que se conoce la dirección física, envía el paquete que contiene los datagrams IP a la dirección física del ruteador. Cuando el ruteador recibe un datagram IP, usa la dirección IP del datagram para enviarlo al destino final de forma similar. Si resulta necesario, el ruteador envía el paquete a la dirección de otro ruteador que puede encaminar el paquete a su destino.

Mensajes de error y control

Otro protocolo del conjunto de protocolos TCP/IP es el Protocolo de control de mensaje Internet (ICMP). Los paquetes ICMP contienen información sobre los errores originados en la red: nodos y "gateways" ó compuertas fuera de servicio, congestión de paquetes en un gateway, etc. El software IP, y no la aplicación, interpretan los mensajes ICMP. El software IP lleva a cabo la acción apropiada con el mensaje ICMP independientemente de la aplicación. Dado que estos mensajes pueden tener que viajar a través de varias redes para alcanzar el destino, se encapsulan en la sección de datos de un datagram IP.

ICMP se utiliza también para verificar la conectividad entre dos nodos. El nodo de origen envía una petición de eco ICMP ó PING y espera una respuesta de eco desde el destino.

Protocolos de nivel de transporte

El nivel de transporte del conjunto de protocolos TCP/IP consta de dos protocolos: el Protocolo de Datagrams de Usuario (UDP) y el Protocolo de Control de Transmisión (TCP). UDP proporciona un servicio de entrega sin conexión y poco fiable para enviar y recibir mensajes desde procesos específicos en los nodos origen y destino. TCP incorpora servicios de entrega de flujo de bytes fiable al servicio de entrega de datagrams de IP.

UDP

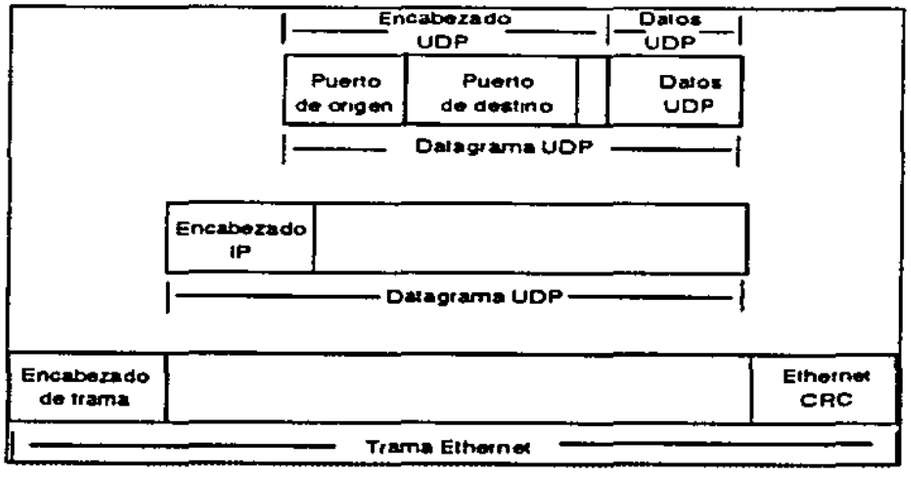
En el conjunto TCP/IP, UDP permite que las aplicaciones intercambien paquetes individuales de información por la red.

UDP define un conjunto de destinos como los puertos del protocolo. Así mismo, el protocolo define dos tipos de puertos de protocolo: asignaciones de puertos bien conocidos y puertos asociados dinámicamente. En el caso de asignaciones de puertos bien conocidos, determinados números de

puertos UDP se reservan para determinadas aplicaciones. Estos números están comprendidos entre 1 y 255, y se utilizan con aplicaciones específicas ampliamente utilizadas. Todas las aplicaciones de UDP hacen uso de dichos números de la misma manera. En el caso de los puertos dinámicamente asociados, las aplicaciones que solicitan servicios a un proceso concreto deben consultar al nodo para determinar el puerto utilizado por el proceso. A continuación, puede enviar los datagrams UDP a este puerto.

UDP permite que varios clientes utilicen el mismo número de puerto y diferentes direcciones IP. Los datagrams UDP que van llegando se entregan al cliente que corresponde al mismo número de puerto y dirección de destino. Si no se encuentra ningún cliente que corresponda, el paquete se suelta.

El datagram UDP se encapsula en uno ó varios datagrams IP, que a su vez se encapsulan en tramas físicas. La figura muestra un datagram UDP encapsulado en un datagram IP, que a su vez está encapsulado en una trama Ethernet. La figura también muestra cómo el concepto de capas, descrito al principio, influye sobre la estructuración de los paquetes enviados a través de la red.



Encapsulamiento de datagrams UDP

En este ejemplo, la dirección IP envía el datagram IP al nodo correcto. En el destino, el software IP extrae el datagram UDP y lo transmite al software de capas UDP. Este envía los datos UDP y la información de control al puerto de protocolo destino especificado. El proceso correspondiente a este puerto utiliza los datos del datagram UDP. Este datagram también contiene un puerto de protocolo de origen que el proceso destino utiliza para responder de forma correcta.

TCP

Para las aplicaciones que deben enviar ó recibir grandes volúmenes de datos, la entrega de datagrams no fiables puede convertirse en una carga. Los programadores de aplicaciones quizás deban desarrollar métodos para tratar los errores y módulos de información de estado a fin de hacer un seguimiento del progreso y estado de la transferencia de datos para cada aplicación. El conjunto de protocolos TCP/IP consigue evitar este problema al utilizar el TCP, que es un protocolo de entrega

de flujo de bytes fiable. TCP establece una conexión entre dos aplicaciones y envia un flujo de bytes al destino exactamente en el mismo orden en el que partieron. Antes de iniciarse la transmisión, las aplicaciones a ambos extremos de la transmisión obtienen un puerto TCP desde sus sistemas operativos respectivos. Estos puertos son análogos a los que utiliza UDP. La aplicación origen de la transferencia, conocida como parte cliente, suele obtener el puerto de forma dinámica. La aplicación encargada de responder a al petición de transferencia, conocida como parte servidor, suele obtener el puerto TCP bien conocido. La parte cliente es, normalmente, la parte activa y se encarga de iniciar la conexión con la parte servidor, que es la parte pasiva.

Del mismo modo que los datagrams UDP, los segmentos TCP se encapsulan en un datagram IP. TCP guarda el flujo en el buffer y espera a que un datagram de tamaño grande se llene de datos antes de enviarlo. Este flujo se caracteriza por carecer de estructura, de ahí que tanto la aplicación emisora como la receptora tengan que llegar a un acuerdo sobre el contenido del mismo antes de iniciar la transmisión. El protocolo TCP usa una transmisión dúplex integral (full-duplex). El dúplex integral significa que pueden enviarse dos flujos de datos simultáneamente en direcciones opuestas. En consecuencia, la aplicación destino puede enviar información de control ó datos de vuelta a la aplicación emisora mientras ésta continúa enviando datos.

El protocolo TCP asigna un número secuencial a cada segmento. La aplicación que se encuentra en el extremo receptor de la conexión, verifica que los números de secuencia se sucedan para asegurar que todos los segmentos se reciben y procesan en el mismo orden que el indicado por estos. El receptor envía un reconocimiento al emisor indicando los segmentos recibidos. TCP permite que el emisor tenga varios segmentos pendientes antes de que el receptor envíe un reconocimiento. Cuando el nodo emisor recibe el reconocimiento, indica a la aplicación que los últimos datos se enviaron satisfactoriamente. Si el nodo emisor no recibe el reconocimiento de un segmento, en un periodo de tiempo determinado, volverá a retransmitir este segmento. Este esquema, llamado retransmisión con acuse de recibo, asegura que la entrega de flujo sea fiable.

Direcciones Internet y físicas

En el nivel de enlace de datos, los nodos de la red que se comunican con otros nodos de la misma utilizan direcciones específicas para esa red. Un nodo puede ser un microcomputador, un servidor de archivos, una impresora inteligente ó cualquier otro dispositivo con una implantación TCP/IP propia.

Todos los nodos tiene una dirección física para el dispositivo de hardware determinado que se conectan con la red. Las direcciones físicas se representan y se asignan de diferentes formas según las redes. Por ejemplo, la dirección física de una red Ethernet se representan con un valor numérico de 6 bytes como, por ejemplo, 08-00-14-57-69-69. La dirección la asigna el fabricante del hardware de la interfaz de la red Ethernet. Las redes X.25 CCITT emplean direcciones físicas X.121 estándar formadas por números de 14 dígitos.

NOTA: Las direcciones físicas también reciben el nombre de direcciones de control de acceso a medios (MAC). Por lo tanto, cuando se mencionen las direcciones físicas ó MAC se hará referencia a las direcciones físicas de redes Ethernet, Token Ring ó FDDI. Las demás redes determinan las direcciones IP a partir de otros algoritmos.

Las direcciones IP de los nodos son direcciones lógicas y se determinan independientemente de cualquier topología de red ó hardware determinado; tienen el mismo formato, sin tener en cuenta el tipo de medios. Se trata de un valor numérico de 4 bytes (32 bits) que identifica tanto la red y el host

local ó el nodo (computador u otro dispositivo) de la red. La dirección IP de 4 bytes se suele representar con notación de puntos decimal. Los bytes se representan por un número decimal mediante números separados por puntos, por ejemplo, 129.47.6.17. En algunos contextos, las direcciones IP se identifican mediante números hexadecimales, por ejemplo, 0x81.0x2F.0x6.0x11 u octales, por ejemplo, 0201.057.06.021.

NOTA: La asignación de direcciones IP a direcciones físicas en redes de emisión como Ethernet, Token Ring ó ARCNET se efectúa mediante el protocolo de resolución de direcciones (ARP).

Los nodos con protocolos TCP/IP primero convierten las direcciones IP de destino en direcciones físicas de hardware MAC y después envían los paquetes a otros nodos de la red. En estos paquetes también se incluye la dirección IP de la aplicación origen. La aplicación destino puede responder a la aplicación emisora utilizando la dirección IP fuente que se encuentra en el paquete.

Dado que las direcciones IP no dependen de un tipo de red en especial, pueden utilizarse para enviar paquetes desde un tipo de red a otro. En cada tipo de red, el software TCP/IP establece la correspondencia entre las direcciones IP y las direcciones físicas de la red. Si un paquete se transmite a otra red, el software TCP/IP convierte la dirección IP destino en la dirección física de un ruteador que se encargará de reenviar el paquete a la red remota. La aplicación receptora utiliza la dirección IP fuente, que se encontraba en el paquete, para responder a la aplicación emisora del mismo modo.

Conversión de direcciones Internet en direcciones físicas

Los diferentes tipos de red utilizan formatos particulares para los paquetes que envían a través de sus nodos. La estructura de estos paquetes incluye, entre otros elementos, la dirección física del nodo destino. Todos los medios físicos tienen una dirección física asignada a los nodos del medio. Las direcciones físicas se denominan también direcciones de control de acceso a medios (MAC). Las redes Ethernet ó Token Ring representan sus direcciones MAC con 6 bytes y ARCNET las representa con 1 byte.

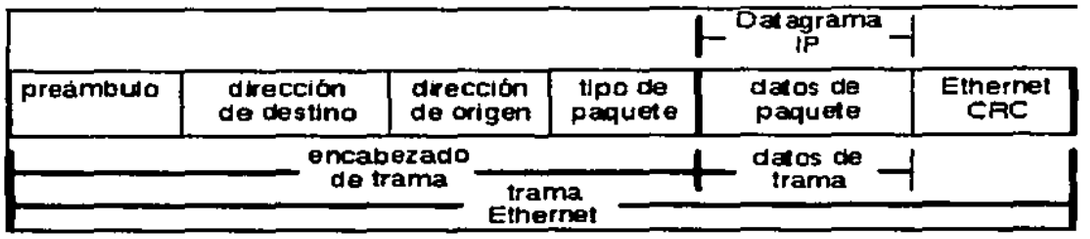
La figura muestra un ejemplo de una dirección física Ethernet. A cada nodo le corresponde una dirección MAC completa y única. Los tres primeros bytes representan un número de identificación de proveedor único y los tres siguientes, que pueden duplicarse entre varios proveedores, un número de identificación de tarjeta asignado a un proveedor.

Fabricante	Tarjeta
0x08 0x00 0x14	0x57 0x89 0x69

Dirección física Ethernet

Las direcciones IP son independientes del hardware que se utilice. Cuando un paquete IP se transmite por la red, en primer lugar se encapsula en la trama física que utiliza la red. La figura muestra un paquete IP encapsulado en una trama Ethernet. El paquete IP contiene una dirección Internet para un

nodo, pero la trama Ethernet debe disponer de una dirección física para poder entregarla en la red. Por consiguiente, el nodo emisor debe poder determinar la dirección física de la red que se corresponde con la dirección IP que contiene el paquete IP.



Encapsulación de datagrams IP

Asignación de direcciones Internet a direcciones físicas

La asignación de direcciones IP a direcciones físicas, ó MAC, en redes de emisión como Ethernet, Token Ring ó ARCNET se efectúa mediante ARP. Cuando un nodo envía un paquete utilizando IP, se debe determinar qué dirección física de la red se corresponde con la dirección IP de destino especificada en el paquete IP. Para determinar la dirección física, el nodo emite una difusión general de un paquete ARP con la dirección IP de destino. El nodo con la dirección IP de destino especificada envía la dirección física de nuevo al nodo que la solicita.

Caché de resolución de direcciones

Para aumentar la velocidad de la transmisión de paquetes y reducir el número de peticiones de difusión que cada nodo de la red debe examinar, los nodos disponen de una memoria caché de resolución de direcciones. Cada vez que un nodo difunde una petición ARP y recibe una respuesta, se genera una entrada en la memoria caché de resolución. Esta entrada asigna la dirección IP a la dirección física.

Cuando el nodo envía otro paquete IP, busca la dirección IP en la memoria caché. Si encuentra la dirección IP, el nodo utiliza la dirección física que corresponde al paquete. El nodo emite peticiones ARP sólo si no encuentra la dirección en la memoria caché.

Conceptos de direccionamiento de IP

En el siguiente tema se describe las direcciones de la red asignadas y direcciones de subred.

Asignación de direcciones de la red IP

Una dirección IP es necesaria para comunicar un nodo con otros nodos usando el conjunto de protocolos TCP/IP, incluidos los nodos de redes privadas ó los de Internet. La dirección de la red se determina a partir de uno de los siguientes modos.

Si quiere utilizar la red como parte de la comunidad Internet, es necesario adquirir una dirección Internet registrada de la siguiente organización:

Centro de información de la red DDN
14200 Park Meadow Dr., Suite 200
Chantilly, VA 22021
USA

Si la red no forma parte de la comunidad Internet, se puede elegir una dirección IP de red arbitraria. En este caso, las direcciones IP de todos los nodos de la red han de cumplir los siguientes requisitos:

* La porción de la red de todas las direcciones debe concordar con la dirección de la red. Por ejemplo, todos los nodos de la red 129.47 deben usar la dirección 129.47.

* La dirección IP de cada nodo de la red debe ser única en la red.

Clases de dirección IP

Cada dirección IP de 4 bytes se divide en dos partes:

* Una porción de la red, que identifica a la red

* Una porción del Host, que identifica al nodo

Las direcciones IP se dividen en tres clases según los dos bits más importantes de los cuatro primeros bytes. Esto se hace para que los ruteadores puedan extraer la porción de la red de la dirección de manera eficiente.

Esta división puede caer en una ó dos ubicaciones de la dirección de 32 bits. Estas divisiones corresponden a las tres clases de dirección IP: Clase A, Clase B, y Clase C. A pesar de la clase de dirección, todos los nodos de una red única comparten la misma porción de la red; cada nodo tiene una porción única.

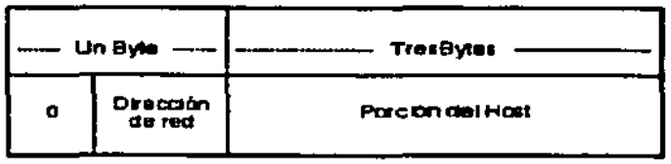
Direcciones de Clase A

Una dirección IP de la clase A consiste en una porción de la red de un byte seguido por una porción del Host de 3 bytes. El bit de mayor orden de la porción de la red se define siempre en 0. Por lo tanto, en una interred, puede haber un total de 126 redes Clase A (de 1 hasta 126), con más de 16 millones de nodos por red (las redes 0 y 127 están reservadas).

Por ejemplo ('n' = dirección de la red y 'h' = dirección del Host):

Clase A 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

(7 bits de la dirección de la red, 24 bits de la dirección del Host)



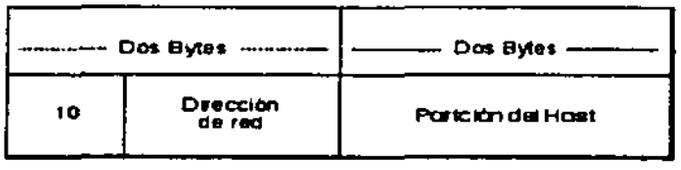
Direcciones de Clase B

Una dirección IP de la Clase B consiste en una porción de la red de dos bytes seguidos por una porción del Host de 2 bytes. Los dos bits de orden superior de la porción de la red están siempre definidos por 10. Por lo tanto, en una interred única pueden haber aproximadamente 16,000 redes de Clase B (de 128.x hasta 191.x), con más de 65,000 nodos por red.

Por ejemplo ('n' = dirección de la red y 'h' = dirección del Host):

Clase B 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

(14 bits de dirección de red y 16 bits de dirección del Host)



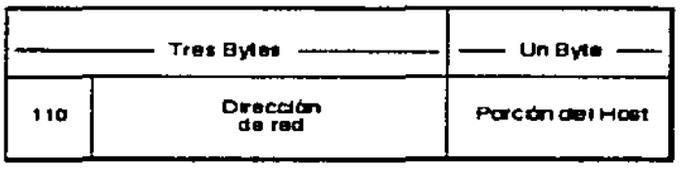
Direcciones de Clase C

Una Dirección IP de Clase C consiste en una porción de la red de tres bytes seguidos por una porción del Host de 1 byte. Los tres bits de orden superior de la porción de la red están siempre definidos en 110. Por lo tanto, en una red única, pueden haber aproximadamente 2 millones de redes Clase C (de 192.x.x hasta 223.x.x), con más de 254 nodos por red.

Por ejemplo ('n' = dirección de la red y 'h' = dirección del Host):

Clase C 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

(21 bits de dirección de red y 8 bits de dirección del Host)



Identificación de las clases de red

Cuando el primer byte de una dirección IP se adapta al rango listado en la parte inferior, identifica a cuál de las tres clases de redes pertenece:

1-126 (1.h.h.h-126.h.h.h) Clase A

128-191 (128.n.h.h-191.n.h.h) Clase B

192-223 (192.n.n.h-223.n.n.h) Clase C

Una dirección IP empezada con 154 es una dirección Clase B, con los primeros dos bytes de la dirección representando la porción de la 'r'ed de la dirección y los dos últimos representando la porción 'h'ost. Por ejemplo, en la dirección IP de 154.1.0.3 la porción de la red es 154.1.0.0, y la porción del Host es #.#.0.3.

La porción de red de la dirección IP ha de ser la misma en todos los nodos conectados a la red. La interfaz de red del servidor conectado a la red 89.0.0.0 debe tener asignado una dirección del Host IP única, como 89.0.0.254.

SUGERENCIA: La clave para seleccionar un número a la porción del Host de una dirección IP es asegurar que el número seleccionado es único; es decir, que ningún otro host de la red tiene la misma dirección IP.

Selección de una clase de dirección apropiada

La selección de una clase determinada de dirección IP debe realizarse a partir de los números de red y porciones de dirección host. Ya que el primer bit, los dos primeros bits ó los tres primeros bits determinan como se ha de interpretar la dirección entera y en dónde se produce la división de la porción de la dirección del Host y de la red deberia conocer las consecuencias de la elección. Si se decide por una clase de red, deberá considerar el número de nodos que se soportarán en la red TCP/IP y el número de redes que se van a configurar.

Por ejemplo, si se utiliza una dirección IP Clase C (los tres primeros bits son de tipo 110 binario), sólo se podrán conectar 254 nodos a la red

Direcciones IP reservadas

Las reglas de direccionamiento IP reservan los siguientes tipos de direcciones IP para propósitos especiales:

Direcciones de la red. Estas son las direcciones IP en las que la porción del Host está definida con ceros. Por ejemplo, 129.47.0.0 es la dirección (o número de red) correspondiente a una red Clase B. Se trata de direcciones de redes y no de nodos de red. Por regla general, ningún nodo tiene asignado una sección del Host formada sólo por ceros.

Direcciones de difusión general. Son direcciones en las que la porción del Host está definida en todos unos. Un paquete con una dirección de difusión general se destina a todos los nodos de la red. Por norma general, ningún nodo tiene asignado una porción del Host formada sólo por unos.

Direcciones de retorno de bucle. La dirección de la red 127.0.0.0, y todas las direcciones del Host en la red, por ejemplo, 127.0.0.1, son reservadas.

Direcciones reservadas. Son direcciones en las que la porción de red está formada por ceros ó todos unos.

Creación de subredes

Una red Internet (en una dirección de la red Internet única) puede dividirse en una ó más redes más pequeñas. En la parte inferior están listadas algunas de las razones para dividir la red:

Usar varios medios. Puede ser imposible, inconveniente ó demasiado caro conectar todos los nodos en un medio de la red única cuando estos nodos están demasiado lejos ó conectados a un medio diferente.

Reducir la congestión. El tráfico entre nodos en una red única usa un ancho de banda de la red. Como resultado, se requieren más anchos de banda cuando el usuario tiene más nodos. La división de los nodos en varias redes reduce el número de nodos de la red. Si los nodos de una red de tamaño pequeño se comunican principalmente con otros nodos de la misma red, el nivel de congestión se reduce.

Reducir el uso del CPU. La reducción del uso del CPU los nodos conectados es similar a la reducción de la congestión. Más nodos en la red causan más difusiones generales en la red. Incluso si una difusión general no se envía a un nodo en particular, cada nodo de una red debe reaccionar ante la misma antes de decidir si debe aceptar ó descartarse.

Aislar una red. La división de una red de mayor tamaño en redes más pequeñas, limita el impacto de uno de los problemas de la red sobre otra. Entre estos problemas se pueden incluir el error de hardware de la red, como una interconexión Ethernet abierta, ó errores de software, como una operación de emisión confusa.

Mejorar el nivel de seguridad. En un medio de red de difusión general como es Ethernet, cada nodo de una red tiene acceso a todos los paquetes enviados a la misma. Si se permite sólo un tráfico de red sensitivo en una red, otros monitores de red pueden evitar el acceso a éste tipo de tráfico.

Hacer uso eficiente del espacio de la dirección IP. Si está asignando un número de red Clase A ó B y tiene varias redes físicas pequeñas, puede dividir el espacio de dirección IP en varias subredes IP y asignarles redes físicas individuales. Con el uso de este método, no necesita conseguir más números de redes IP por cada red física.

Máscaras y direcciones de subredes

Cada subred funciona como si fuera una red independiente. Para redes remotas, sin embargo, las subredes aparecen colectivamente como redes discretas y únicas. Esto significa que la red local sólo necesita una dirección de red IP y estas redes remotas no necesitan poner atención en la ubicación de un nodo en una subred particular.

La comunicación entre un nodo en una subred local y un nodo en una subred diferente es parecida a la comunicación entre nodos de dos redes diferentes. Para un usuario, el encaminamiento entre subredes es transparente. Internamente, el software IP reconoce cualquier dirección IP que esté destinada a una subred y envía estos paquetes al ruteador de la misma.

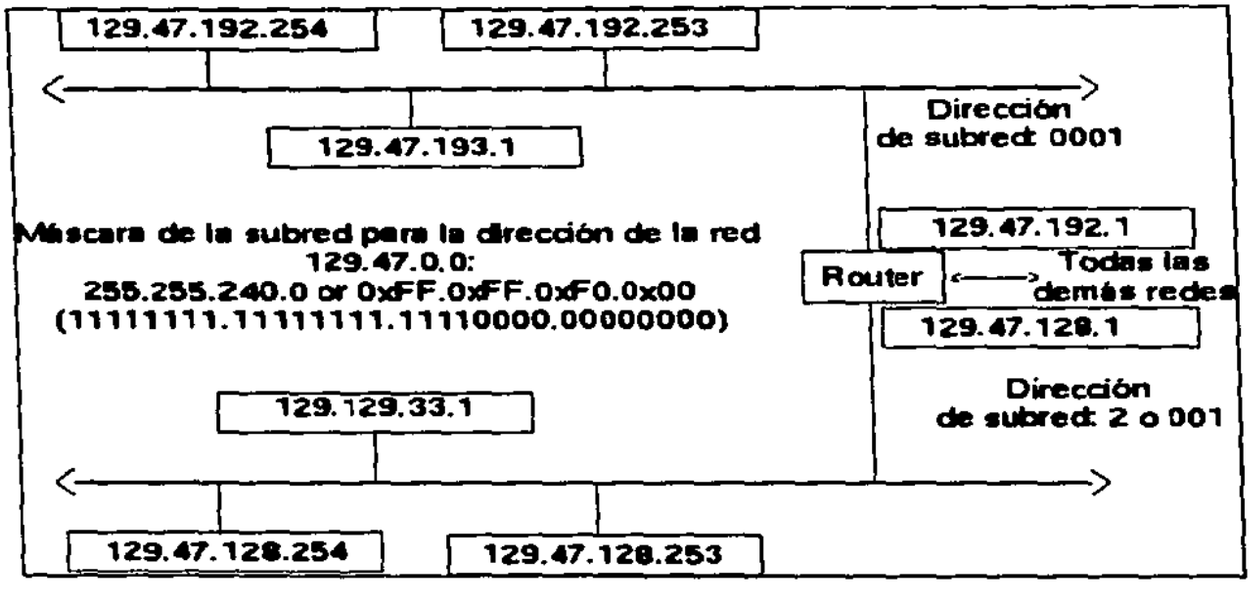
Al igual que en la comunicación entre redes, la información del encaminamiento para la comunicación de la subred entre subredes se mantiene en la tabla de encaminamiento (por IP) para cada nodo ó ruteador. Sin embargo, en el caso de las subredes, dicha información está formada por la dirección de la red y la dirección de la subred.

Cuando una red se distribuye en varias subredes, la porción del Host de la dirección IP se divide en dos partes, al igual que la dirección IP se divide en dos partes. La porción de la dirección del Host especifica la subred de la red IP y el nodo de dicha subred.

Por lo tanto, la dirección IP de 4 bytes consta de las siguientes porciones:

Por ejemplo, si una red tiene la porción de la dirección de la red Clase B 129.47, el resto de dicha dirección se puede dividir en direcciones de subred y del Host. Esta división está controlada por la red local a fin de obtener una mayor flexibilidad en el funcionamiento de la red a nivel local. Por ejemplo, la dirección de subred puede contener cuatro bits de los dos bytes restantes. Esto permite 15 subredes, cada una con 4094 nodos. En otro ejemplo, la dirección de la subred puede contener ocho bits, lo que permite usar 254 subredes (una dirección de subred de todos los unos no es válida), cada una con 254 nodos.

La figura muestra una red IP dividida en dos subredes. El ruteador mostrado dispone de conexiones físicas y direcciones IP en ambas subredes (129.47.128.1 y 129.47.192.1). También podría disponer de dispositivos físicos y direcciones IP (nn.nn.nn.nn) conectados a otras redes.



División de una red en dos subredes

Una máscara de subredes indica cómo se divide la porción del Host de una dirección IP en direcciones de subredes y porciones de dirección del Host local. La máscara de la red está representada por un número de 32 bits en el que las porciones de dirección de red y subred están formadas por una dirección IP completa y todas las del Host por ceros. Por ejemplo, con una porción de la dirección de la red IP de Clase B de 129.47 y una dirección de la subred de 4 bits, la máscara de subred constará de 20 unos y 12 ceros. En resumen, una máscara de subred amplía la porción de la dirección de la red de una dirección IP local.

Direcciones de difusión general

Hay tres tipos de direcciones de difusión general: difusiones generales de red, difusiones generales de subred y las direcciones de difusión general. Una difusión general de red tiene una dirección IP de destino en la porción de la red de la dirección IP definida en la red Clase A, B, ó C, y el campo del Host definido en todos unos. La difusión general de red dirigida se envía a todos los hosts de una red específica.

Si la red se divide en subredes, cada subred tendrá una difusión general de subred. Una difusión general de subred tiene una dirección IP con el campo de la red definido para el identificador de la red, el campo de la subred definido para el identificador de la subred, y el campo del Host definido para todos los 1.

Generalmente, las difusiones generales no se reenvían. La difusión general de red y de subred son reenviados a una red de destino, ó para difusiones generales de la subred, por la intervención de ruteadores cuando el usuario habilita el reenvío de difusiones generales directos.

Una dirección IP con el campo host y el de subred definidos en unos, se interpreta como una difusión general dirigido a todas las subredes de la red. Es decir, el primer ruteador de la red especificada la

difunde a una de sus subredes. Entonces los ruteadores de esta red los reenvía y los difunde a una de sus subredes.

Una dirección IP con todos unos, 255.255.255.255, también son una dirección de difusión general. Está dirigido a todos los hosts de la subred desde donde ha sido originado la difusión general. Esta difusión general no se reenvía a otras redes ó subredes.

Direcciones de multidifusión

Una dirección de multidifusión se usa para enviar paquetes a un grupo de hosts ó ruteadores. Todos los hosts y ruteadores que pertenecen al grupo de multidifusión reciben un paquete con una dirección de multidifusión. Un rango de direcciones Clase D se reservan para direcciones de multidifusión, desde 224.0.0.1 hasta 239.255.255.255.

Se pueden utilizar dos grupos de direcciones de multidifusión. Un conjunto lo usa **OSPF** para realizar una multidifusión de paquetes **OSPF** y para ruteadores **OSPF**. Las direcciones son 224.0.0.5 y 224.0.0.6. El otro conjunto lo usan mensajes de Descubrimiento del Ruteador para realizar la multidifusión de avisos del ruteador y de mensajes de solicitud. Las direcciones son 224.0.0.1 y 224.0.0.2.

RIPII usa la dirección de multidifusión 224.0.0.9.

Conceptos del protocolo de encaminamiento TCP/IP

Ventajas del encaminamiento dinámico

Para que TCP/IP desarrolle funciones de encaminamiento, este debe tener acceso a la información actual sobre las rutas disponibles. Esta información se guarda normalmente en una tabla de rutas, donde las entradas individuales especifican lo siguiente:

* Dirección de destino final

* Dirección del próximo ruteador de la ruta hacia el destino

* Información relativa al costo de acceso al destino (como la distancia ó el número de saltos)

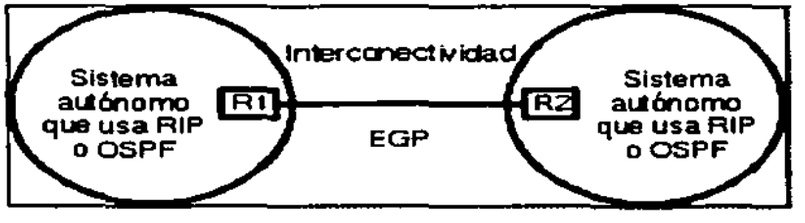
Las entradas en la tabla de rutas pueden hacerse manualmente ó de manera dinámica mediante el uso de protocolos de encaminamiento. Las entradas manuales llamadas rutas estáticas, tienen la desventaja de quedarse obsoletas. Cualquier cambio en la red (tal como un fallo ó la adición de un nuevo nodo) necesita intervención manual para la reconfiguración de las rutas estáticas en todos los ruteadores que tengan acceso al área afectada. Dada la naturaleza dinámica de la mayoría de las redes, el mantenimiento manual de las tablas de rutas estáticas se utiliza solamente en circunstancias especiales.

En la mayoría de las redes, la única manera de responder a los cambios de la red lo suficientemente rápido como para mantener la conectividad es mediante el uso de un protocolo de encaminamiento. Un protocolo de este tipo detecta de manera dinámica un cambio en la red y actualiza todas las tablas de rutas afectadas. El protocolo efectúa esta operación mucho más rápido de lo que podría una persona con el uso de un encaminamiento estático.

Topología y protocolos de encaminamiento

La unidad más grande de una topología de interred es un sistema autónomo (AS- Autonomous System). Este es un conjunto de redes y ruteadores que intercambian información de encaminamiento mediante el uso de un protocolo de encaminamiento, como por ejemplo, RIP ó OSPF. Los protocolos de encaminamiento que se utilizan en el sistema AS se llaman "Internal Gateway Protocol" ó protocolos de compuerta internos (IGP). Normalmente, los ruteadores que tienen un AS comparten información de encaminamiento entre ellos sin ningún problema. De todas maneras, por regla general, la información de encaminamiento que se comparte con otros sistemas AS es restringida. Los ruteadores de diferentes AS usan un protocolo de encaminamiento externo, como el "External Gateway Protocol" ó el Protocolo de Compuerta externo (EGP), para compartir información. Ver la figura.

NOTA: "Gateway" ó compuerta es el término antiguo equivalente a ruteador.



Conexión de dos sistemas autónomos

Protocolos Gateway internos

RIP es un protocolo estándar basado en el algoritmo de vector de distancia. La mayoría de los emplazamientos del TCP/IP continúan utilizando RIP. OSPF es un nuevo protocolo IGP basado en un algoritmo de estado del enlace. OSPF está siendo rápidamente aceptado en los emplazamientos públicos y privados con redes más grandes y complejas. Al instalar emplazamientos de RIP ya existentes, el software permite que coexistan ambos protocolos y que compartan la información de encaminamiento.

Protocolos Gateway externos

Los protocolos de encaminamiento externo, como el EGP, cambian información entre diferentes sistemas autónomos AS. Un "Gateway" de borde obtiene la información de encaminamiento según su propio sistema AS a través del protocolo IPG local. Por eso usa el EGP para compartir información con otros "Gateways" de borde.

RIP (protocolo de información de encaminamiento)

RIP es un protocolo de vector de distancia. Un ruteador RIP difunde periódicamente un mensaje de actualización del encaminamiento que contiene una entrada y el coste para cada red que pueda alcanzar. Los ruteadores RIP escuchan todos los mensajes de difusión. Cada entrada de mensaje de

actualización de encaminamiento recibido se añade a la tabla de rutas local. El ruteador que envía el mensaje de actualización de encaminamiento queda como el próximo ruteador ó salto de la ruta a la red en la entrada. Si un ruteador conoce dos rutas para acceder a la red, toma la que le suponga menor coste. El coste se define a menudo para RIP en términos del recuento de saltos, ó de número de ruteadores en la vía de acceso hacia el destino. RIP permite como máximo un coste ó recuento de saltos de 15.

Una vez que se conoce la ruta, debe consultarse a intervalos, verificando que esta aún es válida. Normalmente, cada 30 segundos los ruteadores RIP difunden un mensaje de actualización de encaminamiento que contiene rutas conocidas. Cuando se adquiere una ruta nueva a partir de un mensaje de actualización de encaminamiento, se activa un temporizador. Si durante los 180 segundos siguientes, los mensajes posteriores no renuevan la ruta, ésta es considerada inservible. Por eso se elimina de la tabla de rutas.

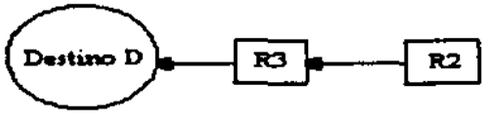
RIPII es un RIP mejorado; en sus rutas, incluye la máscara de subred. La falta de información de máscara de subred limita al RIP a notificar rutas de red, ó necesita ruteadores RIP para suponer que tipo de máscara se utiliza. Cuando se usa RIP en una red con subredes, es necesario que todas las subredes utilicen la misma máscara de subred.

RIPII se puede usar en topologías de red que necesiten máscaras de subred de longitud variable y puede dar soporte a la subred cero. RIPII puede también autenticar cambios de mensaje de encaminamiento. RIPII usa direcciones de multidifusión en lugar de direcciones de difusión. No todos los ruteadores RIP dan soporte al RIPII.

Conceptos RIP

Como RIP no puede detectar ni corregir bucles de encaminamiento, no son válidas las rutas que se han adquirido a través de RIP que excedan de los 15 saltos. Esto quiere decir que la distancia entre cualquier origen y destino de la red no pueden ser superior a 15 saltos. Este límite de recuento de saltos puede hacer que RIP no sea práctico en redes grandes.

Los ruteadores RIP también pueden experimentar inconsistencias en la tabla de rutas. Esto se debe al tiempo que tardan todas las tablas de encaminamiento de RIP en sincronizar entre ellas cuando tiene lugar un cambio ó un tiempo de convergencia en la red. La razón más seria de la convergencia baja de RIP, conocida por el problema de cuenta al infinito, se muestra en el caso de la figura



Convergencia baja con RIP

En la gráfica, las flechas muestran la ruta al destino D. El ruteador R2 ha adquirido ruta al destino D del ruteador R3. Si se desactiva el enlace de R3 al destino D, R3 pierde la ruta hacia D de la tabla de rutas. Como R2 tiene una ruta válida hacia D que aprendió de R3, enviará a éste una actualización de RIP en la que se comunicará que puede acceder al destino D al coste de dos saltos. R3 calcula que puede alcanzar el destino D en tres saltos, uno para llegar a R2 y dos más para el destino D. R3 introduce una nueva ruta hacia el destino D en su tabla de rutas.

Este proceso crea un bucle de encaminamiento. En este caso, cualquier paquete de datos destinado a D, recibido por R3 ó R2, se encaminará de un lado a otro hasta que expire su validez.

Como R3 y R2 siguen actualizándose el uno al otro, el proceso de actualización tarda algún tiempo en resolverse. Dado que R2 ya no va a adquirir de R3 la ruta hacia D con un coste de 1, al final, expira su ruta hacia D con un coste de 2. Por eso R2 sabe que la distancia de R3 al destino D es tres, y calcula el coste nuevo de su ruta al destino D con un coste de cuatro. En la próxima vuelta, R3 incrementa su coste a cinco. Ambos routers siguen incrementando su coste al destino D hasta que finalmente se alcance el número de 16. Esta sincronización de tablas de rutas puede tardar varios minutos.

Creación de subredes con RIP

RIP no puede soportar subredes de manera completa debido a que en sus notificaciones no contiene información de máscara de subred (aunque RIPII si que puede soportarlas). De todas maneras, un ruteador RIP puede obtener información de máscara de subred de sus interfaces. RIP asume que las máscaras de subred son fijas para todas las subredes de la misma red, por eso aplica la máscara de subred obtenida a todas las subredes de la misma red.

Este método de soporte de subred requiere una máscara de subred fija para una determinada red. Como resultado, RIP no da soporte a las máscaras de subred de longitud variable. Además, la información de máscara de subred derivada de la interfaz sólo se aplica en la red a la que pertenece la interfaz. La información de subred de redes remotas no está disponible para el ruteador RIP. Por lo tanto, el RIP no da soporte a las subredes de redes remotas.

Dado que los ruteadores del RIP externos a la red no conocen las subredes utilizadas en una red, RIP requiere que todas las rutas de la subred se agrupen en una sola ruta de red cuando son notificadas desde el exterior. Para que esto se cumpla, todas las subredes deben estar incluidas en los límites de una sola red.

OSPF (Abrir la vía más corta primero)

OSPF es un protocolo de encaminamiento de estado del enlace. Los ruteadores de estado del enlace intercambian información sobre el estado de las conexiones ó los enlaces de sus redes. Con esta información, cada ruteador puede construir la topología de la interconectividad y obtener información de encaminamiento.

A diferencia de RIP, OSPF no tiene el problema de cuenta al infinito. Por lo tanto, su métrico no está limitado a 16. Un métrico OSPF puede ser tan largo como 65535. Con un métrico más grande, se puede construir una interred más grande. Además, esto permite asignar un rango más amplio de costes para los distintos tipos de redes basado en características como por ejemplo ancho de banda.

OSPF también converge en la información de encaminamiento común más rápidamente que **RIP**. Esto se debe a que **OSPF** no tiene el problema de cuenta al infinito y la información de estado del enlace se desborda instantáneamente en lugar de procesarse en cada paso, como ocurre en **RIP**. Una convergencia rápida evita la pérdida de conectividad y de bucles de encaminamiento temporales.

Finalmente, **OSPF** genera menos tráfico. A diferencia de **RIP**, que requiere actualizaciones periódicas, los ruteadores **OSPF** actualizan la información de estado del enlace sólo cuando este cambia ó cada 30 minutos en lugar de los 30 segundos de las actualizaciones **RIP**. Como consecuencia, se dispone de más ancho de banda para el tráfico de datos.

