Universidad Tecnológica de la Mixteca

Monitor de Enlaces IP

Tesis Profesional

Que para obtener el Grado de

Ingeniero en Electrónica

presenta

Alejandro Ernesto Ramírez González

Acatlima, Huajuapan de León, Oaxaca. **Enero '98**

Tesis presentada el 30 de enero de 1998
ante los siguientes sinodales:

Ing. Hugo Suárez Onofre
M.C. José A. Moreno Espinosa
M.C. Enrique Guzmán Ramírez

Asesor:

M.C. José A. Moreno Espinosa

Dedicatorias

A mi madre, por su amor, comprensión y fortaleza en todo momento, principalmente en los últimos meses.

A mi padre, porque su cansancio me permite gozar de estos momentos.

A mis hermanos: Olga, Socorro, Susana, Agustín, Elias, Luz, Miguel, Rosalba y Horacio, por el apoyo otorgado todo este tiempo.

A la madre Edith de San Juan Bosco, por sus múltiples oraciones.

A Tere, por su cariño y comprensión.

Alejandro.

Agradezco de forma especial al:

M. C. José Antonio Moreno Espinosa.

Por su paciencia y ayuda en la realización de este trabajo.

Alejandro E. Ramírez González

Agradecimientos

A todos mis profesores, quienes no dudaron en transmitirme sus conocimientos.

Al Ing. Hugo Suárez Onofre, por su apoyo, consejos y tiempo dedicado en el transcurso de este proyecto.

A las siguientes personas, por su ayuda y buenos consejos: Ing. Gerardo García Hernández, Lic. Carlos Santibañez Morán, Fis. Mat. Gustavo Jiménez Santana, Ing. Heriberto I. Hernández Martínez, M.C. Hiram Ochoa Arriaga, M.C. Enrique Guzmán Ramírez, M.C. Esteban Guerrero Ramírez, Edel V. Peñaloza Aguirre, Lucio Acevedo Jacinto, Claudia Santiago Ramírez, Hernán Acevedo Rodríguez, Roberto Osorio González.

Alejandro E. Ramírez González

Índice

Introducción

Comunicación es la transmisión de información de un lugar a otro, y el empleo de señales eléctricas ha ido reemplazando casi completamente las otras formas de transmisión de información a largas distancias. Esto se debe principalmente a que las señales eléctricas son relativamente fáciles de controlar y viajan a velocidades cercanas a la de la luz.

En las últimas décadas, las computadoras han tenido un impacto de enormes consecuencias en nuestra sociedad. Hoy en día resulta normal realizar una gran diversidad de tareas con la ayuda de las computadoras, lo que ha hecho que ganen popularidad en todas las áreas de trabajo.

En otras épocas, los centros de cómputo aislados se manifestaban como un crecimiento de la industria informática, pero actualmente son las redes de computadoras las que toman la batuta en el crecimiento de dicha industria. Esto se debe al hecho de que las redes permiten a cualquiera que esté conectado a ellas, aprovechar las ventajas de todo un universo de información y entretenimiento.

Una red de computadoras se define como un grupo de computadoras interconectadas a través de uno o varios caminos o medios de transmisión, con el fin de intercambiar la información almacenada en cada una de ellas y permitir la utilización de los recursos computacionales de diferentes computadoras.[1]

Las universidades y centros de investigación de prácticamente todo el mundo no han desaprovechado la oportunidad de poder conectar sus recursos de cómputo en alguna red que les permita estar en contacto unas con otras, con el objeto principal de intercambiar ideas y conocimientos sobre cualquier área de interés.

Las redes de computadoras están clasificadas en base a varios criterios, siendo el más importante la cobertura geográfica por lo que se clasifican en: redes de área local (LANs), redes de área metropolitana (MANs) y redes de área amplia (WANs). En este caso se hablará de redes LANs debido a que a este grupo pertenece la red de la UTM, que cuenta con una dirección Internet tipo C (192.100.170) y tiene una topología de bus a la que están conectadas las estaciones de trabajo.

Una red de área local es una interconexión de computadoras mediante un medio de transmisión dentro de una distancia que no supere unos cuantos kilómetros. Son utilizadas en edificios de oficinas, universidades, centros de investigación, etc. La información intercambiada es especialmente de datos, aunque ya existen redes locales para la transmisión de video y redes soportando aplicaciones multimedia.

Justificación

La razón principal del desarrollo de este trabajo tiene su fundamento en la inquietud sobre la gran cantidad de problemas que se han estado presentando con respecto al ancho de banda de la red; problemas que se han visto reflejados en retardos demasiado prolongados al momento de accesar a la red, gran número de colisiones detectadas, y otras condiciones anormales.

La realización del programa de aplicación no debe confundirse con el deseo mal sano de invadir la privacidad de cada usuario y mucho menos de transgredir la seguridad de la red. Sólo se intenta llevar un control estadístico del aprovechamiento de cada una de las conexiones presentadas en la infraestructura de red.

[1] Black, U. Redes de Computadoras: Protocolos, Normas e Interfaces. Macrobit 1990, pp. 24

Objetivo

En nuestros días, las redes de cómputo es una de las áreas más importantes dentro de las comunicaciones. La utilización óptima de los recursos que la conforman trae grandes beneficios tanto en costos, como en desempeño.

El objetivo de la presente tesis es la creación de un software que apoye a los administradores en el control de la red de la Universidad Tecnológica de la Mixteca, permitiéndoles observar cada uno de los enlaces realizados por cada estación perteneciente a la red, dentro y fuera de la misma.

Contenido

Capítulo 1

Se dará una introducción a la comunicación de datos incluyendo la transmisión síncrona, asíncrona, con detección de errores; y se dará un panorama general sobre las bases en que descansan las redes, básicamente el modelo de referencia OSI y la comunicación conmutada.

Capítulo 2

Se explicará brevemente el desarrollo y forma de trabajar de la tecnología Ethernet, propuesta por Robert M. Metcalfe en su tesis de doctorado. Se incluye una explicación sobre su protocolo de acceso al medio, la forma en que toman los paquetes al viajar sobre ella, y las distintas variaciones de la norma original.

Capítulo 3

Para que las distintas computadoras pertenecientes a las redes se puedan comunicar correctamente, necesitan hablar el mismo idioma. Un protocolo de red es un estándar que define las reglas para que las computadoras se comuniquen. En este capítulo, se analizará la forma de operar de la familia de protocolos TCP/IP, hoy por hoy el estándar más utilizado por institutos de investigación y centros educativos.

Capítulo 4

Mostrará una visión del nacimiento y desarrollo de ese fenómeno tan importante como lo es Internet, la "Red de redes".

Capítulo 5

Se presenta el diseño del Monitor de enlaces IP, software que nos permitirá analizar los datos más importantes de cada enlace descubierto en nuestra red.

Conclusiones

Se expondrán los alcances y logros obtenidos en la ejecución de la aplicación y se darán algunas posibles mejoras, además de las perspectivas del software.

Apéndice A
Contiene el manual de usuario del programa Monitor.

Apéndice B
Contiene el manual de usuario del programa Nslookup.

1

Introducción a la comunicación de datos

Los sistemas de comunicación se encuentran dondequiera que se transmita información de un punto a otro. Algunos ejemplos son el teléfono, la radio, la televisión, etc. Los sistemas actuales de comunicación son necesarios para los negocios, la industria, los bancos, y en general, para el bienestar y la seguridad de los países.

Soméramente diremos que comunicar significa conducir o transmitir información de un lugar a otro, y que un sistema de comunicación está formado por un grupo de elementos que interactúan armónicamente, combinándose para lograr la comunicación.

La comunicación de datos ha llegado a ser una parte fundamental en la rama de la computación. El gran crecimiento de los sistemas de comunicación y su gran influencia dentro de las redes de computadoras ha sido explosivo, ya que las redes mundiales comparten datos relacionados con medicina, finanzas, gobierno, tráfico aéreo, etc. y los grupos de investigación establecen listas de correo electrónico para que puedan compartir información de interés común. Las universidades, por su parte, utilizan su acceso a Internet para reforzar sus programas de estudio, entre otras cosas.

Este capítulo provee un panorama introductorio de la comunicación de datos enfocado a las redes de computadoras, discutiendo sus factores, protocolos y modelos. Estableceremos que el principal objetivo de las redes de computadoras es el compartir recursos, llámense computadoras, programas, datos, etc., que se encuentran esparcidos en distintos lugares. Para ello, se necesita de un sistema de comunicación que facilite el intercambio de datos e información de control apoyado en un modelo por capas que permita su implementación.

El propósito de un sistema de comunicación es transmitir señales que contienen información generada por una fuente localizada en cierto sitio geográfico, a un destino localizado en otro sitio.

En la figura 1.1, se muestran los elementos que intervienen en un sistema de comunicación.