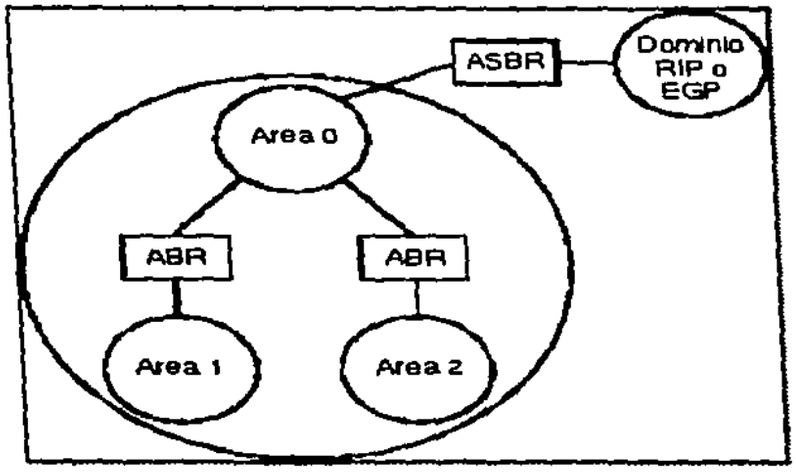
Para obtener más información sobre el protocolo **OSPF**, consulte **RFC** 1583.

Topología OSPF

Las áreas **OSPF** están conectadas de una manera jerárquica. El sistema AS de **OSPF** puede dividirse en diferentes regiones, llamadas áreas. Al estar dividido en áreas, debe haber una área especial llamada área del segmento principal. Todas las áreas **OSPF** están conectadas al área del segmento principal.

Los ruteadores que conectan un área con el área del segmento principal se llaman ruteadores de límite de área. Un ruteador de límite de área tiene al menos una interfaz en un área que no es del segmento principal y una interfaz en un área de segmento principal.

Los ruteadores **OSPF** pueden intercambiar información con otros sistemas AS ó dominios que ejecuten un protocolo de encaminamiento diferente, como **EGP** ó **RIP**. El "Gateway" efectúa los intercambios entre los protocolos de encaminamiento en el límite del dominio de **OSPF**. Este "Gateway" se llama ruteador de límite de sistema autónomo, ó **ASBR**. Un **ASBR** debe ejecutar tanto **EGP** ó **RIP**, como **OSPF**, para adquirir información de encaminamiento de otros dominios u otros sistemas AS. Después la difunde a través del dominio **OSPF** para los ruteadores **OSPF**.



Áreas OSPF

Partición de área

A medida que crece el dominio OSPF, crece la probabilidad de cambio de estado del enlace, debido a que incluye más ruteadores y redes. Por lo tanto, cada cambio del estado del enlace provoca el recuento de rutas en todos los ruteadores, aumentando la carga en el CPU. Además, cada recuento de una ruta lleva más tiempo, dado que hay más redes de destino que contar. Cuando el dominio OSPF se hace muy grande, es posible que desee dividirlo en varias áreas para reducir la carga del CPU.

La partición del dominio OSPF en áreas proporciona varias ventajas. Permite la separación administrativa de diferentes grupos organizativos ó geográficos, como ingeniería ó ventas. La creación de áreas permite limitar el compartir de la información de encaminamiento de las mismas, haciendo un área en particular más segura. Además, reduce el número de notificaciones de estado del enlace (LSA) en el área y permite aislar un área con cambios de topología frecuentes.

Ruteadores de límite de área

Los ruteadores de borde de área (ABR) comparten información que notifica destinos del área de segmento principal al área que no es del segmento principal. Además, los ABR comparten información que notifican los destinos de un área que no es del segmento principal a un área del segmento principal. A estos se le llama anuncios del resumen de enlace.

Ruteadores límite de sistema autónomo

La información de encaminamiento de otros sistemas AS (como RIP) ó a través de protocolos Gateway externos (como EGP) ó de otros protocolos de encaminamiento, pueden combinarse y difundirse a través de los ASBR. Debido a que proporcionan una interfaz a otros sistemas AS y protocolos de encaminamiento, los ASBR tienen acceso a la información de encaminamiento que se ha adquirido de ruteadores que se encuentran fuera del dominio OSPF. Los ASBR pueden ser internos ó ruteadores de borde de área, y no necesitan formar parte del área de segmento principal.

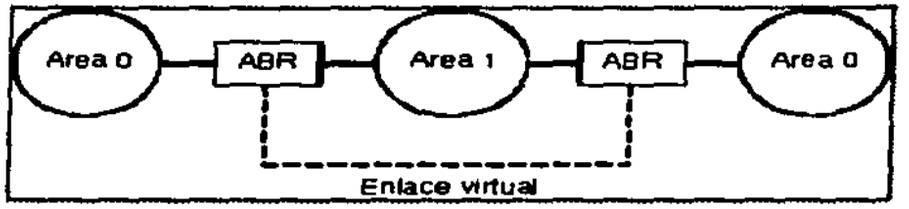
Enlaces virtuales

Un enlace virtual permite ampliar un área de segmento principal al juntar dos áreas divididas. Además, permite aislar un área en la que se efectúen cambios topológicos de manera frecuente.

Las redes y los ruteadores en un área de segmento principal OSPF deben estar interconectados. De todas maneras, al dividir el dominio OSPF en áreas, es posible que el área de segmento principal quede dividida por razones geográficas. Las secciones del área de segmento principal pueden volver a conectarse a través de un enlace virtual.

Un enlace virtual es realmente una vía de acceso a través del área de tránsito, ó de un área que no es de segmento principal. Los ABR a cada extremo del enlace virtual consideran la vía de acceso entre ambos como un enlace punto a punto. Con el uso de ese enlace virtual punto a punto, se vuelven a conectar las diferentes secciones del área de segmento principal seccionada.

El uso de un enlace virtual es complicado y propenso a errores. Por este motivo se recomienda que se trate de mantener el área de segmento principal físicamente conectada. El enlace virtual debería utilizarse sólo en caso de que fuera necesario.



OSPF virtual y áreas de tránsito

Áreas de pseudorutina

OSPF también soporta el uso de áreas de pseudorutina. Cuando sólo hay un ABR para un área, todos los destinos hacia el exterior de ese área pasan a través de ese ruteador. En este caso, es posible que desee configurar el área como un área de pseudorutina. Este tipo de áreas no permiten que los ABR notifiquen rutas externas, entendiéndose por estas las rutas a otras áreas ó rutas externas del dominio OSPF. Los ABR notifican una sola ruta por defecto. Al no generar notificaciones de destinos individuales, un área de pseudorutina ahorra memoria, CPU, y recursos de ancho de banda en todos los ruteadores OSPF.

El área de pseudorutina no permite que los ABR pasen notificaciones de estado del enlace externas a otras áreas. Por este motivo, los ASBR no pueden colocarse en un área de pseudorutina. Un ASBR en un área de pseudorutina hace que circulen notificaciones de enlace exterior sólo dentro del área. Como resultado, todos los ruteadores OSPF que se encuentren fuera del área de pseudorutina no adquieren conocimientos acerca de los destinos exteriores.

Encaminamiento jerárquico

OSPF tiene tres tipos de encaminamiento jerárquico:

El encaminamiento dentro de un área ó encaminamiento de área interna, puede producirse sin tener conocimiento de información de encaminamiento de otras áreas. De todas maneras, para hacer encaminamientos de un área a otra, ó encaminamiento entre áreas, los paquetes deben pasar al ruteador de borde de área local y después al ruteador de límite del área de destino antes de pasar al área de destino.

El encaminamiento entre áreas requiere que se comparta la información de encaminamiento de un área con otros ABR.

Notificaciones de enlaces externos

El encaminamiento entre el dominio OSPF y otros, como por ejemplo RIP ó EGP, se realiza a través de los ASBR. A este proceso se le conoce por el nombre de notificaciones de enlace externo. Los ASBR se ubican en el borde del dominio OSPF. Difunden los destinos exteriores mediante la propagación de notificaciones externas por todo el dominio OSPF.

Hay dos tipos de notificaciones de enlace externo, de tipo 1 y de tipo 2. El significado del métrico de notificación de enlace externo depende del tipo.

Ruteadores y Hosts de OSPF

OSPF es un protocolo de ruteador a ruteador que cambia información de encaminamiento entre ruteadores. Los Hosts no participan en los intercambios de OSPF. Como resultado, a los Hosts no se les informa acerca de los ruteadores y de las rutas descubiertas por el protocolo OSPF. Para proporcionar Hosts con la información de encaminamiento de OSPF, puede utilizar una de las configuraciones siguientes:

* Configuración de Hosts para que usen los ruteadores definidos por defecto.

* Configuración de los Hosts y los ruteadores de OSPF para que puedan intercambiar los mensajes de descubrimiento del ruteador de ICMP. Esto permite que el Host descubra de manera dinámica los ruteadores de la red definidos por defecto.

* Configuración de los ruteadores OSPF para que envíen periódicamente mensajes de actualización de RIP a los Hosts. Estos mensajes informan a los Hosts acerca de todos los destinos disponibles.

El primer método precisa que se configuren Hosts para que usen los ruteadores por defecto manualmente. Este es el único método que funciona si los Hosts no entienden los mensajes de descubrimiento del ruteador ó los mensajes RIP.

El segundo método requiere que los Hosts soporten el mecanismo de descubrimiento del ruteador de ICMP. Si el Host lo soporta, puede configurar el software para que, periódicamente, genere mensajes de notificación de encaminamiento de ICMP que comuniquen a los Hosts que este pueden actuar como el ruteador por defecto.

Para el tercer método se necesita que el Host entienda los mensajes RIP. Muchos Hosts más grandes, como las estaciones de trabajo UNIX entienden el RIP. En ese caso, se puede configurar el software para que vuelque su tabla de rutas en la red utilizando mensajes de actualización de RIP periódicos. (Esta es la opción Sólo enviar). Las desventajas de este método son que provoca desfases en las redes grandes, ya que los mensajes de actualización de RIP son grandes y se difunden cada 30 segundos.

Interacciones entre OSPF y otros protocolos de encaminamiento

En las siguientes secciones se explican las interacciones de OSPF con otros protocolos de encaminamiento.

Preferencia de protocolo

Cuando varios protocolos proporcionan rutas para el mismo destino, éstas se añaden a la tabla de rutas en el siguiente orden de preferencia:

* Las rutas internas de OSPF tienen un nivel de preferencia 1.

* Las rutas externas de OSPF tipo 1 tienen un nivel de preferencia 2.

Las rutas externas de OSPF tipo 2 y las rutas externas de otros protocolos, como RIP, EGP y otras rutas externas tipo 2 tienen un nivel de preferencia 3.

Métricos de rutas externas de OSPF

Si dos rutas tienen la misma preferencia, la ruta con el mejor métrico se añade a la lista de rutas. Por ejemplo, al evaluar dos rutas internas de OSPF para el mismo destino, una con el métrico 10 y la otra con el 20, la primera es la que se añadirá a la tabla de rutas. Si el métrico es el mismo entre una ruta de tipo 2 externa y una ruta de RIP ó de EGP, la ruta recibida de estos dos últimos es la preferente.

Aunque el métrico de la ruta determina la preferencia entre dos rutas diferentes (hacia el mismo destino) generadas por el mismo protocolo, puede que no sea posible determinar esta preferencia al comparar los métricos de dos rutas generadas por dos protocolos diferentes. El significado del métrico difiere de protocolo a protocolo, y no es necesariamente comparable.

El único caso en el que es necesario comparar el métrico de protocolos diferentes es en el nivel 3 de preferencia de protocolo, donde las rutas externas de OSPF tipo 2, RIP y EGP tienen la misma preferencia.

Las rutas de RIP y EGP se consideran comparables. Por este motivo, entre las rutas de RIP y EGP al mismo destino, la ruta con el métrico más pequeño se añade a la tabla de rutas. Sin embargo, la comparación entre rutas de OSPF con rutas de RIP y EGP no es tan sencilla como la comparación entre rutas de RIP y EGP.

Una ruta externa de OSPF tiene dos métricos, uno interno y otro externo. Para las externas tipo 2, el métrico externo se puede comparar a los métricos de RIP y EGP, mientras que el métrico interno es mucho más pequeño que el externo. Por lo tanto, al comparar una ruta externa tipo 2 con una ruta de un RIP ó EGP, el métrico externo de OSPF se compara con el métrico de RIP ó EGP.

Por ejemplo, supongamos que una ruta de RIP y otra de OSPF se presentan en la red de manera simultánea. La ruta de RIP tiene un métrico de 10, y la de externa de OSPF tipo 2 tiene un métrico interno de 100 y externo de 9. En este caso, la ruta OSPF se añadirá a la lista de rutas, ya que el métrico externo de 9 es menor que el de la de RIP de 10.

De todas maneras, si el métrico externo de la ruta externa de OSPF tipo 2 es el mismo que el de la ruta de RIP ó de EGP, se elige la ruta de uno de estos dos últimos. Esto se debe al métrico interno de OSPF. Aunque se considera mucho más pequeño que el métrico externo ó que el métrico de RIP ó de EGP, el métrico interno todavía carga peso al comparar dos rutas del mismo coste. Por ejemplo, si hay una ruta de RIP con un métrico de 10 y una ruta externa de OSPF tipo 2 con un métrico de 10 ambas van dirigidas al mismo destino, entonces la ruta de RIP se añade a la tabla de rutas.

EGP (External Gateway Protocol ó Protocolo de Compuerta Externo)

EGP es un protocolo de encaminamiento externo al que da soporte el software. Los protocolos de encaminamiento externo intercambian información entre AS diferentes. El EGP local adquiere la información sobre su propio AS de los IGP locales. Normalmente, los protocolos externos se usan sólo al conectar con empresas diferentes ó al conectar con un servicio comercial.

La información que EGP recibe del IGP debe estar configurada de manera explícita. El protocolo de encaminamiento externo comparte sólo la información especificada en los filtros de ruta salientes.

Esto es conveniente ya que, normalmente se desea limitar la información intercambiada entre diferentes AS.

EGP intercambia información de encaminamiento entre los AS. Como se mencionó anteriormente, por regla general, la mayoría de las empresas y organizaciones agrupan todos sus ruteadores en un AS, y es posible que las empresas más grandes utilicen más de un AS. En ambos casos, se escoge uno ó más ruteadores de cada AS para que use EGP para comunicarse con el mundo exterior, normalmente sobre Internet. Estos ruteadores de EGP reciben el nombre de Ruteadores externos.

Los ruteadores que pertenecen al mismo AS se llaman vecinos internos, y los que pertenecen a dominios del protocolo de encaminamiento diferentes se llaman vecinos externos.

El primer paso que EGP toma para establecer comunicación entre los ruteadores externos es realizar la adquisición de vecino. Durante la adquisición de vecino, un ruteador externo hace un petición a otro ruteador para compartir información de accesibilidad. El paso siguiente es que el ruteador prueba continuamente si los vecinos EGP responden. Finalmente, los vecinos EGP intercambian la información de accesibilidad mediante el uso de los mensajes de actualización de encaminamiento.

Diseño de red con EGP

EGP tiene una gran limitación: la distancia indicada para un destino en particular no especifica el coste hasta el destino. EGP sólo informa acerca de si el destino es accesible ó no. Dada esta limitación, EGP sólo puede utilizarse en una red de tipo tres. Todos los dominios de protocolo de encaminamiento deben estar conectados a la misma red central, como ARPAnet. Por lo tanto, no puede soportar una topología en bucle.

Otra limitación es que EGP puede notificar sólo una ruta hacia una red determinada. Por lo tanto, es posible que no se comparta la carga del tráfico entre cualquier pareja de máquinas. También, el uso de sólo una vía de acceso para una determinada red puede tener como resultado paquetes que no tomen las vías de acceso óptimas durante ciertas condiciones de tráfico en la red.

Finalmente, es difícil que EGP conmute una ruta alternativa si falla la principal.

Protocolo de descubrimiento del ruteador

El protocolo de descubrimiento del ruteador del protocolo de control de mensaje Internet (ICMP) permite que los Hosts descubran ruteadores en su red y determinen cual van a utilizar como ruteador por defecto. Cuando un Host necesita enviar un paquete a otra red, primero lo envía a un ruteador que lo reenvía al destino. Para que esto se cumpla, el Host necesita saber en que lugar de la red se encuentran los ruteadores y a cual le va a enviar el mensaje.

Al configurar el mecanismo de descubrimiento del ruteador, éste se notifica a sí mismo con mensajes ICMP de notificación de ruteador. El Host presta atención a estos mensajes y decide si debe utilizar un ruteador como el de reenvío por defecto.

Puede configurar el Host para que solicite la notificación de ruteador en redes conectadas. Todos los ruteadores que formen parte de la conexión responden a la petición. Con las respuestas, el Host encuentra a los ruteadores de la red y determina cual va a utilizar.

Es posible que un Host no seleccione el mejor ruteador para reenviar paquetes a un destino determinado. Cuando el ruteador recibe un paquete de un Host que puede reenviar mejor a otro ruteador de la red, usa un mensaje ICMP de redirección para notificar al Host que envie paquetes a un nuevo ruteador.

Mensajes de descubrimiento del ruteador

Son tres tipos de mensajes utilizados por el protocolo de descubrimiento del ruteador para establecer comunicación entre Hosts y ruteadores:

Mensaje ICMP de notificación de ruteador

El mensaje ICMP de notificación de ruteador es un mensaje ICMP de tipo 9. Los ruteadores usan este mensaje para notificar su presencia en la red. Este mensaje se difunde ó se multidifunde a todos los Hosts de la red.

Este tipo de mensaje lleva la dirección IP del ruteador y su nivel de preferencia. Los Hosts usan la dirección IP como la siguiente dirección de saltos para los destinos en otras redes. Los Hosts utilizan el nivel de preferencia para determinar que ruteador va a utilizar para efectuar los reenvios. El ruteador con la preferencia más alta se convierte en el ruteador por defecto.

Para especificar que un ruteador no se va a utilizar para el reenvio de paquetes, se usa un valor de 0x80000000. Los ruteadores que tengan este valor sólo se usan cuando otros ruteadores envian al Host mensajes ICMP de redirección. Estos mensajes de redirección informan al Host para que utilice el ruteador (con un valor de 0x80000000) como el siguiente ruteador de saltos para destinos especificos.

Mensaje ICMP de solicitud de ruteador

El mensaje ICMP de solicitud del ruteador es un mensaje ICMP de tipo 10. Los Hosts usan este mensaje para solicitar notificaciones de ruteador de todas las rutas que forman parte de la red.

Dirección de multidifusión de descubrimiento del ruteador

La dirección de multidifusión de descubrimiento del ruteador es una dirección IP 224.0.0.1. Se reserva para multidifundir a los Hosts el mensaje de notificación de ruteador. La dirección IP 224.0.0.2 se reserva para multidifundir a los ruteadores el mensaje de solicitud de ruteador. Si la red no soporta multidifusión, se utiliza la dirección de difusión general 255.255.255.255 tanto para las notificaciones de ruteador como para los mensajes de solicitud de ruteador.

Rutas estáticas

Las rutas estáticas son entradas de configuración manuales en la tabla de rutas. Para cada red ó destino de Host, el administrador de la red configura el siguiente ruteador de saltos y el coste asociado con la ruta.

Los ruteadores pueden usar rutas estáticas para ó, además de, rutas adquiridas de protocolos de encaminamiento dinámico como RIP ó OSPF. Normalmente, las rutas estáticas se configuran para destinos accesibles a través de interfaces de la red que no utilizan un protocolo de encaminamiento.

Para los Hosts se configura generalmente una ruta por defecto estática. Esta ruta define un ruteador por defecto al que el Host envía todos los paquetes destinados a una red remota. Si el ruteador por defecto no se encuentra en la vía de acceso óptima para un paquete, el ruteador puede enviar un mensaje ICMP de redirección para informar al Host de la vía de acceso más apropiada. En lugar de una ruta estática por defecto, puede usarse el protocolo de descubrimiento del ruteador. Este protocolo permite que el Host adquiera la identidad de un ruteador de la red conectada de manera dinámica.

Las rutas estáticas pueden ser activas ó pasivas. Una ruta estática activa se puede sustituir por una ruta de coste inferior adquirida de un protocolo de encaminamiento dinámico. Una ruta estática pasiva no se puede sustituir por una ruta adquirida de un protocolo de encaminamiento dinámico.

CAPITULO 2 EL MEDIO DE ENLACE

2.1.1.- Introducción

Para comenzar, comentaremos una pequeña pero ilustrativa historia. Jim, un ávido navegador de la Internet, quería actualizar su módem de 2400 baud a un módem de más alta velocidad. Fue a la tienda y pregunto por el mejor módem de 9600 baud y compró un Hayes V-series Ultra Smartmodem 9600 el cual es sin duda uno de los mejores en cuanto a marcas. Jim pensó que tenia el gasto justificado de $800 dólares en el módem. Sin embargo, cuando Jim fue a casa y lo instaló encontró que todas sus conexiones eran aún a 2400 baud. Muchos de los operadores de sistemas quienes corren los "bulletin boards" ó la información de consulta en línea, a los que Jim se conectaba estaban tan confusos como él, pero uno de estos enfocó el problema. Mientras que el módem de Jim era un excelente módem V.32, en el lado del "bulletin board" se estaba usando un módem HST. Jim no estaba bastante seguro de los que significaba, pero regreso a la tienda y explicó el problema. El vendedor hizo con el un trato justo con una oferta: regresándole el módem Hayes y agregando $100, le venderia un U.S. Robotics Dual Standard, el cual, puesto que era más caro que el Hayes Ultra, puede conectarse tanto a módem V.32 y HST a una velocidad alta. Jim estaba muy feliz con su módem nuevo. Sin embargo, no lo estuvo cuando vio el precio de un módem V.42bis en $179, mucho menor del que había pagado por su V.32. Una vez en su casa, Jim llamo al operador de sistema, el cual había entendido en su primer problema y este le dijo que un módem V.42bis sin ninguna otra designación era un módem de 2400 baud, no más rápido que el viejo 2400 baud de Jim.

Pese a que el nombre fue cambiado, la historia de Jim es verdadera e ilustra una de las áreas más comunes de confusión en el campo de telecomunicación hoy en dia. El personaje refleja varias fuentes de confusión. La designación V.32, V.42bis y HST indican la disponibilidad del módem, pero no describen a este. También se estuvo usado la palabra "baud" imprecisamente sin conocimiento de esto. Si un comprador de módem no entiende el lenguaje de la descripción de módem, es fácil que gaste una gran cantidad de dinero y que compre un módem que no funcione más eficientemente que un módem de una tienda comercial.

2.1.2.- ¿Qué es lo que hace a los módem compatibles?

Los módem le hablan a otros módems. El orden para hacer esto se describe a continuación; los dos módem en cuestión deben hablar el mismo "lenguaje", de otra forma estos no pueden comunicarse. En los primeros días de los módem, el "lenguaje" usado por la compañía Hayes Microcomputer Products fue tomando como un estándar por muchas fabricadoras de módem. Para velocidades medias de módems (1200 y 2400 bits por segundo ó bps), este es aún el caso. Muchos de estos módem usan el juego de comando Hayes "AT" y se hablan libremente de uno a cualquier otro.

Cuando los primero fabricantes empezaron a hacer módem de alta velocidad (9600 bps y superiores), ningún estándar claro los involucraba, por lo que varios fabricantes desarrollaron protocolos propietarios. Tales protocolos son propiedad de la compañía la cual los desarrollo y por lo tanto la mayoría son incompatibles con cada otro. Así ninguno de estos módem puede comunicarse con cualquiera de los otros tipos a 9600 bps, puesto que ninguno de estos habla el mismo "lenguaje".

La United Nations, a través de el Comité Consultatif International de Telegraphic et Telephonic (conocido también como CCITT, aunque recientemente haya cambiado su nombre a ITU-TS, se seguirá haciendo referencia a la CCITT), es encargada de establecer un estándar reconocido para las

telecomunicaciones de alta velocidad. La CCITT, con sede en Ginebra, ha definido muchos estándares de telecomunicaciones, algunos de estos relacionados a módem, otros a la transmisión de facsímiles y también a otros paquetes conmutados y otras telecomunicaciones. Todo los estándar CCITT pertinentes a los módem son organizados por la designación "V.nn". Una cosa que hay que guardar en mente es que el protocolo "V-punto" tal como V.32, V.42 y V.42bis son estándares totalmente diferentes, puesto que estos son confundidos comúnmente. El sufijo -bis también causa confusión. Es fácil pensar que el sufijo -bis significa "otro protocolo". Describiremos cada estándar CCITT en su ocasión, luego haremos un sumario de las diferencias.

Antes de comenzar, deberá saber que "baud" no se refiere técnicamente a la velocidad de un módem, sino a un aspecto de como la transmisión ocurre (más precisamente, el número de cambios de estado en la línea de comunicación por segundo). La unidad más pequeña de datos binarios (0 ó 1) es llamada un "bit", esto surge de la abreviación de Binary digiT. Un módem de 300 baud utiliza un método conocido como "frequency shift keying" enviando un bit por baud y es por lo tanto también un módem de 300 bps. Un módem de 1200 bps usualmente es un módem de 300 baud usando un método diferente en el orden de transmitir cuatro bits por baud. ¿Confundido? Simplemente olvídese que una vez escucho la palabra "baud" y use las iniciales "bps".

Otro término usado en la descripción de los módem es "dúplex". Este término, cuando es utilizado en referencia a un módem, indica si un dato es transmitido hacia afuera y recibido simultáneamente a una velocidad designada. Un módem usando el protocolo "full dúplex" pueden transferir datos en ambas direcciones simultáneamente a esa relación de velocidad. El protocolo "Half dúplex" permite a los datos ser enviados solamente a una dirección a la vez. Una señal en el final de la información le dice al módem receptor que este está libre para transmitir. "Asymmetrical dúplex" indica que la información fluye en ambas direcciones simultáneamente, pero a diferente velocidad. "Adaptive dúplex" significa que el módem puede transmitir cualquier cosa desde "full" a "half dúplex", dependiendo de la situación.

2.1.3.- Protocolos CCITT: transmisión de datos ó "velocidad"

Aquí está una breve descripción de los estándares que se manejan en los módem:

V.22: Hoy en día puede ver raramente una referencia al protocolo V.22. Módem usando V.22 son más universalmente llamados módem a relación de "1200 baud" en lugar de módems V.22. Este es un protocolo de transmisión de datos a 1200 bps. Un protocolo de transmisión de datos especifica la "técnica de modulación", ó el método a utilizar para transferir los datos. Este, por lo tanto, dicta la más rápida velocidad a la cual la información puede ser transferida. Así pues, el protocolo de transmisión de datos es frecuentemente llamado protocolo de "velocidad". En adición a la relación de fluido de caracteres, el protocolo de transmisión de datos define tales cosas como el método usado para limitar el efecto de ruido en la línea de teléfono, así que está no es técnicamente un protocolo de "velocidad".

V.22bis: V.22bis es el protocolo de transmisión de datos recomendado por la CCITT para módems de 2400 bps. La técnica de modulación usada por módems V.22bis es transmitir cuatro bits por baud, y esos módems son típicamente módems de 600 baud. Cuatro bits por baud en 600 baud es lo mismo que 2400 bps. Esos módems son usualmente llamados módem de 2400 baud, lo cual es técnicamente, por lo mismo que acabamos de comentar, incorrecto. Desde el punto de vista del consumidor, a este no le importa si su módem es uno de 600 baud transmitiendo cuatro bits por baud ó un módem de 2400 baud transmitiendo un bit por baud. Ambos tienen una "velocidad" de 2400 bps. V.22 es un protocolo "full dúplex".

V.32: V.32 es también un protocolo de transmisión de datos. Este es un 4800 bps y un 9600 bps estándar empleando un método llamado "trellis coded quadrature amplitude modulation" (TCQAM) a 2400 baud. TCQAM codifica 2 ó 4 bits por baud y es un protocolo "full dúplex". Hasta el advenimiento de V.32bis, V.32 fue considerado a ser el estándar para módems de alta velocidad. Sin embargo, este fue introducido solo después de que ciertos propietarios de transmisión de protocolos se habían establecido y por consiguiente los tienen compartido el mercado, pero no han dominado las marcas de alta velocidad de transmisión de datos.

V.32bis: V.32bis es el más nuevo protocolo de transmisión de datos del CCITT, con una aprobación final de las expectativas de estándar en la primavera ó verano de 1991. V.32bis es un protocolo "full dúplex" de 14400 bps, codificando 6 bits por baud a 2400 baud. Ya hay varios módem recién fabricados los cuales se adhieren al estándar V.32bis propuesto. Se considera improbable que cambios importantes puedan ocurrir antes de una aprobación final que podría causar esa "pre-aprobación" del módem V.32bis para ser un no estándar.

Así pues, el protocolo "V-punto" que determina la transmisión de datos ó la "velocidad" es, en el orden del más bajo al más alto, V.22 (1200 bps), V.22bis (2400 bps), V.32 (4800 bps ó 9600 bps) y V.32bis (14400 bps). Todos son protocolos "full dúplex". Los restantes protocolos "V-punto" no determinan la "velocidad", sino que son concernientes con la corrección de error (asegurándose que el dato recibido es una copia exacta del dato enviado) y la compresión de datos (codificando el dato en formas pequeñas para que le tome menos tiempo enviarlas a la relación de velocidad).

2.1.4.- Protocolos CCITT: corrección de error y compresión de datos.

V.42: V.42 es un protocolo de corrección de error. V.42 usa un método conocido como protocolo de enlace a acceso para módems, ó LAP-M. Este ayuda a asegurar que la transmisión de datos es realizada sin error. A diferencia de los protocolos descritos anteriormente, V.42 no se relaciona a la velocidad de transmisión de datos, solamente a sus correcciones. Sin embargo, V.42 puede decrementar el tiempo actual para la transmisión de una velocidad de transmisión dada.

Esto requiere un poco más de explicación. Una forma de asegurar la velocidad de transmisión de datos es la de caracteres por segundo, ó cps. Cada carácter consiste de 10 bits, así módems a 2400 bps tienen una relación teórica de caracteres de 240 cps. (el número de bits por segundo dividido por el número de bits en un carácter). En realidad, esta cantidad es cerrada a 235 cps., puesto que la transmisión no es totalmente eficiente. Esta relación es comúnmente referida como la "comunicación" puesto que esta indica que tantos caracteres el módem puede "colocar a través" en un tiempo dado. Los 10 bits en cada carácter incluyen 8 bits de datos más un bit de "start" y un bit de "stop". El protocolo corrector de error V.42 despojar el exceso de bits start y stop y así reduce el cargado de datos por un 20%. El actual incremento de comunicación es menor, debido la cabecera del protocolo, pero este es alrededor del 15% (270 cps. a 2400 bps con despojo de bits de exceso comparado a 235 cps. a 2400 bps sin este).

V.42bis: V.42bis es un estándar de compresión de datos. Compresión de datos es comúnmente utilizada para reducir el tamaño de un archivo para almacenarlo ó transmitirlo. Archivos pequeños naturalmente toman menor tiempo en transmitirse. V.42bis utiliza un método de compresión llamado codificación "Limpel-Ziv", la cual comúnmente puede ejecutar una compresión a una relación de 4:1 en un archivo de texto ASCII no comprimido, significando cuatro veces más datos que pueden ser enviados en un determinado tiempo a una relación de transmisión dada. Con compresión V.42bis, un módem V.32 (9600 bps) puede lograr una efectiva relación de transferencia de 19200 bps.

Sin embargo, muchos archivos han sido comprimidos antes de que sean transmitidos, usualmente para que estos puedan ser almacenados en menor espacio en un disco duro ó disco flexible. Este proceso comúnmente llamado "archivado", usa algún método de compresión de una variedad de propietarios ó técnicas de compresión de dominio público. Los archivos MS-DOS que han sido comprimidos usualmente utilizan extensiones tales como .ZIP, .LZH, .ARC, .GIF ó .EXE, las cuales identifican la técnica de compresión usada. Si un módem intenta más adelante comprimir un archivo que ya haya sido comprimido, este actualmente incrementará el tiempo necesario para la transmisión. Por lo tanto, el estándar V.42bis incluye la habilidad de "sentir ó detectar" los archivos pre-comprimidos y deshabilitar la compresión de V.42bis para tales archivos.

V.42 y V.42bis son comúnmente confundidos con otros protocolos "V-punto". A diferencia de V.22, V.22bis, V.32 y V.32bis, todos de los cuales definen una velocidad de transmisión de datos; V.42 y V.42bis no tienen efectos en la velocidad, pero son, respectivamente, protocolos de corrección de error y compresión de datos. El módem que nuestro personaje vio anunciado por $179 fue un módem de 2400 bps con habilidad de compresión de datos V.42bis.

2.1.5.- Protocolos propietarios de transmisión de datos.

Los estándares de la CCITT son, por definición, de cobertura mundial y no propietarios. Sin embargo, otros protocolos que existen definen la transmisión, la corrección de error y la compresión de datos. Protocolos de transmisión de datos propietarios en uso en módems comienzan a venderse hoy, incluido el protocolo HST, DIS y PEP. Protocolos de compresión de datos y corrección de error propietarios que se usan hoy incluyen MNP nivel 6 y superior y CSP.

Protocolos de transmisión de datos propietarios de alta velocidad son propiedad de compañías las cuales los desarrollan y no pueden ser usados por ningún otro sin una licencia. La regla cardinal a recordar sobre los protocolos de transmisión de datos es que dos módems con diferente protocolo de velocidad alta no están aptos para comunicarse con algún otro a alta velocidad. Sin embargo, puesto que todos estos módems tienen un protocolo estándar de 2400 bps como un protocolo para "recurrir", esos módem están disponibles para conectarse en muchos casos, pero comunicándose a 2400 bps.

HST: La modulación HST (High Speed Transmission) es similar a V.32 en el factor de que esta usa una técnica de modulación en amplitud de código de cuadratura (TCQAM). A diferencia de V.32, esta no es una "full dúplex", pero intenta enviar datos a un máximo de 14400 bps en una dirección con canal reversivo de tecla de cambio de frecuencias de tanto 300 ó 450 bps. Esto lo hace un módem "asimétricamente dúplex". El canal TCQAM principal codifica hasta 7 bits por baud, a 2400 baud, con un bit usado como paridad, para un máximo teórico de 14400 bps en una dirección. El módem puede conmutar canales como la demanda de datos lo requiera.

El protocolo HST es propiedad de U.S. Robotics (USR). El significado de las iniciales USR y HST son frecuentemente confundidos. Todos los módems HST están hechos por U.S. Robotics, pero U.S. Robotics hace otros módems los cuales no usan el protocolo propietario de la compañía. Por ejemplo, U.S. Robotics hace un módem el cual usa solamente su protocolo HST propietario, el U.S. Robotics Courier HST. Sin embargo, este también hace un módem de alta velocidad que conforma el estándar de la CCITT solamente, el U.S. Robotics Courier V.32. Un tercer y muy popular módem fabricado por U.S. Robotics incluye tanto el protocolo CCITT V.32 y el protocolo HST propietario. Este módem, el U.S. Robotics Dual Standard HST V.32, el cual se conecta a un alta velocidad a módem HST solamente ó a un módem que tiene V.32 solamente, por eso el nombre de Dual Standard. La lógica de ambos protocolos actualmente existe a la par en el módem Dual Standard. Recientemente,

U.S. Robotics ha comenzado a producir módems que utilizan un nuevo protocolo V.32bis, ambos en un módem de protocolo único y un módem Dual Standard.

DIS: El protocolo DIS (Dynamic Impedance Stabilization), como el protocolo V.32, V.32bis y HST, utilizan la modulación de amplitud de cuadratura para enviar a una relación de transmisión de datos de 9600 bps. La principal diferencia entre módems DIS y otros, sin embargo, es el método usado para controlar el "ruido" ó la señal indeseada en la línea de teléfono. Una línea de teléfono "ruidosa" puede causar error en la transmisión de datos ó aún causar pérdida de portadora antes de que la transmisión sea terminada. Los estándares CCITT hacen un llamado para utilizar la cancelación de echo, esto para filtrar ruido externo de señal indeseada. "Echo cancellation" requiere un procesador de señal digital, la cual incrementa grandemente el costo del módem. DIS utiliza un método de mejoramiento de la relación de señal a ruido la cual no requiere el procesador. Así, un módem usando el protocolo DIS es significativamente menos caro que un módem V.32, V.32bis ó un HST. DIS es un producto propietario de CompuCom Corporation.

PEP: La técnica de modulación PEP (Packetized Ensamble Protocol), la cual es un producto propietario de la Telebit Corporation, es totalmente disimilar al protocolo descrito arriba. Este utiliza un método llamado modulación de amplitud de cuadratura adaptiva dinámica (DAQAM). Efectivamente, este despoja a la línea de teléfono dentro de 511 secciones y pone una portadora de 34 baud en cada sección. Codificando hasta 4 bits por baud, PEP alcanza una velocidad máxima de 18000 bps. Cada canal puede estar mandando en una sola dirección, por lo que la operación "full dúplex" se puede tener a 9000 bps. PEP también utiliza "dúplex adaptivo", lo cual significa que la velocidad sobre los varios canales puede ser determinada por el dato comenzado a enviarse. Si el dato es comenzado a enviarse en solamente una dirección, este puede transmitirse a 18000 bps en esa dirección. Sin embargo, si un "full dúplex" es necesitado, los datos serán enviados a 9600 bps en ambas direcciones. Si el tráfico es más pesado en una dirección que en la otra, el protocolo PEP se ajusta para asegurar una relación de transmisión de datos máxima. Módems usando el protocolo PEP son comunes en sistemas usando sistema operativo UNIX.

2.1.6.- Otros protocolos de corrección de error y compresión de datos.

Uno de los más comunes protocolos de corrección de error no CCITT y compresión de datos son los desarrollados por Microcom, Inc. Estos son indicados por las letras MNP (Microcom Networking Protocol) y un número el cual los diferencia entre los varios protocolos. MNP nivel 2-4 (corrección de error) y MNP nivel 5 (compresión de datos) están en uso difundido y son encontrados en los módems de más altas velocidades, incluyendo aquellos que cumplen el estándar CCITT.

La razón para esto es que tanto el estándar V.42 y el estándar V.42bis incluyen un anexo el cual requiere que el MNP nivel 2-4 (para V.42) ó MNP nivel 5 (para V.42bis) este disponible como protocolo para "recurrir". En el caso de corrección de errores, este asegura que si ambos módem no son completamente V.42, al menos MNP nivel 4, el cual es corrección de error, pueda ser usado. MNP nivel 4 es similar a V.42 en que este se despoja del bit de comienzo y de paro para cada carácter de 10-bit, así incrementa la continuidad por alrededor de 15%. El protocolo MNP nivel 4 incluye MNP nivel 2 y 3, los cuales también son protocolos de corrección de error.

Note que algunos módems de 2400 bps no tienen ninguna disponibilidad de corrección de error ó de compresión de datos. Esto son frecuentemente referidos como módems "sin MNP" ó "sin corrección de error". Cuando tales módems son usados para la transmisión de datos. El software (tal como el protocolo de transferencia de archivos Zmodem) es usado para proveer corrección de errores. Módems los cuales tienen al menos corrección de error MNP nivel 4 ó corrección de error V.42 (el

cual incluye MNP nivel 4 como un protocolo al cual "recurrir") pueden intentar usar un protocolo de transferencia de archivos como el Ymodem-G, el cual es más rápido puesto que este envía los datos en un flujo sin software controlador de corrección de error.

MNP nivel 5 es más comúnmente visto en protocolos de compresión de datos no CCITT y es incluido en el estándar CCITT V.42bis como un protocolo al cual recurrir. MNP nivel 5 difiere de V.42bis en dos formas importantes. Primero, mientras que V.42bis usa el protocolo de compresión de datos 4:1, MNP nivel 5 utiliza el método llamado "run length encoding", el cual es solamente un protocolo de compresión de datos 2:1. Microcom desarrollo un protocolo de compresión 4:1 (MNP nivel 9) pero este no prevé mucho de cambio del V.42bis.

La segunda diferencia entre el V.42bis y el MNP nivel 5 es que, mientras que el V.42bis puede "sentir ó detectar" una compresión de archivos previa, y deshabilitar la compresión V.42bis. MNP nivel 5 no tiene este disponibilidad, dejando para futuras comprensiones una transmisión lenta de un archivo ya comprimido. Por lo tanto, si un módem con disponibilidad de MNP nivel 5 (pero sin V.42bis) es usado más frecuentemente para archivos comprimidos previamente, como es el caso de muchos archivos de transferencia de "bulletin board", MNP nivel 5 deberá ser deshabilitado del módem, generalmente esto se hace cambiando un switch DIP ó cambiando el seleccionado el software. Si el módem es usado para transferencia de archivos de texto no comprimidos, MNP nivel 5 deberá permanecer habilitado.

MNP nivel 5 es frecuentemente referido erróneamente como un protocolo de corrección de error. Esto es parcialmente, puesto que el módem intenta ser referido por sus más sofisticadas realizaciones. Asi, un "módem MNP 5" es considerado mejor que un "módem MNP 4". En algunos casos esto es verdad, puesto que MNP nivel 5 siempre incluye MNP 2-4. Sin embargo, es impreciso referirse al módem como un "módem corrector de errores MNP 5". Un módem solo con MNP nivel 2-4 tiene cualquier cosa para hacer corrección de errores, mientras que MNP nivel 5 es estrictamente un protocolo de compresión de datos. Es más preciso describir a tal como un "módem de corrección de error con compresión MNP nivel 5".

Un protocolo no CCITT, y tampoco Microcom de corrección de error y de compresión de datos llamado CSP (CompuCom Speed Protocol) es usado con módems empleando el protocolo de transmisión de datos DIS. Estos mismo módems ofrecen MNP nivel 2-5 como un rutina a recurrir para ciertas ocasiones, cuando el módem DIS se conecta a módems no DIS (a 2400 bmp solamente, puesto que DIS es un protocolo propietario). CSP ofrece compresión de hasta 4:1 en archivos no comprimidos sin degradación aparente de transferencia de archivos en archivos precomprimidos. Esta es una tecnología propietaria de CompuCom Corporation.

2.1.7.- Sumario.

Los protocolos de módems pueden dictar las características de transmisión de datos tales como la velocidad y reducción de ruido de línea telefónica. Ejemplo de este tipo de protocolos incluye V.22, V.22bis, V.32, V.32bis, HTS, DIS y PEP.

Protocolos de módems pueden también proveer corrección de error, al mismo tiempo que incrementan la continuidad alrededor del 15%. Ejemplo de estos tipos de protocolo incluyen V.42 y MNP nivel 2-4.

Finalmente, protocolos de módems pueden comprimir datos que no han sido previamente comprimidos, los cuales abrevian el tiempo de transmisión decrementando el tamaño del archivo. Ejemplo de este tipo de protocolos son V.42bis y MNP nivel 5.

EL protocolo CSP maneja tanto correcciones de error y compresión de datos para módems usando protocolo de transferencia de datos DIS.

2.2.- Encapsulación de la información bajo el protocolo Point to Point (RFC 1134)

2.2.1.- El protocolo Point-to-Point: Una propuesta para la transmisión de datagrams de multiples-Protocolos sobre enlaces punto a punto.

La siguiente propuesta es el producto del protocolo Point-to-Point Working Group de la Internet Engineering Task Force (IETF). Puesto que este documento es puesto a nivel público, los comentarios deberán ser sumitidos a la presidencia de la IETF Point-to-Point Working Group.

El protocolo Point-to-Point (PPP) provee un método para la transmisión de datagram a través de un enlace serial punto a punto. PPP está compuesto de tres partes:

1.-Un método para la encapsulación de datagram sobre enlaces seriales.
2.-Un protocolo de control de enlace extensible (LCP) (Link Control Protocol).
3.-Una familia de protocolos de control de red (NCP) para el establecimiento y configuración de diferentes protocolos de la capa de red.

Este documento define el esquema de encapsulamiento, el LCP básico y un NCP para el establecimiento y configuración del protocolo Internet (IP), llamado el IP Control Protocol (IPCP).

Las opciones y facilidades usadas por el LCP y el IPCP están definidas en documentos separados. Protocolos de control para configuración y utilización de otros protocolos de la capa de red pertenecientes a IP (p.ej., DECNET, OSI) están en espera de ser desarrollados como sean necesitados.

2.2.2.- Introducción

En los últimos años, la Internet ha tenido un crecimiento explosivo en el número de host soportando TCP/IP. La vasta mayoría de esos host están conectados a Redes de Área Local (LANs) de varios tipos, de los cuales, Ethernet se ha vuelto el más común. Muchos de los otros hosts están conectados a través de Redes de Área Amplia (WANs) tales como X.25 de tipo de Redes de Datos Públicos (PDNs). Relativamente pocos de esos hosts están conectados con un simple enlace punto a punto (p.ej., serial). Más aún, enlaces punto a punto son una cantidad de métodos viejos de comunicación de datos y casi cada host soporta conexión punto a punto. Por ejemplo, la interface asincrona RS-232-c.

Una razón del número pequeño de enlaces IP punto a punto es la falta de un protocolo de encapsulación estándar. De estos ahí abundancia de protocolos no estándares (y al menos un estándar defecto) de encapsulación disponibles, pero ninguno de los cuales que haya sido del agrado para ponerlo como Estándar de Internet. En contraste, el esquema de encapsulación estándar existe para la transmisión de "datagram" sobre las LANs más populares.

El propósito de "point-to-point" es más que simplemente un esquema de encapsulación. Los enlaces punto a punto tienden a exacerbar muchos problemas con la familia actual de protocolos de red. Por ejemplo, la asignación y administración de direcciones IP, la cual es un problema aún en ambientes de LAN, es especialmente difícil sobre circuitos punto a punto comuntados (p.ej., dialups).

Algunas direcciones adicionales emitidas por PPP incluyen asincrono (star/stop) y encapsulación sincrona orientada a bit, múltiplexado de protocolo de red, configuración de enlace, pruebas de calidad de enlace, detección de error y opción de negociación para tales disponibilidades como negociación de dirección a nivel de red y negociación de compresión de datos.

Direcciones PPP son emitidas proveyendo un extensible Protocolo de Control de Enlace (LCP) y una familia de Protocolos de Control de Red (NCP) para parámetros de configuración opcionales de negociación y facilidades.

2.2.3.- Puntos de vista sobre PPP.

PPP tiene tres componentes principales:

1. Un método de encapsulamiento de datagram sobre enlaces seriales. PPP usa HDLC como una base de encapsulación de datagram sobre enlaces punto a punto.

2. Un Protocolo de Control de Enlace (LCP) extensible para establecer, configurar y probar la conexión de enlace de datos.

3. Una familia de Protocolos de Control de Red (NCP) para establecer y configurar diferentes protocolos de nivel de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de nivel de red.

El orden para establecer comunicación sobre un enlace point-to-point es el siguiente, el originador PPP deberá primero enviar paquetes LCP para configurar y probar el enlace de datos. Después de que el enlace ha sido establecido y que las facilidades opcionales han sido negociadas según sean necesitadas por el LCP, el PPP originador debe enviar una paquete NCP para escoger y configurar uno ó más protocolos de nivel de red. Una vez que cada uno de los protocolos de nivel de red ha sido configurado, los datagram de cada protocolo de nivel de red podrán ser enviados sobre el enlace. El enlace puede permanecer configurado para la comunicación hasta que explícitamente el paquete LCP ó el NCP cierre el enlace ó hasta que un evento externo ocurra (p.ej., un tiempo de expiración inactivo ó la intervención del usuario).

Es conveniente comentar que esta información está dividida en varias secciones. Una sección discute los requerimientos de PPP para el nivel físico. La otra describe el nivel de enlace de datos incluyendo el formato de la estructura de PPP y el esquema de encapsulamiento del enlace de datos. Una más especifica el LCP incluyendo el establecimiento de la conexión y las opciones del proceso de negociación. La última sección especifica el Protocolo de Control IP (IPCP), el cual es el NCP para el protocolo de Internet y describe la encapsulación del datagram IP dentro de paquetes PPP. Un apéndice hace un sumario de realizaciones importantes del HDLC asincrono y otro apéndice describe un eficiente algoritmo para secuencias de chequeo de estructura (FCS) más rápidas de computadoras.

2.2.4.- Requerimientos de la capa física.

El protocolo point-to-point está diseñado para que pueda operar a través de cualquier interface DTE/DCE (p.ej., EIA RS-232-C, EIA RS-422, EIA RS-433 y CCITT V.35). Solamente el único requerimiento impuesto por PPP es que se tenga un "circuito dúplex", tanto dedicado ó conmutado, el cual puede operar tanto en un modo asíncrono (start/stop) ó en uno síncrono bit-serial, transparente a las estructuras del nivel de enlace de datos de PPP. PPP no impone ninguna restricción con respecto a la relación de transmisión, otras que le son impuestas son por el uso particular de la interface DTE/DCE.

PPP no requiere del uso de señales de control del módem, tales como Request To Send (RTS), Clear To Send (CTS), Data Carrier Detect (DCD) y Data Terminal Ready (DTR). Sin embargo, usando tales señales, cuando se dispone de ellas, puede permitir una mayor funcionalidad y desempeño.

2.2.5.- La capa de enlace de datos.

El protocolo point-to-point usa el principio, terminología y estructura de frame de la International Organization For Standardization's (ISO), con procedimientos de High-level Data Link Control (HDLC) (ISO 3309-1979 2), modificado por ISO 3309:1984/PDAD1 "Assendum 1: Start/stop transmission" [5]. ISO 3309-1979 especifica la estructura del frame HDLC para uso en ambientes síncronos. ISO 3309:1984/PDAD1 especifica modificaciones propuestas al ISO 3309-1979 para permitirle a este el uso en ambientes asíncronos.

El procedimiento de control de PPP utiliza la definición y campo de control de codificación estandarizados en la ISO 4335-1979 3 y la ISO 4335-1979/Addendum 1-1979 4. La estructura de frame de PPP también es consistente con la Recomendación CCITT X.25 LAPB 6, puesto que también está basada en HDLC.

Nota: ISO 3309:1984/PDAD1 es un bosquejo de una propuesta de estándar. En el presente, es igual al ISO 3309:1984/PDAD1: este es estable y está a punto de convertirse en un estándar Internacional. Por lo que se tiene confianza en el uso de este.

Este no es un documento que ya haya sido estandarizado en ISO 3309. Se asume que el lector está familiarizado con HDLC, en caso contrario favor de referirse al apéndice correspondiente. así pues, este documento intenta dar un sumario consistente y sacar puntos de opciones específicos y realizaciones usadas por PPP. Puesto que el "Addendum 1: Start/Stop transmission" aún no está estandarizado y ampliamente disponible, este está resumido en otro apéndice.

2.2.6.- Formato del Frame

Un sumario de la estructura del frame estándar de PPP es mostrado abajo. Los campos son transmitidos de izquierda a derecha.

Flag	Address	Control	Protocol	Information	FCS	Flag
01111110	1111111	0000011	16 bits	*	16 bits	01111110

Esta figura no incluye los bits de start/stop (para enlaces asincronos) ó cualquier bits u octetos insertados para transparencia. Cuando es usado un enlace asincrono, todos los octetos son transmitidos con un bit de start, ocho los bits de datos y un bit de stop.

Para permanecer consistente con la practica de estándares de Internet, y evitar confusión de gente que son lectores de los RFCs (request for comments) (archivos de estándares de comunicaciones), todos los números binarios en la siguiente descripción están en el orden del Bit Más Significante al Bit Menos Significante, leidos de izquierda a derecha, a menos de que se indique otra cosa. Note que esto es contrario al estándar ISO y CCITT practicado, en el cual ordena los bit como son transmitidos (p.ej., orden de bit de red). Tenga esto en mente cuando compare esta documentación con la documentación de estándares internacional.

Secuencia de Banderas (Flag)

La secuencia de las banderas es un octeto único e indica el comienzo ó final de un frame. La secuencia de banderas consiste de una secuencia binaria 01111110 (0x7e en hexadecimal).

Campo de Direcciones (Address)

El campo de direcciones es un octeto único y contiene la secuencia binaria 00000011 (0x03 en hexadecimal), el comando "Unnumbered Information" (UI) con el bit P/F es puesto a cero. Frames con otros valores de campo de Control deberán ser totalmente descartados.

Campo de Protocolo (Protocol)

El campo de protocolo son dos octetos y este valor identifica el protocolo de encapsulamiento en el campo de Información del frame. Los valores más arriba del dato del campo de protocolo son especificados en el más reciente RFC 11 " Assigned Numbers". Los valores iniciales son listados también abajo.

El valor del campo del Protocolo en el rango "cxxx" identifica al datagram como perteneciente al "Link Control Protocol" (LCP) ó protocolos asociados. Valores en el rango "8xxx" identifican al datagram perteneciente a la familia de Network Control Protocols (NCP). Valores en el rango "0xxx" identifican al protocolo de red de datagram especificos.

Este campo de protocolo es definido por PPP y no es un campo definido por HDLC. Sin embargo, el campo de protocolo es consistente con el mecanismo de extensión ISO 3309 para campo de dirección. Todos los protocolos DEBEN ser impar; el bit menos significante del octeto DEBE ser igual a "1". También, todos los protocolos deben ser asignados de tal forma que el bit menos significante del octeto al más significante sea igual a "0". Los frames recibidos, los cuales no completen con estas reglas deberán ser consideradas como un protocolo no reconocido y deberán ser manejadas como se especificó en el LCP. El campo de protocolo es transmitido y recibido con el octeto más significante primero.

El campo de Protocolo es inicialmente asignado como sigue:

Valor (en hex)	Protocolo
0001 a 001f	reservado (transparencia ineficiente)
0021	Internet Protocol
0023	* ISO CLNP
0025	* Xerox NS IDP
0027	* DECnet Phase IV
0029	* Appletalk
002b	* Novell IPX
002d	* Van Jacobson Compressed TCP/IP 1
002f	* Van Jacobson Compressed TCP/IP 2
0031	* Bridging PDU
0033	* Stream Protocol (ST-II)
0035	* Banyan VINES
0201	802.1 D Hello Packets
8021	Internet Protocol Control Protocol
8023	* ISO CLNP Control Protocol
8025	* Xerox NS IDP Control Protocol
8027	* DECnet Phase IV Control Protocol
8029	* Appletalk Control Protocol
802b	* Novell IPX Control Protocol
802d	* Reservado
802f	* Reservado
8031	* Bridging NCP
8033	* Stream Protocol Control Protocol
8035	* Banyan VINES Control Protocol
c021	Link Control Protocol
c023	* User/Password Authentication Protocol
c025	* Link Quality Report
c223	* Challenge Handshake Authentication Protocol

* Reservado para uso futuro; no están descritos en este documento.

Campo de Información (Information)

El campo de Información es cero ó más octetos. El campo de Información contiene el datagram del protocolo especifico en el campo de Protocolo. El final del campo de Información es encontrado por la localización de la secuencia de la bandera de cerrado y permitiendo dos octetos para el campo de secuencia de chequeo de frame. La longitud máxima de default del campo de Información es 1500 octetos. Por acuerdos previos, implementaciones PPP consiguientes pueden usar otros valores para la longitud máxima del campo de Información.

En transmisión, el campo de información puede ser llenado con número arbitrario de octetos hasta la longitud máxima. Esta es responsabilidad de cada protocolo el desechar caracteres llenados a diferencia de la información real.

Campo de chequeo de la secuencia del Frame (Frame Check Sequence (FCS))

El campo de Secuencia de Chequeo de Estructura es normalmente de 16 bits (dos octetos). En un arreglo prioritario, que consiste de implementación de PPP puede usar un FCS de 32 bits (cuatro octetos) para proveer detección de error.

El campo FCS es calculado sobre todos los bits del campo de la Dirección, Control, Protocolo e Información no incluyendo ningún bit de start y stop (asincrono) y ningún bit (sincrono) u octeto (asincrono) insertado para transparencia. Esto no incluye la secuencia de bandera (Flag Sequences) ó el campo de FCS. El FCS es transmitido con el coeficiente del término más alto primero. Para más información en la especificación de la FCS, ver ISO 3309 ó CCITT X.25.

Nota: Una rápida, implementación de "table-driven" del algoritmo FCS de 16 bits es mostrada en el segundo apéndice de esta sección.

2.2.7.- Modificaciones a la forma básica del Frame

El Protocolo de Control de Enlace puede negociar modificaciones a la estructura estándar de PPP. Sin embargo, modificar el frame puede ser siempre claramente distinguido de los frames estándar.

El Protocolo de Control de Enlace (LCP) provee un método de establecimiento, configuración, mantenimiento y terminación de conexiones punto a punto. LCP va a través de cuatro distintas faces:

Fase 1:Establecimiento del enlace y negociación de la configuración.

Antes de que cualquier diagrama de capa de red (p.ej., IP) puede ser intercambiado, LCP debe primero abrir la conexión a través de un intercambio de paquetes de Configuración. Este intercambio es completado, una vez que un paquete de Configure-Ack (descrito abajo) ha sido tanto enviado como recibido. Cualquier paquete que no sea un LCP y que se reciba antes de que este intercambio sea completado será totalmente descartado.

Es importante notar que el LCP maneja configuraciones solamente del enlace; LCP no maneja configuraciones de protocolos de capa de red individuales. En particular, todos los Parámetros de Configuración los cuales son independientes del protocolo de capa de red particular son configurados por LCP. Todas las Opciones de Configuración son asumidas como valores de default a menos que se alteren por una configuración de cambio.

Fase 2: Determinación de la calidad del enlace

LCP permite una opción de fase de determinación de calidad de enlace siguiendo la transición al estado Open de LCP. En esta fase, el enlace es probado para determinar si la calidad del enlace es suficiente para levantar el protocolo de capa de red. Esta fase es completamente opcional. LCP puede retardar la transmisión de la información del protocolo de la capa de red hasta que esta fase sea completada.

El procedimiento para la determinación de la calidad de enlace no es especificado y puede variar de implementación en implementación ó por parámetros de configuración de usuario, pero solamente mientras el procedimiento no viole otros aspectos del LCP. Un método sugerido es usar los paquetes LCP Echo-Request y el Echo-Reply.

Lo que es importante es que esta fase puede persistir para cualquier longitud de tiempo. Por lo tanto, las implementaciones deberán evitar tiempos de salida (timeouts) cuando se espere este par para avanzar a la fase 3.

Fase 3: Negociación de configuración del protocolo de la capa de red

Una vez que LCP ha finalizado la fase de "Link Quality Determination", el protocolo de capa de red puede ser configurado separadamente por el apropiado "Network Control Protocols" (NCP), y puede ser regresado y tomado para bajarlo en cualquier momento. Si un LCP cierra el enlace, este informa al protocolo de capa de red para que este pueda tomar la acción apropiada.

Fase 4: Terminación de enlace.

LCP puede terminar el enlace en cualquier tiempo. Este puede usualmente ser realizado como una petición de una persona, pero puede suceder por un evento físico tal como la perdida de portadora ó la expiración de un periodo de tiempo de espera.

2.2.8.- Automatización del LCP.

LCP es especificado por un número de formato de paquetes y una automatización de estado finito. Esta sección presenta un vistazo de la automatización de LCP, seguido por la representación de este, tanto como un diagrama de estado y una tabla de estado de transmisión.

Estos son tres clases de paquetes LCP:

1.- Paquetes de establecimiento de enlace usado para establecer y configurar un enlace, (p.ej. Configure-Request, Configure-Ack, Configure-Nak y Configure-Reject).

2.- Paquete de terminación de enlace usado para terminar un enlace, (p.ej. Terminate-Request y Terminate-Ack).

3.- Paquete de mantenimiento de enlace usado para mantener y depurar un enlace, (p.ej. Code-Reject, Protocol-Reject, Echo-Request, Echo-Request, Echo-Reply y Discard-Request).

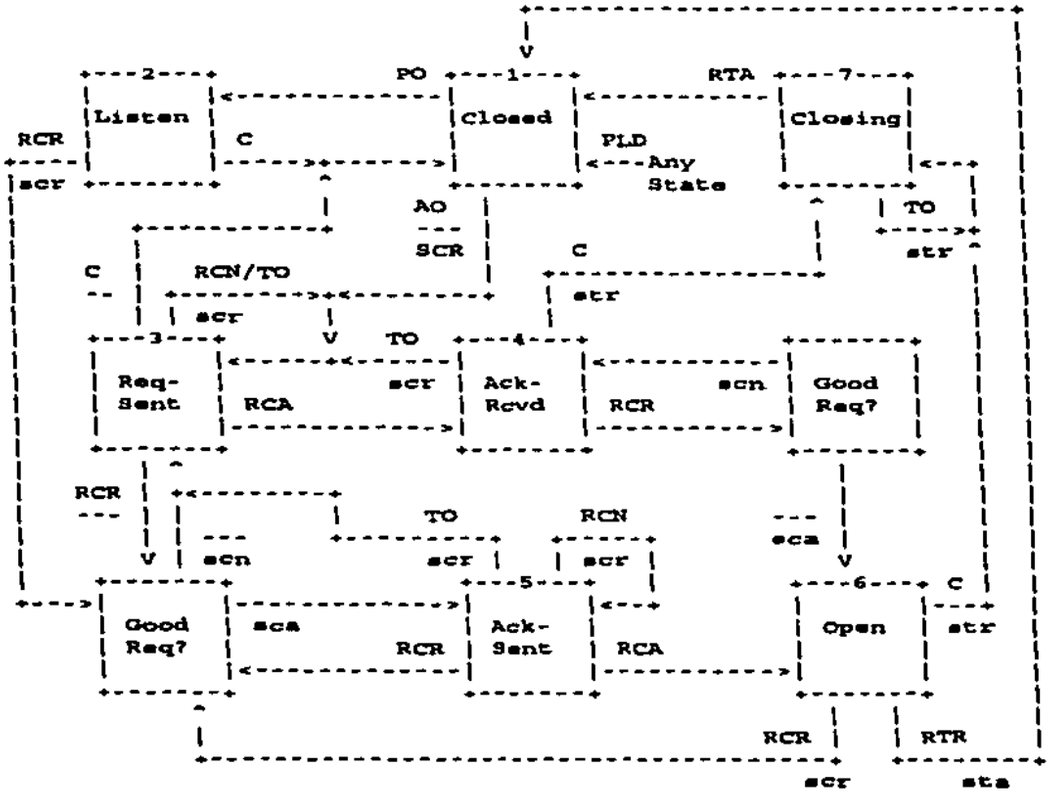
La automatización del estado finito es definida por eventos, transmisión de estados y acciones. Los eventos incluyen recepción de comandos externos tales como Open y Close, expiración del tiempo de Restart y recepción de paquetes desde un par LCP. Las acciones incluyen el inicio de un tiempo de Restart y transmisión de paquetes.

2.2.9.- Diagrama de estados.

El diagrama de estados que sigue describe la secuencia de eventos para la obtención de un acuerdo en las opciones de configuración (abriendo la conexión PPP) y para posterior cerrado de la conexión. El estado de la máquina es inicialmente en el Estado de Cerrado (1). Una vez que el estado Abierto (6) se han encontrado, ambos finales del enlace deben coincidir con la petición de tener un paquete de Configure-Ack, tanto de enviado y recibido.

En el diagrama de estados, los eventos son mostrados bajo líneas horizontales. Las acciones son mostradas bajo líneas horizontales. Dos tipos de paquetes LCP Configure-Naks y Configure-Rejects no son diferenciados en el estado de diagramas. Como será descrito posteriormente, estos paquetes hacen diferentes servicios de funciones similares. Sin embargo, en el nivel de detalle de este diagrama, estos siempre causan la misma transición.

Puesto que una especificación más detallada de la automatización de LCP es dada en una tabla de transición de estado en la siguiente sección, la implementación deberá ser realizada consultando esta en lugar de este diagrama de estados.



Eventos

RCR - Receive-Configure-Request
RCA - Receive-Configure-Ack
RCN - Receive-Configure-Nak or Reject
RTR - Receive-Terminate-Req
RTA - Receive-Terminate-Ack
AO - Active-Open
PO - Passive-Open
C - Close
TO - Timeout
PLD - Physical-Layer-Down

Acciones

scr - Send Configure-Request
sca - Send Configure-Ack
scn - Send Configure-Nak or Reject
str - Send Terminate-Req
sta - Sent Terminate-Ack

2.2.10.- Tabla de transición de estados.

Lo que a continuación se presenta es la tabla de transición de estados completa. Los estados son indicados horizontalmente y los eventos son leídos verticalmente. La transición de Estados y las acciones son representadas en la forma action/new-state. Dos acciones causadas por el mismo evento son representados como action1&action2.

Events	State 1 Closed	2 Listen	3 Req-Sent	4 Ack-Rcvd	5 Ack-Sent	6 Open	7 Closing
AO	scr/3	scr/3	3	4	5	6	scr/3
PO	2	2	2*	4	5	6	sta/3*
C	1	1	1*	1	str/7	str/7	7
TO	1	2	scr/3	scr/3	scr/3	6	str/7*
PLD	1	1	1	1	1	1	1
RCR+	sta/1	scr&sca/5	sca/5	sca/6	sca/5	scr&sca/5	7
RCR-	sta/1	scr&scn/3	scn/3	scn/4	scn/3	scr&scn/3	7
RCA	sta/1	sta/2	4	scr/3	6	scr/3	7
RCN	sta/1	sta/2	scr/3	scr/3	scr/5	scr/3	7
RTR	sta/1	sta/2	sta/3	sta/3	sta/3	sta/1	sta/7
RTA	1	2	3	3	3	1	1
RCJ	1	2	1	1	1	1	1
RUC	scj/1	scj/1	scj/1	scj/1	scj/1	scj/1	1 scj/1
RER	sta/1	sta/2	3	4	5	ser/1	7

Notas:

- RCR+ - Receive-Configure-Request (Good)
- RCR- - Receive-Configure-Request (Bad)
- RCJ - Receive-Code-Reject
- RUC - Receive-Unknown-Code
- RER - Receive-Echo-Request
- scj - Send-Code-Reject
- ser - Send-Echo-Reply
- * - Atención especial necesaria, ver texto

Eventos.

Transición y acciones en el LCP de estado de máquina son causadas por eventos. Algunos eventos son causados por la ejecución de comando en la máquina local final (p.ej. Active-Open, Passive-Open y Close), otros son causados por la recepción de paquetes de un remoto final (p.ej. Receive-Configure- Request, Receive-Configure-Ack, Receive-Configure-Nak, Receive-Terminate-Request y Receive-Terminate-Ack), y aún otros son causados por la expiración del tiempo Restart comenzado como el resultado de otro evento (p.ej. Timeout).

La siguiente es una lista de eventos LCP.

Active-Open (AO).

El evento Active-Open indica la ejecución local de un comando de Active-Open por el administrador de red (humano ó programa). Cuando este evento ocurre, el LCP inmediatamente deberá intentar abrir la conexión intercambiando paquetes de configuración con el LCP par.

Passive-Open (PO).

El evento Passive-Open es similar al evento Active-Open. Sin embargo, en lugar de un inmediato intercambio de paquetes de configuración, LCP deberá esperar por el par a enviar en el primer paquete. Esto solamente puede ocurrir después de un evento Active-Open en el LCP par.

Close ©.

El evento Close indica la ejecución local de un comando Close. Cuando este evento ocurre, LCP deberá inmediatamente intentar cerrar la conexión.

Timeout (TO).

El evento Timeout indica la expiración del tiempo de Restart del LCP. El tiempo de Restart de LCP es comenzado como el resultado de otro evento LCP.

El tiempo de Restart es usado para transmisiones de tiempo fuera de paquetes Configure-Request y Terminate-Request. La expiración del tiempo de Restart causa un evento Timeout, el cual alerta al correspondiente paquete Configure-Request ó Terminate-Request a ser retransmitido. El tiempo Restart DEBE ser configurable, pero el valor de default es tres (3) segundos.

Receive-Configure-Request (RCR).

El evento Receive-Configure-Request ocurre cuando un paquete Configure-Request es recibido desde el LCP par. El paquete de Configure-Request indica el deseo de abrir una conexión LCP y puede especificar las opciones de configuración. El paquete Configure-Request es descrito más detalladamente en la siguiente sección.

Receive-Configure-Ack (RCA).

El evento Receive-Configure-Ack ocurre cuando un paquete Configure-Ack válido es recibido desde el LCP par. El paquete Configure-Ack es una respuesta positiva a un paquete Configure-Request.

Receive-Configure-Nak (RCN).

El evento Receive-Configure-Nak ocurre cuando un paquete válido de Configure-Nak ó Configure-Reject es recibido desde el LCP par. El paquete Configure-Nak y el Configure-Reject son respuestas negativas a un paquete Configure-Request.

Receive-Terminate-Request (RTR).

El evento Receive-Terminate-Request ocurre cuando un paquete Terminate-Request es recibido desde el LCP par. El paquete Terminate-Request indica el deseo de cerrar la conexión LCP.

Receive-Termiante-Ack (RTA).

El evento Receive-Terminate-Ack ocurre cuando un paquete Terminate-Ack es recibido desde el LCP par. El paquete Terminate-Ack es una respuesta a un paquete Terminate-Request.

Receive-Code-Reject (RCJ).

El evento Receive-Code Reject ocurre cuando un paquete Code-Reject es recibido desde el LCP par. El paquete Code-Reject comunica un error que inmediatamente cierra la conexión.

Receive-Unknown-Code (RUC).

El evento Receive-Unknown-Code ocurre cuando un paquete no-interpretable es recibido desde el LCP par. El paquete Code-Reject es una respuesta a un paquete desconocido.

Receive-Echo-Request (RER).

El evento Receive-Echo-Request ocurre cuando un paquete Echo-Request, Echo-Reply ó un Discard-Request es recibido desde el LCP. El paquete Echo-Reply es una respuesta a un paquete Echo-Request. Este no es repetición de un Discard-Request.

Physical-Layer-Down (PLD).

El evento Physical-Layer-Down ocurre cuando la capa física indica que está dada de baja.

Acciones.

Acciones en la máquina de estados del LCP no causados por eventos y que comúnmente indican la transmisión de paquetes y/o el comenzar ó terminar del tiempo Restart. La siguiente es una lista de acciones LCP.

Send-Configure-Request (scr).

La acción Send-Configure-Request transmite un paquete Configure-Request. Este indica el deseo de abrir una conexión LCP con un juego específico de opciones de configuración. El tiempo de Restart es comenzado después que el paquete de Configure-Request es transmitido, para protegerlo contra perdida de paquetes.

Send-Configure-Ack (sca).

La acción Send-Configure-Ack transmite un paquete Configure-Ack. Este reconoce la recepción de un paquete Configure-Request con un aceptable juego de opciones de configuración.

Send-Configure-Nak (scn).

La acción Send-Configure-Nak transmite un paquete Configure-Nak ó Configure-Reject, según sea lo apropiado. Esta respuesta negativa reporta al receptor de un paquete Configure-Request con un inaceptable juego de opciones de configuración. Los paquetes Configure-Nak son utilizados para rechazar todas las negaciones sobre las opciones de configuración, comúnmente porque estas no son reorganizadas ó implementadas. El uso de Configure-Nak contra Configure-Reject está más completo en la sección de formato de paquete LCP.

Send-Terminate-Req (str).

La acción Send-Terminate-Requet transmite un paquete Terminate-Request. Este indica el deseo de cerrar la conexión LCP. El tiempo de Restart es comenzado después de que el paquete Terminate-Request es transmitido, para prevenirlo contra perdidas de paquetes.

Send-Terminate-Ack (sta).

La acción Send-Terminate-Request transmite un paquete Terminate-Ack. Este reconoce la recepción de un paquete Terminate-Request ó de otra forma confirma en la veracidad de que la conexión LCP es cerrada.

Send-Code-Reject (scj).

La acción Send-Code-Reject transmite un paquete Code-Reject. Este indica la recepción de un paquete de tipo desconocido. Este es un error irrecuperable el cual causa la transmisión inmediata del estado Close en ambos lados terminales del enlace.

Send-Echo-Reply (ser).

La acción Send-Echo-Reply transmite un paquete de Echo-Reply. Este reconoce la recepción de un paquete Echo-Request.

Estados.

La siguiente es una descripción más detallada de cada estado LCP.

Closed (1).

El estado final e inicial es el estado de Closed. En el estado de Closed, la conexión es dada de baja y no intenta abrirla; todas las peticiones de conexión desde pares son reejecutadas. Eventos como Physical-Layer-Down siempre causan una transición inmediata al estado de Closed.

Estos son dos eventos los cuales causan una transición hacia un estado Closed: Active-Open y Passive-Open. Suponga un evento Active-Open, un Configure-Request es transmitido, el tiempo de Restart comienza y el estado Request-Sent es introducido. Suponga un evento Passive-Open, el estado Listen es introducido inmediatamente. Suponga la recepción de cualquier paquete, con la excepción de un Terminate-Ack, un Terminate-Ack es enviado, el Terminate-Ack es silenciosamente descartado para evitar la creación de un lazo (loop).

El tiempo Restart no está corriendo en el estado Closed.

La conexión de la capa fisica puede ser desconectada en cualquier tiempo cuando este en el estado LCP Closed.

Listen (2).

El estado Listen es similar al estado Closed en que la conexión es dada de baja y este no intenta abrirla. Sin embargo, peticiones de conexión par no son ampliamente reejecutadas.

Suponga que recibe un Configure-Request, un Configure-Request es inmediatamente transmitido y el tiempo de Restart es inicializado. Las opciones de configuración recibidas son examinadas y la respuesta propia es enviada. Si un Configure-Nak es enviado, el estado Ack-Sent es introducido. De otra forma, si un Configure-Ack ó un Configure-Reject es enviado, el estado Request-Sent es introducido. En ambos casos, LCP existe en su estado pasivo y comienza a abrir activamente la conexión. El paquete Terminate-Ack es enviado en respuesta de tanto el paquete Configure-Ack ó Configure-Nak.

El tiempo Restart no está corriendo en el estado Listen.

Request-Sent (3)

En el estado Request-Sent un intento activo es realizado para abrir la conexión. Un Configure-Request ha sido enviado y el tiempo Restart está corriendo, pero un Configure-Ack aún no ha recibido y tampoco ha sido enviado.

Suponga la recepción de un Configure-Ack, el estado Ack-Received es inmediatamente introducido. Suponga la recepción de un Configure-Nak ó Configure-Reject, las opciones de configuración de Configure-Request son ajustadas apropiadamente, un nuevo Configure-Request es transmitido y el tiempo de Restart es inicializado. Similarmente, suponga la expiración del tiempo de Restart, un nuevo Configure-Request es transmitido y el tiempo de Restart es reinicializado. Suponga ahora la recepción de un Configure-Request, las opciones de configuración son examinadas y si se aceptan, un Configure-Ack es enviado y el estado Ack-Sent es introducido. Si las opciones de configuración no son aceptables, un Configure-Nak ó Configure-Reject apropiado es enviado.

Puesto que este es un destacado Configure-Request, en el estado Request-Sent, debe ser tomado un especial cuidado para implementar el evento Passive-Open y Close; de otra forma, es posible que el par LCP piense que la conexión está abierta. El procesado de ambos eventos debe ser pospuesto hasta que sea asegurado que el par no está abierto. En particular, el tiempo de Restart deberá ser permitido a expirar.

Ack-received (4)

En el estado Ack-Received, un Configure-Request ha sido enviado y un Configure-Ack ha sido recibido, el tiempo de Restart está aún corriendo puesto que un Configure-Ack no ha sido transmitido. Suponga la recepción de un Configure-Request con opciones de configuración aceptables, un Configure-Ack es transmitido, el tiempo Restart es detenido y el estado Open es introducido. Si las opciones de configuraciones son inaceptables, un Configure-Nak ó un Configure-Reject es enviado como apropiado. Suponga la expiración del tiempo de Restart, un nuevo Configure-Request es transmitido, el tiempo Restart es reinicializado y la máquina de estado regresa a un estado Request-Sent.

Ack-Sent (5)

En el estado Ack-Sent, un Configure-Ack y un Configure-Request han sido enviados pero un Configure-Ack aún no ha sido recibido. El tiempo de Restart siempre está corriendo en el estado Ack-Sent.

Suponga la recepción de un Configure-Ack, el tiempo de Restart es detenido y el estado Open es introducido. Suponga la recepción de un Configure-Nak ó Configure-Reject, las opciones de configuración de Configure-Request son ajustadas apropiadamente, un nuevo Configure-Request es transmitido, el tiempo de Restart es reinicializado y la máquina de estado regresa al estado de Request-Sent.

Open (6)

En el estado Open, una conexión existe y los datos pueden ser comunicados sobre el enlace. El tiempo de Restart no está corriendo en el estado Open.

En operación normal, solo dos eventos provocan la transición de salida del estado Open. Suponga la recepción de un comando Close, un Terminate-Request es transmitido, el tiempo Restart es inicializado y el estado de Closing es introducido. Suponga la recepción de un Terminate-Request, un Terminate-Ack es transmitido y el estado Closed es introducido. Suponga la recepción de un Echo-Request, un Echo-Reply es transmitido. Similarmente, los paquetes Echo-Reply y Discard-Request son silenciosamente descartados ó procesados como se esperaba. Todos los eventos causan una transición hacia afuera del estado Open y deberán ser manejados como si la máquina de estados estuviera en el estado Listen.

Closing (7)

En el estado Closing, se realiza un intento activo para cerrar la conexión. Un Terminate-Request ha sido enviado y el tiempo de Restart está corriendo, pero un Terminate-Ack aún no ha sido recibido.

Suponga la recepción de un Terminate-Ack, el estado Closed es inmediatamente introducido. Suponga la expiración del tiempo de Restart, un nuevo Terminate-Request es transmitido y el tiempo de Restart es reinicializado. Después de que el tiempo de Restart a agotado el tiempo de Max-Restart, esta acción puede ser saltada, y el estado Closed puede ser introducido. Max-Restart DEBE ser un parámetro configurable.

Puesto que este es un Terminate-Request destacado en el estado Closing, se debe tomar un cuidado especial para implementar el evento Passive-Open; de otra forma, es posible que el par LCP piense que la conexión está abierta. El procesado del evento Passive-Open deberá ser pospuesto hasta que se asegure que el par no está abierto. En particular, la implementación deberá esperar hasta que la máquina de estados pueda normalmente pasar al estado de Closed desde un evento Received-Terminate-Ack ó un evento Max-Restart-Timeout.

Loop Avoidance

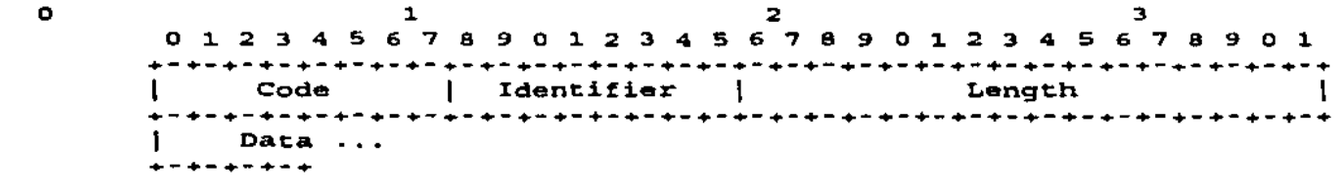
Notará que el protocolo hace un intento razonable por evitar la negociación de lazos de las opciones de configuración. Sin embargo, el protocolo NO garantiza que los lazos no puedan pasar. Como cualquier negociación, si es posible implementar dos implementaciones con políticas de conflicto las cuales hacen convergencia, pero las cuales también toman un tiempo significante para hacerlas. Los implementadores deberán guardar esto en mente y deberán implementar mecanismos de detección de lazo ó tiempos de salida de nivel más alto. Si un tiempo de salida es implementado, este DEBE ser configurable.

Por ejemplo, las implementaciones deberán tomarse con cuidado para evitar bloqueos en vivo de Configure-Request ó Terminate-Request usando un contador Max-Retries. Un bloqueo en vivo de Configure-Request podrá ocurrir cuando un PPP originador envía y reenvía un C-R sin recibir una respuesta (p.ej. la recepción de entradas PPP que pueden haber muerto). Un bloqueo en vivo Terminate-Request podrá ocurrir cuando el PPP originador envía y reenvía un T-R sin recibir un Terminate-Ack (p.ej. el T-A puede haber sido perdido, pero el remoto PPP puede haber terminado ya). Max-Retries indica el número de paquetes retransmisionados que son permitidos antes de que se asegure razonablemente que una situación de bloqueo en vivo existe. Max-Retries DEBE también ser configurable, pero su default debe ser puesto a diez (10) retransmisiones.

Formato del paquete.

Un paquete de control de enlace es encapsulado en el campo de información del frame PPP de la capa de enlace de datos, donde el campo de protocolo indica el tipo hexadecimal c021 (Link Control Protocol).

Un sumario del formato del paquete de protocolo de control de enlace es mostrado a continuación. El campo es transmitido de izquierda a derecha.



Código.

El campo de código es un octeto e identifica el tipo de paquete LCP. El código LCP es asignado como sigue:

1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject
8	Protocol-Reject
9	Echo-Request
10	Echo-Reply
11	Discard-Request

Identificador.

El campo Identificador es un octeto y ayuda para peticiones perdida y repetidas.

Longitud.

El campo de longitud es un octeto e indica la longitud del paquete LCP incluyendo el Código, Identificador, Longitud y el Campo de Datos. Otro octetos fuera del rango del campo de longitud deberán ser tratados como relleno de la capa de enlace de datos y deberá ser ignorado en la recepción.

Datos.

El campo de datos es de cero ó más octetos como sean indicados por el campo de longitud. El formato del campo de Datos es determinado por el campo de código.

Sin tomar en cuenta de cual opción de configuración está habilitada, todos los paquetes LCP son enviados en la forma estándar completa, como si las opciones de configuración no estuviera habilitadas. Esto asegura que el paquete LCP Configure-Request siempre es reconocible aún cuando en el final del enlace misteriosamente crea que el enlace a sido abierto.

Opciones de configuración.

Las opciones de configuración LCP permiten modificaciones a las características estándar del enlace point-to-point para ser negociadas.

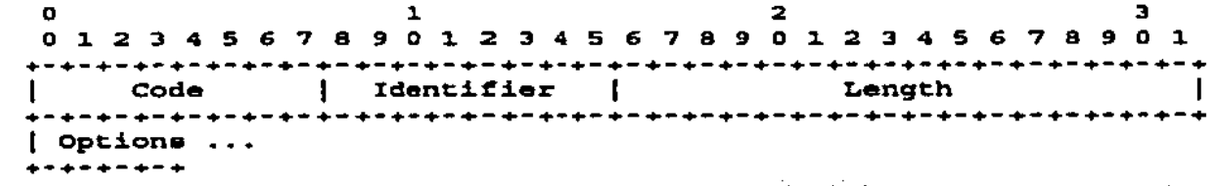
Las negociaciones modificables incluyen cosas tales como el número de las unidades máximas recibidas, el mapeado de caracteres de control asincrono, el método de autentificación de enlace, el método de encriptación de enlace, etc. Las opciones de configuración por si mismas son descritas en documentos separados. Si no se incluyen las opciones de configuración en el paquete Configure-Request, el valor de default para las opciones de configuración es asumido. El final de la lista de opciones de configuración es indicado por el final del paquete LCP.