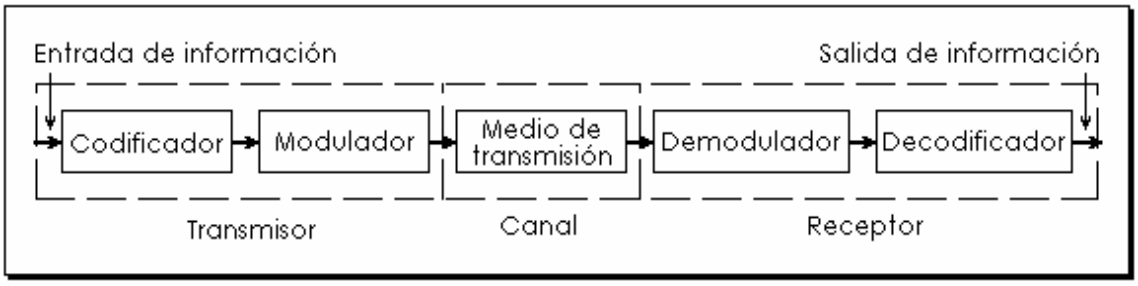


Figura 1.1 Sistema de comunicación

El codificador elige la mejor forma de la señal para optimizar su detección en la salida. El decodificador efectúa la operación inversa para tomar la mejor decisión, basadas en las señales disponibles, de que un mensaje dado fue efectivamente enviado. Aunque las funciones del codificador y del modulador son semejantes en que ambos preparan la señal para una más eficiente transmisión, el proceso de codificación está concebido para optimizar la detección de errores en un mensaje que está siendo transmitido, mientras que el proceso de modulación está diseñado para imprimir la señal de información sobre la onda que se va a transmitir. El demodulador realiza la operación inversa a la del modulador para restaurar la señal en su forma original. Por su parte, el medio de transmisión es la piedra angular del sistema ya que tiene la función de llevar la señal generada por el transmisor hasta el receptor.

Al enviar datos por líneas de comunicación se habla frecuentemente de la velocidad en "bits por segundo (bps)" y de los bauds o baudios. La velocidad en bits por segundo es la cantidad de bits que se transmiten por segundo y los baudios es el cambio de estados en la línea.

Las señales transmitidas en un sistema de comunicación son utilizadas para comunicar datos, que pueden clasificarse en:

- Datos analógicos, y
- Datos digitales.

Los datos analógicos provienen de variables que cambian continuamente con el tiempo y pueden tomar un número infinito de valores dentro de un cierto intervalo. Ejemplos de estas variables son la temperatura ambiente, la presión atmosférica, las ondas sonoras, etc. Por su parte, los datos digitales provienen de variables que solamente pueden tomar un número finito de valores discretos, como los diferentes caracteres que componen un texto, el conjunto de números, etc.

Para transmitir datos a través de un sistema de comunicación es necesario utilizar señales que los representen y se propaguen a través del canal de comunicación. Estas señales pueden clasificarse en:

- Señales analógicas, y
- Señales digitales.

Las señales analógicas varían continuamente con el tiempo y pueden tomar un número infinito de valores dentro de un cierto intervalo. Ejemplos de estas señales son las señales eléctricas o electromagnéticas para transmitir datos.

Las señales digitales, en teoría, solamente pueden tomar un número finito de valores diferentes y, por lo general, sólo pueden cambiar de valor en periodos predeterminados. Las señales digitales pueden ser señales eléctricas, rayos infrarrojos o rayos láser.

De acuerdo con las señales utilizadas para transmitir información e independientemente del tipo de datos que se envíen, la transmisión puede clasificarse en:

- Transmisión digital, y
- Transmisión analógica.

En la transmisión digital, las señales son más fáciles de generar, sin embargo cuando se transmite una señal digital por un conductor eléctrico, ésta sufre una mayor atenuación y distorsión que una señal analógica.

La atenuación y distorsión dependen de las características del medio (conductor eléctrico) y de la velocidad de transmisión, siendo más grandes a mayores velocidades y distancias.

Para contrarrestar este problema se utilizan repetidores cada cierta distancia. La función de un repetidor es reconocer o decodificar la señal digital que le está llegando y generar una nueva señal reestablecida idéntica a la original. Por esta razón, también se le denomina repetidor regenerativo. En una transmisión digital no se utilizan amplificadores.

En la transmisión analógica, las señales sufren una menor atenuación y distorsión que las señales digitales, aunque también se atenúan y distorsionan. Estas señales son más complicadas de generar que las señales digitales, pero pueden viajar a mayores distancias antes de que la atenuación y la distorsión provoquen que la señal no se pueda recuperar.

De manera similar a lo que ocurre en las señales digitales, las señales analógicas sufren mayor atenuación y distorsión tanto al viajar a mayores distancias como al variar más rápidamente su valor.

En las transmisiones analógicas se utilizan amplificadores para restituír en la señal la potencia perdida debido a la atenuación, pero también amplifican la señal de ruido, lo cual no ocurre con los repetidores regenerativos utilizados en las transmisiones digitales.

1.1
Transmisión y sincronización

Si dos dispositivos están enlazados a través de un medio de transmisión para intercambiar datos, se necesita un alto grado de cooperación entre ellos. La temporización (velocidad, duración y espaciamiento) de esos bits deben ser los mismos tanto para el transmisor como para el receptor. Para esto existe la sincronización que es uno de los puntos principales de la comunicación de datos.

La comunicación de datos puede hacerse en forma serial o en forma paralela. En comunicación serial se transmite solo un bit a la vez, y en comunicación en paralelo se transmiten varios bits, cada uno en un canal de comunicación diferente, por lo general se transmite un carácter u octeto (se utiliza el término octeto en lugar de byte porque algunas máquinas tienen tamaños de palabras mayores de ocho bits) a la vez. La comunicación en paralelo se utiliza principalmente en impresoras y en multiprocesadores de alta velocidad.

En redes de computadoras se utiliza primordialmente la comunicación serial. A continuación se describirán las diferentes formas de comunicación serial utilizadas en la comunicación de datos.

En cuanto a la sincronización entre el transmisor y el receptor, la comunicación puede ser síncrona o asíncrona.

Transmisión asíncrona

El primer tipo de comunicación que se utilizó fue la comunicación asíncrona. En este tipo de comunicación la sincronización se realiza a nivel carácter o a cada octeto. Cuando la línea de transmisión está ociosa, se encuentra en el estado '1', al transmitir un caracter se envía la siguiente información:

- Un bit de inicio que pasa la línea al estado '0' durante el tiempo que dura en transmisión un bit.
- Los siete u ocho bits del carácter, manteniendo la línea en el estado '0' o '1' durante el tiempo de transmisión de un bit, dependiendo del bit a transmitir.
- Uno o dos bits de paro, los cuales se envían manteniendo la línea en el estado '1'.

La comunicación asíncrona no es muy eficiente debido a los bits de inicio y de paro.

Transmisión síncrona

En la comunicación síncrona se transmiten bloques de caracteres o bits. En el primer caso la sincronización está orientada a caracteres y en el segundo a bits.

En este tipo de comunicación los relojes del transmisor y el receptor deben estar sincronizados. Una posibilidad es tener un canal exclusivo para enviar la señal de sincronización y otra es incluir la información de sincronización entre los mismos datos.

En la transmisión síncrona orientada a caracteres se transmiten bloques de caracteres, generalmente de 8 bits. Cada bloque de información contiene dos o más caracteres de sincronización (SYNC) al inicio, los cuales sirven para que el receptor reconozca el inicio del bloque y sincronice su reloj.

Los caracteres de sincronización son un patrón fijo preestablecido que no debe ocurrir en ninguna otra parte del bloque de información.

La información de control al inicio, entre otras cosas, contiene la longitud del bloque de datos para que el receptor sepa hasta dónde debe continuar recibiendo caracteres de ese bloque.

Después siguen todos los caracteres de datos y finalmente otros caracteres de control, generalmente un CRC (Chequeo por Redundancia Cíclica), que se utilizan para verificar que el bloque de información haya sido recibido sin errores.

En la comunicación síncrona orientada a bits también se transmiten bloques de información, pero ahora cada bit será tratado en forma independiente para efectos de la transmisión.

El bloque de información en este caso consta de una señal que lo precede, que es una secuencia predeterminada de bits, además de un conjunto de bits de control, un conjunto de bits de datos, otro conjunto de bits de control y finalmente una señal que lo sucede, que por lo general tiene la misma secuencia que la señal precursora.

La secuencia de bits de inicio que constituye la señal precursora no debe existir en ninguna otra parte del bloque de información, excepto en la señal sucesora.

De acuerdo con las señales que se utilizan para transmitir la información, la comunicación puede estar formada por señales analógicas o digitales, como se ha mencionado con anterioridad.

Los diferentes formatos que se utilizan dependen del tipo de datos (analógicos o digitales) que se desea transmitir, así como del tipo de señales (analógicas o digitales) que se utilizan para la transmisión.

1.2
Técnicas de detección de errores

Las redes de comunicación de datos no están libres de errores, aun cuando en la actualidad la probabilidad de que haya errores sea baja.

Para tener comunicaciones confiables se han ideado técnicas de detección de errores. Éstas consisten en colocar bits adicionales en las tramas de información que permitan determinar si la información se recibió correctamente o no.

También se han construído códigos de corrección de errores automática (códigos de Hamming), los cuales permiten no solamente detectar errores, sino también corregirlos. Estos códigos tuvieron mucho éxito cuando las comunicaciones no eran tan confiables como ahora y las velocidades de transmisión eran bajas.

Para incluír la información necesaria para corregir los errores debe transmitirse una cantidad de bits considerable, además de los bits de información, lo cual origina una baja en la eficiencia en la transmisión.

En la actualidad, dada la baja incidencia de errores y las altas velocidades de transmisión, el enfoque que se toma es simplemente detectar los errores y, en caso de que ocurran, pedir la retransmisión de las tramas.

Cuando una trama es transmitida, pueden ocurrir tres cosas al recibirla:

- La trama llega sin errores.
- La trama llega con uno o más errores de bits detectados.
- La trama llega con uno o más errores de bits no detectados.

Examinaremos las dos técnicas más comunes de detección de errores:

- Bit de paridad.
- Chequeo por Redundancia Cíclica (CRC).

Bit de paridad

La primera técnica que se creó para detectar errores fue añadir un bit de paridad a cada bloque de bits transmitidos, es decir a cada carácter. Por ejemplo, si se están transmitiendo caracteres del código ASCII de 7 bits, se añade un octavo bit para hacer que el número de bits en el grupo 1 sea par si se está utilizando paridad par e impar si se usa paridad impar.

El código para la letra A en ASCII de 7 bits es 1000001. Si se utilizara paridad par, poniendo el bit de paridad al final, se transmitiría la secuencia 10000010. Para transmitirlos con paridad impar, se enviaría la secuencia 10000011.

Este esquema detecta algunos errores pero no es muy confiable.

Chequeo por Redundancia Cíclica (CRC)

Actualmente la técnica que más se utiliza es el chequeo por redundancia cíclica o CRC (Cyclical Redundancy Check). Esta técnica consiste en lo siguiente:

- Se toma el bloque de información a enviar (I) como una secuencia de bits que forman un polinomio, sin importar cuántos bits sean.
- Se divide esta secuencia, que está multiplicada por 2^N, entre un polinomio predefinido (P) de orden N(N+1) bits, utilizando aritmética en módulo 2.
- El residuo (R) es un polinomio de grado N-1, que se denomina CRC (N bits).
- Se transmite la secuencia de bits $2^N I + R$.

En el extremo receptor se realiza la división de todos los bits recibidos (la información más el CRC) entre el mismo polinomio que se utilizó para calcular el CRC. Si el residuo obtenido es cero, se toma la trama de información como válida. En caso contrario, se desecha y se solicita su retransmisión.

La efectividad de este técnica depende del grado del polinomio empleado. Característicamente se utilizan CRC de 16 o 32 bits, lo cual da una probabilidad de que una trama con errores sea tomada como válida con un orden de 10^{-18}.

1.3
Estructura de redes de comunicación

Las redes de comunicación de datos son utilizadas para que varias computadoras se comuniquen y puedan intercambiar datos y aplicaciones, así como compartir recursos de cómputo, almacenamiento, impresión, etc.

En su forma más simple, la comunicación de información toma lugar entre dos estaciones que están conectadas directamente por algún medio de transmisión. Una estación puede ser una computadora, una terminal, teléfonos u otros dispositivos de comunicación. Sin embargo, es impráctico para dos estaciones estar conectadas directamente por las siguientes razones:

- Las estaciones pueden estar muy alejadas geográficamente y sería demasiado caro establecer un enlace dedicado entre ellas.
- Pueden existir un conjunto de estaciones que requieran un enlace con otras en varias ocasiones y, excepto para pocas de ellas, es difícil proveer un cable dedicado entre cada par de estaciones.

En el último punto, cada estación tendría un enlace punto-a-punto con otra estación, topología que es conocida como malla. Si existieran N estaciones se necesitarían N(N-1)/2 enlaces full-duplex y cada dispositivo necesaitaría (N-1) puertos de E/S. Con lo que el costo del sistema, en términos de cableado y hardware de E/S, crecería proporcionalmente al cuadrado del número de estaciones.

La solución reside en conectar cada estación a una red de comunicación, como se muestra en la figura 1.2, que puede diseñarse para minimizar el costo de transmisión y proveer conexión total a más estaciones conectadas.

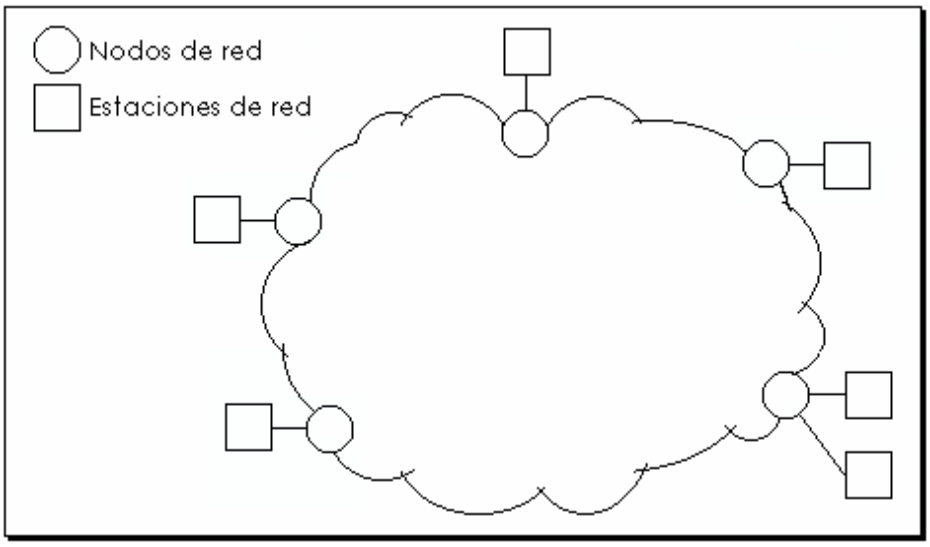


Figura 1.2 Interconexión a través de una red de comunicación

Las redes de computadoras están clasificadas en base a varios criterios, siendo el más importante la cobertura geográfica, por la que se clasifican en:

- Redes de área local (LANs).
- Redes de área metropolitana (MANs).
- Redes de área amplia (WANs).

Redes de área local

Las redes de área local o LANs (Local Area Networks), son utilizadas para comunicar un conjunto de computadoras en un área geográfica pequeña, comunmente un edificio o un conjunto de edificios cercanos, como universidades, centros de investigación, etc. La información intercambiada es principalmente de datos aunque empiezan a aparecer redes locales para la transmisión de video y soportando aplicaciones multimedia.

En el mundo existen más de un millón de redes locales y su crecimiento está considerado como el más fuerte del mercado.

Redes de área metropolitana

Estas redes también conocidas como MANs (Metropolitan Area Networks), cubren por lo general un área geográfica restringida, de dimensiones de una ciudad.

Suministra el transporte de datos a grandes velocidades (del orden de 100 Mbps) utilizando fibra óptica. Típicamente una MAN conectará LANs de más baja velocidad a través de una ciudad o región, solucionando las limitaciones de ancho de

banda. Para salvaguardar todos los datos transmitidos, las redes metropolitanas emplean mecanismos de autorecuperación para asegurar el grado más alto de disponibilidad y confiabilidad de la red. Las MANs son diseñadas de manera que el transporte sea fácilmente compartido por muchos clientes.

Las aplicaciones más sobresalientes de las redes metropolitanas son:

- Interconexión de LANs.
- Interconexión de Conmutadores Privados de Voz (PBX's).
- Interconexión de computadoras.
- Transmisión de aplicaciones CAD/CAM.
- Transmisión de video.

El uso de sistemas de fibra óptica para realizar la transmisión asegura virtualmente que las MANs no lleguen a su máxima capacidad en un futuro cercano. Estas redes pueden ser públicas o privadas.

Redes de área amplia

Las redes de área amplia, también conocidas como WANs (Wide Area Networks), son las primeras redes de comunicación de datos que se utilizaron. Estas redes cubren áreas geográficas muy grandes, del tamaño de un país o del mundo entero, como el caso de Internet que se verá en el capítulo 4.

Las redes de área amplia utilizan como parte de las facilidades de comunicación de datos, redes públicas y privadas. Además, pueden incluír la interconexión de varias redes heterogéneas, con muy distintas filosofías, arquitecturas y diferentes protocolos de comunicación.

Las redes WANs emplean conmutación de paquetes, inicialmente a baja velocidad (hasta 19 200 bps) con el protocolo X.25. Sin embargo, con las tecnologías recientes más rápidas y los requerimientos de las nuevas aplicaciones (multimedia), impulsan el empleo de nuevos protocolos como frame-relay y cell-relay, con los que se alcanzan velocidades de transmisión en el orden de Megabits/seg.

Hasta ahora se ha visto cómo se codifican y se transmiten los datos entre dos computadoras a través de un medio de transmisión, sin embargo, al hablar de una red de computadoras se entiende implícitamente que se tienen varias computadoras comunicándose a través de la red. La forma de construír una red que soporte la comunicación entre las computadoras constituye la topología de la red de comunicación. Pero toda red de computadoras consta de tres elementos básicos:

- Computadoras.
- Nodos de conmutación.
- Líneas de transmisión.

Las computadoras son los elementos que tienen la capacidad de cómputo y es donde residen los datos y las aplicaciones. En la tecnología de redes se les denomina computadoras estación o simplemente estaciones.

Los nodos de conmutación son generalmente computadoras especializadas llamada IMP (Interface Message Proccesor), aunque en algunos textos también se les denomina nodos intermedios, elementos de conmutación, etc.

Una computadora se conecta a la red a través de un nodo de conmutación y éste puede tener varias computadoras conectadas a él y a su vez debe estar conectado a otro u otros nodos de conmutación en la red.

Las líneas de transmisión con frecuencia son llamadas circuitos de comunicación, canales de comunicación o enlaces de comunicación, términos definidos inicialmente en la red ARPAnet. La función de estas líneas es conectar directamente tanto los nodos de conmutación entre sí, como las computadoras a los nodos de conmutación.

Existen dos tipos de canales de comunicación:

- Canales punto a punto.
- Canales multipunto.

Un canal punto a punto conecta directamente dos nodos de conmutación y la transmisión en él puede ser unidireccional (simplex), bidireccional alterna (half duplex) o bidireccional completa (full duplex).

En las redes de comunicación generalmente se utilizan canales de comunicación bidireccional completa.