A menos que se especifique otra cosa, una opción de configuración especifica deberá ser listada no más de una vez en la lista de opciones de configuración. Opciones de configuración especificas pueden saltarse esta regla general y pueden ser listadas más de una vez.

También, a diferencia de otras especificaciones, todas las opciones de configuración se aplican en "half-duplex". Cuando se negocian, estas se aplican a solo una dirección del enlace, comúnmente en la dirección de recepción cuando es interpretado desde el punto de vista del enviador del Configure-Request.

Formato.

Un sumario del formato de la opción de configuración es mostrado a continuación. El campo es transmitido de izquierda a derecha.



Tipo.

El campo Tipo es un octeto e indica el tipo de opción de configuración. Los valores más altos del dato del campo de tipo son especificados en el más reciente RFC 11 "Assigned Numbers".

Longitud.

El campo de Longitud es un octeto e indica la longitud de esta opción de configuración incluyendo el campo de Tipo, Longitud y Datos. Si una opción de configuración negociable es recibida en un Configure-Request pero con una longitud invalida, un Configure-Nak deberá ser transmitido el cual incluye la opción de configuración deseada con una Longitud y Datos.

Datos.

El campo de Datos es cero ó más octetos e indica el valor u otra información para esta opción de configuración. El formato de longitud del campo de Datos es determinado por el campo de Tipo y Longitud.

Un protocolo de control de red (NCP) PPP para IP.

El IP Control Protocol (IPCP) es responsable de la configuración, habilitación y deshabilitación del modulo de protocolo IP en ambos finales del enlace point-to-point. Como en el Link Control Protocol, este es completado a través de un intercambio de paquetes. Paquetes IPCP pueden ser no intercambiados hasta que LCP haya alcanzado la fase de Negociación de Configuración de Protocolo de la capa de red. De igual forma, datagram IP no pueden ser intercambiados hasta que IPCP abra la conexión primeramente.

El IP Control Protocol es exactamente el mismo que el Link Control Protocol con las siguientes excepciones:

* Campo de protocolo de la capa de enlace de datos.
* Campo de código
* Timeouts.
* Tipos de opciones de configuración.

Enviado de un Datagram IP.

Antes de que un paquete IP pueda ser comunicado, tanto el protocolo de control de enlace y el IP Control Protocol deben alcanzar el estado Open.

Un paquete IP es encapsulado en el campo de información del frame de la capa de enlace de datos PPP donde el campo del protocolo indica el tipo en hexadecimal 0021 (Internet Protocol).

La máxima longitud de un paquete IP transmitido sobre un enlace PPP es la misma que la máxima longitud del campo de información de un frame de la capa de enlace de datos PPP. Los datagram IP largos deberán ser fragmentados como sea necesario. Si un sistema deseara evitar la fragmentación y reensamblar, este deberá usar la opción 12 de TCP Maximum Segment Size, ó un mecanismo similar, para alertar a los otros del enviado de datagram largos.

2.3.- Una propuesta para la transmisión de un Datagram IP sobre línea serial: SLIP.

2.3.1.- Introducción.

La familia de protocolos TCP/IP corre sobre una variedad de medios de red: LAN de IEEE 802.3 (Ethernet) y 802.5 (Token Ring), lineas X.25, enlaces satélitales y líneas seriales. Estos son estándares de encapsulamiento para paquetes IP definidos por muchas de esas redes, pero estas no son estándares para líneas seriales. SLIP, Serial Line IP, es comúnmente un estándar defecto, utilizado para conexiones seriales punto a punto corriendo TCP/IP. Este no es un estándar Internet.

2.3.2.- Historia.

SLIP tiene sus orígenes en la implementación de 3 COM UNET TCP/IP desde el principio de 1980. Este es meramente un protocolo de estructuración de paquete: SLIP define una secuencia de caracteres que estructura los paquetes IP en una línea serial y nada más. Este no provee direcciones, identificación de tipo de paquete, mecanismo de detección de error/corrección ó compresión. Puesto que el protocolo es demasiado pequeño, sin embargo, es usualmente muy fácil de implementar.

Alrededor de 1984, Rick Adams implemento SLIP para 4.2 Berkeley UNIX y Sun Microsystems workstations y relacionó este al mundo. Este es rápidamente capturado como una forma fácil y confiable de conectar host TCP/IP y ruteadores con líneas seriales.

SLIP es comúnmente usado en enlaces seriales dedicados y algunas veces para propósito de marcado y es comúnmente usado con velocidades de línea entre 1200bps y 19.2Kbps. Este es útil para permitir mezclado de host y ruteadores para comunicarse uno con los otros (host-host, host-ruteador y ruteador-ruteador son todas las comunes configuraciones de red SLIP).

2.3.3.- Disponibilidad.

SLIP está disponible para muchos sistemas basados en Berkeley UNIX. Este es incluido en el estándar 4.3BSD versión de Berkeley. SLIP está disponible para Ultrix, Sun UNIX y muchos otros sistemas derivados de Berkeley UNIX. Algunos concentradores terminales e implementaciones de IBM PC también son soportadas.

SLIP para Berkeley UNIX está disponible via FTP anónimo desde ***uunet.uu.net*** en ***pub/sl,shar.Z***. Asegúrese de transferir el archivo en modo binario y de correrlo a través de un programa descompresor de UNIX. Tome el archivo resultante y úselo como un shell script para el UNIX/bin/sh (por ejemplo, /bin/sh sl.shar).

2.3.4.- Protocolo.

El protocolo SLIP define dos caracteres especiales: END y ESC. END es 300 en octal (192 en decimal) y ESC es 333 en octal (219 en decimal) no debe confundirse con el carácter ASCII ESCape, para el propósito de esta discusión, ESC indicará el carácter ESC de SLIP. Para enviar un paquete, un host SLIP simplemente comenzará enviando el dato en el paquete. Si el byte de dato es del mismo código que el carácter END, una secuencia de dos byte de ESC y 334 en octal (220 en decimal) es enviada en su lugar. Si es el mismo que un carácter ESC, una secuencia de dos byte de ESC y 335 en octal (221 en decimal) es enviada en su lugar. Cuando el último byte en el paquete ha sido enviado, el carácter END es entonces transmitido.

Phil Karn sugiere un simple cambio al algoritmo, el cual es tanto en el comienzo así como al final del paquete con un carácter END. Este podría igualar cualquier byte erróneo el cual haya sido causado por ruido en la línea. En el caso normal, el receptor simplemente vera dos caracteres "back-to-back" END, el cual generará un paquete IP malo. Si la implementación de SLIP no arroja el paquete IP de longitud cero, la implementación IP ciertamente lo hará. Si este fue el ruido de la línea, el dato recibido debido a esto será descartado sin afectar al siguiente paquete.

Puesto que este no es una especificación SLIP "estándar", no hay un tamaño máximo de paquetes definidos para SLIP. Este es probablemente mejor aceptar el tamaño de paquetes máximo usado por el driver de Berkeley UNIX SLIP: 1006 bytes incluyendo el IP y cabeceras de protocolo de transporte (no incluyendo caracteres de estructura). Por lo tanto cualquier nueva implementación de SLIP deberá ser preparada para aceptar 1006 bytes de datagrams y no deberá enviar más de 1006 bytes en un datagram.

2.3.5.- Deficiencias.

Estas son varias realizaciones que a muchos usuarios le gusta que SLIP pudiera proveer, lo cual no lo hace. En toda rectitud, SLIP es simplemente un protocolo diseñado totalmente hace mucho tiempo cuando ese problema no emitían una importancia real. Los siguientes son comúnmente defectos preservados en el protocolo SLIP:

-direccionamiento:

ambas computadoras en un enlace SLIP necesitan conocer la dirección IP de la otra máquina, para el propósito de ruteo. También, cuando usa SLIP para ruteo de host a dial-up, el esquema de dirección puede ser totalmente dinámico y el ruteador puede necesitar informar al host marcador de la dirección IP del host. SLIP comúnmente no provee un mecanismo para host para comunicar la información de direccionamiento sobre una conexión SLIP.

-identificación de tipo:

SLIP no tiene un campo de tipo. Así, solo un protocolo puede estar corriendo sobre una conexión SLIP, tanto en una configuración de dos computadoras DEC corriendo ambas TCP/IP y DECnet, este no espera que tenga TCP/IP y DECnet compartiendo una línea serial entre ellos mientras usa SLIP. Puesto que SLIP es "Serial Line IP", si una línea serial conecta dos computadoras con protocolos múltiples, estas computadoras deberán estar disponibles para usar más de un protocolo sobre la línea.

-detección/corrección de error:

ruido de líneas telefónicas puede corromper los paquetes en transito. Puesto que la velocidad de la línea es probablemente totalmente baja (como de unos 2400 baud), la retransmisión de datos es muy costosa. La detección de error no es absolutamente necesaria en un nivel SLIP puesto que cualquier aplicación IP deberá detectar paquetes dañados (cabeceras IP y checksum de UDP y TCP deberán ser suficientes), a través de algunas aplicaciones comunes como NFS usualmente ignora el checksum y depende en el medio de la red para detectar paquetes dañados. Puesto que este es tomado a todo lo largo para retransmitir un paquete el cual fue corrompido por el ruido de la línea, este podría ser

eficiente si SLIP pudiera proveer algún orden de mecanismos de corrección de errores simples por sí mismo.

-compresión:

puesto que líneas dial-in son demasiado lentas (usualmente 2400 bps), la compresión de paquetes podría causar grandes mejoras en paquetes continuos. Usualmente, flujo de paquetes en una conexión TCP única tienen pocos campos cambiados en las cabeceras IP y TCP, así un simple algoritmo de compresión pueden simplemente enviar las partes que cambian de las cabeceras en lugar de las cabeceras completas.

Algunos trabajos están comenzando a realizarse por varios grupos para diseñar e implementar un sucesor al SLIP el cual podría direccionar algunas ó todas sus problemas.

2.4.- Comandos de módems.

2.4.1.- ¿Qué es "Hayes"?

Dennis Hayes fundo la Hayes Micromodems hace algunos años. Algunas personas creen que el invento el módem. Podrá decirse que lo hizo y que no lo hizo. Los módems físicos actuales han estado en nuestro alrededor de forma silenciosa por un buen tiempo. Lo que Hayes invento fue uno de los primeros módems diseñados específicamente para microcomputadoras. Los módems de Hayes estaban bien construidos, pero para esos días, lo mismo se decía de una buena cantidad de módems. La circuitería de las secciones de modulación y demodulación de los módems están contenidas en juego de chips estándar fabricados por Rockwell, XR y unos cuantos fabricantes. Lo que hace a los módems Hayes ser el "estándar" fue la interface de programación que Dennis Hayes creo.

Una interface en términos electrónicos es simplemente otra palabra para el método de conexión. Los conectores pueden ser físicos ó virtuales. Virtual significa que este actúa como una conexión real, pero no es una conexión físicamente real. Un ejemplo de una conexión virtual es un software conmutador. Este actúa como un conmutador que puede estar conectando a un luz y este puede cambiar a otro sistema para pasar de un estado de encendido ó apagado; para nuestro caso del módem, podrá ser un carácter en la pantalla, aunque este no es real, porque se conmuta al tocarse. Una interface de programación es una conexión virtual entre dispositivos ó módulos en un programa. Los módulos Hayes vienen con una interface de programación que le permite a la gente escribir programas que utilizan los módems, para poder realizar estos en una forma en el que el programador no tenga que escribir comandos para marcar, conectarse, cambiar la relación de baud ó desconectarse. El módem Hayes contiene un microprocesador, este en realidad no es diferente del que utilizan las computadoras hoy en día, sin embargo, su propósito de este es solamente observar al carácter que está comenzándose a enviarse. Si una línea comienza con las letras "AT", el módem sabe que el siguiente grupo de caracteres que puede ver contienen un comando para él (módem). El comando puede decirle que conteste el teléfono (ATA), que marque un número telefónico (ATDT832-1398), que apague la bocina (ATM0), que encienda la bocina (ATM1) y una variedad de otros comandos. De igual forma esta interface regresa al programa de la computadora enviando mensajes reales y comprensibles como "OK", "CONNECT 9600", "RINING", "BUSY" y otros más. A los programadores les gusta trabajar con estos comandos, pues les ofrece dos ventajas; Primeramente, todo lo que necesitan hacer fue enviar caracteres al módem, para hacer todos lo tipos de actividades de telecomunicaciones complejas y segundo, si el módem que este utilizando para emitir estos comandos utiliza la estructura de comandos "AT" (ó es compatible con Hayes), no

importara que el módem sea reemplazado por otro nuevo ó mejorado, siempre y cuando este también utilice esta estructura, el módem podrá seguir trabajando con el software que el programador tenga instalado. Hayes a sustituido algunas de las fallas que tenia IBM. IBM originalmente tenia la idea de la ROM-BIOS en estas máquinas como una conexión virtual entre un programa y la computadora. IBM por lo tanto debe entonces tener que cambiar la forma en la que la computadora trabaja en una manera transparente para el software, tantas veces como el software utilice las llamadas ROM-BIOS. Los que tienen conocimientos en computadoras saben que, la ROM-BIOS en la PC original trabaja demasiado lento por lo que los programadores toman cortes pequeños alrededor de este. Este domina a la PC y el futuro de las PC hacen que estén por siempre compatibles en hardware con las máquinas originales. El juego de instrucciones "AT" de Dennis Hayes se convirtió en el estándar para comunicaciones de computadoras personales, Macintosh, Atari y próximamente para todos los dispositivos de comunicaciones digitales. Muchos fabricantes hacen módems que son compatibles con los juegos de comandos de módems Hayes 300/1200 y el Hayes 2400B, con alguna expansión ó creando computadoras que la gente llama "superset" del juego de instrucciones originales de Hayes "AT".

Cuando compre un módem, puede ver una etiqueta que diga "Hayes Compatible", esto significa que este utiliza el juego de instrucciones "AT" y sigue la misma estructura de comandos que tenia el original Hayes 300/1200 ó la serie de módems Hayes 2400 (este es una ligera diferencia entre el comando 300/1200 y el 2400). Esto no significa que estos sean iguales de buenos como un Hayes, por ejemplo, estos podian ser mejores. Con todo esto solamente queremos dejar claro que usted puede utilizar el 99% de todo el software de comunicación desarrollado para su PC con este módem. Pero quedaria el saber cual es el otro 1% del software incompatible. Estos son definidos por los registros almacenados en un módem Hayes y demás compatibles. Estos registros almacenados (ó registros S) tienen información de comunicación vital. Estos almacenan todos los parámetros de los módems usados para comunicarse. Estos registros pueden ser accesados, tal como un programador puede escribir directamente a su pantalla y desviar la ROM-BIOS. Si un programador escribe ó lee un registro S, este espera a que el módem utilice ese registro S para la misma cosa que el módem escribió para lo que originalmente lo tenia usado. Puesto que un módem reclama por ser un "Hayes Compatible", es dudoso que si esta compatible al 100% con el "hardware" Hayes, entonces este programa necesita ser modificado cuando sea usado con un módem de marca diferente. Muchos de los más recientes programas BBS donde se escriben para esta compatibilidad de hardware, podrían no operar apropiadamente sin estos. ¿Qué módem deberá comprar entonces?. Esto depende de la aplicación y las disponibilidad económica.

2.4.2.- Aprendiendo a hablar mnemónico.

En el mundo de la computación los mensajes son llamados mnemónico. Un ejemplo popular de un mnemónico es el icono con el que se accesa en el mouse. Otro ejemplo podría ser el nombre de comando usado en los programas en lenguaje ensamblador para los códigos, aún otros pueden ser el nombre que usted asigna a un rango de celdas en un programa de hoja de cálculo. Los mnemónico son un tipo de pseudo-lenguaje que puede ser más fácil de comprender que un lenguaje completo. Ahora, son muchas formas diferentes de mirar el juego de instrucciones AT, pero la mejor es pensar que son una serie de mnemónico que le ayudan a controlar su módem. En el juego de instrucciones AT significa "attention". Esta es una forma para que el microprocesador en el módem distinga entre un carácter normal que empieza a ser enviado a éste y un comando. Este es también dos maneras de que un módem compatible con AT opere; el modo comando y el modo en-línea. Cuando enciende su

computadora y carga un programa de comunicación, esta comunicando al módem en un modo comando. Cuando su módem se conecta a un BBS ó a cualquier otro servicio, el módem se conmuta automáticamente al modo de en-línea. Cuando esta en el modo de comando, usted le puede hablar al módem usando el comando AT y cambiar muchas de las formas en que su módem funcionará. Cuando esta en el modo en-línea, usted no puede comunicarse con el módem con los comandos AT (hay un forma de regresar al modo de comando mientras esta en-línea, pero será discutida posteriormente). La belleza del modo comando no solo es apreciada por la gente que escribe los programas de comunicación, sino también puede (y debe) ser apreciada por usted.

Después de que usted haya cargado el programa de comunicaciones (digamos Procomm, Qmodem ó Telix, por ejemplo) podrá notar que puede teclear caracteres en el teclado y que estos son desplegados en la pantalla. ¿Como pasa esto?. No, la computadora no hizo un eco de lo que usted tecleo en la pantalla, como un escritor de cartas, usted en su lugar tiene un programa que toma un carácter y lo envía a la pantalla. Una buena prueba de esto es intentar teclear caracteres cuando su computadora esta "hang-up" ó descolgada. Nada pasara; MS-DOS no hace el eco para command.com y programas que usen MS-DOS ó sus propios esquemas de eco. Cuando se esta comunicando con un módem usted envía caracteres escribiéndolos en su teclado. Esos caracteres son entonces enviado a su módem. En el módem, entonces, son enviados de regreso a su computadora, donde el programa que usted este utilizando los colocara en la pantalla. Esto es técnicamente referido como una operación "Full-Duplex" y un "Local Command Echo". En este modo, usted puede cambiar muchos de las caracteristicas de operación de su módem tecleando pocas letras. Todo lo que necesita hacer es seguir unas reglas simples; Primero, todos los comandos deben empezar al principio de la linea y las primeras 2 letras deben ser AT. Segundo, usted puede colocar múltiples comandos de linea, todos en una misma linea, hasta alrededor de 40 caracteres. Tercero, todos los caracteres que usted teclee deben ser comandos legitimos para su tipo de módem, de otra forma vera la palabra **ERROR** de regreso. Intente el seleccionado de la computadora con el programa de comunicación y teclee el comando ATH1 y presione return. Este puede tomar su teléfono "off-hook" (descolgado) y deberá oir un tono de marcado. Para colocar el teléfono de regreso en "on-hook" (colgado), teclee ATH0 y presione return.

Usando el comando AT, puede poner su módem para aplicaciones especiales. Por ejemplo, muchos programas BBS no les gusta ver el comando local echo, asi este es un comando ATE0 que puede ser usado para cambiar este echo a off. Si usted hace esto, puede notar que desde ese punto en cada carácter que usted teclee al módem este no será desplegado. El módem puede aún responder y enviar la palabra **OK** ó **ERROR** de regreso a la pantalla, pero este no hará eco de los caracteres que usted tecleé. Para regresar el eco local de nuevo, solamente presione return (esto para asegurarse que está comenzando una nueva linea puesto que usted no esta seguro desde que el eco fue puesto en off), teclee ATE1 y presione return. El módem responderá con **OK** y ahora usted puede ver los caracteres con eco otra vez. Puede comenzar el programa y decirle al módem que quiere apagar la bocina todo el tiempo tecleando ATM1 y así hay infinidad de comandos que pueden ser utilizados por su programa de módem para que trabaje en la forma en que a usted le guste. Revise rápidamente el manual que viene con su módem, si no lo tiene ó lo perdió, existen varias literaturas en relación a los comandos de los módem compatibles con Hayes, es cuestión de buscarlos, más adelante se explican algunos de estos. A este conjunto de comandos también se le llama flujo de inicialización. Estos son el conjunto de comandos que son puestos automáticamente en su módem por su programa de comunicaciones cada vez que se inicia éste. Un flujo de inicialización apropiado puede ser importantes para algunas aplicaciones.

Por ejemplo un programa "bulleting board" usualmente no opera propiamente si el flujo de inicialización es incorrecto. Muchos programas de comunicación le permiten personalizar este juego de comandos cada vez que inicie. Lo que ponga en el flujo de inicialización es ejecutado totalmente para usted. En nuestro ejemplo previo, si desea apagar la bocina cada vez que el programa de comunicaciones es cargado, entonces el flujo de inicialización es ATM0. Si desea regresar códigos de resultados extendidos que puedan decirle si el módem ve una señal de ocupado, su flujo de inicialización es AT X4. Si desea tanto la bocina apagada como el código extendido, su flujo de inicialización será AT M0 X4. Cualquier comando legal para su módem puede ser colocado en este flujo de inicialización. Puede también manipular el contenido de algo llamado Registro-S. Un Registro-S es una localización de memoria en el módem. Cada localización es marcada con un número S0, por ejemplo, grabando cuantas veces el teléfono ha sonado. El Registro S6 pone un tiempo que es contado de forma decreciente en un pre-determinado número de segundos que el módem esperará hasta que este intente hacer una conexión. S11 controla la velocidad que el comando de marcado de teclas de tono tomará para enviarlos hacia la compañía telefónica.

Los Registros-S son diferentes de los comandos AT, primeramente se tiene muchos Registros-S y la forma en que estos son utilizados varia de un fabricante a otro (en otras palabras, estas pueden ó no pueden ser compatibles con Hayes). Los primeros 16 registros S, sin embargo, han sido universalmente implementados para trabajar de la misma forma que con el Hayes original de los 1200. Su módem puede tener más ó menos de estos registros que los de un Hayes. Algunos módems han cerrado a 99 de estos registros S. Afortunadamente, usted no necesita estar familiarizado con los registros-S como con los comandos AT. Algunos trucos simples con los Registros-S es todo lo que necesita para conocer el uso de su módem apropiadamente. Poniendo estos comandos de Registro-S en su flujo de inicialización tendrá una poderosa herramienta fácil para el seleccionado de inicio de su módem, pero esto requiere de un análisis de las características de su equipo y su tipo de conexión.

Para cambiar el contenido de un Registro-S, solamente teclee (en una nueva línea de cursor) ATSx=nnn (donde x=a un numero de Registro-S y nnn=a un parámetro de 3 dígitos). Por ejemplo, para cambiar el tiempo en que un módem espera a ser contestado puede ser desde el tiempo de default de 30 segundos hasta 255 segundos, esto se realiza tecleando ATS7=255, para leer un valor de un Registro-S, se teclea ATSx? (donde x es el numero de Registro-S). Para ver el valor del registro S7, simplemente teclee ATS7?. El valor actual en el registro S7 puede ser desplegado en una forma de 3 dígitos (030 es el default, para 30 segundos). Todos los Registros-S tienen valores de default, pero estos pueden ser cambiados. Por ejemplo, supongamos que desea esperar por un minuto para conectarse a un BBS en lugar de 30 segundos; puede cambiar el valor del Registro-S7 para que su módem realice esta función apropiadamente. Así su flujo de inicialización (incluyendo lo que mencionamos) ahora se convierte en AT M0 X4 S7=60. El único limite al número de comandos que puede utilizar es normalmente de 40 caracteres (para la mayoría de los módem).

2.4.3.- Análisis del funcionamiento de un módem.

La mayoría de los módem incorporan un modo de comando basado en un microprocesador, el cual le permite a usted y a su teclado de computadora (ó software de comunicación), conversar e interactua con su módem. Cuando su módem está en el modo de comando, tiene acceso a un sistema de comunicación completo el cual le permite utilizar un número de realizaciones, incluyendo el juego de los comandos básicos AT (en algunos casos también se tiene la capacidad de marcado V.25bis). Los comandos básicos le permiten introducir números telefónicos para ser marcados automáticamente,

configurar varias opciones de módems y monitorear la actividad del teléfono. En relación a los comandos AT básicos y sus capacidades, su módem también puede realizar acciones avanzadas tales como corrección de error, compresión de datos, conversión de velocidad y más. Lo que se pretende es explicar el modo de comandos y mostrar como usar cada comando AT básico.

2.4.4.- Estados funcionales.

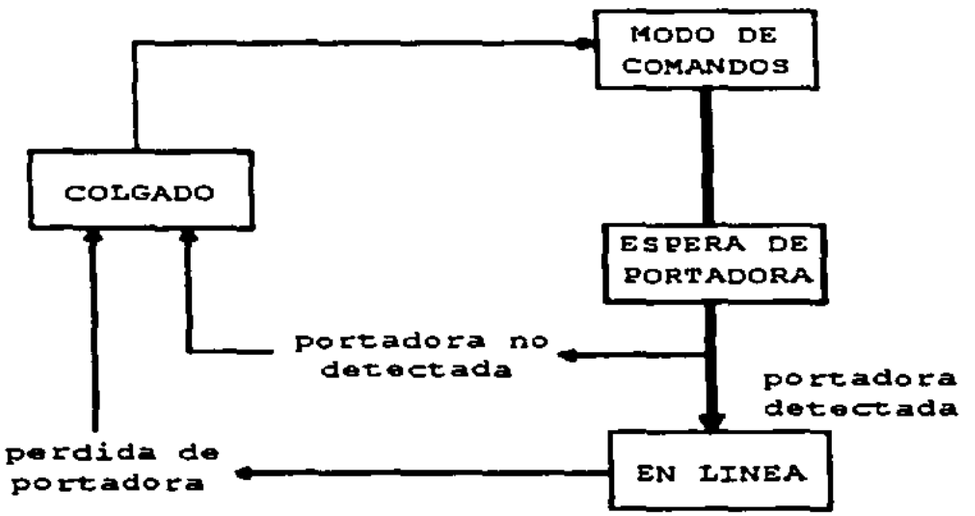
La mayoría de los módems pueden estar en uno de los dos estados funcionales. Estos son: "Modo de Comando" y "En linea". (Esto también incluye un estado entre estos estados, "Esperando la portadora", esto es, cuando el módem esta fuera del modo de comando pero realmente aún no esta en linea. Cuando el módem es inicialmente encendido, este puede estar en el modo de comando y estar listo para recibir comandos desde el teclado ó software y responder a cualquier comando del modo de comandos.

El módem entra en el estado de en linea después de que marco e hizo la conexión con otro módem, entonces detecta un tono de señal de portadora válido. Si no hay señal de portadora dentro de un cierto tiempo de frame, el módem puede abandonar la llamada y reintroducirse al modo de comando.

Una vez que esta en el modo de en línea, el módem sale de este si pierde la portadora ó se cuelga intencionalmente. Cuando sucede esto, el módem cuelga y vuelve a entrar en el modo de comando.

Muchos módems pueden salir del estado de en linea si perder la señal de portadora. Esto puede ser completado introduciendo cierto carácter de "escape" mientras esta en linea, el cual podrá traer al módem de vuelta al modo de comandos sin terminar la conexión.

Los módems también pueden estar en el estado de en linea sin pasar a través del proceso de marcado, introduciendo tanto el comando D ó el comando A. Por lo general, los módems de hoy en dia tiene el siguiente flujo de estados para las condiciones mostradas:



Existe una amplia variedad de operaciones de auto-marcado y opciones del módem que pueden ser controladas cuando el módem esta en el modo de comando. Un breve sumario de estos comandos es mostrado a continuación:

AT	Attention código que preside a todos los comandos
A	Answer modo de contestar
A/	Repite el último comando
A:	Continua el remarcado hasta que la llamada es contestada
&A	Answerback (propiedad del fabricante)
$A	Auto-Reliable Buffering
#A	Auto Speed Detect
B	Blind or Smart Dialing
B	Bell ó CCITT answer tone select
&B	Transmit Buffer Size
&BS	Maximum Block Size
$BA	Baud Adjust
&C	Carrie-Detect control
D	Dialing
$D	DTR dialing
&D	DTR control
E	Echo commands
&E	Error Correction/Data Compression commands
$E	Enable/Disable Error a 300 bmp
$EB	Asynchro Word Length Command
$F	Enable/Disable Error Auto-Reliable Fallback Character
#F	Fallback modems when on-line
&F	Fetch Factory default values
&G	Guard Screens
H	Hook on/off control or Hand up
$H	Help screens
I	Identify modem model/revision
L	List stored telephone numbers
L5	List current configuration parameters
L6	List current S-Register Values
L7	List additional configuration parametres
#L	V.42 Mode Select (LAP-M or MNP)
M	Monitor speaker control
&M	Synch/Asynch control
$MB	Modem Baud rate
$MI	MI/MIC Control
N	Number stored or dialed
O	On-Line from Command Mode
P	Pulse dial
&P	Set Pulse ratio
Q	Result Codes Enable/Disable (suppress responses), No Response Answer Modes Result code select
&Q	Result code select
Rn	Reversing the mode of operation
&R	ClearR-to-Send control

$R	Retransmit count
S=	S-Register, set vaule
S?	S-Register, read vaule
&S	Data-Set-ready control
$SB	Serial Port Baud rate
$SP	UUCP/"Spoofing"
T	Tone dial
#T	Enable/Disable Trellis Coded Modulation
U	U-loop test
V	Verbose or Terse result codes
W	Wait for new dial tone
&W	Store configuration parameters to RAM
X	X-tended-Extended or Basic result codes an Call Progress
Z	Zap (reset modem)
+++	Escape to Command Mode when on-line
,	Pause in dialing
:	Revert to Command Mode when on-line
;	Continuous redial until answered
!	Flash On-Hook
@	Quit Anwer

2.4.5.- Comandos y opciones

Muchos módems modernos tienen, como ya lo comentamos, la incorporación de realizaciones inteligentes como lo son la corrección de error, la compresión de datos y la conversión de velocidad dentro del mismo módem. La corrección del error en el módem es vía el estándar CCITT V.42. La compresión de datos puede ser tanto por el estándar CCITT V.42bis ó MNP Clase 5.

La corrección de error de su módem esta incorporado vía CCITT con el estándar V.42. V.42 actualmente utiliza dos protocolos de corrección de error, LAP-M y MNP Clase 3 & 4. La corrección de error MNP Clase 3 & 4 emerge como una industria estándar de una cantidad de fabricantes de módems. Ahora esta es de dominio público y ha sido implementado en docenas de marcas de módems que ofrecen corrección de error con una amplia instalación mundial en los cientos de miles de unidades. La corrección de error LAP-M es similar a MNP Clase 3 & 4, pero es la versión estándar de la CCITT con la cual la compresión de datos CCITT V.42bis esta basada.

La compresión de datos de los módems existe en los dos modos diferentes: V.42bis y MNP Clase 5, V.42bis es la técnica más reciente de compresión que requiere corrección de error usando LAP-M. V.42bis es una muy eficiente técnica de compresión que puede proveer una relación de compresión de hasta 4 a 1 dependiendo del tipo de archivo transmitido. La compresión MNP Clase 5 requiere la corrección de error usando MNP Clase 3 & 4. Este es un estándar más viejo y más establecido que ofrece compresión de datos en el rango de 2 a 1 en el cual también depende del tipo de dato.

La forma en que su módem trabaja usando esta alta realización es seleccionando un modo de operación, utilizando el modo de selección de comandos (Mode Select Command) V.42 (#Ln- el default es #L0). La selección #Ln determina como el módem opera con respecto tanto a las técnicas de corrección de error como con la transmisión de datos. El seleccionado de default le permite a un

par de módems el negociar cual modo de corrección de errores V.42 (LAP-M ó MNP) será usado en la transmisión. LAP-M puede ser preferido sobre MNP. Seleccionando la técnica de corrección de error puede también seleccionar automáticamente la técnica de compresión de datos, puesto que V.42bis requiere LAP-M y MNP Clase 5 requiere MNP 3 & 4.

La realización de conversión de velocidad le permite al módem operar a una velocidad sobre la línea telefónica y a otra velocidad en el puerto serial RS232C/V.24. Esto le permite a la computadora ó terminal comunicarse con el módem a una velocidad fija de hasta 57.6 kbps, mientras que el módem opera a varias velocidades de hasta 14.4 kbps y más recientemente a 28.8 kbps. Esta habilidad es vital si la compresión de datos esta activa (su terminal ó computadora debe presentar los datos a la línea telefónica a una alta velocidad a la cual el módem esta enviándolas a la línea telefónica.)

2.4.6.- Como V.42 detecta y corrige errores.

El método de corrección de errores ha estado con nosotros por largo tiempo, pero su incorporación dentro del hardware ó firmware de baja, mediana y alta velocidad asíncrona de marcado de los módems es relativamente nueva. Algunos de los más conocidos métodos de corrección de error que no incluyen XMODEM y Kermit (para software de transferencia de archivos asíncronos), X.PC (protocolo de software asíncrono de Tymnet), SDLC y HDLC, dos populares protocolos comunes asíncronos en el ambiente de mainframe IBM V.42, es funcionalmente similar a SDLC y HDLC, con algunas cosas extras.

La principal ventaja del hardware basado en el protocolo de corrección de error V.42 sobre los otros protocolos basados en software está en la "lanzada". La lanzada es el efecto que el uso del protocolo tiene en términos de la relación de datos. Por ejemplo, la transmisión V.42 usando un módem 9600 bps tiene un lanzado efectivo de alrededor de 9800 bps. El mismo módem usando software basado en X.PC podrá tener un lanzado efectivo de menos de 9600 bps. Otra forma de visualizar esto es que V.42 tiene una eficiencia de alrededor de 108%, mientras que X.PC tiene una eficiencia de alrededor del 91%.

La razón de esta ventaja de lanzado es que V.42 convierte caracteres de datos asíncronos a flujos de datos asíncronos, haciendo a esto un protocolo orientado a bit en lugar de orientado a carácter. Muchos caracteres asíncronos consisten de un bit de comienzo, ocho de datos y un bit de paro, para un total de diez bits por carácter. V.42 remueve el bit de inicio y de paro, lo cual resulta en una reducción de 20% en el total de bits y un 20% de mejoramiento en eficiencia. Sin embargo, el orden para que el protocolo funcione, V.42 añade alrededor del 12% en 8% más lo que necesita para mantener una relación de transmisión de 9600. Este colchón es muy benéfico durante periodos de actividad de corrección de error moderados (usualmente causados por líneas telefónicas ruidosas), puesto que el módem puede soportar niveles de transmisión moderados mientras este se mantiene a un lanzado de 9600 bps.

El protocolo de detección de error V.42 utiliza una técnica CRC (Cyclical Reduncancy Check) de 16-bit. Simplemente iniciado, un módem con V.42 envía datos codificados a otro módem con V.42 y el módem receptor está disponible para determinar donde hay cualquier error. Si existe este, el módem receptor le dice al módem enviador que reenvíe el dato erróneo hasta que este sea correcto.

Técnicamente hablando, cuando se usa V.42, el módem "enviador" utiliza una función polinomial para calcular el número de 16 bits el cual es una función de todos los datos enviados en un "mensaje" ó "bloque" particular, y luego envía esos 16 bits en el final del bloque. El "bloque" puede incluir hasta 64 caracteres. El módem V.42 "receptor", puesto que esta recibiendo el bloque, calcula su propia versión del número de 16 bits. Luego este compara el número con el número de 16 bit enviado con el bloque. Si los números son los mismos, el bloque esta libre de errores. Si son diferentes, un error ha ocurrido en algún lugar del bloque. Así es como los errores son detectados.

Una vez que el error es detectado, la corrección de error del módem receptor es activada. Supongamos que el enviador manda 8 bloques (el protocolo permite hasta 8 bloques a ser enviados antes de recibir un reconocimiento ó acuse de recibido), y el bloque 6 contiene un error. El módem receptor podrá enviar un mensaje de regreso hacia el envidor de que este tiene detectado un error en el bloque 6. El enviador, reorganiza que el último bloque correcto enviado antes del error fue el bloque 5, este señala para regresar al bloque siguiente del bloque 5, el cual es el bloque 6. En otras palabras, si el enviador tiene enviados 8 bloques y el receptor detecta un error en el bloque 6, el enviador regresa al bloque 6 y comienza la retransmisión de bloques desde este punto. Esto es algunas veces referido como el método de corrección de error "go-back-n", donde n es el primer bloque errado.

2.4.7.- Opciones de compresión de datos.

Existen módems equipados con compresión de datos V.42bis y MNP Clase 5. CCITT V.42bis es un estándar de compresión de datos internacional, el módem debe de estar en el modo de corrección de error antes de que pueda comprimir datos (corrección de error LAP-M para compresión de datos V.42 ó corrección de error MNP para compresión de datos MNP 5). Usando el comando #L, puede seleccionar cual corrección de error utilizara.

Cuando utilice un protocolo de transferencia de archivos para enviar y recibir datos, el tipo de protocolo usado puede tener gran efecto en la ganancia de velocidad debido a la compresión. En general, un protocolo el cual usa bloques de datos grandes (entre más largos mejor) puede transferir archivos más rápidamente. Un ejemplo de esto podrá ser YMODEM, el cual envía 100 caracteres por bloque. Este también puede ayudar para tener el puerto serial del módem receptor del módem apto para la velocidad más alta posible (57,600 bps), aún si el módem enviador es puesto a una velocidad baja.

Para lograr una relación de velocidad la cual sea más alta que la relación de baud del módem, es necesario utilizar la característica de conversión de velocidad del módem cambiando el Baud Adjust a off ($BAO) y operando el puerto serial a una velocidad más alta que la relación de baud del módem. Por ejemplo, si el módem esta conectado a 2400 baud ($MB2400), el puerto serial debe ser puesto a 4800,9600, 19200, 38400 ó 57600 bps ($SB57600).

El orden para hacer uso de la compresión de datos es que el módem necesita ser manejado en su capacidad total. En otras palabras, el *dato* necesita ser presentado en suficiente volumen (transferencia de archivos u operaciones de lotes) y la velocidad para obtener los beneficios máximos para la compresión. La característica del módem de compresión de velocidad debe de ser habilitada para utilizar el puerto a una velocidad más alta que la velocidad de conexión del módem. La compresión de datos trabaja localizando hileras repetidas de caracteres y repitiendo esas hileras

usando un código de palabras más corto. La técnica tiene la habilidad de aprender a actualizarse continuamente en su tabla de compresión durante la transmisión.

Cuando se opera un puerto serial a una velocidad más alta que la relación de baud del módem, algunos tipos de control de flujo deberán de ser usado ó los paquetes pueden ser perdidos.

La compresión de datos puede ser deshabilitada ó habilitada con los comandos &E14 y &E15. Para habilitarla , introduzca el comando AT&E15; para deshabilitar la compresión utilice AT&E14.

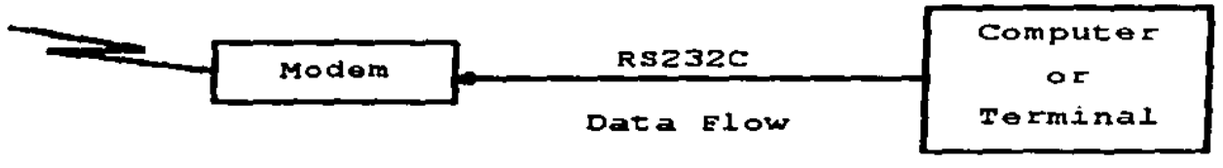
Nota: La condición para que la compresión de datos tome lugar, tanto el módem originador como el receptor en ambos extremos del enlace deben tener compresión y corrección de error habilitadas.

2.4.8.- Introducción al control de flujo.

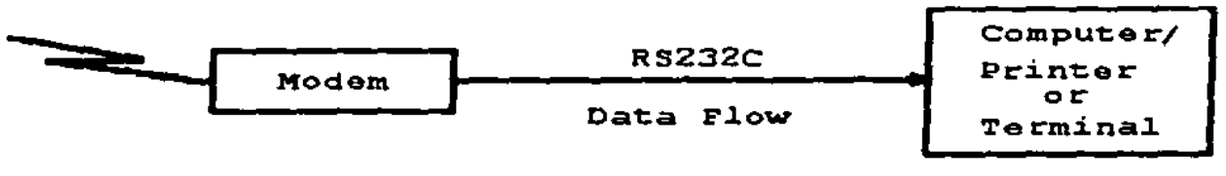
El control de flujo se refiere a la técnica usada por dispositivos de computadoras para detener y reiniciar el flujo de datos desde una hacia otra. El control de flujo es necesario para que un dispositivo no reciba más datos de los que puede manejar. En el caso de los módems, este es necesario para el control de flujo en ambas direcciones. Como se ilustra en la figura, el control de flujo para los datos desde su computadora a su módem es llamado Modem-Initiated Flow Control y el control de flujo de los datos pasando desde el módem a su computadora es llamado Computer/Terminal-Initiated Pacing.

Los módem soportan tanto controles de flujo ya sea por hardware ó por software de Modem Initiated Flow Control y en Computer/Terminal-Initiated soportan control de flujo de hardware, software y una versión especial usada por sistemas compatibles con Hewlett Packard llamado Pase ENQ/ACK. El módem le permite al hardware y software que envía, el pasar a través del mismo ó de otro dispositivo de enlace final para que su computadora ó terminal pueda controlar la actividad de inicio ó de paro a través de su módem. Este es llamado Xon/Xoff Pass-Through.