Un canal multipunto, a diferencia del anterior, soporta varios dispositivos conectados al mismo canal. Cuando un dispositivo transmite sobre el canal, todos los demás dispositivos conectados a él pueden escuchar la transmisión; debido a esto, estos canales son comúnmente denominados "canales de difusión". En este caso, los dispositivos conectados al canal lo comparten, por lo que es necesario definir una política del uso del canal ya que no debe haber dos o más dispositivos transmitiendo simultáneamente a través de él.

1.4
Topologías físicas de red

La topología física de una red local se refiere a la forma en que se conectan físicamente las computadoras (u otros dispositivos) a la red. Por razones económicas las redes locales utilizan topologías simples, a diferencia de las redes de área amplia que generalmente utilizan una topología en malla.

A continuación, discutiremos las tres topologías físicas LAN que soporta el uso eficiente de los recursos de red. Pero debemos mantener en mente que una red también tiene una topología lógica que define la forma de las funciones de red y frecuentemente las redes tienen una topología lógica distinta a la física.

El bus.

El bus es la forma más simple de red multinodo. Aquí, todas las estaciones de la red están conectadas directamente a un cable central llamado bus o backbone. Cada estación tiene una dirección asignada y es un número único que la identifica. Permitiendo con esto, que cada una de ellas reconozca un mensaje que le está destinado y al mismo tiempo les permite direccionar mensajes a otra estación específica.

Cuando una estación transmite un mensaje, la señal eléctrica viaja a lo largo del bus y de acuerdo a los protocolos de red, cada estación puede capturar sólo los mensajes que están destinados a ella.

Esta topología está limitada en el número de estaciones que pueden estar en un segmento. Cada estación agregada al cable, absorbe parte de la señal eléctrica, por esto, un segmento puede soportar hasta 30 estaciones, más allá de estas, se tendrá que incluir un repetidor.

La ventaja de la topología de bus es que utiliza una cantidad mínima de cable y requiere hardware de red barato, por lo que es barata y fácil de instalar. Los protocolos de las redes Ethernet corren sobre una topología de bus.

Estrella.

En esta topología, un sistema central (un servidor o hub) conecta a los anfitriones o estaciones de trabajo directamente por medio de un cable individual. Debido a esto, la topología de estrella utiliza más cable que las topologías de bus y anillo. En general, esta topología es la más cara de todas.

El hub puede ser pasivo, donde sólo envía los datos de una máquina a otra; o puede ser un hub inteligente, el cual incluye algunas funciones adicionales para que trabaje como puente, transfiera archivos entre diferentes tipos de redes, etc.

Aparte de ser una topología muy cara, presenta la desventaja de sufrir el efecto de cuello de botella, porque todos los datos deben pasar a través del hub.

Anillo.

El nombre de esta topología radica en el hecho de que todas las estaciones están conectadas una con otra formando un círculo cerrado. Así, cada una de ellas está atada directamente a otras dos, una a cada lado de ella y, contrario al bus en el que la señal es direccionada en el cable, esta topología opera pasando la señal de estación a estación alrededor del anillo. Cada estación recibe un mensaje, si el mensaje es para ella lo captura, en caso contrario lo retransmite a la próxima estación. Con esto, el mensaje es amplificado y acondicionado, con lo que se disminuye la pérdida de información y se incrementa el número de nodos que puede soportar la red. Sin embargo, esta topología no ofrece un punto central para el manejo de la red.

Esta topología es relativamente cara y difícil de instalar, pero es muy robusta, ya que si falla un dispositivo no significa que falle toda la red.

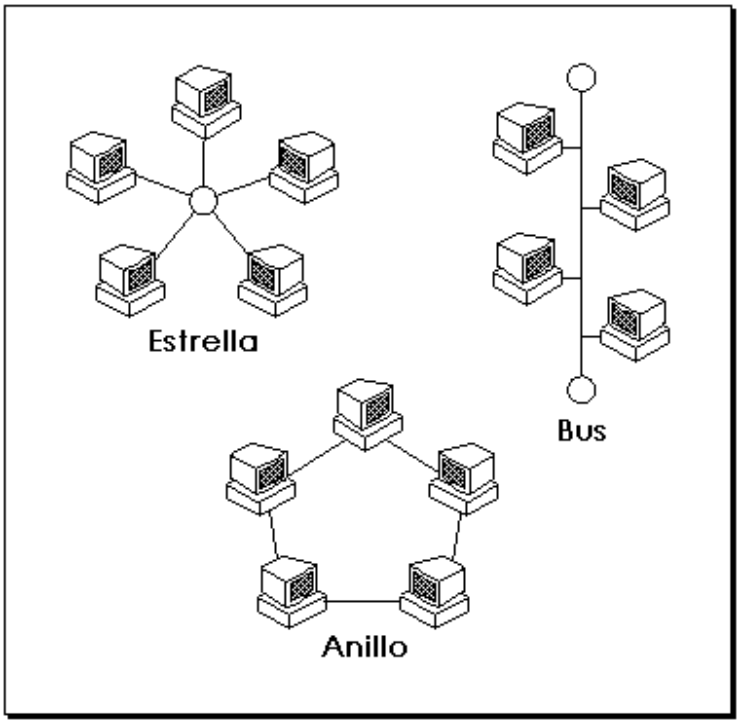


Figura 1.3 Topologías físicas de una LAN

El IEEE creó el proyecto 802 en febrero de 1980 para identificar y formalizar los estándares de LAN para velocidades de datos superiores a 2.0 Mbps. Con lo que se crearon los estándares 802. Estos estándares dividen la capa de enlace del modelo OSI en dos subcapas: la de Control de Acceso al Medio (MAC) y la de Control de Enlace Lógico (LLC). La primera se relaciona con las técnicas de acceso al medio físico compartido.

Mientras que algunas tecnologías de LANs poseen diferentes implementaciones de la subcapa MAC porque sus métodos de compartir el medio son diferentes, todas las LANs IEEE tienen la misma subcapa LLC. La ventaja de esto es que los mecanismos de las capas superiores pueden ser los mismos, sin importar el tipo de hardware de red.

1.5
Redes conmutadas

Las redes de comunicación conmutada consisten de una colección interconectada de nodos, en la cual los datos son transmitidos desde la fuente al destino, ruteándolos a través de redes de nodos.

Algunos nodos sólo estarán conectados a otros nodos, por lo que su tarea será la conmutación interna de los datos. Otros nodos tendrán una o más estaciones conectadas a él, de tal manera que podrán aceptar y entregar datos de y hacia esas estaciones.

Usualmente, las redes no están totalmente conectadas, no hay un enlace directo entre cada par de nodos, pero es deseable tener más de una ruta a través de la red para cada par de estaciones. Esto realza la confiabilidad de la red.

Existen básicamente tres tipos de redes de conmutación:

- Conmutación de circuitos.
- Conmutación de paquetes.
- Conmutación de mensajes.

Conmutación de circuitos

La comunicación mediante conmutación de circuitos implica que existe una ruta de comunicación dedicada entre las dos estaciones. Esa ruta es una secuencia conectada de enlaces entre nodos de red. En cada enlace físico, un canal está dedicado a la conexión. El ejemplo más claro de este tipo de comunicación es la red telefónica.

La comunicación vía conmutación de circuitos implica tres fases:

- Establecimiento del circuito. Antes de que una señal pueda transmitirse, se debe establecer un circuito estación a estación.
- Transferencia de datos. Una vez que se ha establecido el circuito, la información puede transmitirse.
- Desconexión del circuito. Después de la transferencia de datos la conexión se termina, generalmente por la acción de alguna de las estaciones.

Aquí, la ruta de conexión es establecida antes de que se inicie la transmisión de datos, de tal manera que la capacidad del canal debe reservarse entre cada par de nodos en la ruta y cada nodo debe tener la capacidad de la conmutación interna para manejar la petición de conexión. Los switches deben tener la inteligencia para permitir esa asignación y permitir una ruta a través de la red.

Las desventajas de este tipo de comunicación son:

- La capacidad del canal está dedicada para la duración de la conexión, aunque no haya datos para transmitir.
- Existe un retardo provocado por la petición de conexión. Sin embargo, una vez que se ha establecido el circuito, la red es efectivamente transparente al usuario y la información es transmitida a velocidades fijas, sin otro retardo que el provocado por los enlaces de transmisión.

Conmutación de paquetes

Las redes de telecomunicaciones de conmutación de circuitos para grandes distancias fueron diseñadas originalmente para tráfico de voz, y la mayoría del tráfico continúa siendo voz. Y como la capacidad del canal está totalmente dedicada para un enlace, para conexiones de voz proporciona un desempeño importante, debido a que la mayoría del tiempo se ocupa el canal. Pero, para conexiones de datos, este tipo de circuto resulta ineficiente porque:

- En una conexión típica de estación a nodo, la línea está ociosa la mayoría del tiempo.
- En una red de circuitos conmutados, la conexión transmite los datos a una velocidad constante, de tal manera que cada dispositivo que esté conectado debe transmitir y recibir a la misma velocidad que el otro. Esto limita la utilidad de la red al interconectar una variedad de estaciones y terminales.

La conmutación de paquetes resuelve estos problemas. Aquí, los datos son transmitidos en pequeños paquetes, de tal manera que si el transmisor tiene un mensaje grande para enviar, éste debe dividirse en una serie de paquetes, donde cada uno contendrá una porción de los datos del usuario además de información de control necesaria para rutear el paquete a través de la red y entregarlo al destino correcto. En cada nodo de la ruta, el paquete es recibido, almacenado brevemente y enviado al próximo nodo.