Modem-Initiated Flow Control



Computer/Terminal Initiated Pacing



Para ponerlo en términos más simples, el "Flow Control" es algo que el módem esta haciendo a la computadora, mientras que el "pacing" es algo que la computadora hace al módem. Cuando el módem esta operando en el modo V.42, este usa su memoria ó buffer para almacenar datos según como estos sean recibidos. Durante los periodos de error causados por retransmisión ó compresión demasiado baja, su buffer podrá llenarse. Para prevenir sobreflujo de buffer y la subsecuente pérdida de datos, el módem utiliza el control de flujo para señalar a la computadora conectada a su puerto RS232C/V.24 que el buffer del módem esta cerrado por estar lleno. Esto causa que la computadora detenga la transmisión de datos hasta que el módem este disponible para tener vacio el buffer lo suficiente como para aceptar más datos, para lo cual el módem señaliza a la computadora que puede restablecer la transmisión.

Alguno módem pueden darle a escoger métodos de control de flujo. Una de las opciones es "Xon/Xoff", el cual utiliza caracteres especiales en la transmisión de datos; otro es el "Hardware Flow Control", el cual utiliza la salida CTS en la interface RS232C/V.24 (Clear to Send-Pin 5). Muchas terminales y computadoras soportan uno ó ambos de estos métodos.

Control de flujo Xon/Xoff (&E5)

Xon/Xoff es el método más comúnmente utilizado para el control de flujo. Bajo este método, los caracteres de control conocidos como "Xon" y "Xoff" son insertados por el módem dentro de los datos para iniciar y detener el flujo de datos desde la computadora ó terminal a la cual el módem está conectado. Xoff, el cual es un Control-S, detiene el flujo de datos y Xon, el cual es un Control-Q, restaura este. Con consideraciones a datos binarios, el control de flujo Xon/Xoff, no es recomendado puesto que un carácter Xoff puede ser parte del dato y podrá disparar un Xoff hacia el módem ó al paquete de software el cual podrá detener el flujo de datos.

Control de flujo de Hardware (&E4)

Con el Control Flow Hardware, el módem utiliza su interface RS232C/V.24 para controlar el flujo de datos desde la computadora ó terminal a la cual esta conectado. La señal CTS (Clear to Send) ó Pin 5 de la interface RS232C/V.24 es dada de baja para detener el flujo de datos y posteriormente es dada de alta para reiniciarla.

2.4.9.- RS232C/V.24 Especificaciones de la interface.

La interface RS232C/V.24 de los módems ha sido diseñada para coincidir con las especificaciones eléctricas dadas por la EIZ (Electronic Industries Association) RS232C/CCITT (Consultative Committee for Telegraph and Telephone) del estándar V.24. Todas las señales generadas por el módem son de aproximadamente 10 volts cuando se miden a través de una carga de 3000 ohms ó mayor. Los circuitos receptores del módem pueden aceptar señales en el rango de 3 a 25 volts. Los voltajes son por lo tanto:

Negativo=voltaje más negativo que -3 volts con respecto a la señal de tierra.
Positivo=voltajes más positivos que +3 volts con respecto a la señal de tierra.

Información de la señal	Negativa	Positiva
Estado Binario	Uno	Cero
Condición de señal	Marca	Espacio
Función de control y tiempo	Off	On

La impedancia de salida de todos los circuitos del módem el cual acepta señales desde la terminal procesadora de datos ó equipo CPU tiene resistencia DC de 4.7 K.

La siguiente carta lista los pins de la interface RS232C/V.24 y circuitos presentes en el conector de la interface RS232C/V.24 del módem. Todos los otros pines del módem están sin usar.

Pin assignment	multi-tech designation	eia circuit	ccitt circuit	signal source*	circuit funtion
1	PG	———	101	———	Protective Ground
2	SD	BA	103	DTE	Trasmitted Data
3	RD	BB	104	DCE	Received Data
4	RTS	CA	105	DTE	Request to Send
5	CTS	CB	106	DCE	Clear to Send
6	DST	CC	107	DCE	Data Set Ready
7	SG	AB	102	———	Signal Ground
8	CD	CF	109	DCE	Data Carrier Detector
9	+V	+V	———	DCE	Test Voltage
12	HS	———	———	DCE	High Speed
15	TC	DB	114	DCE	Transmit Clock
17	RC	DD	115	DCE	Receive Clock
20	TR	CD	108/2	DTE	Data Terminal Ready
22	RI	CE	125	DCE	Ring Indicator
24	XTC	DA	113	DTE	External Trasmit Clock
24	OOS	CN	142	DTE	Terminal Busy

*DTE=Data Terminal Equipment (terminal ó computadora)
DCE=Data Communications Equipment (el módem)

2.5.- Características de otros medios de enlace físico.

2.5.1.- ISDN (Red Digital de Servicios Integrados).

Durante más de un siglo, el sistema telefónico ha presentado la infraestructura fundamental para la comunicación internacional. Este sistema que se diseño para transmisiones analógicas de voz, ha demostrado que es inadecuado para resolver las necesidades de comunicaciones modernas, como por ejemplo, la transmisión de datos fax y video. La demanda de usuarios, de estos y otros servicios, ha propiciado que se establezca un compromiso internacional para sustituir una parte considerable del sistema telefónico, en el mundo entero, por un sistema digital muy avanzado, durante la última parte del siglo XX. A este nuevo sistema se le conoce como ISDN (red digital de servicios integrados), y su principal objetivo consiste en la integración de servicios de voz, con los servicios que no utilizan voz.

Dado que ISDN es un rediseño del sistema telefónico, la coordinación internacional la esta llevando a cabo en el CCITT y en muchos grupos de investigación afiliados.

2.5.2.- Servicios de ISDN.

Dado que una de las razones primordiales de ISDN ha sido la demanda de nuevos servicio y el deseo de su integración con la telefonía de voz, resulta muy conveniente realizar el estudio de ISDN. Aunque el servicio principal seguirá siendo voz, este puede enriquecerse con algunos otros. Los servicio de transmisión de datos del ISDN permitirán a los usuarios conectar su terminal u ordenador a cualquier otro lado del mundo. Este tipo de comunicación es actualmente posible con dicho servicio.

2.5.3.- Arquitectura del Sistema ISDN.

La idea principal detrás de ISDN es la del bus digital de datos, que viene a ser un conducto conceptual entre el usuario y el proveedor de servicios portadores por el que fluyen los bits. Lo importante aquí es, que el flujo de bits fluye por el bus en ambas direcciones, independientemente de su procedencia, ya sea que se haya originado con un teléfono digital, una terminal digital, una máquina digital fax u otro tipo de dispositivo. El bus digital de bit soporta, generalmente, varios canales independientes mediante una multiplexión por división en el tiempo de flujo de bits. El formato exacto del flujo de bits y su multiplexión es una parte de las especificaciones de la interface.

2.5.4.- Red Digital Integrada.

Desde hace algunos años Teléfonos de México comenzó a desarrollar su Red de Servicios Integrados (RDI, podríamos decir que es algo muy similar a ISDN, como una red superpuesta) a la red telefónica tradicional, la cual ha tenido gran aceptación entre los usuarios. En la actualidad ya existen otras compañías como IUSANET (subsidiaria de IUSACELL), e INFRATEL (propiedad de BANAMEX), que ofrecen el servicio de renta de canales de comunicación básicos y primarios. La Red Digital Integrada (RDI) es una red totalmente digital y adicional a la red telefónica pública, apta para soportar todo tipo de señales de información, ofreciendo a los grandes usuarios de TELMEX un medio para dar solución a sus requerimientos de comunicación de voz y datos en altas velocidades con la mayor disponibilidad y calidad de servicio. La RDI utiliza diversas tecnologías para establecer sus medios de transmisión, como son radios digitales, fibra óptica e inclusive enlaces satélitales, todos ellos digitales y con una gran capacidad para transmisión de información. Aquí hay que establecer que Teléfonos de México ha realizado tendidos de fibra óptica por toda la República Mexicana, con lo que la tecnología principal que utiliza RDI es la transmisión de señales digitales vía fibra óptica, aunque existen todavía comunicaciones que se realizan vía radios digitales ó a través de satélite.

La RDI esta formada por dos redes de telecomunicaciones: la red terrestre y la red satélital. La red terrestre proporciona servicios comuntados digitales punto a punto y servicio de conducción de señales digitales, servicios tales como troncales digitales de 64 kbps para conmutador digital con conexión a 2.048 Mbps, líneas privadas para conducción de señales punto a punto ó multipuntos tipo E0 (64 kbps) y E1 (2.048 Mbps) y circuitos privados para conducción de señales nacionales e internacionales tipos E0 y E1. La red satélital ofrece la conducción de señales a base de circuitos dedicados (enlaces en renta para transmisión de voz y datos en canales de 64 kbps), ó bien, conducción de señal en acceso por demanda (enlaces en renta para transmisión de voz y datos en canales de 9.6 a 19.2 kbps, con asignación por demanda).

Esta red tiene una cobertura nacional a 29 de las ciudades más importantes y a cualquier punto dentro del Distrito Federal. El funcionamiento de esta red es transparente al usuario, ya que todas las

funciones de operación, mantenimiento y administración son llevadas a cabo por TELMEX, el cual se compromete a mantener la calidad de los enlaces, proporcionando el re-enrutamiento en caso de falla y operar la red para mantener una muy elevada confiabilidad en los enlaces por el hecho de tener todos los enlaces doblemente respaldados.

Existen algunas ventajas al contratar los servicios de la RDI, ya que se trata de disponer de una red de telecomunicaciones que sea altamente redituable financiera y físicamente para las empresas. Algunas de estas ventajas son la alta confiabilidad existente, disponibilidad inmediata, gran capacidad en el manejo de tráfico, amplia variedad de servicios, un monitoreo computarizado las 24 horas del día los 365 días del año y atención inmediata ante cualquier contingencia que se presente. Existen algunos requisitos que deben de cumplir las compañías que desean rentar canales de RDI, como son el número mínimo de canales a rentar y su capacidad, así como proporcionar un local con características específicas para la instalación del equipo de TELMEX.

2.5.5.- Enlaces Satélitales.

Un sistema de comunicaciones satélitales es realmente un sistema de microondas con un repetidor en el espacio exterior. Esencialmente el satélite recibe una señal de la Tierra, la amplifica y la retransmite hacia una ó más estaciones terrenas. Un sistema satélital consiste en un transponder, una estación terrena para controlar sus operaciones y estaciones en tierra de usuarios con los equipos necesarios para aprovechar los recursos del sistema satélital. La mayoría de los satélites geosíncronos se encuentran ubicados a 36,000 km por encima del Ecuador y aún cuando su primer uso fue la transmisión de llamadas de larga distancia y señales de televisor a regiones ó zonas continentales, se han comenzado a emplear con más frecuencia para enlaces de redes privadas de comunicación de datos.

Este tipo de enlaces generalmente se utilizan para enlaces punto a multipunto, ya que el satélite retransmite la información que recibe a toda una área geográfica del país, lo que se denomina huella, siendo esta, por lo general, una extensión amplia, pero en nuestro caso, lo que se utiliza es un enlace punto a punto. En México la Secretaría de Comunicaciones y Transportes es la entidad encargada de la administración y mantenimiento de los satélites domésticos del país, que actualmente son el Morelos II y el Solidaridad. Ante esta Secretaría hay que realizar los trámites para obtener la renta de frecuencia ó ancho de banda necesario para transmisión de todo tipo de información.

La UNAM cuenta con una amplia experiencia en este tipo de enlaces dado que existen 8 enlaces satélitales propios de 32, 64 y 128 kbps de voz y datos que comunican a centros de extensión de la UNAM en diversas partes de la República. Se utilizan enlaces vía satélite para la comunicación entre diferentes campus en regiones alejadas del país, cuya localización geográfica no permite otro tipo de comunicación. Tal es el caso del enlace con la Estación "Puerto Morelos" del Instituto de Ciencias del Mar y Limnología en el estado de Quintana Roo, del enlace con el Observatorio Astronómico Nacional a cargo del Instituto de Astronomía en la Sierra de San Pedro Mártir en Baja California y del enlace a la estación "Tetitlán" del Servicio Sismológico Nacional a cargo del Instituto de Geofísica en la Sierra de Guerrero. Todos los enlaces son de acceso múltiple por división de frecuencia (FDMA) e utilizan un Ruteador, que en este caso pueden ser Traslan, HP ó Cisco, para empaquetar la señal Ethernet en los canales pequeños antes mencionados. Los canales de voz se digitalizan y comprimen en 8 kbps a fin de integrarse al canal mediante multicanalización. En Ciudad Universitaria existen dos antenas parabólicas orientadas al Satélite Morelos II, con objeto de que en emergencias, una pueda respaldar a la otra. La primera y la más antigua se encuentra en el Instituto de Astronomía y la segunda en la Dirección General de Servicios de Cómputo Académico.

También se tienen enlaces satélitales no propios de la UNAM, establecidos con Instituciones públicas del país, tales como universidades e institutos. En estos enlaces la UNAM proporciona sus instalaciones existentes y la institución todo lo que haga falta. Actualmente se tienen enlaces con la Universidad Autónoma de Chiapas, la Universidad Autónoma de Ciudad Juárez, la Universidad de Quintana Roo y el Instituto Mexicano del Transporte en Querétaro. A continuación se mencionan algunos de los enlaces vía satélite que parten de la UNAM:

Observatorio de San Pedro Mártir, Baja California Norte, 64 kbps 1 línea telefónica
Laboratorio de Investigación de Astronomía y Física en Ensenada, Baja California Norte. 128kbps 2 líneas
Enlace con la National Science Foundation Network en Boulder Colorado, 128 kbps
Estación marítima en Mazatlan Sinaloa 64 kbps 2 líneas
Laboratorio de energía solar en Temixco, Morelos 64 kbps 2 líneas
Estación concertadora de sismógrafos en Tetitlán, Costa de Guerrero. 19 kbps
Estación marina en Puerto Morelos, Quintana Roo. 32 kbps 2 líneas
Ciudad científica en Cuernavaca, Morelos 128 kbps
Estación de trabajo de Salamanca, Guanajuato 19 kbps
Instituto de Geología, Hermosillo Sonora, 64 kbps 2 líneas
Universidad Autónoma de Ciudad Juárez 64 kbps
Universidad Autónoma de Quintana Roo 128 kbps
Instituto Mexicano del Transporte, Querétaro, 128 kbps

2.5.6.- Conectividad Internet en México.

En México la conectividad a Internet apareció primero en las Universidades y recientemente han aparecido proveedores comerciales de acceso a Internet. La primer Institución conectada fue el ITESM y luego le siguió la UNAM. El ITESM adquiere una conectividad vía red digital integrada al nodo más cercano a la NSFnet en Texas, en E.U. La UNAM sale vía satélite a ENCAR, un nodo de la NFSnet en Colorado.

Posteriormente varias Universidades públicas y el IPN obtienen conectividad a Internet, la mayoría vía el ITESM de Monterrey. Se crea MEXnet como un organismo que regularía Internet en México desde el punto de vista de los académicos. La SCT nombra al CONACyT como órgano regidor de Internet en México, ya que el coordina los esfuerzos de la red tecnológica nacional (casi toda vía satélite).

Al final, no existe una organización muy fuerte y la UNAM adquiere independencia al obtener un enlace RDI a Texas.

Con la desregulación norteamericana en el ramo de las telecomunicaciones, ahora es posible que cualquiera contrate una alimentación a Internet con un proveedor norteamericano ó subsidiario para traer a México (vía satélite ó red digital integrada de Telmex) una entrada que a su vez podría re-vender. De esta forma se han instalado en México varios proveedores independientes de Internet. Otros proveedores comerciales han surgido de concesiones otorgadas por la UNAM, el ITESM y el consorcio INFOTEC (del CONACyT).

2.5.7.- Ancho de banda .

La diferencia básica entre los diferentes tipos de conexión disponibles es el ancho de banda requerido, es decir, la capacidad del enlace de comunicaciones para transmitir una cantidad de información por una unidad de tiempo. ¿Qué tanta información obtendré en determinado tiempo?. Si mis aplicaciones a usar demandan mayores anchos de banda (como podrán ser transferencia de imágenes y/o sonido), ¿será necesario un ancho de banda más grande?. Recordamos que los costos más importantes en la implementación y operación de una conectividad son los gastos de telecomunicaciones.

Las nuevas aplicaciones multimedia, como el sistema de WWW requieren de anchos de banda cada día mayores; dado que transfieren imágenes, sonido ó videoclip, requieren de un ancho de banda varias veces mayor al necesario para transferir una archivo, un correo ó un documento de texto. Sin embargo hay que tener en cuenta que de nada sirve obtener un enlace de gran ancho de banda, si el proveedor del acceso a Internet no tiene una conexión propia con ancho de banda igual ó mayor: si ese fuera su caso, se convertiría en un cuello de botella, además si se cumpliera la premisa anterior, si el proveedor de Internet tiene problemas de comunicaciones ó tiene demasiado tráfico (tiene demasiados clientes) el ancho de banda efectivo puede estar muy disminuido.

2.5.8.- Proyección del uso de la conexión.

En primera instancia sería bueno saber que tanto será el acceso y los servicios que se requieren, por lo general esto no se puede saber con exactitud, menos aún cuando la persona desconoce los beneficios del acceso a Internet, por lo que aquí haremos una revisión de los productos ofrecidos para la gente que desconoce su utilización, puede servir también para la gente que apenas esta en la decisión de escoger un software, para checar sus necesidades y tomar la decisión que incluya sus requerimientos.

* Uso de la conexión a Internet.

    Correo electrónico. Qué tanta cantidad de correos puede recibir.
    Conferencias ó Foros públicos.
    Proyectos en colaboración.
    Recursos de información.
    Servicios de información en línea.
    Mercadotecnia y ventas.
    Solo como usuario.
    Solo como proveedor de servicios.

* Capacidad presupuestal.
* Utilización de aplicaciones Multimedia en la Internet.
* Cantidad de información a accesar. Tanto para obtener como para proveer a la Internet.
* El proveedor de Internet ofrece esto a un precio razonable.

2.5.9.- Enlaces temporales.

Existen dos tipos de enlaces a Internet: Los temporales y los dedicados. Los temporales, que son los que nos atañen, son económicos, pero de poco ancho de banda, mientras que los dedicados suelen ser más caros, aunque de un ancho de banda mayor. Además si se piensa proveer documentos ó publicidad en linea, es necesario optar por una conexión permanente y dedicada, aunque aqui convendría valorar la posibilidad de unirse a un consorcio que por una renta ponga la ayuda en uno de sus equipos, para que este disponible todo el tiempo. De esta forma los clientes siempre pueden accesar la información.

2.5.10.- Enlaces conmutados por emulación.

La forma más simple de conectarse a Internet, es a través de un módem que nos permite acceder a un servidor público que tenga acceso a Internet. Muchos de los servicios comerciales más populares funcionan de esta manera (CompuServe, Spin, Internet de México). En este caso, nuestra computadora local deberá utilizar un software de emulación de terminal para poder ejecutar comandos en la máquina remota. El problema en este caso es que nuestra máquina local no tiene acceso directo a Internet y varias aplicaciones, como Mosaic ó Netscape, los navegadores ó visores de información más conocidos; estos no pueden operar si la computadora local no corre TCP/IP. Solo las interfaces de texto de Internet pueden utilizarse (gopher, wais), normalmente en este caso, la transferencia de archivos debe hacerse en dos pasos (FTP al servidor remoto y otro protocolo de transferencia para los archivos a la máquina local, como kermit, zmodem, ymodem, etc.).

Esta deficiencia en el servicio puede ser compensada por el proveedor por medio de una interface gráfica propietaria, esto es una forma de ver la información desarrollada por el propio proveedor, la cual nos permite de una forma transparente para nosotros, acceder a servicios similares. La conexión en todo caso es temporal, lo que implica que los gastos de telecomunicaciones son reducidos. Normalmente cuando uno adquiere estos servicios, conjuntamente se le asigna un buzón de correo electrónico.

2.5.11.- Enlaces conmutados SLIP/PPP.

Para poder acceder a los servicios de WWW y otras herramientas de Internet localmente, en la actualidad es posible obtener acceso via módem a un servidor conectado a Internet, utilizando un protocolo especializado en la transferencia de paquetes TCP/IP por la línea telefónica. SLIP (Serial Line Internet protocol) y PPP(point-to-point protocol) son protocolos que permiten esto, siendo el primero el más popular y antiguo.

En este caso, nuestra máquina local se encuentra virtualmente conectada a Internet mientras dura la conexión. Muchos de los servicios tradicionales de información están optando por migrar a este servicio para proporcionar a sus clientes acceso completo a Internet.

El único inconveniente es que se debe utilizar una velocidad rápida de transferencia de datos (>9600 bps) para que el servicio sea práctico y la comunicación no sea extremadamente lenta. Esto es

posible hacerlo desde algunos puntos de la Ciudad de México, aunque va en aumento conforme la red telefónica local es convertida de analógica a digital.

Estos enlaces SLIP puede convertirse de temporales a permanentes si dedica un módem en el servidor del proveedor para que reciba nuestra señal en cualquier momento. Sin embargo es más costo-efectivo contratar en este caso un enlace digital.

2.5.12.- Emuladores SLIP.

Han aparecido en el mercado varios productos que permiten enviar paquetes TCP/IP a través de sesiones conmutadas por emulación, sin instalar el SLIP, lo cual puede ser a veces problemático. Estos programas emulan el SLIP, de manera no tan eficiente, por lo que la comunicación es un poco más lenta que el caso anterior.

2.5.13.- Equipos requeridos e instalación.

El equipo requerido para establecer este tipo de enlace es tan solo una computadora, un módem (rápido) y software de comunicaciones que usualmente suministra el proveedor.

La instalación requiere lo siguiente:

* Dirección TCP/IP (suministrada por el proveedor).
* Nombre del Dominio (normalmente el del proveedor).
* Mascara de sub-red (también proporcionada por el proveedor).
* Software de TCP/IP.
* Software de SLIP.

2.5.14.- Costos.

Para la cuestión económica puede tomarse como base las siguientes caracteristicas con los diversos proveedores del acceso a Internet:

* Instalación.
* Servicios proporcionados.
* Cuota mensual.
* Horas incluidas.
* Costo de horas adicionales.
* Renta de teléfono (constante para una cantidad de tiempo).

2.5.15.- Puntos a evaluar en el proveedor.

* ¿Tiene el equipo necesario? ¿Puedo manejar aplicaciones Multimedia?.
* ¿Tiene la asistencia de menú ó interface para facilitar el acceso?.
* ¿Con que frecuencia el proveedor tiene todos sus módem ocupados?.
* ¿Cual es su política para agregar más módems?.
* ¿Cuanto espacio en disco obtiene?.
* ¿Cuánto buzones obtiene? ¿Como se pagan los mensajes recibidos y/o enviados?.
* ¿Qué tan congestionado esta el servidor del proveedor? ¿La respuesta es rápida a los comandos?.
* ¿Es un número local para conectarse al servidor ó una larga distancia?.
* ¿Cómo se manejan las actualizaciones del software que me proporcionan?.
* ¿Necesito aprender más sobre TCP/IP?.
* ¿El proveedor suministra direcciones estáticas ó dinámicas?.

2.5.16.- Enlaces dedicados.

Los enlaces dedicados es la solución para una conectividad rápida y permanente a Internet. Normalmente se establecen a través de un enlace telefónico digital punto-a-punto, denominado Red Digital Integrada (RDI). También es posible utilizar otros servicios de telecomunicaciones X.25 y la transmisión vía satélite, siendo estos últimos más económicos por el momento aunque poco eficientes. Además, la mayoría de los proveedores de Internet solo aceptan entradas vía RDI, por lo que todas las demás partes del enlace de comunicaciones se hacen con RDI asegurando un servicio más adecuado. Los enlaces se venden en diferentes anchos de banda:

Tipo	Velocidad
Analógico	9.6, 14.4, 19.2 kbps
Digital (RDI)	64 kbps (T0), 2Mbps (T1), 45 Mbps (T3)
Frame Relay	56 kbps, 128, 256, 512 kbps
SMDS	64 kbps, 2Mbps, 4Mbps, 10Mbps

El costo aumenta considerablemente con el ancho de banda, de tal forma que los enlaces T3 son inalcanzables. Estos enlaces son contratados al Telmex y son como llaves abiertas de agua, cuesta lo mismo que se use ó no se use. Es posible que nuestro proveedor se encargue de arreglar estos asuntos por nosotros, aunque la renta mensual de los gastos de telecomunicaciones (por el momento, lo más costoso de la conexión a Internet) se paga a Telmex.

Apéndice B.

HDLC Asincrono.

Este apéndice es un sumario de las modificaciones al ISO 3309-1979 propuesto en ISO 3309:1984/PDAD1. Estas modificaciones permiten que HDLC sea usado con enlaces asincronos de 8 bits.

Consideraciones de la Transmisión.

Cada octeto es delimitado por un elemento start y uno stop.

Secuencia de Bandera.

La secuencia de bandera es un octeto único e idéntico tanto en el principio como en el final del frame. La secuencia de bandera consiste de la secuencia binaria 01111110 (0x7e en hexadecimal).

Transparencia.

En enlaces asincronos, el procedimiento de un carácter de relleno (stuffing) es utilizado. El octeto escape de control es definido como el binario 01111101 (0x7d en hexadecimal) cuando la posición del bit es numerada 87654321 (no 76543210, Tenga Cuidado).

Después de la computación del FCS, el transmisor examina el frame entrante de entre las dos secuencias de bandera. Cada secuencia de bandera, octeto de escape de control y octeto con valores menores que el hexadecimal 0x20 es reemplazado por dos secuencias de caracteres consistiendo del octeto de control de escape y el octeto original complementado con 6 bits (p.ej., or exclusiva con 0x20 en hexadecimal).

Previo a la computación del FCS, el receptor examina el frame entrante entre las dos secuencias de banderas. Para cada octeto de escape de control, ese octeto es removido y 6 bits del siguiente octeto son complementados. Un octeto de escape de control inmediatamente precedido de la secuencia de bandera que lo cierra indica un frame invalido.

Nota: La inclusión de todos los octetos menores que el hexadecimal 0x20 permite todos los caracteres de control ASCII (10) excluyendo DEL (Delete) para ser transparentemente comunicado a través de casi todos los equipos de comunicación de datos conocidos.

Un pequeño ejemplo puede ser más claro. Un paquete de datos es transmitido en un enlace como sigue:

0x7e es codificado como 0x7d, 0x5e.
0x7d es codificado como 0x7d, 0x5d.
0x01 es codificado como 0x7d, 0x21.

Abortando una transmisión.

En enlaces asincronos, los frames pueden ser abortados transmitiendo un bit de stop "0" donde un bit "1" es esperado (error del frame) ó por la transmisión de un octeto de escape de control seguido inmediatamente por una secuencia de bandera de terminación.

Tiempo de llenado del Inter-frame.

En un enlace asincrono, el tiempo de llenado de inter-octetos e inter-frame deberá ser acompletado por la transmisión continua del bit "1" (marca de estado de retención).

Nota: En un enlace asincrono, el tiempo de llenado del inter-frame visualizado como un tiempo de llenado de un inter-octeto extendido. Haciéndolo asi puede salvar un octeto para cada frame, decrementando el retardo e incrementando el ancho de banda. Esto es posible puesto que una secuencia de bandera puede servir tanto como un frame que cierra y como un frame que comienza. Después teniendo recibido cualquier frame, un receptor desocupado puede siempre estar en un estado de comienzo de frame.

Transmisores robustos deberán evitar utilizar este truco, puesto que el precio por decrementar el retardo es decrementar la confiabilidad. Enlaces ruidosos pueden causar que el receptor reciba caracteres garabatos e interpretar estos como un parte de un frame llegando. Si el transmisor no transmite una nueva secuencia de bandera de apertura antes de enviar el siguiente frame, entonces este frame podrá ser añadido a los caracteres ruidosos causando un frame invalido (con alta confiabilidad). Los transmisores deberán evitar esto transmitiendo una secuencia de bandera de apertura cuando crea que un "tiempo apreciable" ha pasado desde la secuencia de bandera que cerro la previa. Es sugerido para que las implementaciones puedan tener el mejor resultado enviando siempre una secuencia de bandera si un frame nuevo no es back-to-back con el último. El valor máximo de un "tiempo apreciable" no es lo suficientemente grande que la relación de tecleado de un tecladista lento promedio, digamos 1 segundo.

Implementación del Frame Check Sequence (FCS) rápido.

Método de computación del FCS.

El siguiente código provee una tabla vista como una computadora para el calculo de la secuencia de chequeo del frame tal como el dato arribar a la interface. La tabla es creada por el código en la sección 2.

```
/*
   * FCS lookup table as calculated by the table generator in section 2.
   */
  static unsigned short fcstab[256] = {
      0x0000, 0x1189, 0x2312, 0x329b, 0x4624, 0x57ad, 0x6536, 0x74bf,
      0x8c48, 0x9dc1, 0xaf5a, 0xbed3, 0xca6c, 0xdbe5, 0xe97e, 0xf8f7,
      0x1081, 0x0108, 0x3393, 0x221a, 0x56a5, 0x472c, 0x75b7, 0x643e,
      0x9cc9, 0x8d40, 0xbfdb, 0xae52, 0xdaed, 0xcb64, 0xf9ff, 0xe876,
      0x2102, 0x308b, 0x0210, 0x1399, 0x6726, 0x76af, 0x4434, 0x55bd,
      0xad4a, 0xbcc3, 0x8e58, 0x9fd1, 0xeb6e, 0xfae7, 0xc87c, 0xd9f5,
      0x3183, 0x200a, 0x1291, 0x0318, 0x77a7, 0x662e, 0x54b5, 0x453c,
```

```
    0xbdcb, 0xac42, 0x9cd9, 0x8f50, 0xfbcf, 0xea66, 0xd8fd, 0xc974,
    0x4204, 0x538d, 0x6116, 0x709f, 0x0420, 0x15a9, 0x2732, 0x36bb,
    0xce4c, 0xdfc5, 0xed5e, 0xfcd7, 0x8868, 0x99e1, 0xab7a, 0xbaf3,
    0x5285, 0x430c, 0x7197, 0x601e, 0x14a1, 0x0528, 0x37b3, 0x263a,
    0xdecd, 0xcf44, 0xfddf, 0xec56, 0x98e9, 0x8960, 0xbbfb, 0xaa72,
    0x6306, 0x728f, 0x4014, 0x519d, 0x2522, 0x34ab, 0x0630, 0x17b9,
    0xef4e, 0xfec7, 0xcc5c, 0xddd5, 0xa96a, 0xb8e3, 0x8a78, 0x9bf1,
    0x7387, 0x620e, 0x5095, 0x411c, 0x35a3, 0x242a, 0x16b1, 0x0738,
    0xffcf, 0xee46, 0xdcdd, 0xcd54, 0xb9eb, 0xa862, 0x9af9, 0x8b70,
    0x8408, 0x9581, 0xa71a, 0xb693, 0xc22c, 0xd3a5, 0xe13e, 0xf0b7,
    0x0840, 0x19c9, 0x2b52, 0x3adb, 0x4e64, 0x5fed, 0x6d76, 0x7cff,
    0x9489, 0x8500, 0xb79b, 0xa612, 0xd2ad, 0xc324, 0xf1bf, 0xe036,
    0x18c1, 0x0948, 0x3bd3, 0x2a5a, 0x5ee5, 0x4f6c, 0x7df7, 0x6c7e,
    0xa50a, 0xb483, 0x8618, 0x9791, 0xe32e, 0xf2a7, 0xc03c, 0xd1b5,
    0x2942, 0x38cb, 0x0a50, 0x1bd9, 0x6f66, 0x7eef, 0x4c74, 0x5dfd,
    0xb58b, 0xa402, 0x9699, 0x8710, 0xf3af, 0xe226, 0xd0bd, 0xc134,
    0x39c3, 0x284a, 0x1ad1, 0x0b58, 0x7fe7, 0x6e6e, 0x5cf5, 0x4d7c,
    0xc60c, 0xd785, 0xe51e, 0xf497, 0x8028, 0x91a1, 0xa33a, 0xb2b3,
    0x4a44, 0x5bcd, 0x6956, 0x78df, 0x0c60, 0x1de9, 0x2f72, 0x3efb,
    0xd68d, 0xc704, 0xf59f, 0xe416, 0x90a9, 0x8120, 0xb3bb, 0xa232,
    0x5ac5, 0x4b4c, 0x79d7, 0x685e, 0x1ce1, 0x0d68, 0x3ff3, 0x2e7a,
    0xe70e, 0xf687, 0xc41c, 0xd595, 0xa12a, 0xb0a3, 0x8238, 0x93b1,
    0x6b46, 0x7acf, 0x4854, 0x59dd, 0x2d62, 0x3ceb, 0x0e70, 0x1ff9,
    0xf78f, 0xe606, 0xd49d, 0xc514, 0xb1ab, 0xa022, 0x92b9, 0x8330,
    0x7bc7, 0x6a4e, 0x58d5, 0x495c, 0x3de3, 0x2c6a, 0x1ef1, 0x0f78
};

#define PPPINITFCS      0xffff  /* Initial FCS value */
#define PPPGOODFCS      0xf0b8  /* Good final FCS value */

/*
 * Calculate a new fcs given the current fcs and the new data.
 */
unsigned short pppfcs(fcs, cp, len)
    register unsigned short fcs;
    register unsigned char *cp;
    register int len;
{
    while (len--)
        fcs = (fcs >> 8) ^ fcstab[(fcs ^ *cp++) & 0xff];

    return (fcs);
}
```

Generador de tabla rápida FCS.

El siguiente código crea una mirada a la tabla usada para calcular el FCS.

```
/*
 * Generate a FCS table for the HDLC FCS.
 *
 * Drew D. Perkins at Carnegie Mellon University.
 *
 * Code liberally borrowed from Mohsen Banan and D. Hugh Redelmeier.
 */

/*
 * The HDLC polynomial: x**0 + x**5 + x**12 + x**16 (0x8408).
 */
#define P       0x8408


main()
{
   register unsigned int b, v;
   register int i;

   printf("static unsigned short fcstab[256] = {");
   for (b = 0; ; ) {
      if (b % 8 == 0)

                  printf("0);

      v = b;
      for (i = 8; i--; )
         v = v & 1 ? (v >> 1) ^ P : v >> 1;

      printf("0x%04x", v & 0xFFFF);

      if (++b == 256)
         break;
      printf(",");
   }
  printf("0;0);
}
```

Drivers de SLIP

Las siguientes funciones en lenguaje C envian y reciben paquetes SLIP. Estas dependen de dos funciones, send_char() y recv_char(), las cuales envian y reciben un único carácter sobre líneas seriales.

```
/* SLIP special character codes
   */
  #define END             0300    /* indicates end of packet */
  #define ESC             0333    /* indicates byte stuffing */
  #define ESC_END         0334    /* ESC ESC_END means END data byte */
  #define ESC_ESC         0335    /* ESC ESC_ESC means ESC data byte */

  /* SEND_PACKET: sends a packet of length "len", starting at
   * location "p".
   */
  void send_packet(p, len)
        char *p;
        int len; {

    /* send an initial END character to flush out any data that may
     * have accumulated in the receiver due to line noise
     */
      send_char(END);

    /* for each byte in the packet, send the appropriate character
     * sequence
     */
        while(len--) {
              switch(*p) {
              /* if it's the same code as an END character, we send a
               * special two character code so as not to make the
               * receiver think we sent an END
               */
              case END:
                    send_char(ESC);
                    send_char(ESC_END);
                    break;

              /* if it's the same code as an ESC character,
               * we send a special two character code so as not
               * to make the receiver think we sent an ESC
               */
              case ESC:
                    send_char(ESC);
                    send_char(ESC_ESC);
                    break;
             /* otherwise, we just send the character
              */
```

```
            default:
                  send_char(*p);
                  }

            p++;
            }

      /* tell the receiver that we're done sending the packet
       */
      send_char(END);
      }

/* RECV_PACKET: receives a packet into the buffer located at "p".
 *      If more than len bytes are received, the packet will
 *      be truncated.
 *      Returns the number of bytes stored in the buffer.
 */
int recv_packet(p, len)
      char *p;
      int len; {
      char c;
      int received = 0;

      /* sit in a loop reading bytes until we put together
       * a whole packet.
       * Make sure not to copy them into the packet if we
       * run out of room.
       */
      while(1) {
            /* get a character to process
             */
            c = recv_char();

            /* handle bytestuffing if necessary
             */
            switch(c) {

            /* if it's an END character then we're done with
             * the packet
             */
            case END:
                  /* a minor optimization: if there is no
                   * data in the packet, ignore it. This is
                   * meant to avoid bothering IP with all
                   * the empty packets generated by the
                   * duplicate END characters which are in
                  * turn sent to try to detect line noise.
                   */
                  if(received)
```

```
                return received;
        else
                break;

    /* if it's the same code as an ESC character, wait
     * and get another character and then figure out
     * what to store in the packet based on that.
     */
    case ESC:
        c = recv_char();

        /* if "c" is not one of these two, then we
         * have a protocol violation.  The best bet
         * seems to be to leave the byte alone and
         * just stuff it into the packet
         */
        switch(c) {
        case ESC_END:
                c = END;
                break;
        case ESC_ESC:
                c = ESC;
                break;
                }

    /* here we fall into the default handler and let
     * it store the character for us
     */
    default:
        if(received < len)
                p[received++] = c;
        }
    }
}
```

Capítulo 3 EL ACCESO A INTERNET.

3.1.1.- ¿Qué es un proveedor de servicios de Internet (Internet Service Provider ISP)?

Un Proveedor de servicios de Internet (ISP) es una compañía que conecta a miembros del público en general a la Internet. Estas se pueden distinguir por ser de servicios de información, tales como CompuServe ó America Online, por sus énfasis en las herramientas de la Internet tales como USENET News, Gopher, WWW, etc. Tradicionalmente los sistemas de bulletin board (BBSs) normalmente no tienen acceso directo hacia la Internet y frecuentemente son limitados solamente a USENET news y correo sin ningún otro servicio de Internet. En general se pueden clasificar a los proveedores del servicio en la siguientes categorías:

* Cuenta de shell Unix.- A los usuarios les es dado el infame prompt "%" ó alguna otra variación como entrada al sistema. Algunas veces un menú simple les es también proveído. Pero en general la base del sistema es Unix y normalmente el usuario no puede tomar una total ventaja de los servicio ofrecidos sin conocer al menos unos pocos de los comandos de Unix. El uso del navegador de WWW Lynx como un menú se esta convirtiendo más y más en algo común.

* Proveyendo acceso SLIP, CSLIP ó PPP al personal.- Esto les permite conectarse como un host de Internet, usando su propio software. Macintosh y Microsoft Windows, en particular, devotamente aprovechan estas características. Esta es la forma más común de obtener gráficas directamente a través de un World Wide Web, pero también esta tiene algunas desventajas, como se verá más adelante.

* Proveyendo acceso al personal con una BBS personalizado con realizaciones de Internet especializadas (newsreaders, etc.).

Mucha gente a intentado poner en conjunto alguna forma de acceso a Internet bajo un software comercial ó shareware de DOS ó Windows BBS. Muchos de los desarrolladores han tenido éxitos notables en esta tarea. En particular, la falta de un "newsreaders" ó interface para leer mensajes de alta calidad para USENET hace al sistema increíblemente confuso para utilizarse. La llegada de la lectura en línea del correo puede ayudar a esto. Desafortunadamente, muchos de los lectores en línea intentan mutilar las malas cabezas (de los mensajes de correo) y son una fuente principal de molestia (y ocasionalmente de diversión) de una cantidad de lectores de USENET. El formato QWK es particularmente una mala víctima de este practica; este pone todas las líneas en mayúscula y limita estas a 20 caracteres, lo cual es considerado un formato extraordinariamente muy pobre por los lectores de USENET. Los BBS de DOS y los basados en Unix han creado un formato diferente de lectura en línea el cual se piensa que puede trabajar mucho mejor para aplicaciones USENET, desafortunadamente, todavía no se ve mucho en operación y algunos usuarios consideran que este sistema es confuso y tienen dificultad para navegar.

Note que los programa de lectura fuera de línea, aún aquellos que trabajan con USENET, no pueden ayudarlo cuando utiliza un WWW ó Gopher, los cuales requieren accesar al sitio en tiempo real.

TBBS, un programa basado en DOS, tiene un sistema llamado IPAD, el cual es aparentemente un 486/66 corriendo algún software especializado e incluyendo una interface de ruteo interna. Esto es completamente caro, pero podrá darle al sistema operativo TBBS una extensión cuando este tenga una conexión de Internet administrada.

Los principales BBS actualmente tienen un modulo de Internet con varias limitaciones, por ejemplo, el procesado del correo y las lecturas aún deben de ser realizadas via UUCP. Basado en las grabaciones de la respectiva del paquete, se asume que los paquetes de TBBS podian ser mejores que el anterior. Sin embargo, se piensa que probablemente los mejores paquetes desarrollados para usuarios de Internet deben de ser desarrollados por sistemas de Internet en lugar de los existentes BBS comerciales.