Tomemos como ejemplo la figura 1.4 y consideremos que un paquete será enviado desde la estación A a la estación E. El paquete contendrá información de control que indique que el destino final es E. El paquete es enviado desde A al nodo 4, donde se almacena el paquete, se determina el próximo nodo al que será enviado (supongamos que al 5) y se apila el paquete para su salida al enlace 4-5. Cuando el enlace está disponible, el paquete es transmitido al nodo 5, quien direccionará el paquete al nodo 6 y finalmente a E.

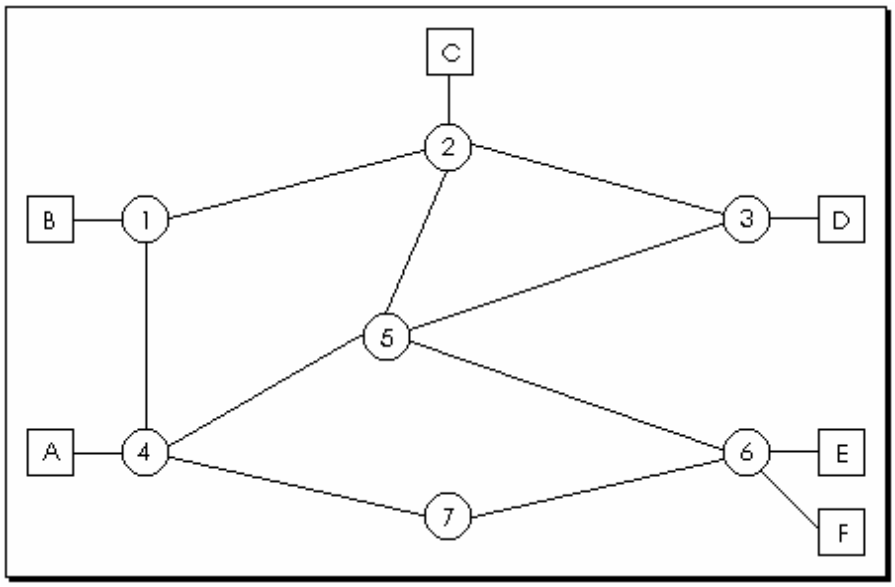


Figura 1.4 Red general de conmutación

Las ventajas con respecto a la comunicación de conmutación de circuitos son:

- La eficiencia de la línea es mayor desde que un simple enlace nodo a nodo puede ser compartido dinámicamente por muchos paquetes más tiempo. Estos paquetes son almacenados y transmitidos tan rápido como sea posible sobre el enlace. Por el contrario, en la conmutación de circuitos, el tiempo de un enlace nodo a nodo está predeterminado utilizando multiplexación síncrona por división de tiempo, y mucho

de éste último puede estar ocioso debido a que puede estar dedicado a una conexión ociosa.
- Las redes de conmutación de paquetes pueden realizar conversiones con respecto a la velocidad de los datos. Dos estaciones de diferentes velocidades pueden intercambiar paquetes debido a que cada una se conecta a su nodo y se adecúa a su propia velocidad.
- Cuando el tráfico llega a ser demasiado en una red de conmutación de paquetes, algunas llamadas son bloqueadas, rechazando las peticiones de nuevas conexiones hasta que la carga de la red disminuya. En una red de circuitos conmutados, los paquetes se siguen aceptando, pero el retardo en su entrega aumenta.
- Se utilizan las prioridades. Si un nodo tiene muchos paquetes en espera de ser transmitidos, puede enviar antes que nada los paquetes de mayor prioridad, permitiendo menos retardo en estos paquetes que los que tengan menor prioridad.

Una estación que tiene un mensaje para enviar a través de una red de paquetes conmutados que sea mayor que el tamaño máximo de paquete permitido, dividirá el mensaje en paquetes y los enviará, uno a la vez, por la red. Para manejar este flujo de paquetes al intentar rutearlos a su destino, existen dos enfoques: datagramas y circuito virtual.

En el enfoque de datagramas, cada paquete es tratado independientemente, sin ninguna referencia sobre los paquetes que se han enviado anteriormente. Refiriéndonos nuevamente a la figura 1.4, supongamos que la estación A tiene un mensaje formado por 3 paquetes para enviar a E. Transmite los tres paquetes al nodo 4, quien debe tomar una decisión de ruteo para cada paquete. Cuando llega el primero lo podría direccionar al nodo 5 o al 7; el nodo 4 determina que la lista de paquetes para el nodo 5 es más corta que para el nodo 7, asi que lo pone en la lista de paquetes para el nodo 5. De igual forma con el segundo paquete. Pero para el tercer paquete, el nodo 4 determina que ahora la lista es más corta para el nodo 7 y decide enviar el paquete 3 al nodo 7. De esta forma los paquetes con el mismo destino no siguen la misma ruta, y es posible que el paquete 3 llegue primero que el paquete 2 al nodo 6 y por lo tanto los paquetes sean entregados a E en diferente secuencia de como fueron enviados, y es responsabilidad de E reordenarlos. También es posible que un paquete sea destruído en la red. También es responsabilidad de la estación E detectar la pérdida de paquetes y tomar las medidas adecuadas para recuperarlos. En esta técnica, cada paquete tratado independientemente es conocido como **datagrama**.

En la técnica de **circuito virtual**, una ruta predefinida es establecida antes de que cualquier paquete sea enviado. Por ejemplo, supongamos que A en la figura 1.4 tiene uno o más mensajes que enviar a E. Primero envía un paquete especial de control referido como paquete de petición de llamada (CR) al nodo 4 pidiendo una conexión lógica con E. El nodo 4 decide la ruta de la petición y de todos los paquetes subsecuentes al nodo 5, el cual hace lo mismo con el nodo 6, quien finalmente entrega el paquete de petición de llamada a E. Si E está preparado para aceptar la conexión, envía un paquete de aceptación de llamada a 6 quien lo pasa al nodo 5, al 4 y finalmente a A. Las estaciones A y E ahora pueden intercambiar datos sobre la ruta que se ha establecido. Debido a que la ruta es fija para la duración de la conexión lógica, algunas veces es similar a un circuito en una red de conmutación de

circuitos, y ésta es referida como circuito virtual. Ahora cada paquete contiene un identificador de circuito virtual además de los datos. Cada nodo de la ruta preestablecida sabe dónde direccionar tales paquetes, por lo que no se requiere tomar decisiones de ruteo. Al final, una de las estaciones termina la conexión con un paquete de petición de limpieza (CR) y en cualquier momento cada estación puede tener más de un circuito virtual a cualquier otra estación.

La característica principal de esta técnica es que una ruta entre estaciones se establece antes de que se transfieran datos. Esto no significa que sea una ruta dedicada como circuitos conmutados, debido a que los paquetes llegan a un nodo y son almacenados para su salida. La diferencia con la técnica de datagrama y circuito virtual es que el primero necesita tomar decisiones de ruteo para cada paquete y en el segundo sólo se lleva a cabo una vez para todos los paquetes.

Si dos estaciones desean intercambiar datos sobre un periodo de tiempo largo, existen ventajas en los circuitos virtuales. Primero, la red puede proveer servicios relacionados al circuito virtual incluyendo secuencia y control de error. La secuencia se refiere al hecho de que todos los paquetes siguen la misma ruta y llegan en el mismo orden. El control de error es un servicio que asegura no solo que los paquetes lleguen en secuencia apropiada, sino también correctamente. Esto es, si un paquete en una secuencia del nodo 4 al 6 falla al llegar al nodo 6 o llega con errores, este nodo puede solicitar la retransmisión del paquete al nodo 4. Otra ventaja es que los paquetes deberían transitar sobre la red más rápidamente con un circuito virtual al no tomar decisiones de ruteo para cada paquete.

Una ventaja de la técnica de datagrama es que si se desea enviar unos cuantos datagramas, la entrega será más rápida. Otra ventaja es que debido a su naturaleza primitiva, es más flexible. Por ejemplo, si una parte de la red está muy congestionada, los datagramas pueden tomar rutas alternas. En cambio, el circuito virtual sigue la ruta predeterminada aun cuando cruce por la zona congestionada. Otra ventaja es que con datagramas la entrega es inherentemente más confiable. En el circuito virtual, si un nodo falla, todos los circuitos virtuales que pasen por ese nodo estarán perdidos. Con la técnica de datagrama, si un nodo falla, los paquetes subsecuentes podrán encontrar una ruta alterna que salte dicho nodo.

Conmutación de mensajes

Aquí se transmiten mensajes de un lado al otro de la red. La transmisión es tal que el "canal" no queda expuesto a períodos de silencio, es decir, cuando no se transmite un mensaje el canal queda disponible para ser usado por otras estaciones.

Los mensajes se establecen en un canal a través de un multiplexor por división de tiempo por lo cual a un mismo tiempo el canal puede estar compartido por varios usuarios.

Este sistema surgió con la necesidad de satisfacer la demanda de distintos usuarios telegráficos, que necesitaban realizar una transmisión sin respuesta inmediata. El diálogo es no convencional (no dialogan las terminales) ni se efectúa en tiempo real.

Una terminal envía un mensaje a un centro de conmutación de mensajes (CCM) archivándose a un disco magnético. Se le asigna una posición de memoria correspondiente a la terminal de origen formándose así "colas" de espera de mensajes. El mensaje es transmitido a la terminal de destino cuando le llega el turno, siempre y cuando la misma esté desocupada. Luego de enviado el mensaje, la red le informa a la estación de orígen qué pasó con el mensaje transmitido.

Cada mensaje lleva la identificación de la información de orígen y del destino. El mensaje puede esperar en el CCM por espacio de una hora y puede ser difundido simultáneamente a varios usuarios. Cada usuario puede solicitar que sus mensajes permanezcan por más tiempo en el CCM pagando un abono extra.

El encaminamiento de la información se establece según prioridades, y los CCM controlan y corrigen errores antes de que el mensaje sea transmitido a otro CCM. El segundo CCM recibe la información, la analiza, efectúa el chequeo de errores, agrega nueva información de control y la transmite hacia el otro CCM o usuario.

1.6
El modelo de referencia OSI

Cuando se utiliza un conjunto de computadoras que cooperan para realizar un trabajo, el panorama se complica un poco ya que es necesario tener equipo (hardware) y programas (software) que les permita a las computadoras comunicarse.

El equipo de comunicación está relativamente estandarizado y presenta pocos problemas, aun cuando sea fabricado por diferentes proveedores; sin embargo, los programas de comunicación presentan un serio problemas de compatibilidad, aunque sean proporcionados por el mismo proveedor.

Para tratar de resolver este problema, la Organización Internacional de Estándares (ISO) creó un subcomité en 1977 que propuso un modelo para la interconexión de máquinas. Este subcomité presentó el modelo OSI (Interconexión de Sistemas Abiertos), el cual fue adoptado en 1983. Este modelo no constituye un estándar, sino que es simplemente una guía que se ha utilizado para definir estándares.

Este modelo proporciona una base conceptual para crear estándares, especificando solamente las funciones que deben realizarse y la forma en que debe efectuarse la interconexión a nivel de interfaz. Pero no especifica nada respecto a la forma interna en que estas funciones deben construirse.

Para desarrollar el modelo de referencia OSI se tomó el enfoque de partir las funciones de comunicación en forma vertical, definiendo un conjunto de capas o niveles que realizaran estas funciones. Un nivel proporciona servicios al nivel superior y se apoya en los servicios que le proporciona el nivel inferior. Además, un nivel en una máquina se comunica en forma horizontal con el nivel correspondiente en la otra máquina mediante un conjunto de reglas que constituyen el protocolo de comunicación entre dichos niveles. Cada nivel tiene su propio protocolo de comunicación.

Los cambios realizados en un nivel no deben afectar al resto de los niveles, suponiendo que se siguen las mismas reglas de comunicación entre el nivel modificado y los niveles adyacentes.

Cada uno de los niveles se diseñó pensando en que pudiera comunicarse directamente con el nivel correspondiente en la máquina con la que se está comunicando, usando una comunicación de igual a igual, aun cuando para hacerlo se apoye en los servicios que proporciona el nivel inferior.

Algunos de los principios que se usaron para definir los niveles del modelo OSI son:

- No crear más niveles de los requeridos para no complicar innecesariamente el diseño.
- Crear una frontera donde la definición de servicios sea pequeña y la comunicación a través de la frontera sea mínima.
- Crear niveles diferentes cuando las funciones que se realicen sean esencialmente diferentes.
- Mantener funciones similares dentro del mismo nivel.
- Crear una frontera cuando sea conveniente para estandarizar una interfaz.
- Crear un nivel cuando se necesite un nivel diferente de abstracción.

Siguiendo los principios anteriores, la ISO creó el modelo de referencia de siete niveles, como se muestra en la siguiente figura.

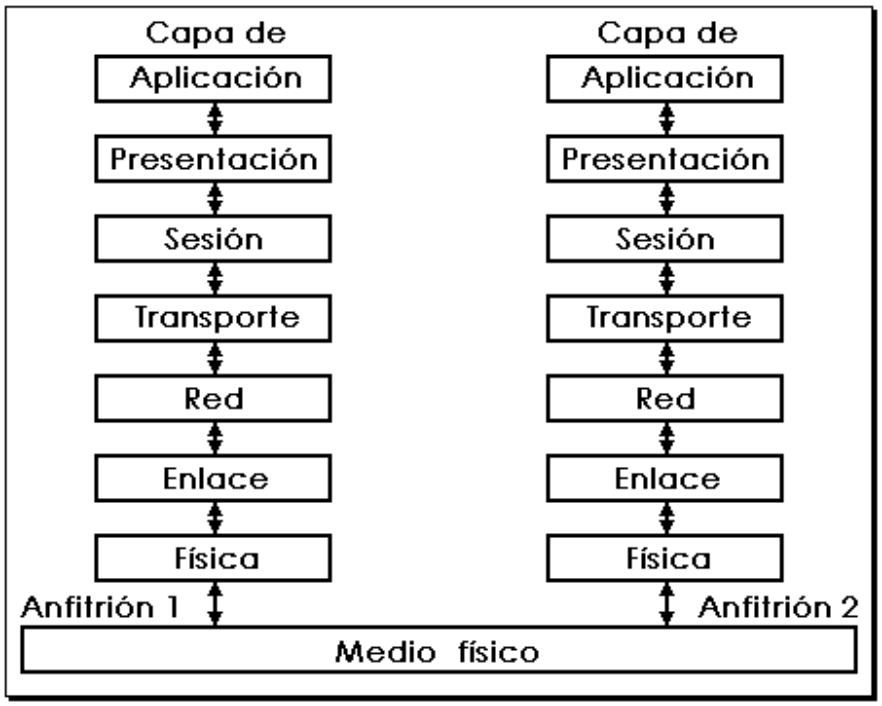


Figura 1.5 Capas del modelo de referencia OSI

A continuación, se explica brevemente lo que cada capa debe hacer comenzando por la capa inferior.

- Capa física. En esta capa es donde se genera la corriente y el voltaje eléctrico, los pulsos físicos u ópticos responsables de mover los datos. Las unidades que se manejan aquí son los bits.
- Capa de enlace. Es el primer nivel que recoge los bits y maneja los datos como paquetes. Aquí se lleva a cabo la corrección y detección de errores, de la misma manera que se desechan los paquetes defectuosos.
- Capa de red. Rutea los paquetes a través de múltiples dispositivos para asegurarse de que lleguen a su destino. El Protocolo Internet (IP) opera en este nivel, así como el IPX de NetWare. En esta capa también opera el servicio "sin conexión".
- Capa de transporte. Es un nivel de transición (el último de los niveles que maneja el ruteo de paquetes y la recuperación de errores). Esta capa resuelve cualquier deficiencia que ocurra en el nivel de red. Si los paquetes son recibidos correctamente en el nivel de red, esta capa llega a ser muy simple. Pero si el sistema de comunicación no provee el servicio de transmisión de paquetes confiable, este nivel lo compensará llegando a ser, obviamente, más complejo. TCP opera en esta capa.
- Capa de sesión. Esta capa mantiene la transmisión "orientada a conexión". El proceso de crear y romper conexiones en este nivel es el hecho de establecer y destruír sesiones.
- Capa de presentación. Se ocupa de los aspectos de sintaxis y semántica de la información que se transmite. Esto es, las diferencias en la representación de los distintos estándares (ASCII, EBCDIC, ect.) se corrigen aquí.
- Capa de aplicación. En esta capa se encuentra el software de las aplicaciones de los usuarios.

1.7 Resumen

Un sistema de comunicación de datos es un conjunto de elementos que interactúan para lograr transmitir información de un lugar a otro. Entre sus principales funciones se encuentran: la segmentación, sincronización, detección y corrección de errores, etc. Para poder adaptar la comunicación de datos a las redes de computadoras la Organización Internacional de Normas creó el modelo de referencia OSI, donde todas las actividades se encuentran jerarquizadas en siete capas, que tienen un carácter individual pero al mismo tiempo están estrechamente relacionadas. Por otra parte, de acuerdo al área geográfica que abarcan, las redes de computadoras pueden catalogarse en redes de área amplia, de área metropolitana o de área local.

2

La tecnología Ethernet

Las redes locales permiten la interconexión de diferentes dispositivos (computadoras, procesadores, impresoras, etc.) y su gran aceptación se debe a que facilitan el intercambio de información y permiten compartir recursos.

Ethernet es una red local que cumple con todos los requerimientos de las redes locales, y desde sus inicios ha sido motivo de gran discusión; pero sigue siendo la mayor base instalada en redes locales para ambientes de oficina, universidades pequeñas, etc. Producto de las diferentes opciones que se pueden elegir con las implementaciones desarrolladas, de su tecnología madura, económica y sencilla que ha logrado cubrir convenientemente las necesidades de distintos usuarios como lo muestran las distintas variantes de la norma que se han desarrollado. En particular 10BaseT se ha hecho muy popular ya que aprovecha las ventajas del cableado estructurado. Todo lo anterior ha hecho de Ethernet la tecnología de red local más utilizada con más de 40 millones de dispositivos conectados en distintas redes.

En este capítulo se verán los principios generales en que se sustenta el funcionamiento de las redes tipo Ethernet. Se presentarán algunas características y modos de operación de las distintas redes locales tipo Ethernet.

Una red local está formada por un conjunto de computadoras y otros dispositivos interconectados dentro de un área geográfica limitada, con el fin de compartir recursos e intercambiar información. La gran mayoría de las redes locales se caracterizan por:

- Radio de acción pequeño, hasta de unos cuantos Km.
- Velocidades de transmisión del orden de millones de bits/seg.
- Ambiente relativamente libre de errores de transmisión.
- Medio de comunicación compartido por todos los dispositivos conectados a la red.
- Flexibilidad en la tecnología, es decir, facilidad en la modificación y reconfiguración de la distribución física de los dispositivos conectados a la red.

Ethernet, el tipo de red local más difundido en la actualidad, cumple con todas las características anteriores. Su primera implementación fue desarrollada en Xerox, por Robert M. Metcalfe, a principios de los 70's para conectar hasta 100 estaciones de trabajo en un área de 1 Km transmitiendo información a 2.94 Mbps. Es concebida y recomendada en ambientes de oficina, universidades pequeñas, etc.