3.1.2.- Todo acerca de los Web Browsers.

Tiene que tener una cuenta SLIP/PPP para habilitar el uso de cualquier "browser" o visor de Web gráfico. Existe una ironia real sobre Mosaic y Netscape: Ellos atraen a los usuarios, porque la gente quiere ver gráficas en el Web. Pero también esto aleja a los usuarios, puesto que muchos sitios utilizan gráficas grandes y mapas de imágenes que se tardan una eternidad para cargarse. En relación a esto, alrededor del 40 % de los browser gráficos de usuarios actualmente corren con la opción de imagen desactivada, de acuerdo a análisis de algunos de los archivos de log. Puede pensarse en Mosaic y Netscape como una herramienta que esta a la cabeza para sus tiempos, puesto que el uso más popular tiene el veneno escondido de la lentitud dentro de ellos. Por esta razón, mucha gente esta viendo el enviarlos a ISDN, el cual promete proveer al usuario un enlace de 56k ó conexiones más altas. Sin embargo, esto no es la panacea, el enlace entre las máquinas es también pesadamente sobrecargado, y a menos de que esto sea curado, no podrá ISDN subir más la velocidad.

Otro problema con Mosaic es que este requiere de librerias de Mosaic para construir. Esto significa que tiene que escoger entre levantar una forma binaria ó pagar para una licencia Motif. Muchas personan optan por un paquete llamado Chimera, que trabaja mucho como Mosaic.

Lynx, un cliente WWW orientado a VT-100, trabaja muy bien si no necesita absolutamente gráficos. Las gráficas pueden ser automáticamente bajadas al sistema del cliente si desea. Esto es lo que hace que los usuarios del Web deshabiliten las gráficas puesto que estas vienen demasiado lentas en una conexión tipica de SLIP de 14.4kbps.

Netscape resuelve muchos de los problemas de Mosaic y tiene pocos problemas nuevos. Netscape mantiene una ventaja que es cargar toda lo de las imágenes y datos asociados con un URL concurrentemente. En base a esto, puede leer el texto como este va llegando y ver parte de la gráfica, aún si no todo ha llegado aún. Esto es un increible ahorro de tiempo y hace que Netscape sea el más claro browser que se escoger desde el punto de vista de consumidor.

Netscape tiene algunos pocos problemas irritantes aún. Si no se tiene comprado su multimillonario sistema de servidor, este le manda a los usuarios un mensaje de que estos no están utilizando un esquema de transmisión segura de Netscape cada vez que estos intenten transmitir algo en una forma.

SlipKnot es un browser gráfico corriendo bajo windows que esta basado en el uso de Lynx desde el comando de línea Unix, este es una solución excepcionalmente hábil que podrá incrementarse en popularidad. Es mucho más fácil de instalar que el genuino SLIP, y no es muy lento.

3.1.3.- La extensión de Netscape y diseño HTML.

Netscape es ahora el mejor navegador conocido para su extensión propietaria a HTML. Lo más popular son los centrados, los tamaños de las letras, los fondos y las tablas, a ultimas fechas se ha incrementado al creatividad y por ejemplo puede verse secuencias en movimiento, los llamados

"frames", que no es más que la información dividida en secciones interrelacionadas, aplicaciones de audio y video que actúan independientes, etc.. Desafortunadamente, el uso de muchas de estas realizaciones pueden crear paginas que son virtualmente imposibles de leer en cualquier otro browser. Si es cierto que Netscape tiene ahora una sobredemanda sobre el mercado compartido, 25 % de los usuarios de la red aún utilizan otros browser- frecuentemente Lynx, el browser no gráfico y Mosaic, el original, aunque Explorer de Microsoft esta también en la competencia.

Algunas personas dicen que la extensión Netscape es tan importante que el hablarse a ese 25% es prácticamente intentar hablar con personas con diferentes lenguajes. Esto no es tan critico, puesto que se pueden crear paginas que se vean bien con cualquier browser.

3.2.1.- ¿Qué es el World-Wide Web?

Por cincuenta años, la gente ha soñado con el concepto de una base de datos de conocimiento universal - información que puede ser accesada por las personas en todo el mundo y de acceso fácil a otras piezas de información para que cualquier usuario pueda rápidamente encontrar las cosas que buscan, revolucionando todos los aspectos de la interacción entre humano e información.

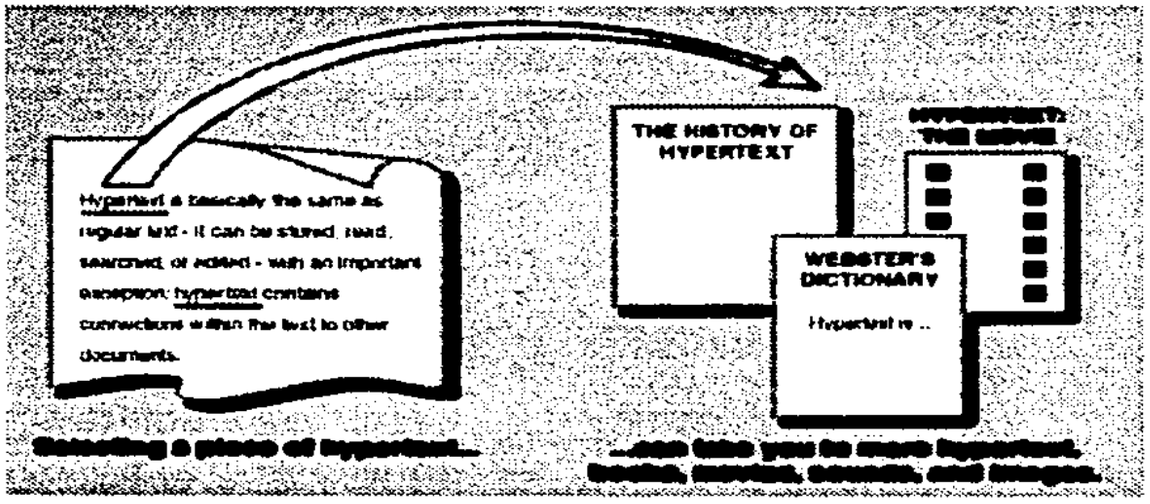
El World-Wide Web es oficialmente descrito como un "recabador de información de hypermedios de área amplia con el propósito de dar un acceso universal a un gran universo de documentos". El proyecto World-Wide Web (WWW, W3) ha realizado esto, proveyendo a usuarios en computadoras en red un consistente significado para accesar una variedad de medios. Utilizando un software de interface para el Web llamado Mosaic, el proyecto Web ha cambiado la forma de ver de la gente y la de crear la información - este ha creado una primera y real red global de hypermedio.

Las tempranas ideas de tales sistemas tienen su principal aplicación en el adelanto de la ciencia y la educación. A través de que el proyecto World-Wide Web adquiere potencia para hacer un impacto significante es esas áreas, este es posesionado para revolucionar muchos elementos de la sociedad, incluyendo comercio, politica y literatura.

3.2.2.- ¿Qué es hypertexto e hypermedia?.

La operación del Web se entrega principalmente en hypertexto como resultado de la interacción con los usuarios. El hypertexto es básicamente lo mismo que un texto regular - este puede ser almacenado, leído, buscado, ó editado - con una importante excepción: el hypertexto contiene conexiones dentro del texto a otros documentos.

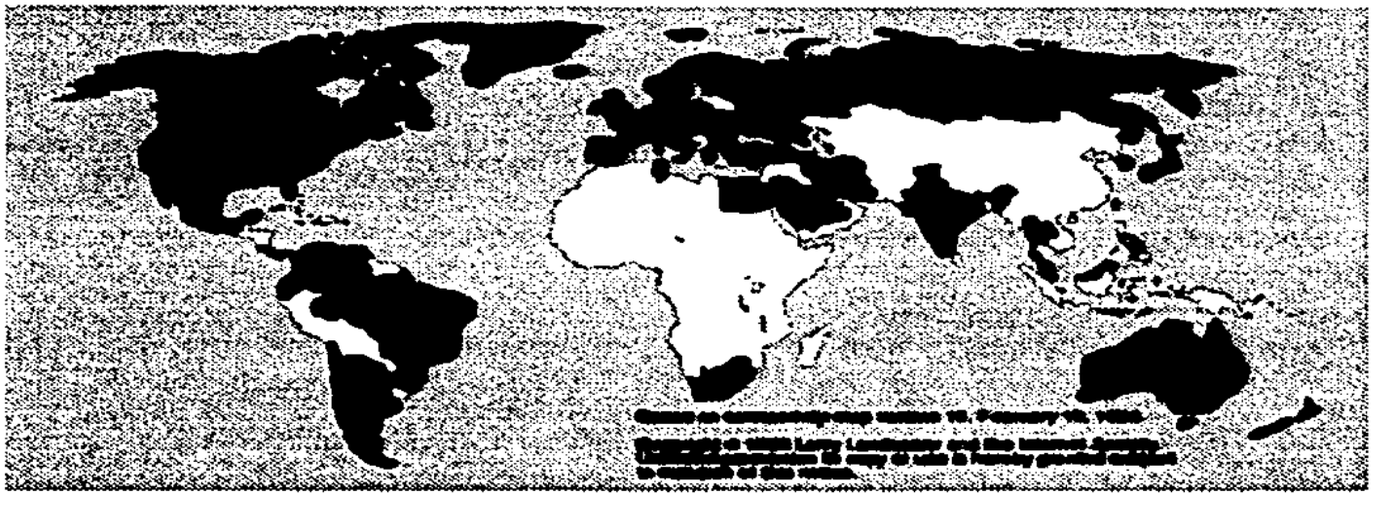
Por ejemplo, suponga que esta disponible para que de algún modo (con un mouse ó con el teclado) dispone de la palabra "hypertexto" en la sentencia. En un sistema de hypertexto, podrá obtener uno ó más documentos relacionados al hypertexto que aparceria ante usted. Este nuevo texto que aparece podrá por si mismo tener enlaces y conexiones a otros documentos a su vez, continuamente seleccionando textos podrá tomarlo en un viaje de asociaciones libres de información. De esta forma, hypertexto enlaza, llama a hyperenlaces, con la que puede crear una red compleja de conexiones virtuales.



Hypermedia es el hypertexto con una diferencia - los documentos hypermedia contienen enlaces no solamente a otras piezas del documento, sino también a tras formas de medios - sonidos, imágenes y videos. Las imágenes por si mismas pueden ser seleccionadas para que estas enlacen a sonidos ó documentos. Hypermedia simplemente combina hypertexto y multimedia.

3.2.3.- ¿Qué es Internet?.

La Internet es la palabra utilizada para describir una red de computadoras masiva de cobertura mundial. La palabra "Internet" literalmente significa "una red de redes". En si misma, la Internet esta compuesta de miles de pequeñas redes regionales dispersadas a través de todo el globo. En cualquier dia esta conecta alrededor de 20 millones de usuarios sobre 50 paises. El World-Wide Web es más comúnmente utilizado en la Internet; este no significa lo mismo. El Web se refiere al cuerpo de la información - un espacio abstracto de conocimiento, el cual a través de la Internet se refiere a el lado fisico de la red global, una masa gigante de cables y computadoras.



En la figura se muestra con negro los paises que tienen conectividad con Internet. Los paises en blanco, sin embargo, pueden tener acceso a correo electrónico, acceso a redes locales pero no una conectividad total a Internet.

Nadie es "dueño" de la Internet - puesto que estas son compañias que ayudan a manejar diferentes partes de la red que ata a cada uno junto con los otro, este no es un cuerpo gobernador solitariamente en la Internet. Las redes dentro de diferentes paises es fundado y administrado localmente de acuerdo a las politicas locales.

El tener acceso a Internet usualmente significa que uno tiene acceso a un número de servicios básico: correo electrónico, conferencias interactivas, acceso a recursos de información, nuevas redes y la posibilidad de transferir archivos.

El World-Wide Web usa la Internet para transmitir documentos hypermedia entre usuarios de computadores internacionalmente. Muchos en la misma forma, nadie es "dueño" del World-Wide Web. La gente es responsable del documento, son los autores y hacen posible la publicidad de estos en el Web. Vía Internet, cientos de miles de gentes alrededor del mundo hacen que la información este disponible desde sus casas, escuelas y lugares de trabajo.

Es posible utilizar usar el software de World-Wide Web sin tener que utilizar la Internet. Pero el acceso a Internet es necesario para hacer un uso completo y participar en el World-Wide Web.

3.2.4.- ¿Cómo fue creado el Web?.

El World-Wide Web comenzó en Marzo de 1989, cuando Tim Berners-Lee de la European Particle Physical Laboratory (conocido como CERN) propuso el proyecto a ser utilizado como resultado de la búsqueda de transporte e ideas efectivas a través de la organización. Las comunicaciones efectivas fueron un acierto de CERN por muchos años y sus miembros se localizaron en varios paises.

El propósito del proyecto original era un simple sistema utilizando hypertexto en red para transmitir documentos y comunicar a una cantidad de miembros en su comunidad. No era la intención la de añadir sonido ó video y la capacidad de poder transmitir imágenes no fue considerada.

Por finales de 1990, la primera pieza del software de Web fue introducida en una máquina NeXT. Esta tenia la capacidad para ver y transmitir documentos hypertexto a otras gentes en la Internet y venia con la posibilidad de editar documentos hypertexto en la pantalla. Fueron dadas demostraciones al comité CERN y seminarios y una demostración fue dada en la conferencia Hypertext '91.

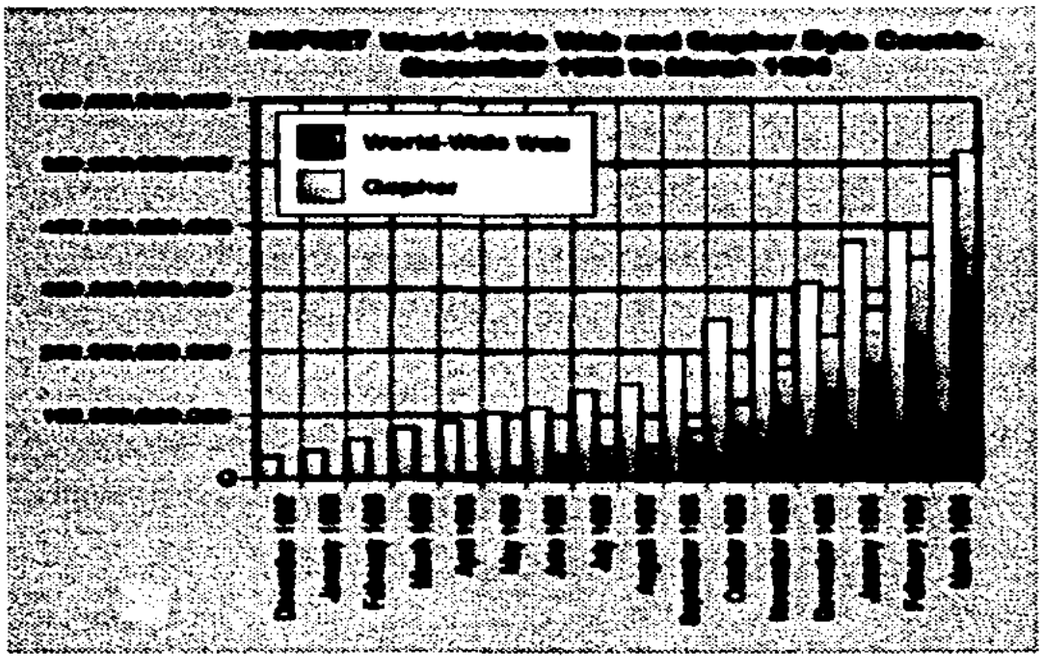
Alrededor de 1992, Tim continuo hablando y bautizando el proyecto, como pequeñas ayudas de desarrolladores comenzaron a ser voluntarios para trabajar el las piezas del World-Wide Web.

Puesto que cientos de gentes alrededor del mundo han contribuido y aportado en este proyecto, este ha resultado de proporciones globales.

3.2.5.- ¿Qué tan popular es el Web?.

Desde Enero hasta Diciembre de 1993, la cantidad de trafico de red (en bytes) a través de la red de Norte America National Science Foundation's (NSF) atribuye al Web un uso multiplicado por 187

veces. En Diciembre de 1993 el Web fue marcado en el lugar 11 de todos los servicios de red en términos trafico de bytes - solamente doce meses antes, este estaba en el lugar 127.



En Junio de 1993, Matthew Gray, un MIT, corrió un pequeño programa el cual automáticamente atraviesa enlaces dentro de la red Web para intentar determinar simplemente cuantos sitios existen que ofrecen información sobre el World-Wide Web. Este pequeño "World-Wide Web Wanderer" encontró alrededor de 100 sitios en ese tiempo y alrededor de doscientos mil documentos. En Marzo de 1994 este robot encontró alrededor de 1,200 sitios únicos. Esto demuestra un poco la relación de crecimiento de los Web en todo el mundo.

Brian Pinkerton en la Universidad de Washington ha estado corriendo un programa similar llamado el "WebCrawler". Su última corrida a mediados de Mayo de 1994 encontró alrededor de 3,800 sites de Web únicos.

Dado que muchos sitios son privados (escondidos detrás de firewalls de corporaciones ó no conectados a la Internet pública), se podrá hablar de al menos de 4,500 servidores Web de hypertexto alrededor del mundo.

Basado en las estadísticas de los sitios de Web, se estima que el número de usuarios de Web que se tienen conocimiento en todo el mundo es más ó menos de dos millones. Sin embargo, considerando el número de host que frecuentan las áreas más populares del Web, es correcto hablar de alrededor de 250,000 a 500,000 usuarios activos actuales del Web hoy en día.

Un caso de estudio - Honolulu Community College.

Honolulu Community College oficialmente anuncio la apertura de su site de hypermedia - el primer sitio de Web en Hawaii y el primero sistema de información de amplitud-campus de hypermedia en el

Web - para finales de Mayo de 1993. Una exhibición de dinosaurios, mapas interactivos, peliculas y publicaciones fueron ofrecidas e inmediatamente atrajeron a la audiencia internacional.

Por Septiembre de ese año (después de 105 días de servicio), recibían más de 23,000 peticiones de documentos y más de 112,000 peticiones de gráficas y de otros medios por casi 5,000 host separados en la red. Hoy en día, el sitio recibe alrededor de 7,000 peticiones por día en promedio, de las cuales principalmente vienen de afuera de Hawaii.

Desde que el sitio abrió, HCC ha recibido visitadores virtuales que van desde Xerox, Digital Equipment Corporation, Apple Computer, Cray, IBM, MIT's Media Lab, NEC, Sony, Fujitsu, Intel, Rockwell, Boeing, Honeywell y AT&T (el cual ha sido uno de los más frecuentes visitadores), y otras cientos de corporaciones.

Visitadores colegiales han sido reportados desde Stanford, Harvard, Carnegie-Mellon, Cornell, MIT, Michigan State, Rutgers, Purdue, Rice, Georgia Tech, Columbia, University of Texas y Washington University así como otros campos en el Reino Unido, Alemania y Dinamarca por nombrar algunos.

Visitadores gubernamentales han entrado desde varios departamentos en la NASA, incluyendo Jet Propulsion Laboratories, Lawrence Livermore National Laboratories, la National Institute of Health, la Superconducting Supercollider project y la USDA, así como sitios gubernamentales en Singapur y Australia.

Puesto a la operación de los servicios de HCC cuando estos eran relativamente pocos sitios en el mundo, y parte debido a esta popularidad, el crecimiento en el tráfico a reflejado estrechamente el crecimiento del Web.

La popularidad de otros sitios de Web.

El Global Network Navegator es una revista electrónica publicada por O'Reilly y Asociados sobre el World-Wide Web. Esta ofrece noticias, un calendario de eventos de Internet y lugares de ventas virtuales en los cuales las compañias pueden promover sus servicios. Este tiene alrededor de 12,000 subscriptores registrados y recibe alrededor de 150,000 a 200,000 peticiones de documentos y medios por semana por gente de todo alrededor de la Internet.

Quizás el mejor ejemplo del crecimiento del uso del Web puede verse en el National Center for Supercomputing Applications (NCSA). El NCSA produce un número de productos de software populares para el uso de World-Wide Web y su sitio de Web es usado como documentación para sus productos así como el lugar donde se conjuntan anuncios sobre nuevos eventos en el Web. En Julio de 1993 el sitio de NCSA recibió al menos un millón de peticiones por semana y su tráfico continua en crecimiento.

3.2.6.- ¿Quién viaja en el Web?.

Una comparación informal de estadisticas de host de 15 gobiernos, investigación, educacional y sitios de Web corporativos en marzo de 1994 mostró que la gente que navega por el World-Wide Web sigue el mismo rol de la Internet regularmente.

Lo mostrado en la gráfica siguiente es en relación a los cinco Web más usados, esto es tomado en relación a su dominio y la cantidad en porciento del total de cada sitio de host Web recibidos. Luego a esa estadistica es el porcentaje estimado del total de host en la Internet para esos dominios.

U.S. Educational (.edu)	48%	27%
U.S. Commercial (.com)	28%	30%
U.S. Government (.gov)	9%	6%
United Kingdom (.uk)	7%	5%
Canada (.ca)	5%	4%

Los cinco más usados World-Wide Web, por dominios.

En Enero de 1994, James Pitkow (pitkow@cc.gatech.edu) y Mimi Recker en el Georgia Institute of Technology ayudaron al primer examen de usuario de World-Wide Web. Fuera de las 1,300 respuestas válidas, los resultados indican las siguientes estadisticas sobre los mismos encuestados:

* 56% están entre los 21 y 30 años de edad,
* 94% son hombres,
* 69% se localizan en Norte America y
* 45% se describe a si mismo como un profesional y 22% como un estudiante graduado.

Puesto que esto es imposible conocerlo por completo, se puede suponer que el gran número de viajantes del World-Wide Web consiste de popularidad dentro de campus en los cuatro último años dentro de los Estados Unidos.

3.2.7.- ¿Porqué es tan popular el Web?.

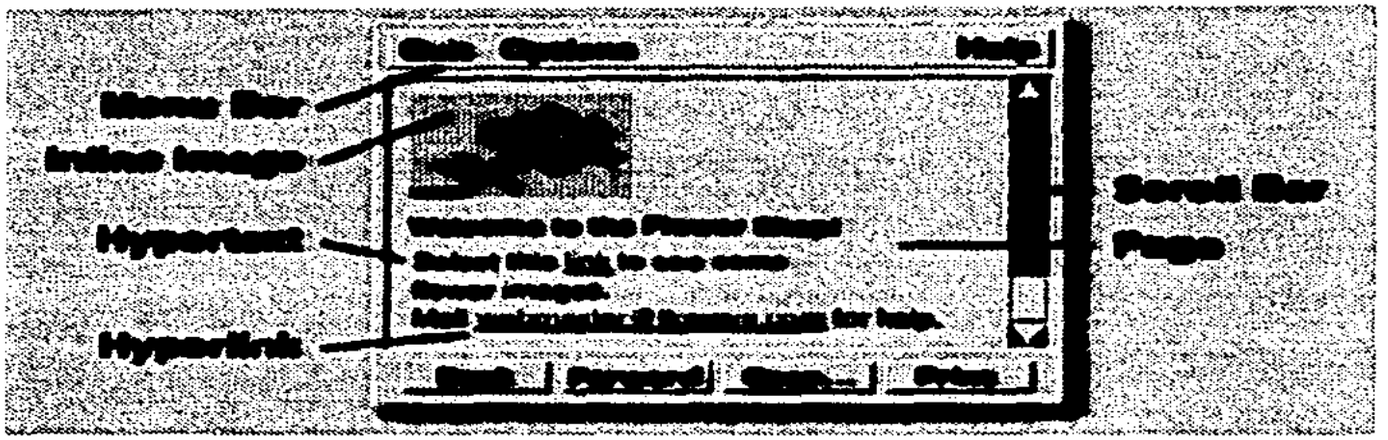
El Web ofrece una interface de fácil uso para los recursos tradicionales dificiles de manejar en la Internet. Es probablemente por este fácil uso así como la popularidad de muchas interfaces gráficas para el Web lo que causa la explosión del tráfico del Web en 1993.

La potencia del uso de hypertexto de redes y multimedia ha llevado a muchos usuarios a crear y explorar innumerables aplicaciones innovativas en la Internet. No es de sorprenderse que muchos usuarios educacionales pongan sus productos para evacuación de otros usuarios.

3.2.8.- ¿Qué es lo que hace que el Web se vea así?.

El World-Wide Web existe virtualmente - esta no es una forma estándar de ver ó navegar sobre este. Sin embargo, muchos software de interface para el Web tienen funciones similares y generalmente trabajan de la misma forma, no importando la computadora ó el tipo de pantalla utilizado. Por ejemplo, muchos usuarios navegan alrededor del Web usando una interface de solo texto y están en disponibilidad de ver toda la información textual en uso con una pantalla gráfica.

La de abajo es una figura de una interface gráfica típica de World-Wide Web que puede verse en cualquier pantalla de computadora. Esta puede ser en blanco y negro ó en color. En este ejemplo, la interface -llamada también el browse de Web - trabaja en una ventana y puede ser un programa de software en cualquier computadora con una interface gráfica, tales como Macintosh ó una computadora IBM-compatible con Microsoft Windows.



El browser tiene una barra de menú en lo alto, donde el usuario puede salirse, obtener ayuda en el uso del programa y cambiar ciertas características de exhibición tales como el tamaño de la letra de la pantalla, el color del fondo, etc.

Una barra de deslizamiento permite al usuario deslizar la página del documento hacia arriba y hacia abajo. Puesto que no esta limitado en cuanto al tamaño de ancho ó pequeño del documento de hypertexto, la barra de deslizamiento es frecuentemente necesitada en caso de que el documento es más grande que la ventana de visión.

Puesto que son diferentes las formas en que puede ser representado un documento en la pantalla, esta es frecuentemente llamada una página. Usualmente, esa responsabilidad para crear una colección dada de documentos interrelacionados también crea un documento especial el cual se intenta que se vea primeramente - uno que contiene información introductoria y/o un menú maestro dentro de esa colección. Este tipo de documento es llamado una home page y es generalmente asociado con un sitio particular, persona ó nombre de colección. Este ejemplo muestra el home page de Flower Shop's.

Este ejemplo tiene una foto de una flor, el texto en un estilo bold (""Welcome to the Flower Shop!") e hypertexto el cual esta como una simple palabra subrayada. Esta palabra ("link") es un hypertexto (ó enlace) - comúnmente, haciendo click en esta con un mouse produce que otro documento aparezca en la pantalla, el cual puede contener más imágenes e hypertextos para otros lugares. Esta no es una forma para representar texto que es enlazado a otras cosas - algunos browser subrayan, otros usan un color especial y muchos dan una variedad de opciones para los usuarios.

Imágenes tales como la foto de la flor, las cuales son parte del documento y son desplegadas dentro de la página, son llamadas imágenes en línea.

Frecuentemente usuarios crean sus propios documentos personales con colecciones de sus enlaces favoritos ó información bibliográfica y los hacen públicamente disponibles. Puesto que estas páginas son también llamadas home page (estas son un "home" virtual para el usuario), estas pueden ser llamadas "personal pages" ó "hyplans" (plan hypermedia).

En el fondo de la pantalla están un juego de botones de navegación - puesto que un usuario puede ir a muchas pantallas deferentes seleccionando enlaces de hypertexto, estas necesitan de algún método de regresar en alguno de los pasos y revisar el documento que ha sido explotado. El botón de regreso muestra el documento visto previamente. El botón de avance puede mostrar la página en el orden que el usuario previamente vio antes.

Un botón de abrir permite al usuario conectarse a otros documentos y recursos de red especificando la dirección del documento ó recurso a conectar. El usuario puede estar disponible para conectarse a un documento almacenado localmente en la misma máquina utilizada ó una almacenada en algún otro país.

El botón de impresión le permite al usuario imprimir el documento que se ve en la pantalla. El usuario puede escoger imprimir el documento con imágenes y formatearlas como se ven en la pantalla ó como un documento de texto solamente.

La página lista una dirección de correo electrónico - webmaster@flowers.com. Una convección del Web es nombrar a la persona a cargo de administrar el sitio World-Wide Web como "webmaster"- cualquier problema con el hyperenlace, imágenes, documentos ó preguntas sobre el sitio deberá ser enviadas via correo a la dirección del webmaster.

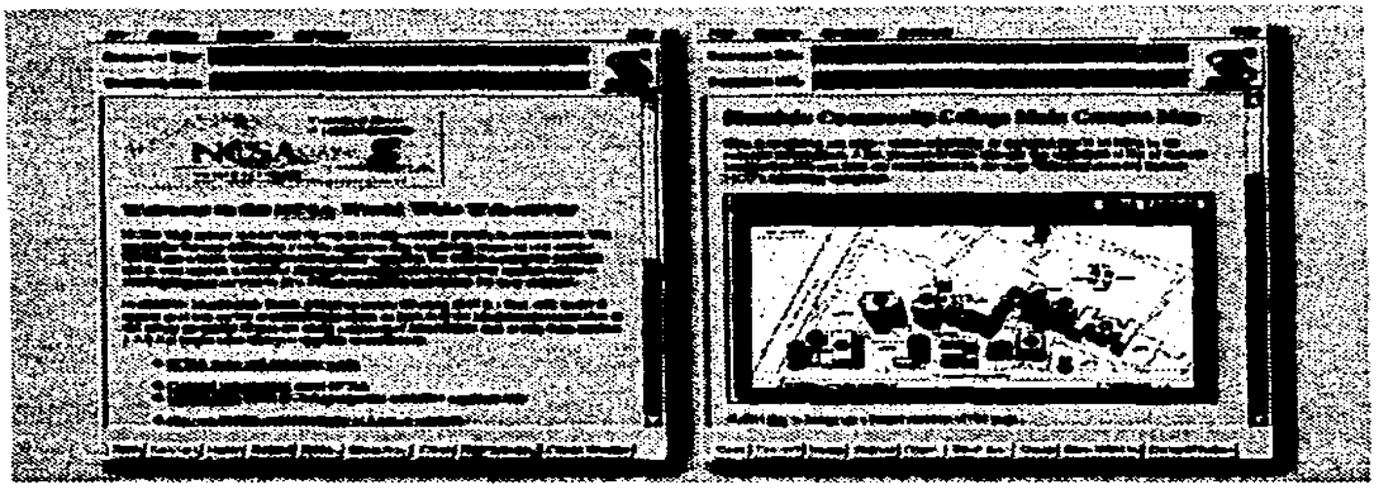
3.2.9.- ¿Qué es Mosaic?.

Meses después de los propósito originales de la CERN, la National Center for Supercomputing Applications (NCSA) comenzó un proyecto para crear una interface para el World-Wide Web. Una de las misiones de la NCSA era ayudar a la comunidad investigadora científica proveyendo un software no comercial ampliamente disponible. Otros de los puntos es investigar nuevas búsquedas de tecnologías con la esperanza de que interesados comerciales estén en disponibilidad de ganar de estos. Es esta forma, el proyecto de Web fue ampliamente apropiado. El Software Design Group de la NCSA comenzó a trabajar en una interface de plataforma múltiple y versátil para el World-Wide Web, y la llamo Mosaic.

A principios de 1993, la primer versión del browse de Web de NCSA fue disponible para la comunidad de Internet. Puesto que versiones beta fueron distribuidas, Mosaic a desarrollado una fuerza seguida por el tiempo que esta fue oficialmente liberada. Puesto que ésta permite ver documentos con imágenes y un formato de media tales como que el video y sonido sean transferidos sobre la Internet y dirigidos por el documento, esto convierte al browse del Web como la opción para aquellos trabajos en computadoras con interacción gráfica. En 1993 el producto Mosaic de la NCSA ganó el premio Internet Multicasting Service por la aplicación más innovativa y el premio InfoWorld Industry Archievement.

Puesto que el número total de servicios tradicionales pueden ser manejados y debido a esta facilidad, posesionarse y hacer click con la interface de hypertexto, Mosaic pronto se convirtió en la más popular interface para el Web. Actualmente versiones de Mosaic pueden correr en máquinas basadas

en UNIX tales como Sun, Silicon Graphics y workstations DEC así como en una IBM-compatible corriendo Microsoft Windows y computadoras Macintosh.



Mosaic de NCSA para X Windows.

3.2.10.- ¿Qué es lo que Mosaic puede hacer?.

Mosaic tiene las siguientes caracteristicas:

* Una interface gráfica manejando el mouse.
* La habilidad de desplegar documentos hypertexto e hypermedia.
* La habilidad de desplegar texto electrónico en una variedad de tipo de letra.
* La habilidad de desplegar formatos de elementos de presentación.
* Soporte para peliculas (MPEG-1 y QuickTime).
* La habilidad para desplegar caracteres definidos en la ISO 8859 (varios lenguajes).
* Soporte a formas electrónicas interactivas, con una variedad de elementos de formas básicas.
* Soporta gráficas interactivas (en formato GIF ó XBM) de hasta 256 colores dentro del documento.
* La habilidad para hacer enlaces de hypermedia básicos y soportando los siguientes servicios: FTP, gopher, telnet, NNTP, WAIS.
* La habilidad de extender estas funcionalidades creando un script personal.
* La habilidad de tener otro control de aplicaciones desplegadas remotamente.
* La habilidad de enviar el contenido a una red de usuarios corriendo en múltiples plataformas.
* Soporte para los estándares actuales de HTTP y HTML.
* La habilidad de guardar una historia de los hyperenlaces atravesados.
* La habilidad para almacenar y revisar una lista de documentos vistos para uso futuro.

3.2.11.- ¿Qué esta disponible en el Web?.

Actualmente el Web ofrece lo siguiente a través de un hypertexto y en algunos casos por medio de alguna interface de hypermedio:

* Cualquier servidor a través de Gopher.
* Cualquier servidor a través de WAIS (Wide-Area Information Servers).
* Cualquier servidor a través de sitios FTP anónimos.
* Servicio completo de Archie (servicio de búsqueda de FTP).
* Servicio completo de Veronica (un servicio de búsqueda de Gopher).
* Servicio completo de CSO, X.500 y whois (servicio de directorio telefónico de Internet).
* Servicio completo de finger (un programa de búsqueda de usuarios Internet).
* Cualquier cosa en Usenet.
* Cualquier cosa accesible a través de telnet.
* Cualquier cosa en hytelnet (una interface de hypertexto para telnet).
* Cualquier cosa en techinfo ó texinfo (servicio de información de formas de campo amplio).
* Cualquier cosa en hyper-g (un sistema de hypertexto de red en uso por toda Europa).
* Documentos de hypertexto e hypermedia con formato HTML.

3.2.12.- ¿Cómo trabaja el Web?.

El software de Web es diseñado alrededor de una arquitectura cliente-servidor distribuida. Un cliente de Web (llamado un navegador ó browser de Web, si este está en la disponibilidad de poder interactuar) es un programa el cual puede enviar peticiones de documentos para cualquier servidor de Web. Un servidor de Web es un programa que, una vez recibida la petición, envía el documento pedido (ó un mensaje de error, si es el caso) de regreso al cliente que hizo la petición. Utilizando una arquitectura distribuida significa que el programa del cliente puede estar corriendo en una máquina separada completamente de lo que es el servidor, posiblemente en otro cuarto y más aún en otro país. Puesto que la tarea de almacenamiento de documentos es dejada al servidor y la tarea de presentación del documento es dejada al cliente, cada programa puede concentrarse en sus deberes y regresar independientemente una de la otra.

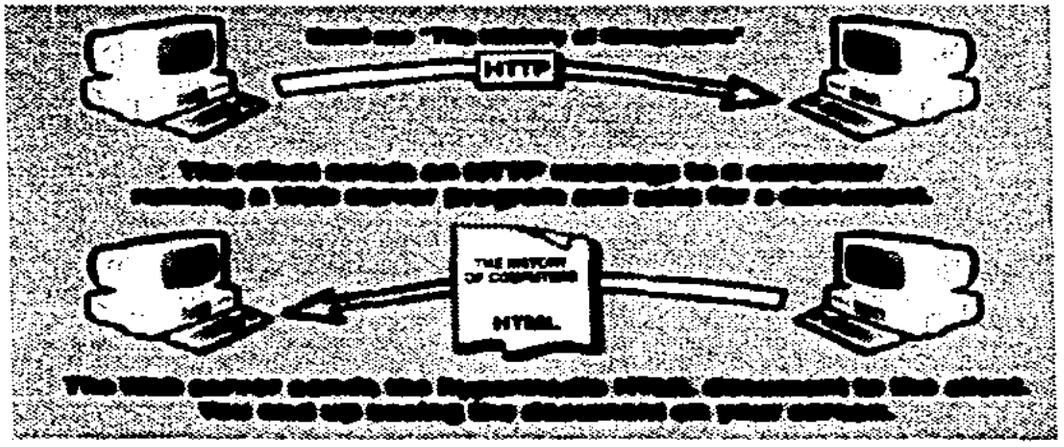
Puesto que los servidores operan solamente cuando los documentos son requeridos, esto pone una mínima cantidad de carga de trabajo en la computadora donde están corriendo.

Este es un ejemplo de como trabaja el proceso:

1.- Corriendo el cliente de Web, el usuario selecciona un hyperenlace en una pieza del hypertexto conteniendo a otro documento "The History of Computers", por ejemplo.

2.- El cliente de Web utiliza la dirección asociada con ese hyperenlace para conectarse a el servidor Web en una dirección de red específica y pregunta por el documento asociado con "The History of Computers".

3.- El servidor responde enviando el texto y cualquier otro medio que este dentro del texto (fotos, sonido ó películas) hacia el cliente, el cual se las reenvía para presentarlas en la pantalla del usuario.



El World-Wide Web esta compuesto de miles de estas transacciones virtuales a través de todo el mundo, creando un flujo de información de los web.

Servidores futuros de Web incluyen la habilidad de encriptación y autentificación de clientes - podrá estar disponible para enviar y recibir datos seguros y ser más selectivos, como para la información que reciben de los clientes. Esto podrá permitir una cantidad de comunicación más libre de los usuarios del Web y puede asegurar que datos sensitivos serán mantenidos en privado. Esto podrá también comprometer la seguridad de servicios comerciales y educacionales los cuales desean mantener su información localmente. Mejoras en la seguridad podrían facilitar la idea de hypertextos "pay-per-view", un concepto que muchos comerciantes interesados están persiguiendo.

El lenguaje que el cliente y servidor de Web utilizan para comunicarse con cada otro es llamado Hypertext Transfer Protocol (HTTP). Todos los clientes y servidores de Web deben estar disponibles para poder hablar HTTP para enviar y recibir documentos hypermedia. Por esta razón, el servidor de Web son frecuentemente llamado servidor HTTP.

La frase "World-Wide Web" es frecuentemente utilizada para referirse a la colección de servidores de red hablando HTTP así como al cuerpo global de información disponible usando el protocolo.

3.2.13.- HTML - El Hypertext Markup Language.

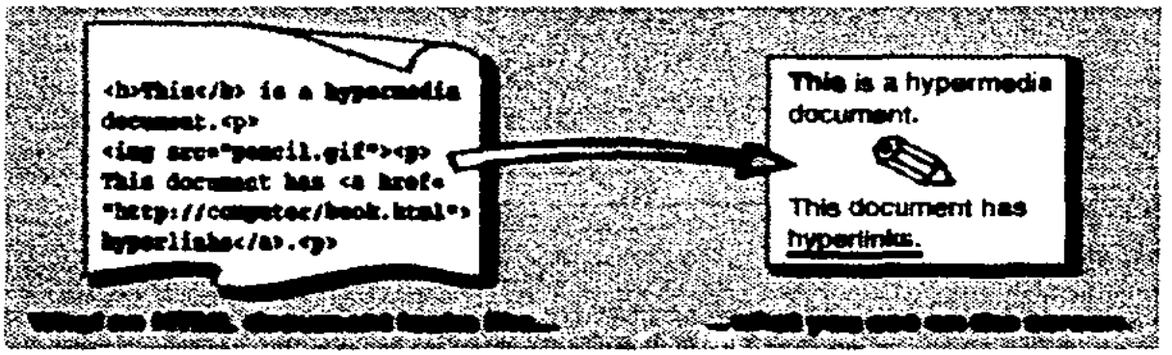
El lenguaje estándar de los usuarios de Web para crear y reconocer documentos hypermedia es el Hypertext Markup Language (HTML). Esto esta lejanamente relacionado al Standard Generalized Markup Language (SGML), un método de representación de documentos en lenguaje formateado. Lenguajes tales como HTML el cual sigue el formato SGML, permitiendo documentos escritos para separar información de la presentación de los documentos - esto es, documentos conteniendo la misma información pueden ser presentados en un número de formas diferentes. Los usuarios tienen la opción de controlar elementos visuales tales como tipo de letras, tamaños y espacios entre párrafos sin cambiar la información original.

HTML tiende ampliamente a este uso fácil. Los documentos Web son comúnmente escritos en HTML y son nombrados con el sufijos ".html". Documentos HTML no son más que archivos ASCII

estándar de 7-bit con códigos formateados que contienen información sobre su estructura (estilo de texto, titulos de documentos, párrafos, listas) e hyperenlaces.

Software de convención libre esta disponible para trasladar documentos desde muchos otros formatos dentro de HTML. Existen filtros que pueden convertir archivos en RTF (Rich Text Format), WorkPerfect y FrameMaker.