Ethernet toma su nombre en recuerdo de aquella teoría del siglo XIX según la cual el universo estaba suspendido en una especie de éter por el que las ondas electromagnéticas podían propagarse.

En 1978 se publica la primera norma como un trabajo conjunto de las empresas Xerox, Intel y DEC. Ésta es la base del estándar ANSI/IEEE 802.3 publicado en 1983 por el IEEE.

En Ethernet, el canal de comunicación común es un cable coaxial, el bus, con impedancias (resistencias que opone el medio al paso de la señal) de terminación en los extremos, al que se conectan todos los dispositivos que forman la red (figura 1.3).

Cada sitio en la red local tiene un identificador único: su dirección. Cuando una computadora desea enviar información a otro dispositivo, simplemente forma un paquete con el mensaje, la dirección del destinatario, su propia dirección y otra información. En el ambiente de redes locales, a estos paquetes se les llaman tramas. Una vez formada la trama, ésta se envía en serie, bit por bit a través del cable. Las señales en el bus son omnidireccionales (se difunden en los dos sentidos del cable), de tal manera que todos los dispositivos conectados a la red detectan la información. Aquel dispositivo que reconozca en la dirección destino su propia dirección, sabe que la trama contiene información dirigida a él y por lo tanto la leerá del bus. Los demás sitios ignorarán la trama.

2.1
Protocolo de acceso

Como en casi todas las redes locales, se tiene un canal común a todas las estaciones a través del cual se envía la información. Todos los nodos que se conectan a la red deben obedecer una serie de reglas y convenios para establecer cuándo y cómo se puede acceder al canal común. A estas reglas se les conoce como

"protocolos de acceso al medio", y para Ethernet el protocolo utilizado es "Acceso Múltiple con Sensado de Portadora y Detección de Colisiones" o CSMA/CD.

Una estación que desea transmitir escucha primero si alguien está transmitiendo (está sensando la presencia de portadora). Si encuentra libre el medio envía la trama, en caso de encontrarlo ocupado espera a que se libere y transmite su trama inmediatamente.

En CSMA/CD la estación que transmite "escucha la señal en el cable". Si lo que recibe es lo que está enviando, todo va bien, en caso contrario, supone que ha ocurrido una colisión. Al detectar una colisión, la estación transmisora aborta su trama y en su lugar envía una señal de cuatro a seis octetos reforzando la colisión para garantizar que las demás estaciones involucradas en la interferencia también puedan detectar la colisión. Después de enviar esta señal, la estación espera durante un intervalo de tiempo aleatorio y vuelve a intentar la transmisión de la trama escuchando en el bus para ver si éste se encuentra libre.

Con este protocolo de acceso, las redes Ethernet ofrecen un tiempo de respuesta inmediato cuando el tráfico en el bus es muy poco. Conforme se va incrementando el tráfico, las probabilidades de colisión aumentan así como los tiempos de espera, precisamente para tratar de disminuír la posibilidad de colisiones múltiples. En un ambiente de mucho flujo de información, los tiempos de respuesta serán considerables y, sobre todo, no predecibles. Referente a ésto último, CSMA/CD es un protocolo de detección de portadora. Sin embargo, la mayor parte de las implementaciones de Ethernet, incluyendo las especificaciones definidas por Xerox, Intel y DEC, no utilizan una señal modulada para enviar su mensaje como se usa en las transmisiones de radio y televisión, por poner un ejemplo. A los sistemas que, como Ethernet, no utilizan una portadora para enviar su información se les conoce como sistemas de transmisión en banda base. En ellos, todo el ancho de banda del medio es utilizado por la señal que se está transmitiendo.

Si no se cuenta con una portadora, ¿cómo puede detectarse entonces si hay o no una transmisión en curso? Ethernet utiliza un tipo de señalización conocido como "codificación Manchester" que garantiza que en cada bit transmitido ocurrirá una transición de nivel lógico de la señal. Esta transición, que ocurre a la mitad del intervalo de un bit, permite al receptor sincronizarse con el transmisor, pues siempre pueden existir pequeñas variaciones entre la velocidad de uno y otro. Por otro lado, una estación que desea transmitir un mensaje se dará cuenta si el bus está libre o no al detectar las transiciones de una posible señal.

Una red Ethernet no puede excederse un límite máximo, pues de lo contrario el tiempo de propagación aumentaría, haciendo que el protocolo de acceso no trabaje correctamente.

La trama debe tener un mínimo de 512 bits, es decir, 64 octetos. Si ésta fuera menor, la estación transmisora terminaría de transmitir la trama en un tiempo menor a la ventana de colisión (intervalo máximo de tiempo que puede transcurrir antes de detectar una colisión) y, por lo tanto, podría no entenderse de que su mensaje fue alterado por una colisión.

2.2
La trama Ethernet 802.3

Para tener una mejor comprensión de la manera en que operan las redes tipo Ethernet, conviene analizar los campos que integran las tramas de información que se transmiten por el bus. Además, es precisamente en la estructura de estas tramas donde se manifiestan algunas de las diferencias más importantes entre la trama IEEE 802.3 y la especificación original de Ethernet.

Figura 2.1 La trama Ethernet 802.3

Preámbulo

Es un campo de 7 octetos con el código 10101010. Al transmitir estos octetos en codificación Manchester, se genera una señal cuadrada que sirve para sincronizar a los receptores en la red.

Delimitador de inicio de trama (SFD)

Es un octeto formado por el patrón 10101011. El último par de bits interrumpe la onda cuadrada formada por el preámbulo y los primeros bits de este octeto. Esta interrupción sirve para indicar dónde se inician los campos con información útil.

Dirección destino

Como se ha mencionado, cada estación en la red tiene un identificador único que es su dirección. Este campo contiene la dirección del sitio al que se envía la trama. Si el bit más significativo es un '1', la trama está dirigida a varias estaciones (multidifusión), no a una sola. Las direcciones destino con todos los bits en '1' son tramas dirigidas a todos los sitios en la red (difusión).

Ethernet utiliza 6 octetos para los campos de direcciones. Con esto se tiene un rango de 2^{48} valores, con la intención de garantizar que ningún otro dispositivo en el mundo pueda tener una misma dirección. Los distintos fabricantes de interfaces Ethernet obtienen una licencia con un rango de direcciones válidas que le son asignadas por el IEEE (Instituto de Electricistas e Ingenieros en Electrónica). Por ejemplo, cualquier dirección cuyos primeros 3 octetos son 00-00-0C hexadecimal corresponde a un dispositivo CISCO, mientras que 02-60-8C es 3Com.

En la norma IEEE 802.3 se permiten utilizar campos de direcciones de 2 o de 6 octetos, pero para una misma red local las direcciones deben tener el mismo tamaño. Además, para redes con direcciones de 6 octetos, el segundo bit más significativo (bit 46) tiene un significado especial: si es '1' el ámbito de validez de la dirección es local; de lo contrario es universal, es decir, asignada como única dirección en el mundo por el IEEE.

Dirección fuente

Contiene la dirección de la estación que generó la trama. Desde luego no tiene sentido que este campo tenga todos los bits en '1' pues indicaría dirección de difusión.

Tipo de trama o longitud

Para Ethernet este campo contiene el tipo de trama. En la mayor parte de los casos esto permite identificar cómo interpretar el campo de datos, pues indica el tipo de protocolo de capas superiores que lleva la trama. Por ejemplo, si la trama contiene información del protocolo de red IP de Internet, este campo contiene el valor (08-00) hexadecimal.

Para IEEE 802.3 este campo indica el número de octetos válidos en el campo de información. Puede tomar valores de 0 a 1508.

Información

En este campo viaja la información que se transfiere de un sitio a otro. Para determinar el tamaño de la trama se toman en cuenta todos los campos excepto el preámbulo y el delimitador de inicio de trama. De esta manera, para redes con direcciones de 6 octetos, el tamaño mínimo de campo de información debe ser de 46 octetos. En caso de que la estación emisora quiera enviar menos de 46 octetos, se deben agregar caracteres de relleno (padding) para completar los 46 octetos requeridos.

Para garantizar un comportamiento más justo y evitar que una estación se adueñe de la red, también se ha definido un tamaño máximo de la trama de 1518 octetos. En otras palabras, la unidad más grande de información que puede ser transferida entre dos estaciones a la vez es de 1500 octetos, suponiendo campos de direcciones de 6 octetos.

Secuencia de verificación de trama

El último campo es un código de chequeo por redundancia cíclica (CRC) de 32 bits, calculado con los campos de dirección fuente y destino, tipo (o longitud) e información para tratar de predecir la integridad de la trama. La estación transmisora calcula el CRC y lo añade a la trama cuando la envía por la red. El receptor recibe la trama y nuevamente calcula el CRC. Si el valor calculado es diferente al recibido, se supone que la trama ha sido alterada por ruido en el medio, por lo que se descarta.

2.3
Redes locales tipo Ethernet

La red especificada por Xerox, Intel y DEC, corresponde a una sola implementación de Ethernet, en la que se basa el estándar 10Base5 de la norma IEEE 802.3. Posteriormente, varios fabricantes han decidido implementar variantes de la norma respondiendo a las diferentes necesidades de los usuarios. Así surgieron una gama de tecnologías que han sido incorporadas a revisiones posteriores de la norma IEEE 802.3.

Para poder identificar rápidamente una implementación particular, se ha establecido una nomenclatura especial formada por tres parámetros: la velocidad de transmisión, la técnica de señalización y el tamaño del segmento. Por ejemplo, 10Base5 significa una red a 10 Mbps, con señalización en banda base y con un tamaño máximo de 500 metros.