El actual HTML estándar soporta la creación de documentos hypertexto básicos y estructuras, pero esta limitado en la capacidad para soportar técnicas de estructura muy complejas encontradas en documentos tradicionales de publicistas.



3.2.14.- En relación a los Uniform Resource Locators.

El World-Wide Web usa a los que son llamados Uniform Resource Locators (URLs) para representar enlaces de hypermedia y enlaces a servicios de red dentro de documentos HTML. Es posible representar casi a cualquier archivo ó servicio en la Internet con un URL.

La primera aparición de el URL (antes de los dos "/") especificaba el método de acceso. El segundo es comúnmente la dirección de la computadora de datos ó localización del servidor. Más adelante, partes pueden especificar el nombre de los archivos, el puerto a conectar ó el texto a buscar en una base de datos. Una URL es siempre una linea única sin espacios.

Sitios que corren servidores de World-Wide Web son comúnmente nombrados con www al comienzo de la dirección de red.

Aquí unos ejemplos de URLs:

* file://www.hcc.hawaii.edu/sound.au - Recibe un archivo de sonido y lo toca.

* file://www.cit.com/picture.gif - Recibe una figura y la coloca, tanto en un programa separado ó dentro de un enlace hypermedia.

* file://www.eff.org/directory/ - Despliega el contenido de un directorio.

* http://www.hcc.hawaii.edu/directory/book.html - Conecta a un servidor HTTP y recibe un un archivo HTML.

* ftp://www.xerox.com/pub/file.txt - Abre una conexión FTP a www.xerox.com y recibe un archivo de texto.

* gopher://www.hcc.hawaii.edu - Conecta al Gopher en www.hcc.hawaii.edu.

* telnet://www.hcc.hawaii.edu:1234 - Hace un Telnet a www.hcc.hawaii.edu en el puerto 1234.

* news:alt.hypertext - Lee las últimas noticias de Usenet conectándose a un host (NNTP) de noticias especificado por el usuario y regresa el articulo en el formato de hypermedia de newsgroup alt.hypertext.

Muchos browser de Web le permiten al usuario especificar un URL y conectarse a ese documento ó servicio. Cuando selecciona hypertexto en un documento HTML, el usuario envía una petición para abrir un URL. En este caso, el hyperenlace puede ser hecho no solamente para otros textos y medios, sino también para otros servicios de red. El browser de Web no es simplemente un cliente de Web, sino también proporciona una disponibilidad completa de cliente FTP, Gopher y telnet.

HTML puede incluir URL email, asi los hyperenlaces pueden ser hechos para enviar correo electrónico automáticamente. Por ejemplo, seleccionando una dirección de email en un lugar del hypertexto podrá abrir un programa de correo, listo para enviar un email a esa dirección.

3.2.15.- ¿Qué software esta disponible?.

Los clientes del World-Wide Web (browser) están disponibles en las siguientes plataformas y ambientes:

Navegadores de texto solamente:
- Terminales tontas, casi en cualquier plataforma de UNIX.
- Texto solamente utilizando emulación vt100, para SunOS4.1.x, IBM AIX, DEC OSF/1, DEC Ultrix y VAX Multinet.
- Texto solamente con Macintosh, para Mac SE y superiores con System 7.x.
- Navegadores escritos en perl están disponibles.
- Navegadores escritos para ambientes emacs están disponibles.

Navegadores con interface gráfica:
- Sun 4/Sun OS 4.1.x.
- Silicon Graphics IRIX 4.x.
- VMS.
- Linux.
- DEC MIPS Ultrix, DEC Alpha AXP, OSF/1.
- IBM RS/6000, AIX 3.2.
- HP 9000/700, HP/UX 9.x.
- NeXT, NeXTStep 3.0.
- Commodore Amiga, AmigaOS 3.0.
- IBM compatibles, 80386 y superiores con 4 MB RAM, bajo Windows 3.1 en modo mejorado.
- Computadoras Macintosh, System 7.x, 68020 y superior ó Power Macintosh.

Servidores World-Wide Web están disponibles para las siguientes plataformas y ambientes:

* Muchas versiones de UNIX.
* HP, SGI y SUN system.
* DEC MIPS Ultrix, DEC Alpha AXP.
* Perl.
* Macintosh, 68020 ó mejor, Power Macintosh, System 7.x.
* NeXTStep.
* VM, VM/CMS, VM/XA, VMS.
* Windows 3.1 y Windows NT.

3.2.16.- ¿Cómo puedo obtener más información?.

Mucha de esta información esta disponible en la Internet. La mejor forma de obtener información en el Web sin un browser ó navegador es hacer un telnet a info.cern.ch ó un gopher a info.cern.ch. La información de como puede ser obtenido un software se puede encontrar aqui.

Si no conoce como usar FTP, Gopher ó telnet, existen docenas de libros disponibles de como entrar y utilizar Internet. puesto que son demasiados los libros que se enlistarian, aquí están uno cuantos que son mencionados por la Unofficial Internet Book List (para recibir la lista, enviar un correo a savetz@rahul.net)

The Internet Guide for New Users
Daniel P. Dern, McGraw-Hill, ISBN: 0-07-016511 (paperback)

The Internet Starter Kit for the Macintosh
Adam Engst, Hayden Books, ISBN: 1-56830-064-6

The Internet Unleashed
Martin Moore, others, Sams Publishing, ISBN: 0-672-30466-X

PC Internet Tour Guide
Michael Fraase, Ventana Press, ISBN: 1-56604-084-1

The Whole Internet User's Guide and Catalog
Ed Krol, O'Reilly and Associates, ISBN: 1-56592-025-2

Zen and the Art of Internet
Brendan Kehoe, Prentice Hall, ISBN: 0-13-010778-6

Navegadores disponibles por telnet

http://info.cern.ch/hypertext/WWW/FAQ/Bootstrap.html:

telnet info.cern.ch (or telnet 128.141.201.74)

Este es un browser de Web CERN de texto-solamente.

telnet ukanaix.cc.ukans.edu

Este sitio de la University of Kansas usa el browser de solo-texto Lynx, el cual trabaja mejor en una terminal con emulación vt100. Entre como www.

telnet www.njit.edu

Entre como www. Este es un browser de solo-texto del New Jersey Institute of Technology.

telnet vms.huji.ac.il (or telnet 128.139.4.3)

Este browser de solo-texto esta en la Hebrew University of Jerusalem en Israel trabaja en una base de datos de lenguaje dual Hebrew/English .

telnet fserv.kfki.hu

Este sitio esta en Hungary tiene una conexión lenta y deberá ser usado solo localmente. Entre como www.

telnet info.funet.fi (or telnet 128.214.6.100)

Este sitio esta en Finland.

Información general del Web

Pagina principal del CERN World-Wide Web

http://info.cern.ch/hypertext/WWW/TheProject.html

Pagina principal de Mosaic NCSA

http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/mosaic-docs.html

Información en WWW

http://www.bsdi.com/server/doc/web-info.html

Una lista de clientes World-Wide Web en CERN

http://info.cern.ch/hypertext/WWW/Clients.html

La lista "oficial" de servidores World-Wide Web en CERN

http://info.cern.ch/hypertext/DataSources/WWW/Servers.html

El archivo comp.infosystems.www FAQ (Frequently Asked Questions)

http://siva.cshl.org/~boutell/www_faq.html

Lista de herramientas y utilerias de conversión

http://info.cern.ch/hypertext/WWW/Tools/Overview.html

http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/faq-software.html

Como escribir a Web gateway y servidores

http://info.cern.ch/hypertext/WWW/Daemon/Overview.html

Información en HTML y HTTP

Como escribir en HTML

http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLPrimer.html

Tutorial de HTML

http://curia.ucc.ie/info/net/htmldoc.html

http://fire.clarkson.edu/doc/html/htut.html

Guia de estilos de HTML

http://www.willamette.edu/html-composition/strict-html.html

http://bookweb.cwis.uci.edu:8042/Staff/StyleGuide.html

http://info.cern.ch/hypertext/WWW/Provider/Style/Overview.html

HTML FAQ

http://www.umcc.umich.edu/~cc/www/html_faq.html

Referencias rápidas de HTML

http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLQuickRef.html

Especificaciones oficiales HTML

http://info.cern.ch/pub/www/doc/html-spec.multi

El HTML DTD (Document Type Definition)

http://info.cern.ch/hypertext/WWW/MarkUp/HTML.dtd.html

HTML+ DTD

ftp://15.254.100.100/pub/htmlplus.dtd.txt

El último bosquejo de HTML+

ftp://ds.internic.net/internet-drafts/draft-raggett-www-html-00.*

Especificaciones de HTTP

http://info.cern.ch/hypertext/WWW/Protocols/HTTP/HTTP2.html

Información y reportes en Multimedia e Hypermedia

http://cui_www.unige.ch/Chloe/MultimediaInfo/index.html

http://www.cs.bgsu.edu/SIGLINK/HomePage.html

"State of the Art Review on Hypermedia Issues And Applications", March 1994

http://www.csi.uottowa.ca/~dduchier/misc/hypertext_review/

"Computer Supported Cooperative Work Report", July 1993

ftp gorgon.tft.tele.no, in directory /pub/groupware

"Network Access to Multimedia Information", June 1993

ftp ftp.ed.ac.uk, in directory /pub/mmaccess

"Hypermedia and Higher Education", April 1993

gopher lewsun.idlw.ucl.ac.be, the /digests/IPCT menú.

alt.hypertext Frequently Asked Questions list

Obteniendo Browser de Web y Servidores

ftp info.cern.ch, in directory /pub/www

ftp ftp2.cc.ukans.edu, in directory /pub/WWW/lynx

ftp ftp.ncsa.uiuc.edu, in directory /Mosaic

ftp ftp.law.cornell.edu, in /pub/LII/Cello/

ftp max.physics.sunysb.edu, in /pub/amosaic

ftp ftp.omnigroup.com, in /pub/software/

ftp ftp.cs.unlv.edu, in /pub/chimera

ftp oac.hsc.uth.tmc.edu, in /public/mac/MacHTTP/

gopher hopf.math.nwu.edu

ftp austin.bsdi.com, in /plexus

ftp emwac.ed.ac.uk, in /pub/https

Una lista más extensiva de browser puede ser encontrada en http://info.cern.ch/hypertext/WWW/Clients.html, y una lista de servers puede ser encontrada en http://info.cern.ch/hypertext/WWW/Daemon/Overview.html.

3.3.- Interacción con Windows.

3.3.1.- El Socket para Windows.

El Trumpet Winsock es un Socket de Windows 1.1 compatible con el stack TCP/IP el cual provee un nivel de red estándar para utilizar muchas aplicaciones de red en Windows y por si mismo ha sido el principal vehículo para la difusión del uso de Windows Sockets 1.1.

3.3.2.- Instalando el Trumpet Winsock.

El Trumped Winsock solamente puede correr en su PC bajo las siguientes condiciones. Debe tener tanto un manejador de paquetes disponible que sea utilizado por programas de red ó si desea utilizar SLIP, un puerto de comunicaciones libre. Adicionalmente, los manejadores de paquetes solamente pueden ser utilizados de manera confiable bajo modo mejorado utilizando WINPKT. El modo estándar puede ser utilizado, pero debe tenerse cuidado para evitar fallas en el sistema. NDIS y ODI pueden ser utilizados vía manejadores de paquetes, pero su uso no es soportado. PKTMUX puede también ser utilizado en lugar de WINPKT y deben ser versión 1.2c ó posteriores, pero de nuevo su uso no es soportado.

Si tiene ya instalado algún tipo de paquete de red TCP/IP, es muy probable de que este sea el Trumpet Winsock y tenga algún mensaje de su configuración del sistema al instalar Trumpet Winsock, posiblemente aún para intentar desinstalar el paquete de red. Alternativamente, puede ser que el Winsock disponible para su paquete ya instalado haga que no sea requerido el Trumpet Winsock.

3.3.3.- Utilizando Trumpet Winsock sobre Internal SLIP/PPP .

SLIP es un protocolo simple el cuál permite una conexión serial Asincrona para enviar el protocolo Internet (IP). Generalmente necesitara tener acceso a un servidor el cuál pueda entender el protocolo SLIP. SLIP, por lo general, se accesa vía línea telefónica y con la ventaja de módem de alta velocidad, TCP/IP se vuelve confiable sobre una conexión de marcado ó dial-up.

PPP (Protocolo Point to Point) es un protocolo que es más complicado que SLIP, el cual ofrece corrección de error y es mucho más confiable que SLIP.

El Trumpet Winsock tiene la facilidad de manejar una conexión SLIP así como la habilidad de usar script de marcado para entrar y salir de su servidor SLIP.

3.3.4.- Instalando el Winsock para usuarios sobre Internal SLIP/PPP.

Antes de que haga cualquier cosa, copie el archivo **winsock.dll, tcpman.exe, hosts, services** y **protocol** a un subdirectorios diferente:

p.ej. c:\trumpet

los archivos esenciales son:

winsock.dll	la base del driver TCP/IP.
tcpman.exe	el programa controlador para el Winsock.
sendreg.exe	el programa de registro.
hosts	lista de nombres de host.
services	lista de servicios de Internet.
protocol	lista de protocolos de Internet.

modifique la línea de ruta en su autoexec.bat para que contenga la referencia al subdirectorio creado:

p.ej. path c:\dos;c:\windows;**c:\trumpet**

Asegúrese que se activa reiniciando la computadora ó ejecutando el autoexec.bat de nuevo. Ahora esta listo para iniciar windows.

Desde windows, inicie tcpman seleccionando File/Run desde el File Manager, luego teclee "tcpman". Si este falla, es muy probable que la ruta este incorrecta.

Asumiendo que es un usuario novato, una pantalla de instalación aparecerá dando un número de opciones a llenar. Necesita llenarla detalladamente para habilitar el funcionamiento de paquetes TCP. Si no tiene claro alguno de estos términos, intente buscar ayuda en algún centro de soporte calificado de Internet - puede salvarlo de desperdiciar mucho tiempo.

Primeramente, escoja Internal SLIP ó Internal PPP. Algunos de los parámetros pueden estar disponibles y otros no disponibles.

Dirección IP	su dirección IP de Internet ó "bootp" en algunos casos solamente. Utilice bootp solamente si su servidor lo soporta, se otra forma el winsock podria tardarse hasta 2 minutos y un mensaje de "Unable to perform bootp" apareceria. El winsock no funcionara debido a que el bootp fallo.
Nombre del servidor	su nombre del servidor de dirección IP para búsquedas de DNS. Puede proveer más de una dirección, separándolas con espacios (direcciones IP solamente).
Servidor de Tiempo	en el presente sin uso - futuras API de winsock pueden soportar esto (direcciones de IP solamente).
Sufijo de Dominio	un espacio separa la lista de sufijo de dominios a ser utilizada cuando se resuelven nombres en el sistema DNS.
MTU	Maximum Transmission Unit ó unidades de transmisión

	máxima. Relacionado al TCP MSS... usualmente TCP MSS + 40 (Numérico). Para SLIP, se sugiere 256 inicialmente.
TCP RWIN	TCP Receive Window. Es recomendado que el valor de estos sea alrededor de 3 ó 4 veces el valor de TCP MSS (Numérico). Para SLIP se sugiere 848.
TCP MSS	TCP Maximum Segment Size, Es recomendado que sea el valor más pequeño cuando se esta utilizando SLIP - p.ej. 512 bytes para SLIP y más bajo para CSLIP. CSLIP esta disponible para comprimir datos más eficientemente cuando este es menor que 255 (numérico). Para SLIP se sugiere 212 inicialmente.
puerto SLIP	su número de puerto de comunicación ..1=com1, 2=com2, etc., (numérico)
relación de baudio	la velocidad a la que desea correr (numérico). Hasta 115200 es soportado, puesto que velocidades más altas de 19200 requieren hardware apropiado.
hardware handshake	recomendado si su enlace lo soporta.
Compresión Van Jacobson CSLIP	si su servidor lo soporta. Puede tener que ajustar MTU, MSS y RWIN para tenerlo más apropiado.
Detección de estatús en línea	si su modem lo soporta, seleccione detección de estatús en línea DCD ó DSR. Necesitara asegurarse de que el módem tiene un seleccionado de default de AT&C1 para que esto funcione.

El resto de los detalles deberán de estar desactivados y no necesita intentar llenarlos.

Cuando se tenga esto, seleccionar <OK> y si todo esta bien, el Trumpet Winsock será inicializado. Esta listo para iniciar utilizando el winsock.

3.3.5.- Entrando en el servidor.

Puede utilizar tanto el login manual ó el automático realizado desde un script para accesar al servidor. Para la primer vez utilice el manual y entre a la red con los comandos apropiados. No olvide utilizar la tecla <esc> para salir cuando haya finalizado. Después de entrar, necesitara poner su dirección IP si esta es dada dinámicamente.

Si desea utilizar otro programa terminal para marcar al servidor, no olvide emitir AT&D0 ó deshabilitar DTR cuando salga del programa. Intente enviar ping a una dirección IP de host conocida para ver que todo funcione.

3.3.6.- Problemas con el internal SLIP.

Cheque su relación de baudio...

Si su hardware maneja variaciones con un módem externo, asegúrese de que el cable está correctamente conectado.

Por default, todos los marcados deben ser realizados con 8 bits, sin paridad. Esto podía no funcionar para usted...

Una vez que tenga determinada la secuencia de entrada, podrá iniciar un login script. Muchos proveedores de Internet pueden tener su propio script para conectarse a sus sistemas.

3.3.7.- Utilizando Trumpet Winsock con manejadores de paquetes.

Primeramente, por si no conoce que es un manejador de paquetes, esta es una pieza pequeña del software el cual se coloca entre la tarjeta de red y su programa de TCP. Este provee una interface estándar con la cual muchos programas pueden utilizarse de manera similar a las llamadas al BIOS utilizando interrupciones de software.

¿Porqué es llamado un manejador de paquetes?. Esto es porque las redes modernas envían la información utilizando paquetes de información en lugar de enviar la información por byte ó por carácter a la vez. Por ejemplo, Ethernet envia la información en paquetes de hasta 1514 bytes de longitud. La razón de enviarlos por paquetes es que la información puede ser transmitida mucho más eficientemente en paquetes.

El centro del concepto de manejo de paquetes es un vector el cual es utilizado para comunicarse con este. La familia de los procesadores 80x86 permite a los programas comunicarse con el sistema operativo a través de lo que llaman "interrupciones de software", la cual siempre tiene un número en el rango de 0 a 255. Este es determinado como "vector" y es uno de los mecanismos para pasar el control al sistema operativo MS-DOS. Usualmente los vectores son expresados en hexadecimal, con un rango de 0x00 a 0xFF. El 0x al principio del número significa que estamos utilizando números hexadecimales en lugar de decimales. Estos también pueden ser expresados en la notación de 00H a FFH, ó $00 a $FF. Si esta tratando con manejadores de paquetes, la notación hexadecimal es mucho más común, pero ocasionalmente esta también es expresada en decimal. Ejemplos de interrupciones de software en uso en las PC son 0x10 para el BIOS del vídeo, ó 0x21 para llamadas a DOS.

Manejadores de paquetes son solamente permitidos para tener un vector de interrupción de software en el rango de 0x60 a 0x7F. Normalmente, puede seleccionar 0x60 como el lugar de default para instalar su manejador de paquetes, pero ciertas configuraciones de máquinas pueden hacer al vector inoperable. Simplemente escoja uno que este libre - el manejador de paquetes deberá decirle si puede utilizar este ó no.

El Trumpet Winsock también utiliza un manejador de paquetes virtuales especiales "wrapper" el cual habilita a su manejador de paquetes para que pueda funcionar correctamente en Windows. Mientras que el manejador de paquetes es una forma eficiente para comunicarse con su tarjeta de red, este podía no trabajar correctamente desde Windows sin una pequeña ayuda. El programa "WINPKT" fue escrito por algunas personas astutas en la Internet para permitir al manejador de paquetes el trabajar correctamente dentro de Windows asegurándose de que los paquetes vayan directamente a la "máquina virtual" correcta bajo Windows en modo mejorado. Una "máquina virtual" puede ser tanto en sesión de Windows ó en cualquier sesión de DOS activa dentro de Windows. Para más detalles refiérase a la documentación del sistema Windows.

En adición a esto, puede necesitar tener algunos sobreentendidos de vectores IRQ y direcciones I/O que pueden ser relevantes para instalar su tarjeta de red.

¿De donde obtengo un manejador de paquetes?

En estos días, los manejadores de paquetes son usualmente proporcionados con las tarjetas de red, otra forma son las colecciones de manejadores de paquetes de dominio público que pueden ser obtenidas desde uno llamado "Crynwr Packet Driver Collection"

3.4.- Herramientas de Internet .

3.4.1.- Gopher.

Gopher.- El cliente de Internet Gopher es utilizado para buscar y recibir archivos desde el servidor Gopher desde cualquier lugar de la Internet. Esto es debido a un servicio de entrega de documentación distribuida. El servidor Gopher almacena archivos que contienen texto ó datos binarios, información de directorios, imágenes ó sonido. Los enlaces a otros servidores Gopher resultan de la cooperación de las redes amplias para formar el web de Gopher global, frecuentemente llamado el Gopherspace.

El cliente de Gopher también provee gateways ó enrutamiento a otros sistemas de información (World-Wide Web, WAIS, archie, WHOIS) y para servicios de red (Telnet, FTP). Gopher es frecuentemente la forma más conveniente de navegar en un directorio FTP y bajar archivos.

El cliente de Gopher presenta la información al usuario como una serie de submenues (reensamblando la organización de un directorio dentro de muchos subdirectorios y archivos). Sin embargo, los subdirectorios y los archivos pueden ser localizados tanto en el servidor local del Gopher ó en un servidor Gopher situado en un sitio remoto. No importando que tan lejos este la información, todos los términos de esta son presentados en un menú que aparenta que vienen de un mismo lugar. Cliente de Gopher de dominio público están disponibles para: MS-DOS, MS-Windows, OS/2 Macintosh, CMS,VMS, NeXT, Unix, X-Windows. Los clientes están disponibles por FTP anónimos.

Si no tiene un cliente Gopher es su máquina, puede utilizar un cliente remoto de Gopher vía una sesión de Telnet ó por correo electrónico a un sitio GopherMail. Para accesar a un cliente remoto de Gopher, realice una sesión de Telnet a cualquiera de estos sitios:

info.anu.edu.au	Australia (login: info)
tolten.puc.cl	Columbia
ecnet.ec	Ecuador
gopher.chalmers.se	Sweden
consultant.micro.umn.edu	USA
gopher.uiuc.edu	USA
panda.uiowa.edu	USA (login: panda)

En el login: teclear gopher (a menos de que se especifique otra cosa) y un menú principal se desplegara. Un cliente de gopher se ve diferente en diferentes plataformas, puesto que estos toman ventaja de las disponibilidades de la plataforma (mouse, funciones gráficas, sistemas X-Windows). Sin embargo todas las implementaciones ofrecen el mismo juego de funciones y comandos.

Después de emitir un comando de gopher, estará automáticamente conectado a un servidor gopher de default el cual fue especificado cuando su software de cliente fue instalado. El cliente de Gopher presenta una interface de manejo de menú simple que no requiere ningún conocimiento especial por parte del usuario. Este es un ejemplo de un menú:

Internet Gopher Information Client v2.0.12

Information About Gopher

1. About Gopher.
2. Search Gopher News <?>
3. Gopher News Archive/
4. comp.infosystems.gopher (Usenet newsgroup)/
5. Gopher Software Distribution/
6. Gopher Protocol Information/
7. University of Minnesota Gopher software licensing policy.
8. Frequently Asked Questions about Gopher.
9. gopher93/
10. Gopher| example server/
11. How to get your information into Gopher.
--> 12. New Stuff in Gopher.
13. Reporting Problems or Feedback.
14. big Ann Arbor gopher conference picture.gif <Picture>

Press ? for Help, q to Quit, u to go up a menú Page: 1/1

Cualquier termino puede ser seleccionado del menú tecleando su número de linea, luego presionando la tecla de RETURN, ó moviendo el cursor (—>) en los términos y presionando RETURN. Cada término en el menú puede ser:

* un subdirectorio
* un archivo de texto
* un archivo binario
* un archivo de sonido
* un archivo de imagen
* un libro de teléfonos (información de directorios)
* una búsqueda de índices
* una sesión de Telnet

Los términos en los gopher pueden tener un símbolo de identificación seguido de estos. En el ejemplo, "<?>" significa un completo indice de búsqueda de texto, "/" significa un subdirectorio, "<Pictures>" significan un archivo de imágenes y los que no tienen símbolo por lo general son archivos de texto. Algunos clientes de Gopher no están disponibles para manejar ciertos tipo de archivos (p.ej. archivos de sonido), y algunos clientes despliegan solamente archivos de tipos que ellos pueden manejar ó archivos de los que se supone se esta interesado. Otros despliegan todos los tipos de archivos.

Cuando un termino es seleccionado desde el menú Gopher, este es procesado de acuerdo a su tipo. Si selecciona un término el cual representa un archivo de sonido, una imagen ó una sesión de Telnet, el cliente de gopher determinará el software apropiado es su computadora para visualizar la imagen,

reproducir el sonido ó inicial una sesión de Telnet. Cuando la tarea sea completada, el control es regresado al cliente de gopher. En cualquier tiempo es posible terminar la sesión (quit), para cancelar el proceso actual (el comando que realiza esta función varia dependiendo del cliente del gopher instalado) ó también se puede pedir ayuda (help).

Muchos clientes de gopher le permiten guardar una extracción de la localización exacta de los términos de gopher que considera que utilizará más frecuentemente, almacenando la información en una serie de marcas de libro ó "bookmarks".

3.4.2.- VERONICA.

VERONICA.- Este le ayuda a encontrar información basada en Gopher sin tener que hacer una búsqueda de menú por menú ni de sito por sitio. Este provee una búsqueda de palabras para más de 500 menúes de gopher. Veronica no tiene que ser iniciada como otra conexión ó aplicación, este es accesible desde el nivel más alto del menú gopher ó desde otros servidor gopher. Cuando escoger una búsqueda por veronica le preguntara que introduzca una palabra. Una forma simple de buscar con veronica es introducir una simple palabra y presionar RETURN. No importa si la palabra fue escrita con mayúsculas ó minúsculas. El servidor de veronica regresa un menú de gopher compuesto de los términos cuyos títulos coinciden con la palabra especificada. Los términos pueden ser accesados como un menú de gopher.

3.4.3.- World-Wide Web.

World-Wide Web.- También llamado WWW ó W3) es un sistema de información basado en hypertexto. Cualquier palabra en un documento hypertexto puede ser especificada como un puntero hacia un documento de hypertexto diferente donde puede ser encontrada información perteneciente a la palabra seleccionada. Los lectores pueden abrir un segundo documento seleccionando la palabra , utilizando diferentes métodos, dependiendo de la interface; en un sistema basado en el mouse como lo es el Windows, bastará con hacer click en la palabra y así solamente la parte del documento enlazado la cual contiene información relevante se desplegará.

El segundo documento mostrado podría contener por si mismo enlaces a documentos futuros. Los lectores no necesitan conocer donde esta el documento referenciado, puesto que este puede ser obtenido y presentado como sea necesitado. El World-Wide Web utiliza hypertexto sobre la Internet: los documentos enlazados pueden ser localizados en diferentes sitios de la Internet.

El World-Wide Web también provee acceso a muchas de las otras herramientas de Internet y se esta volviendo ampliamente utilizado para convertirse en el principal acceso a los recursos de Internet. Debe de estar en la red TCP/IP internacional (la Internet) para que su computadora pueda accesar como cliente a los WWW de dicha red. Se encuentra en la red pero no tiene un cliente de WWW en su máquina, puede de todas formas entrar al World-Wide Web puesto que varios sitios ofrecen un acceso interactivo público para cliente de WWW.

Los usuarios accesan al World-Wide Web fácilmente vía un cliente llamado un navegador ó browser, el cual provee un acceso transparente hacia el servidor WWW. Para accesar desde un cliente remoto de WWW, haga un telnet hacia el sitio del cliente. Si es nuevo en el WWW, el telnet lo deberá hacer hacia info.cern.ch. No necesita una clave para esto y entrara inmediatamente al WWW en modo de navegador.

Muchos clientes remotos están es sitios con servidores WWW reteniendo información en áreas especificas. Haga un Telnet al sitio del cliente y en la clave ponga www, no necesita password.

3.4.4.- WAIS.

WAIS.- Servidor de información de área amplia, es una base de datos conteniendo muchos documentos basados en texto (puesto que WAIS puede contener sonido, fotos ó video). La base de datos de WAIS se refiere a la fuente. Las bases de datos pueden ser organizadas en diferentes formas, utilizando varios sistemas de base de datos, pero la ventaja es que el usuario no requiere aprender ó saber el lenguaje de peticiones para las diversas bases de datos. El cliente de WAIS utiliza un lenguaje natural de petición para encontrar documentos los cuales contienen la palabra buscada. La base de datos de WAIS están disponibles para cualquier generó.

Son muchos los servidores de WAIS a través de la red. La base de datos de los directorios de servidores esta disponible en varios sitios, los cuales pueden ser pedidos para encontrar que base de datos esta disponible para un tema en particular. El directorio de bases de datos de los directorios de los servidores esta también disponible via un ftp anónimo hacia ftp.wais.com bajo el directorio /pub/directory-of-servers.

Las interfaces de los clientes difieren significativamente en las diferentes plataformas, pero las peticiones ó búsquedas son realizadas de la misma forma no importando la interface en uso.

* Paso 1: El usuario selecciona un juego de bases de datos a ser buscadas.
* Paso 2: El usuario formula una petición que consiste de una palabra a ser buscada.
* Paso 3: Cuando la petición esta corriendo, WAIS pregunta por la información en cada base de datos seleccionada.
* Paso 4: Las lineas de documentos que satisfacen la petición son mostradas. El documento seleccionado contiene la palabra pedida y unos paréntesis. Seleccione el documento de acuerdo al número de coincidencias.
* Paso 5: Para recibir un documento, el usuario simplemente lo selecciona de la lista de resultados. El cliente de WAIS recibe el documento y muestra su contenido en la pantalla.
* Paso 6: Si no fueron suficientes los documentos encontrados, el usuario puede declarar una pregunta diferente.
* Paso 7: Una búsqueda futura podrá verse para documento los cuales tengan un gran número de palabras en común con el documento seleccionado.

3.4.5.- ARCHIE.

ARCHIE.- Es un servicio el cual le ayuda al usuario a localizar archivos y directorios en servidores FTP anónimos de cualquier parte de la Internet. Administradores de todo el mundo registran servidores FTP anónimos con el servicio de archie; una vez al mes el servicio archie corre un programa el cual escanea los directorios y nombres de archivos contenidos en cada uno de los servidores FTP registrados, y genera una gran lista de todos los archivos y directorios contenidos en todos los servidores registrados. Más de 1000 sitios anónimos de FTP se presentan en estas listas, la cual es referenciada como la base de datos de archie. La base de datos archie actualmente contiene más de 2,100,000 nombres de archivos.

La base de datos archie esta disponible en varios servidores archie y en la cual todos contienen la misma información. Los administradores también pueden proveer una pequeña descripción del paquete de software contenidos en los archivos ó directorios de su sitio.

Los archivos están disponibles en sitios FTP anónimos conteniendo paquetes de software para varios sistemas (MS-Windows, MS-DOS, Macintosh, Unix, etc.), utilerias, información ó documentación, listas de correo ó archivos de discusión de grupos Usenet. En muchos sitios FTP, los recursos son organizados en directorios y subdirectorios. La base de datos archie contiene tanto la ruta del directorio y el nombre del archivo.

La base de datos archie esta disponible para todos los usuarios de la Internet, y puede ser accesada también vía correo electrónico.

Son tres formas de poder accesar la base de datos archie: vía un cliente local, una sesión interactiva de Telnet ó con un correo electrónico. Las reglas para poder accesar archie son básicas:

* evitar conectarse durante horas de trabajo; muchos de los servidores archie no son máquinas dedicadas-también tiene funciones locales.
* hacer sus preguntas lo más especificas posibles; la respuesta puede ser más rápida y corta.
* la interface de usuario instalada en su máquina le ayuda a reducir el cargado en el sitio del servidor, utilice esta.
* utilice el servidor archie más cercano a usted y en particular, no cruce por lineas trasatlánticas.

Accesando desde un cliente local, puede realizarse desde una interface gráfica (GUI), la cual lo puede habilitar para que active la funciones de archie desde el mouse. Un cliente que no esta en interface gráfica requiere que se teclee el comando de archie. Si se omiten los parámetros una lista de posibilidades le serán mostradas con una pequeña descripción de cada uno.

El resultado es una lista de sitios FTP con sus direcciones las cuales contienen archivos ó directorios los cuales coinciden con el argumento, junto con el tamaño del archivo, la fecha de la última modificación y su directorio. Por default esta lista es ordenada por dirección de host.

Puede también utilizar una sesión de Telnet para conectarse a un servidor archie interactivamente. En el acceso teclee: archie. El sistema lo dejará en prompt de archie> indicando que el servidor esta listo para las peticiones del usuario.

Los usuarios que están limitados a la conectividad vía correo electrónico pueden también accesar a los servidores archie. La interface de correo electrónico hacia un servidor archie reconoce una serie de comandos que igualmente se utilizan con Telnet.

Los comandos de archie son puestos en la parte del cuerpo de un mensaje de correo ó sea, donde se escribe el mensaje principal. Las lineas de comandos comienzan en la primera columna; todas las líneas que no coincidan con un comando válido serán ignoradas.

3.4.6.- HYTELNET.

HYTELNET.- Es un sistema browser de hypertexto cuyas bases de datos contienen direcciones de sitios de Internet las cuales pueden ser alcanzadas vía Telnet (estas incluyen librerías, sistemas de información, Gopher, WAIS, WWW y Freenets), información sobre Telnet por el mismo,

información sobre el uso de librerías de catálogos y un glosario de Internet. La base de datos es bajada y almacenada localmente para asi poder añadir información nueva a la versión local de la base de datos, quizás para incluir nuevos sitios ó alguna información de ayuda local. Una versión de html de la base de datos Hytelnet esta ahora disponible en servidores World-Wide Web.

Es claramente importante poseer la versión más actualizada de las bases de datos, los usuarios se encuentran en una lista de correo electrónico la cual les informa de una nueva versión del programa Hytelnet, y también sobre cambios y adiciones a los archivos de la base de datos.

Comandos añadidos en el sistema Hytelnet lo hacen más fácil de utilizar para iniciar sesiones Telnet en sitios seleccionados desde la base de datos. Existen versiones de Hytelnet para Unix, IBM PC y computadoras Apple Macintosh las cuales están conectadas a la Internet (red TCP/IP). Hytelnet es usado normalmente como un sistema local, pero la versión de Unix esta disponible para prueba vía Telnet a access.usask.ca, con el login de hytelnet (todo con minúsculas y no requiere password). La versión WWW de la base de datos puede ser vista en la URL:http://www.cc.ukans.edu/hytelnet_html/START.TXT.html. Esta versión de la base de datos puede ser bajada a un servidor WWW local utilizando el URL http://www.cc.ukans.edu/hytelnet_html.tar.Z. Los archivos que constituyen un sistema Hytelnet local están disponibles vía FTP anónimo a ftp.usask.ca,en el directorio de /pub/hytelnet. Los archivos de la base de datos, para utilizarse con todas las versiones de software están incluidas en el directorio conteniendo la versión IBM PC. La base de datos Hytelnet es constantemente actualizada con nuevos sitios los cuales se añaden regularmente.

3.4.7.- WHOIS.

WHOIS.- El servicio WHOIS provee una forma de encontrar direcciones de correo electrónico, direcciones postales y números de teléfonos de usuarios de la red. Este puede también entregar información sobre la red, organizaciones de redes, dominios y sitios. Este servicio fue originalmente llamado NICNAME, pero ahora WHOIS es ampliamente utilizado.

La Internet Registration Service mantiene una base de datos importante de información de redes, la base de datos InterNIC. El nombre de los contactos administrativos y técnicos para el registro de dominios es automáticamente introducido en la base de datos cuando el dominio ó el número IP es procesado por la autoridad coordinadora de Internet. Cada entrada de la base de datos tiene un manejador, un identificador único, un nombre, un tipo de grabación y otros varios campos dependiendo del tipo de grabación.

Antes de Abril 1, 1993, La Network Information Center (NIC) de la Defense Data Network (DDN) fue la autoridad coordinadora de Internet y esta mantenía una base de datos conocida como la base de datos NIC. La base de datos NIC esta ahora restringida para información sobre el dominio .mil. Sitios individuales de Internet también mantienen bases de datos conteniendo información sobre otros sitios. Muchos sitios académicos mantienen sus propias bases de datos con información sobre sus miembros y estudiantes.

La información mantenida es esas bases de datos esta disponible por servidores WHOIS los cuales reciben peticiones de clientes WHOIS, utilizando el protocolo WHOIS, se busca en la base de datos y luego se envia de regreso la información. La implementación actual de WHOIS tiene sus limitaciones lo cual significa que no es eficiente al tratar con un volumen de información grande y numerosas peticiones: los varios servidores WHOIS no tienen conocimiento de cada otro, una base de

datos es mantenida en cada sitio del servidor y finalmente nuevas funcionalidades han sido implementadas localmente en varios sitios y no son propagadas a otros. Un nuevo protocolo extendido **WHOIS++**, se ha especificado. este incluye varias mejoras locales para el servicio **WHOIS**, las cuales pueden ser la mejora en la sintaxis de preguntas y su arquitectura que permita un servicio de directorios distribuido real para la Internet entera.

WHOIS esta actualmente disponible para todos los usuarios de la red TCP/IP (la Internet). Los servidores **WHOIS** pueden ser accesados utilizando un cliente **WHOIS** local, el cual puede interactuar con el servidor a través de la Internet ó vía una sesión de Telnet interactiva. En adición, la InterNIC ofrece una interface de correo electrónico para la base de datos que es mantenida.

Los servidores **WHOIS** solamente deberán ser utilizados para emitir preguntas en relación a información especifica. No es usualmente aceptable hacer una serie extendida de preguntas para asi obtener una sección grande de directorios.

Una lista de sitios **WHOIS** esta disponible vía FTP anónimo de rtfm.mit.edu en el archivo /pub/whois/whois-servers.list. Cada servidor **WHOIS** individual ofrece información sobre la organización a la cual pertenece: este no comparte un directorio común con otros servidores **WHOIS** y no conoce donde encontrar información sobre otras instituciones. El servicio de **WHOIS** esta documentado en un Request For Comment de Internet (RFC 1400).

3.4.8.- X.500.

X.500.- Es un protocolo el cual especifica un modelo de servicios de directorios localmente conectados para formar un directorio global distribuido. La base de datos local retiene y mantiene una parte de la base de datos global y la información de directorio esta disponible vía un servidor local llamado un Directory System Agent (DSA). El usuario recibe la entrada de directorios para ser accesada desde el servidor local. X.500 también supone funciones de administración de datos (adición, modificación y borrado de entradas).

Cada termino (entrada) en el directorio X.500 describe a un objeto (p.ej. a una persona, un recurso de la red, una organización) y tiene un identificador único llamado el Distinguished Name (DN) ó nombre distinguido. Las entradas consisten de una colección de atributos (p.ej. para una persona esta puede ser su último nombre ó apellido, nombre de la organización, dirección de correo electrónico). Las entradas se encuentran navegando a través del Directory Information Tree (DIT) ó árbol del información del directorio. En lo alto del árbol esta el mundo, el cual subdivide a los siguientes niveles por países, los siguientes son las organizaciones. La información de gentes, recursos, etc., esta almacenada dentro de las organizaciones.

Puesto que mucha de la información disponible hoy en día vía X.500 es sobre gente y organizaciones, el diseño de directorios X.500 esta también disponible para almacenar información sobre otras entidades (u objetos), tales como recursos de red, aplicaciones ó hardware. Varios proyectos utilizan esa disponibilidad de directorio (p.ej. los RFC de Internet (Request For Comments) están listados en el directorio global). X.500 es un protocolo OSI (Open System Interconnection), el cual fue nombrado por ser el número consecutivo para las recomendaciones que emite la CCITT(comité consultivo internacional de telegrafía y telefonía).

Puesto que X.500 es parte de la definición estándar de OSI, el acceso a OSI no es necesario para utilizar servicios de directorio. Muchos servicios de X.500 están disponibles tanto en la Internet

como por correo electrónico. Existen tres formas de accesar a los servicios X.500: vía un cliente local, vía una sesión interactiva (Telnet ó acceso X.25) a un cliente remoto ó por correo electrónico. En adición, herramientas de red tales como WWW y Gopher proveen acceso a servicios de directorio X.500 a través de gateways.

X.500 es utilizado principalmente para buscar información sobre la gente (dirección postal, número de teléfono, dirección electrónica, etc.) Los campos de base para la búsqueda son el nombre de la persona, el nombre de la organización de la persona (y departamento dentro de la organización) y el pais.

En el mundo de X.500, un cliente local es llamado un Directory User Agent (DUA) ó agente usuario de directorio. Los dominios públicos y comerciales de los DUA están disponibles para numerosas plataformas extendiéndose desde mainframes hasta computadoras personales. El rango existe desde comandos en linea simples basados en cliente hasta cliente basados en sofisticadas interfaces de usuario gráficas las cuales requieren dispositivos apuntadores. Para una comprensible lista de DUA, su descripción y donde encontrarlos, consulte la documentación Internet RFC 1292 / FYI 11 - A Catalog of Available X.500 Implementations. (Un catalogo de implementaciones X.500 disponibles).

Los DUA provistos por un sitio remoto pueden tener interfaces de usuario orientadas a manejo de menú, en línea, ó sistemas basados en X Window, ejemplos de cada uno son dados a continuación:

* orientado a línea: de, dish, fred
* manejador de menú: sd (formalmente conocido como widget)
* Sistemas X Window: Xdi, Xlookup (ó xlu), pod

La disponibilidad de estos rangos de DUA esta desde la facilidad de búsquedas básicas hasta una funcionalidad de X.500 completa. Para usuarios novatos es recomendado intentar con de (directory enquiries) puesto que este tiene una interface de usuario muy simple. de fue diseñado como un DUA de acceso público y esta accesible desde cualquier tipo de terminal. Este soporta las funciones básicas de X.500: lectura, búsqueda y listado.

Cuando "de" es invocado, le es pedido que llene en cuatro campos la petición especifica. En todos los campos, el valor desde la petición previa es el valor de default. Presione RETURN para aceptar este ó introduzca un nuevo valor. Todas las búsquedas son con minúsculas. Los cuatro campos a llenar son:

Nombre personal
Nombre del departamento
Nombre de la organización
Nombre del pais

La organización de redes noruega (UNINETT) ofrece una interface de correo electrónico para X.500. Para utilizar esta, envié un correo a: Directory@UNINETT.NO con la palabra a encontrar en el campo de Subject:. La parte del cuerpo del mensaje contiene las peticiones de búsqueda, una por mensaje. Un archivo de ayuda es regresado si el cuerpo del mensaje contiene la palabra ayuda. Existen varios documentos relacionados con X.500:

RFC 1292 A Catalog of Available X.500 Implementations,

RFC 1308 Executive Introduction to Directory Services Using the X.500 Protocol,

RFC 1309 Technical Overview of Directory Services Using the X.500 Protocol.

La fuente oficial de información en X.500 es la recomendación X.500 publicada por el CCITT (Libro Azul, Volumen VIII - Fasciculo VIII 8, Data Communication Networks Directory, Recomendación X.500-X.521, CCITT, 1988, ISBN 92-61-03731-3). Este documento también esta disponible por correo electrónico: enviar el comando GET ITU-5233 para itudoc.itu.ch ó vía gopher en gopher.itu.ch.

3.4.9.- NETFIND.

NETFIND.- Esta utileria provee una simple facilidad de directorio de paginas blancas. Este da el nombre de una persona en la Internet y una descripción aproximada de donde trabaja la persona, Netfind intenta localizar su teléfono y la información de su buzón de correo electrónico de la persona. Esto lo realiza utilizando una base de datos de dominios y host en la red. Se puede utilizar el primer nombre, el último ó su login name de la persona.

Si la persona empezada a buscarse esta en un sitio al cual no esta directamente conectado a la Internet (p.ej. el sitio esta conectado solamente a través de un gateway enviador de correos), Netfind informara al usuario que la persona no puede ser encontrada.

Netfind utiliza el protocolo de Internet SMTP y finger. Debido a la naturaleza dinámica del procedimiento de búsqueda de Netfind y las variaciones en la disponibilidad de la Internet, se pueden obtener resultados diferentes de una misma búsqueda en diferentes ocasiones.

Deberá estar en la red Internacional TCP/IP (la Internet) para poder utilizar el Netfind. No es posible un acceso por correo electrónico hacia Netfind. El software esta actualmente disponible solamente para Sun corriendo SunOS 4.0 ó posteriores.

Netfind requiere el nombre de una persona, indicar donde trabaja la persona; este entonces buscará en su base de datos para encontrar el domino al cual coincida con lo especificado. Si se coinciden con más de un dominio, Netfind desplegará la lista de dominios que coinciden y preguntara para que se seleccionen hasta tres para buscar. Si se coinciden con más de 100 dominios, Netfind listara algunos de los dominios coincidentes /organizaciones y pedirá que se formule una búsqueda más especifica. Puede utilizar cualquiera de las partes de un nombre de organización (ó cualquiera de los componentes de este nombre de dominios) como claves en la búsqueda. Utilizando más de una clave implica una lógica AND de las claves. Especificando demasiadas claves puede causar que la búsqueda falle.

Cuando la búsqueda esta completada (ó interrumpida), Netfind hace un sumario de los resultados de la búsqueda. Este sumario incluye problemas al buscar dominios remotos, información sobre los más buscados e información sobre donde y cuando la persona acceso por última vez. Si más de una persona es localizada por una búsqueda, el sumario no incluye información sobre los correos electrónicos de estos ni su más reciente/actual acceso. El formato de petición es:

El nombre, el cual puede ser el primero, el último ó su login name (solamente puede ser especificado uno) de la persona a buscarse.

El lugar, el cual describe donde trabaja la persona, dando el nombre de la institución ó la ciudad/estado/país. Si conoce el nombre del dominio de la institución (p.ej. cs.colorado.edu, donde el nombre del host es brazil.cs.colorado.edu) puede especificar la dirección de dominio como una palabra, omitiendo los puntos (p.ej. cs colorado edu). La parte de host del nombre del dominio (p.ej. brazil) no puede ser utilizada como palabra. Las palabras no son sensitivas a mayúsculas ó minúsculas y pueden ser especificadas en cualquier orden, puesto que utilizan una muy común tecla primero podrá causar que el buffer interno se sobrellene y que alguno dominios se pierdan.

Utilizando más de una clave implica la lógica "and" de las claves. Especificando demasiadas claves puede causar que las búsquedas fallen. Si esto sucede, intente especificando pocas claves.

La versión de acceso remoto de Netfind tiene una sección grande de ayuda. También existe un juego de preguntas comunes con el software relacionado, en el directorio Doc. Estas preguntas cubren Funcionalidad, Metodología, Cargado en red y sitios remotos, Privacidad, Dirección futura y Trabajos relacionados.

3.4.10.- TRICKLE.

TRICKLE.- Provee una fácil y rápida alternativa al FTP, si esta ó no con acceso a la Internet. TRICKLE trabaja con un número de sitios FTP anónimos (computadoras en la red Internet que permites un acceso público y recobran software y archivos) para distribuir archivos en peticiones ó por subscripción.

Son varios los servidores TRICKEL a través del mundo y estos cooperan para distribuir archivos eficientemente. El usuario pide un archivo emitiendo un comando al servidor TRICKLE más cercano, el cuál lo envia a su cache de disco local, ó desde un sitio FTP el cual contiene el archivo. Si esta subscrito a un particular archivo ó directorio, podrá recibir un sumario semanalmente de los archivos que hayan sido añadidos al directorio al que esta subscrito.

Cualquiera con acceso a correo electrónico puede utilizar TRICKLE. Usuarios de EARN/Binet pueden utilizar mensajes interactivos (tales como TELL ó SEND) para entregar sus comandos a TRICKLE. Cuando envíe un comando a un servidor TRICKLE, este a su vez ejecuta un comando ó le envia un mensaje con la dirección del servidor TRICLE para su área.

Los archivos que están disponibles en TRICKLE están organizados en directorios principales los cuales contienen muchos subdirectorios. La misma estructura de directorio es utilizada en todos los servidores TRICKLE. Estos son algunos de los principales directorios utilizados actualmente:

Directory	Source FTP Site	Contents
MSDOS	oak.oakland.edu	Large MS-DOS software archive
MISC	oak.oakland.edu	Software for VM, VMS, Unix
SIGM	oak.oakland.edu	SIG/M CP/M archive
PC-BLUE	oak.oakland.edu	PC-BLUE MS-DOS archive
CPM	oak.oakland.edu	CP/M Software Archive
ARCHIVES	oak.oakland.edu	Various discussion group archive

| UNIX-C oak.oakland.edu Unix and C code software archive
| MACINTOS oak.oakland.edu Macintosh software archive |
| OS2 ftp-os2.nmsu.edu Large archive of OS/2 software
| AMIGA nic.funet.fi Large Amiga collection |
| KERMIT watsun.cc.columbia.edu Kermit network software |
| TEX rusinfo.rus-uni-stuttgart.de TeX software and fonts
| WUARCHIVE wuarchive.wustl.edu MS-DOS and others |
| EXPO-MIT export.lcs.mit.edu Unix and others |
| UUNET ftp.uu.net Unix and others |
| SUMEX-AIM sumex-aim.stanford.edu Macintosh and others |
| GARFIELD garfield.catt.ncsu.edu Multimedia (pictures and sounds)
| X11 export.lcs.mit.edu X-Windows software distribution
| LINUX nic.funet.fi Linux system software distribution
| VM-CMS ubvm.cc.buffalo.edu VM/CMS utilities |
| |
+---+

No todos los directorios están disponibles en todos los servidores. Si su servidor no provee el directorio que usted escogió, puede utilizar cualquier otro TRICKLE para encontrarlo. Si su servidor esta temporalmente cerrado, también puede utilizar otro en su lugar.

Los comandos de TRICKLE deberán ser colocados en el cuerpo del mensaje de correo, un comando por línea. Cualquier número de comandos (hasta su límite diario de comandos) pueden ser colocados en un mensaje. El número de mensajes que tiene permitido por día esta definido por el administrador del servidor. Este es comúnmente de entre 25 a 50 comandos. Todos los comandos comienzan con (/). Si esta suscrito a un directorio, podrá recibir un sumario mostrando cuales archivos han sido añadidos a este. El sumario podrá llegar uno por semana, dependiendo de como sea la actividad en el sitio FTP y podrá mostrar el nombre, tamaño y fecha de cada archivo añadido. Si esta suscrito a un archivo, una nueva copia del archivo puede ser enviada tan pronto como su servidor TRICKLE sea informado de que una nueva versión del archivo ha sido almacenada en su sitio FTP.

El comando /HELP puede ser envía a cualquier servidor TRICKLE, el cual regresara una muy detallado archivo de ayuda. Una guía breve de TRICKLE esta disponible de la lista de archivos de documentación de EARN. Envíe un correo a LISTSERV@EARNCC.EARN.NET. ó LISTSERV@EARNCC.BITNET. En el cuerpo del mensaje escribir: GET TRICKLE MEMO.

3.4.11.- BITFTP.

BITFTP.- Este provee una interface de correo entre usuarios de EARN, Bitnet y redes asociadas y sitios FTP en la Internet. Los comandos son especificados por el usuario en el mensaje de correo y pasados a un servidor BITFTP el cual realiza la conexión al sitio FTP. Cuando el servidor termina la interacción con el sitio FTP ó esta falla debido a un error, una transcripción del resultado es enviado de regreso al usuario, junto con el archivo pedido, si este existe.

El formato en el cual los archivos serán enviados hacia el usuario puede ser definido dentro del mensaje. BTFTP esta disponible solamente para usuarios de EARN, Bitnet y otras redes NJE regionales. Para entrar al usuario le es pedido que entre al servidor más cercano a el. Si no sabe cual es, puede enviar su mensaje a BITFTP@BITFTP (en EARN/Bitnet) y este lo enviara al servidor

BITFTP correcto. BITFTP acepta peticiones vía correo electrónico, incluyendo mensajes de IBM NOTE y formatos PROFS así como transferencia de archivos NJE.

BITFTP implementa un gran número de comandos FTP del TCP/IP de IBM para VM, utilizando la misma sintaxis. Este software esta documentado en el manual de User's Guide de IBM TCP/IP para VM. BITFTP no soporta múltiples peticiones de archivos (el comando mget), tampoco soporta el enviado de archivos a sitios FTP (el comando put). Debe utilizar el comando ftp para especificar el host al cual se conectara. Este debe de ser su primer comando en su archivo de correo. Puede especificar el formato en el que quiere que BITFTP utilice para enviarle los archivos. Una guía para los servicios de BITFTP puede ser obtenida enviando un correo con el comando help al servidor BITFTP. Información adicional puede ser encontrada en por NETHELP@EARNCC.EARN.NET (ó NETHELP@EARNCC.BITNET). La información sobre TCP/IP y FTP en general puede ser obtenida de varias fuentes.

3.4.12.- LISTSERV.

LISTSERV.- Es una lista de distribución para administración de paquetes. El servidor LISTSERV mantienen una lista conteniendo nombres y direcciones de correos electrónicos de las computadoras de los usuarios. Cualquier miembro de una lista puede enviar mensajes de correo electrónico direccionados a la lista, la cual el servidor enviara a todos los otros miembros de la lista. Este servicio provee un significado conveniente para el intercambio de ideas e información entre los miembros de una lista. Existen muchas listas diferentes, las cuales contienen usuarios los cuales comparten intereses particulares. Los servidores de LISTSERV pueden grabar un archivo de trafico de correo, almacenar todos los mensajes asociados con sus listas y buscar en sus bases de datos archivos. Este sistema utiliza los recursos de las computadoras y redes de manera eficiente.

Cualquiera que pueda enviar un correo electrónico, conforme al estándar RFC822 a una dirección EARN/Bitnet y que tenga una dirección de correo propia puede utilizar LISTSERV. Cada día, la gente utiliza LISTSERV desde HEPnet, Internet, CompuServe, MCIMail y muchas otras redes a través de todo el mundo. LISTSERV corre en sistemas IBM VM/CMS en la red Internacional NJE (EARN/Bitnet).

Los comandos de LISTSERV son enviados en un mensaje de correo a el servidor LISTSERV@host-id, donde host-id es la dirección NJE de su computadora ó su nombre de dominio de Internet. LISTSERV ignora el Subjet: la línea de la cabecera del correo, por los que sus comandos deben estar en el cuerpo del mensaje. Se pueden poner varios comandos en el mensaje, pero cada uno separado por una línea. También puede enviar mensajes interactivos, este es el más conveniente y más rápido método para usarse. Esto solamente funcionara cuando este activo el enlace entre su computadora y el LISTSERV, si el mensaje falla puede enviar su comando via correo.

La forma más eficiente de utilizar LISTSERV es direccionar un correo al LISTSERV en el cual exista el host que se intenta conectar. Sin embargo si se quiere suscribir a una lista, pero no conoce en cual servidor esta, puede utilizar el nodo de computadora especial de LISTSERV en la red EARN/Bitnet ó LISTSERV.NET en muchas otras redes y esta enviara su mensaje al servidor correcto. Estos son algunos servidores LISTSERV disponibles:

Host Computer Site	Country

EARNCC	EARN Office, Paris	France
DEARN	GMD, Bonn	Germany
HEARN	Katholieke Universiteit Nijmegen	Netherlands
SEARN	Kungliga Tekniska Hoegskolan, Stockholm	Sweden
BITNIC	BITNET Network Information Center	USA
PUCC	Princeton University, New Jersey	USA

LISTSERV provee comandos especiales para administración de las listas, a los cuales se les da unos privilegios especiales en el orden de uso. Los servidores LISTSERV pueden proveer de un rango diverso de información para uso general, incluyendo archivos de ayuda. Las peticiones de información deben ser direccionadas al servidor LISTSERV. Una ayuda esta disponible en cada servidor LISTSERV. Para obtener una copia de este archivo, utilice el comando Info. La documentación detallada de LISTSERV (y servicios relacionados) esta disponible desde el DOC FILELIST en LISTSERV@EARNCC.EARN.NET (ó LISTSERV@EARNCC.BITNET). Este incluye la guia de usuario de LISTSERV la cual esta disponible tanto en postscript como en formato de texto. Para obtener una lista de documentación disponible utilice el comando INDex.

3.4.13.- USENET.

USENET.- Algunas veces llamado Netnews, es una enorme colección de mensajes los cuales están disponibles para usuarios de todo el mundo por el significado de los protocolos UUCP y NNTP (Unix to Unix Copy Program y Network News Transport Protocol, respectivamente). Sitios de computo individuales nombran a alguien para ver la calidad de los mensajes recibidos y para decidir que tantos mensajes pueden ser guardados antes de que sean removidos para hacer una nuevo conjunto. Comúnmente los mensajes son almacenados en lapsos menores a una semana, en promedio lotes de nuevos mensajes Usenet semanales ocupan alrededor de 60 Mb de espacio en disco.

Cada mensaje Usenet pertenece a un grupo - existen algunos cientos de estos, el cual contiene mensajes de un particular tema. Los usuarios enviando mensajes Usenet debe direccionar cada mensaje a un newsgroup ó grupo particular. Los grupos formados pueden ser de diversos temas. La calidad de las discusiones pueden ser excelentes, pero esto no siempre esta garantizado. Algunos newsgroup tienen un moderador el cual checa los mensajes del grupo y decide cuales son apropiados para ser distribuidos.

Algunos en el newsgroup aportan unas fuentes de información muy útiles y ayudas en los temas técnicos. Si los usuarios de un grupo necesitan encontrar algo sobre un determinado tema, se envían la pregunta al newsgroup apropiado y un experto en el tema de cualquier parte del mundo puede ofrecerse a proporcionar la respuesta. Las listas de Frequently Asked Questions ó FAQ (respuestas a preguntas comunes) se han compilado y están disponibles periódicamente en algunos newsgroups.

Los mensajes pueden tener tanto texto plano e información codificada en binario. Cada mensaje tiene una serie de lineas de cabecera las cuales definen como el mensaje esta llegando, que ruta tomo en la red y alguna otra información administrativa.

Usenet fue originalmente desarrollada para sistemas Unix en 1979. Al cabo de un año, 50 sitios Unix estaba participando. Ahora, estos son miles de sitios corriendo un número de sistemas operativos en

una variedad de plataformas de hardware comunicándose via Usenet a todo alrededor del globo. Los mensajes de muchas listas de correo de Bitnet LISTSERV también son distribuidos en Usenet.

Dentro de EARN, una red de distribución de Usenet ha sido desarrollada la cual provee una distribución eficiente del trafico Usenet lo cual minimizar la carga de la red para los países participantes.

Los newsgroups de Usenet pueden ser leidos por miles de sitios alrededor del mundo. En adición, varios sitios proveen un servicio de dial-up ó de marcado. Si no sabe si su sitio tiene acceso a Usenet, cheque con la gente de soporte. Muchas computadoras de red pueden accesar el servicio de Usenet via paquetes de software especial.

Muchos newsgroups están conectados a una lista de correo con la cual quedan unidos. Para una lista de estos newsgroups y sus listas de correo asociadas, envie un correo a LISTSERV@AMERICAN.EDU con la línea: GET NETGATE GATELIST. Muchos de los documentos los cuales aparecen en los newsgroups están disponible via correo electrónico desde mail-server@rtfm.mit.edu. Para instrucciones, envie un mensaje con el subject HELP.

Si su sitio provee acceso a Usenet, entonces lo que necesita es utilizar uno de los muchos paquetes de software disponibles para buscar a través de los mensajes (al menos uno es probable encontrar en su computadora). Estos paquetes pueden tanto accesar a su servidor de news local como utilizar el Network News Transfer Protocol (NNTP) para accesar al servidor news en alguna otra computadora de la red.

Si Usenet no esta disponible para usted y le gustaria tener acceso desde su sitio, contacte a su administrador de sistema. Deberá leer un articulo de como volverse un sitio USENET el cual es informado periódicamente por el newgroup. Este también esta disponible por un FTP anónimo a rtfm.mit.edu en /pub/usenet/news.answers/site-setup ó por un correo electrónico hacia mail-server@rtfm.mit.edu dentro de la línea: send usenet/news.answers/site-setup.

Un servicio experimental esta disponible el cual le permite obtener mensajes Usenet via correo electrónico:
* enviando un mensaje de correo electrónico a listserv@cc1.kuleuven.ac.be. Recibirá instrucciones en respuesta a un mensaje consistiendo del comando /nnhelp.

* enviando un mensaje de correo electrónico a netnews@db.stanford.edu. Le serán enviadas instrucciones en respuesta al mensaje consistente de la palabra help.

Muchos paquetes de software están disponibles para leer y distribuir mensajes Usenet en una variedad de sistemas operativos (Unix, VMS, VM/CMS, MVS, Macintosh, MS-DOS y OS/2) y ambientes (X-Window y MS-WIndows). En adición a los paquetes de software especificamente diseñados para ser lectores de news, muchos otros programas de comunicaciones, particularmente interfaces de correo también proveen el acceso a Usenet. Muchos, no todos, de los lectores de news proveen los servicios básicos:

* Subscribiéndose a un newsgroup: Su software lector de news puede hacerlo accesible inmediatamente a ese grupo, para que pueda leer su contenido rápido y fácilmente.

* Cancelar la subscripción a un grupo: Removiendo el grupo fácilmente de la lista de acceso.

* Leyendo buzones de newsgroup: Su lector de news presentara un nuevo mensaje - buzón -que llega. y guarda cuales tiene enviados y cuantos no ha leido.

* Secuencia de discusión: Reenvio a un buzón donde están agrupados todos con el buzón original, para que los lectores puedan leer el mensaje dentro de un newsgroup el cual están formando parte de una discusión ó tema.

* Buzón de un nuevo grupo: Puede participar en un grupo de discusión, su lector de news sabe de donde enviar su buzón.

* Respondiendo a un correo: Puede enviar una respuesta al newsgroup ó a un autor de un correo.

Los newsgroup de Usenet están por si mismos agrupados dentro de categoría; 8 de las principales son alt, comp, misc, news, rec, sci, soc y talk; perteneciendo a alternativas, computación, misceláneos, relacionados a sistemas de news mismos, recreación, científicas, social y de habla. El mensaje de muchas listas de correo de LISTSERV Bitnet son también distribuidas en Usenet.

Otras categoría principales basados en áreas de temas particulares (p.ej. bionet, biz, vmsnet) pueden ser distribuidas a todo lo ancho del mundo y tienen su categoria en base a su área geográficas, en organización (p.ej. ieee) ó por interés comercial (p.ej. clari).

Los programas News se comunican con cada otro de acuerdo al protocolo estándar, algunos de los cuales son descritos por el Internet Request For Comments (RFC). Copias de los RFC son frecuentemente puestos en la red y se obtienen de sitios para archivos. Los actuales RFC de news liberados son:

RFC 977 especifica NNTP, el Network News Transfer Protocol,

RFC 1036 especifica el formato de articulos Usenet.

Algunos de los newsgroups traen articulos y discusiones en el udo de los Usenet, los más notables: news.announce.newsusers, news.answers y news.newusers.questions.

Muchos de los articulos los cuales aparecen periódicamente en estos newsgroups ó en otros también están disponibles desde rtfm.mit.edu por un FTP anónimo ó por un correo electrónico a: mailserver@rtfm.mit.edu.

3.4.14.- NETSERV.

NETSERV.- Este es un servidor el cual provee acceso rápido a un deposito de archivos de datos, los cuales son del interés de la comunidad EARN/Bitnet. Todos los usuarios pueden recibir archivos y usuarios privilegiados pueden almacenar nuevas versiones de archivos y suscribirse a los archivos de su elección. Los usuarios privilegiados tienen un password NETSERV.

En orden para obtener una carga balanceada en la red y una respuesta de tiempo de uso, NETSERV utiliza servidores distribuidos: estos son un gran número de servidores en la red para que los usuarios no viajen tan lejos para encontrar un servidor, por lo que la misma información esta disponible para todos los servidores. Los directorios (ó archivos) de NETSERV están arreglados históricamente, con

NETSERV FILELIST hasta arriba. Esta lista de archivos puede ser obtenida enviando el comando GET NETSERV FILELIST a cualquier NETSERV. La lista de archivos contiene una descripción corta de los archivos y los códigos de acceso para cada archivos. Estos códigos representan los privilegios de "get" y "put" requeridos para cada archivo. Existen servidores NETSERV en muchos paises diferentes. Para encontrar cual servidor esta más cercano a usted, envíe el comando QUERY SERVICE a cualquier servidor. En EARN, solamente un NETSERV es permitido para un país. Sin embargo, si un pais tiene un número grande de nodos, servidores adicionales pueden ser instalados.

NETSERV acepta el acceso a correo electrónico de usuarios en cualquier red. Los comandos deberán ser colocados en el cuerpo del archivo de correo (la línea de tema es ignorada). Para usuarios en la red EARN/Bitnet, NETSERV esta accesible vía mensajes interactivos. Comandos de usuarios privilegiados pueden requerir de un password, para ser enviados de esta forma. NETSERV no tiene ninguna limitación en la entrega, excepto que no puede ordenar el mismo archivo más de una vez por dia. Un gran archivo de ayuda puede ser obtenido enviando el comando GET NETSERV HELPFILE a cualquier NETSERV. Una lista de correo esta disponible como NETSERV@HEARN.NIC.SURFNET.NL (o NETSERV@HEARN.BITNET). Información adicional puede ser obtenida en U001212@HEARN.NIC.SURFNET.NL(ó U001212@HEARN.BITNET).

3.4.15.- MAILBASE.

MAILBASE.- Es un servicio de información electrónica con muchas de las mismas funcionalidades de LISTSERV. Este permite a grupos del Reino Unido administrar sus propios temas de discusión (lista de Mailbase) y asociar archivos. El servicio de Mailbase esta corriendo como parte de la JANET Networked Information Services Project (NISP) con base en la Universidad de Newcastle. Los comandos deberán ser enviados en un correo electrónico a base@mailbase.ac.uk. Más de un comando puede estar en cualquier orden, en mayúsculas, minúsculas ó combinado. Para una lista de documentación en línea sobre Mailbase, enviar el comando: index mailbase. Puede utilizar el comando "send" para recobrar esos documentos que le interesan. Por ejemplo para recuperar un archivo de respuesta a preguntas frecuentes, enviando el siguiente comando: send mailbase userfaq. El soporte a usuario esta también disponible enviando las preguntas en un mensaje de correo electrónico a: mailbase-helpline@mailbase.ac.uk. Archivos públicos en Mailbase están también disponibles por FTP anónimos a mailbase.ac.uk

3.4.16.- FTPMAIL.

FTPMAIL.- Es un sistema el cual hace a la utileria de FTP disponible para usarse con correo electrónico para la Internet. Ciertas computadoras en la Internet ofrecen un servicio ftpmail a todos los usuarios de Internet. Esta computadoras tienen una cuenta especial de ftpmail y los usuarios pueden incluir peticiones de FTP en mensajes de correo electrónico los cuales son direccionados a estas cuentas. Las sesiones de FTP son automáticamente traidas en respuesta a la petición FTP de correo y el resultado de la sesión FTP son enviados a los usuarios vía correo electrónico. Si el sistema ftpmail falla al conectarse al servidor FTP denominado, un apropiado mensaje de correo es enviado al usuario explicando que pasa.

Varios sitio en la Internet ofrecen un servicio ftpmail y ninguno con acceso a correo electrónico puede utilizar este. Los usuarios no utilizan el servicio ftpmail en sitios remotos de ellos. Los paquetes de ftpmail están basados en script hechos en perl, los cuales están disponibles en:

- src.doc.ic.ac.uk: /packages/ftpmail
- grasp1.univ-lyon1.fr: /pub/unix/mail/tools/ftpmail
- ftp.sterling.com: /mail/ftpmail

3.4.17.- PROSPERO.

PROSPERO.- Es un sistema de archivos distribuido que contiene archivos virtuales, los cuales representan un recurso de Internet. Así, un archivo puede representar una sesión de Telnet a un host particular, este puede representar un archivo en un WAIS junto con la información necesitada para accesar al servidor, este puede representar un archivo en el índice de nombres de archivo, ó podrá representar un archivo el cual esta disponible utilizando FTP junto con la información necesitada para obtener el archivo.

A los usuarios individuales les es dado un espacio virtual en el sistema de archivos, donde pueden crear nuevos archivos virtuales. Estos también están disponibles para copiar archivos dentro de su espacio virtual hasta cualquier lugar en el sistema global de Prospero. Puesto que cada archivo virtual es meramente un enlace a un archivo real, cualquier cambio al archivo real puede ser visible para el usuario. Sitios Internet utilizando Prospero son dando un prefijo global (similar a un nombre de sitio) el cual significa que el sitio puede accesar a archivos de cada otro. Un directorio maestro es mantenido y los usuarios son animando a organizar sus propios proyectos y papeles de tal forma que pueda permitirles añadirlos fácilmente al directorio maestro. Por ejemplo, un usuario deberá considerar crear un directorio virtual (en cualquier lado de su sistema virtual) el cual contendrá puntos para copiar de cada uno de los papeles que el quiera que estén disponibles para los demás. Un enlace puede ser creado desde el directorio virtual hasta el directorio autor maestro, haciendo al directorio virtual disponible para otros usuarios. Cualquier cambio futuro a los archivos reales puede estar inmediatamente disponible para otros usuarios.

Para poder utilizar Prospero, debe de estar en la red Internacional de TCP/IP (la Internet) y debe tener Prospero corriendo en su computadora. Antes de que empiece a utilizar el sistema de archivos Prospero, un sistema virtual debe ser creado para usted. Sin embargo Prospero, como es empacado, esta configurado para que una vez que compile el cliente pueda teclear: vfsetup guest y empezar a trabajar directamente utilizando un sistema virtual invitado en la USC Information Science Institute. La última versión de Prospero esta disponible como el archivo prospero.tar.Z vía FTP anónimo desde prospero.isi.edu en el directorio /pub/prospero.

Los siguientes archivos están disponibles vía FTP anónimo a prospero.isi.edu. Estos también están disponibles a través de Prospero.

- Anonymous FTP: /pub/papers/prospero/prospero-oir.ps.Z,
- Prospero: /papers/subjects/operating-systems/prospero/prospero-oir.ps.Z.

Esta es una primera lectura muy útil. Da un buen vistazo de Prospero y lo que hace. Este también describe un modelo de Sistema Virtual del cual Prospero es un prototipo de implementación.

- Anonymous FTP: /pub/papers/prospero/prospero-bii.ps.Z,
- Prospero: /papers/subjects/operating-systems/prospero/prospero-bii.ps.Z.

Este documento describe como Prospero puede ser utilizado para integrar servicios de información Internet, incluyendo Gopher, WAIS, archie y World-Wide Web.

3.4.18.- IRC.

IRC.- Internet Relay Chat, es un sistema de conversación en tiempo real. Este es similar al comando talk el cual esta disponible en muchas maquinas de la Internet. IRC hace todo lo que hace talk, pero este permite a más de dos usuarios hablar a la vez, con acceso a través de la Internet global. Este también provee muchas otras realizaciones útiles. Lo fundamental para la operación de IRC es el concepto del canal: cada canal es una conversación. Cuando se une a un IRC, primero introduce un canal nulo y este puede estar disponible para enviar cualquier mensaje hasta que introduzca un canal de charla (a menos de que tenga instalado una conversación privada de alguna forma). El número de canales es esencialmente ilimitado.

IRC esta en red sobre muchas partes de Norte América, Europa y Asia. Cualquier cosa que teclee puede ser transmitido instantáneamente alrededor del mundo a otros usuarios que estén conectados a su canal. Estos pueden responder a su mensaje. Los temas de discusión en IRC son variados. Técnicos y políticos son los más populares, especialmente los concernientes a eventos actuales del mundo. IRC es también una forma de expandir sus horizontes, puesto que gente de muchos países y culturas están en el sistema, las 24 horas del día. Muchas de las conversaciones son en ingles, pero algunas veces se ven canales en Alemán, Japonés y Finlandés y ocasionalmente otros lenguajes. Los clientes y servidores de IRC están disponibles vía FTP anónimo en varios sitios, notablemente en cs.bu.edu.

Muchos de los servidores hosts de IRC a través de la red son conectados vía una estructura de árbol. Estos entregan el control y el dato de mensaje para avisar de la existencia de otros servidores y sus usuarios y el canal y otros recursos que el usuario empieza a ocupar. Para obtener ayuda en IRC, teclee /help y siga las instrucciones. Si tiene problema, puede preguntar por algún operador de canal en IRC, por ejemplo #twilight_zone and #eu-opers. Varios documentos de IRC están disponible vía FTP anónimo de ftp.kei.com y cs.bu.edu.

3.4.19.- RELAY.

RELAY.- El sistema le permite al usuario intercambiar mensajes. Cada usuario se firma en el servidor RELAY y coloca su ID en su actual lista de usuario. Luego el usuario debe entrar a un canal del sistema RELAY y estará listo para intercambiar mensajes con otro usuario actualmente firmado en ese canal. Los comandos para el sistema RELAY comienzan con un carácter (/), cualquier cosa que no inicie con el slash es considerado un mensaje y es enviado a todos los otros usuarios. Todos los servidores RELAY están en la red global EARN/Bitnet. Cada servidor RELAY provee un servicio a una colección especifica de uno ó más nodos, designados como una área de servicio. Los usuarios se firman al RELAY más cercano y son también virtualmente firmados a todos los RELAY a los cuales estén enlazados. Muchos RELAY son cerrados durante horas pico; solamente un RELAY esta abierto las 24 horas del día.

RELAY también esta disponible para usuarios EARN/Bitnet con acceso a mensajes interactivos los cuales no han sido expresamente ejecutados desde el sistema por el administrados del RELAY. RELAY esta disponible en las siguientes direcciones EARN/Bitnet (y otros sitios). Nombres cortos para cada máquina RELAY son dados entre paréntesis.

```
+-------------------------------------------------+
|                                                 |
| RELAY@ASUACAD (Sun_Devils)  RELAY@PURCCVM (Purdue)      |
| RELAY@AUVM  (Wash_DC)    RELAY@SEARN  (Stockholm)     |
| RELAY@BEARN (Belgium)    RELAY@TAMVM1 (Aggieland)     |
| RELAY@CEARN (Geneva)     RELAY@TAUNIVM (Israel)       |
| RLY@CORNELLC (Ithaca_NY)  RELAY@TREARN (EgeRelay)     |
| RELAY@CZHRZU1A (Zurich)   MASRELAY@UBVM (Buffalo)     |
| RELAY@DEARN (Germany)    RELAY@UFRJ   (RioJaneiro)    |
| RELAY@DKTC11 (Copenhagen) RELAY@UIUCVMD (Urbana_IL)   |
| RELAY@FINHUTC (Finland)   RELAY@USCVM  (LosAngeles)   |
| RELAY@GITVM1 (Atlanta)    RELAY@UTCVM  (Tennessee)    |
| RELAY@GREARN (Hellas)     RELAY@UWAVM  (Seattle)      |
| RELAY@HEARN (Holland)     RELAY@VILLVM (Philadelph)   |
| RELAY@ITESMVF1 (Mexico)   RELAY@VMTECQRO (Queretaro)  |
| RELAY@JPNSUT00 (Tokyo)    RELAY@VTBIT  (Va_Tech)      |
| RELAY@NDSUVM1 (No_Dakota) RELAY@WATDCS (Waterloo)     |
| RELAY@NYUCCVM (NYU)       RELAY@YALEVM  (Yale)        |
|                                                 |
+-------------------------------------------------+
```

RELAY esta disponible para usuarios en la red EARN/Bitnet vía mensajes interactivos (p.ej. el comando TELL de VM ó el comando SEND de VMS/JNET). Todas las máquinas de servidores RELAY están en sistemas IBM VM/CMS, pero no tiene que ser un usuario de VM para poder utilizar RELAY. Sin embargo, si no esta en la red de EARN/Bitnet, no puede utilizar RELAY. CHAT, una interface de pantalla completa para enviar y recibir mensajes de TELL para sistemas VM es particularmente útil para usuarios de RELAY. CHAT esta disponible desde cualquier NETSERV.

Una vez registrado, el archivo RELAY INFO y RELAY USERGUIDE son enviados al usuario. Estos dos archivos dan una descripción completa de RELAY. Una guía breve de RELAY esta disponible desde la lista de archivos de documentos EARN. Envie un correo a LISTSERV@EARNCC.EARN.NET (o LISTSERV@EARNCC.BITNET). En el cuerpo del mensaje, escribir: GET RELAY MEMO.

Conclusiones:

En el primer capitulo se abarcaron los puntos claves de la conexión a Internet, todo esto de forma básica y simple, de tal forma que el lector pueda comprender el concepto escencial del uso de esta red, el cual en su forma más sencilla es la disponibilidad de obtener información.

Se dieron términos básicos y comprensible tanto para personas relacionadas al tema como para los que lo desconocen totalmente. Aquí justificaremos la estructura del trabajo, el cual si bien pretende ayudar a las personas con el manejo de la Internet y sus conceptos fundamentales, de la forma más comprensible, tampoco es una especie de regla general que se tenga que cumplir y olvidarse de lo demás, por lo que el trabajo requiere del interés del lector para relacionarse más con los puntos que se van desarrollando. Uno de los principales temas de discordancia es el de la nomenclatura de los términos, puesto que estos temas son desarrollados en su mayoría en Ingles, existe la dificultada de poderlos expresar en nuestro idioma y además que guarden la relación con otros. En este trabajo se optó por expresar el término en Ingles, dar en el momento que surja la traducción ó explicación del termino y dejarlo en Ingles para las siguientes ocasiones, esto con el fin de involucrar a los lectores con los términos que realmente se manejan en el mundo de la Internet y que ellos mismos lo adecuen a lo que consideren la mejor explicación. Otro punto de importancia en el desarrollo del trabajo esta plasmado en la estructura misma del documento. El trabajo fue desarrollado de tal forma que no tiene una sección donde concentre los puntos básicos y otra donde profundice en los temas, si existen subdivisiones que puede saltarse un lector por considerarlas de poca importancia ó muy especificas, de las cuales no esta dispuesto a conocerlas porque nunca las aplicara, sin embargo siempre es conveniente tener esos puntos de referencia para cualquier problema.

En fin, la primera parte, como todas, es una introducción simple al tema a tratar, lo que valdria la pena para las personas que deseen conocer más del tema seria el apéndice el cual habla bastante de lo que es la comunicación y los términos utilizados. También se dan algunas ayudas sobre ciertos puntos y sobretodo, se intenta dar la confianza mostrandolo de forma clara y simple de lo sencillo que puede ser entrar en la red. Los apéndices describen de forma más detallada la mecánica de cada tema. Muchos de los datos ahi encontrados son información general, datos históricos, conceptos claves, funcionamiento, opciones en la forma de trabajar, reglas generales, etc.

Para el segundo capitulo se explican las bases de la conexión, desde los elementos básicos e indispensables, también se explica la forma de trabajar de cada uno y los detalles a revisar para una configuración optima y por lo tanto un enlace satisfactorio. Se presentan las diversas formas en las que se puede trabajar dependiendo siempre del equipo con que se cuente, se analizan los estándares a utilizar y algunas opciones para configurar, si bien todo depende de las caracteristicas del equipo, también es muy cierto que no todo esta siempre probado y que configurando opciones con el método de prueba y error puede resultar una opción para obtener buenos resultados, pero como siempre se recomienda tener un respaldo de la configuración antes de cambiarla.

Otro punto del tema es la comparación de otros tipos de enlace, pero esto es solo como información para el usuario, puesto que recordemos que la base de este trabajo es la comunicación con medios disponibles comúnmente, ó sea una línea telefónica convencional. Para finalizar este capitulo se dieron puntos importantes a tomar en cuenta para la contratación de un servicio de Internet, esto en de vital importancia para el futuro, sobretodo para las personas que no están muy relacionadas a dichos temas y que por ser principiantes se "embarcan" con cualquier proveedor.

Recordemos que este es uno de los puntos básicos para tener un buen servicio.

En el último capitulo hablamos de como se realiza la conexión pero desde el punto de vista de la aplicación; esto es como interactua la máquina con la información que viaja en la Internet, el software que permite ver la información, los servicio disponibles, la forma de poder obtener la información con los diversos softwares, terminologia utilizada, utilerias no muy utilizadas, etc. Recordamos que el propósito de este trabajo no esta enfocado al uso y navegación de la Internet, ni de algún software especial y menos de sus caracteristicas especiales. Puesto que es una parte escencial del trabajo, se explicara su funcionamiento, su interacción con la máquina y las utilerias comunes. Resaltando nuestro propósito de ayuda, se comentan utilerias que pueden hacer de función de otras las cuales no estén disponibles en nuestro software.

Básicamente el trabajo gira en base a tres elementos que se consideran importantes: TCP/IP (primer capitulo), el modem y los protocolos de comunicación via telefónica (segundo capitulo) y el software que une a estos y permite ver el resultado (capitulo tres). El punto clave es poder dar esa posibilidad de comprender y poder realizar una inspección para determinar cualquier error que se presente y en el mejor de los casos resolverlo ó en caso contrario utilizar herramientas optativas que realicen la función deseada.

Bibliografía

Guide to Network Resource Tools
EARN Association
May 20, 1994

Trumpet Winsock v.2.0
By Peter R. Tattam, 1994

Big Dummy's Guide to the Internet
Mitch Kapor (Electronic Frontier Foundation)
Steve Cisler (Apple Computer Inc.)

Entering the World-Wide Web: A guide to Cyberspace
By Kevin Hughes
Enterprise Integration Technologies, May 1994.

Modem 101: An Introductory lesson in High-Speed Modems

Multitech, Owner's manual

RFC 1134: Point to Point Protocol

RFC 1055: A nonstandard for transmission of IP datagrams over serial lines: SLIP

Guia de referencias de TCP/IP de NetWare 4.1

TCP IP Runtime System SCO.