10Base5

El medio de transmisión es un cable coaxial de 50 ohms de impedancia. Este cable tiene un grosor aproximado de un centímetro, y generalmente es de color amarillo o naranja con marcas circulares cada 2.5 mts, que indica dónde se puede conectar una estación. El cable coaxial corre a lo largo de la oficina o edificio donde está instalada la red, y a través de él viajan las tramas entre las estaciones a una velocidad de 10 Mbps en banda base con señalización Manchester.

Un segmento de red puede tener un máximo de 500 mts. Y debe tener resistencia de terminación en sus extremos que absorban las señales para evitar que éstas se reflejen, provocando efectos de eco. Aunque el segmento tiene 200 marcas, no permite que haya más de 100 dispositivos conectados en un mismo segmento de red.

El alcance y las capacidades de la red pueden aumentarse conectando dos segmentos a través de un repetidor. Puede haber un cable coaxial que sirve sólo para unir dos repetidores, a lo que se conoce como segmento de enlace, y no debe tener ningún otro dispositivo conectado a él.

Debido a las limitaciones impuestas por la ventana de colisión de CSMA/CD, la red tiene restricciones en el tamaño máximo permisible:

- No puede haber más de 1024 dispositivos en una red.
- Entre dos estaciones cualquiera, no puede haber más de 4 repetidores.
- Por lo tanto, entre dos estaciones cualquiera no debe haber más de 5 segmentos, limitando la distancia máxima entre nodos a 2.5 Km.
- De los 5 posibles segmentos que separan a dos dispositivos, solo 3 pueden ser segmentos de red, los otros dos serán segmentos de enlace.

10Base2

También conocida como cable delgado o CheapNet, utiliza un cable coaxial más delgado, de 5 mm de diámetro. Fue concebida como una alternativa más económica a 10Base5 y se recomienda en ambientes universitarios y de oficina para interconectar computadoras personales y estaciones de trabajo.

Ya que el cable delgado es más propenso al ruido, la longitud máxima de los segmentos se reduce a 100 mts. También el número de nodos permitidos en un segmento de red se reduce a 30 como máximo, pero éstos ya no deben colocarse en puntos específicos separados 2.5 mts. Sino que pueden colocarse en cualquier parte con una separación mínima de 0.5 mts.

La velocidad de transmisión, la técnica de señalización, el número de segmentos y repetidores, la ventana de colisión, etc. son las mismas que 10Base5.

1Base5

Diseñada inicialmente por AT&T como una alternativa aún más económica que 10Base2, esta implementación utiliza par trenzado de alambre de cobre no blindado (UTP) muy similar al que se ocupa en la red telefónica. Cada dispositivo se conecta a un concentrador por medio de dos pares trenzados, uno para transmisión y otro para recepción, resultando en una topología de estrella. Por eso a 1Base5 se le conoce popularmente como StarLan.

La transmisión de la información se hace en código Manchester, pero como las características eléctricas del par trenzado lo hacen mucho más propenso al ruido, se decidió reducir la velocidad de transmisión a 1 Mbps manteniendo una longitud de segmento (del concentrador a la estación) de 250 mts.

Cuando un concentrador detecta una trama en uno de sus puertos, regenera la señal y la difunde por los demás, incluyendo el puerto del emisor original. Si el concentrador detecta la emisión de tramas desde dos puertos diferentes, entonces genera una señal especial llamada presencia de colisión (CP) que difunde por todos los puertos hasta que todas las estaciones han dejado de transmitir. Con el fin de que las estaciones puedan detectar la ocurrencia de una colisión, la señal CP es fácilmente identificable, pero no respeta las reglas de codificación Manchester.

El número de puertos que un concentrador puede soportar no se especifica en el estándar, pero difícilmente excede los 48 dispositivos. Varios concentradores pueden conectarse en cascada formando una topología de árbol, con el fin de extender el alcance geográfico de la red así como el número de dispositivos conectados.

En esta topología se permiten hasta 5 niveles de concentradores. El nivel más alto está formado por un concentrador llamado concentrador cabeza (H HUB) y ejecuta las funciones descritas anteriormente. Los demás concentradores se conocen como concentradores intermedios (I HUB) y tienen la función de transmitir ya sea la trama que reciben o, si detectan una colisión, la señal de presencia de colisión a todos los puertos, asi como a su concentrador superior. Asimismo, si detectan una trama o una señal de presencia de colisión por la liga que los une a su concentrador superior, deben difundir esta señal por todos los puertos inferiores. De esta manera, la topología física de árbol-estrella, se comporta en realidad como un bus lógico.

10Broad36

El cable coaxial de 75 ohms empleado es el mismo que se utiliza en la transmisión de televisión por cable. También trabaja a 10 Mbps, pero la información no se transmite en banda base, sino modulada por fase sobre una portadora a una frecuencia determinada (DPSK). Esta implementación tiene como justificación el poder usar el mismo cable de la red para otros propósitos paralelamente a la transmisión de datos, mediante la técnica de multiplexación en frecuencia. Por ejemplo, algunas frecuencias podrían asignarse para transmitir audio o video, mientras que otras se utilizarían para la red local.

En banda ancha generalmente se utiliza una transmisión unidireccional, es decir, que la señal que genera un circuito emisor está dirigida solamente hacia un

extremo, no se difunde por todo el cable como ocurre en banda base. Por esta razón, existen dos modos de operación en 10Broad36 dependiendo de si se utiliza un solo cable o si la red está formada por dos, uno para transmisión y el otro para recepción. En cualquier caso, la red termina en un dispositivo terminal (HeadEnd). El tamaño máximo permitido para un segmento es de 1800 mts. Por lo que la distancia máxima que recorre una trama en la red es de 3600 mts.

Cuando se tiene un solo cable, la unidad de acoplamiento transmite la trama unidireccionalmente hacia el dispositivo terminal con una frecuencia f1. El dispositivo terminal utiliza un remodulador para trasladar y retransmitir la trama a una frecuencia f2. Al igual que en 10Base5, el emisor recibe la trama y la compara con lo enviado. En caso de error, asume que se ha producido una colisión, por lo que envía la señal de refuerzo de colisión (CE) en una frecuencia especial, adyacente a f1.

En sistemas con cable dual, uno se utiliza para transmisión y el otro para recepción. En este caso la transmisión y recepción de señales se hace a una misma frecuencia, y el dispositivo terminal únicamente funciona como una especie de repetidor que conecta los dos extremos de los segmentos. En este caso la unidad de acoplamiento requerirá de dos conectores, uno para cada cable.

Cada canal de datos de la red local requiere un ancho de banda de 14 MHz y son necesarios 4 MHz adicionales para la transmisión de la señal de refuerzo de colisión. Así, se necesitan 18 MHz en el cable por cada canal de datos (por cada red local) en un ambiente con doble canal, y 36 MHz en instalaciones con un solo cable.

10BaseT

Las ideas en que se fundamenta 1Base5 son muy buenas, pero el hecho de que la transmisión se efectúe a 1 Mbps hace que su integración con otras implementaciones a 10 Mbps sea compleja. 10BaseT también usa UTP como medio de comunicación entre las estaciones, y un concentrador que ahora se llama repetidor multipuertos, pero la transmisión se hace a una velocidad de 10 Mbps. El precio que se paga es que ahora la distancia máxima entre la estación y el concentrador es mucho menor de 200 mts.

Al igual que en 1Base5, la configuración más sencilla es una topología de estrella con dos pares trenzados uniendo cada dispositivo con un puerto del concentrador. Una alternativa cada vez más común permite usar fibra óptica entre la tarjeta de red y el repetidor multipuertos, facilitando que el dispositivo se separe hasta 500 mts del repetidor.

La principal diferencia con 1Base5, además de la velocidad de transmisión, consiste en que en 10BaseT todos los repetidores multipuertos tienen la misma función. De hecho, cuando se conectan varios repetidores multipuerto, éstos no forman un árbol como en 1Base5, sino una configuración similar a la de 10Base5 donde el repetidor multipuertos se compara exactamente igual que un repetidor normal.

Por lo general, los repetidores multipuertos ofrecen al menos un puerto con la interfaz adecuada para poder enlazarse al cable grueso de 10Base5 o al delgado de 10Base2. Con ello un usuario puede aprovechar su base instalada en cable coaxial e ir

formando nuevas expansiones de la red usando 10BaseT con la garantía de que obtendrá una integración total.

Con 10BaseT pueden concebirse una multitud de configuraciones. De hecho, una de sus mayores ventajas es precisamente su flexibilidad al cambio. Una topología común consiste en conectar todas las estaciones de un mismo piso a un repetidor multipuertos, y conectar todos estos repetidores a un cable grueso que hará las veces de espina dorsal.

Las restricciones que se aplican a esta implementación son las mismas que en 10Base5: entre dos estaciones cualesquiera no debe haber más de cuatro repetidores y no puede haber más de cinco segmentos de los cuales 2 deben ser de enlace. La distancia máxima que puede cubrirse con la red es por tanto de 500 mts.

Sobre esta tecnología se basa la red local de la Universidad Tecnológica de la Mixteca.

10BaseF

Es una Ethernet a 10 Mbps corriendo sobre fibra óptica. Junto con su predecesor, FOIRL, son recomendadas para backbone entre edificios, ya que no se ve afectada por el ruido. Dependiendo de la tecnología de señalización y del medio usado, su alcance puede llegar a los 3 Km.

2.4
Ventajas y desventajas de Ethernet

El liderazgo de Ethernet se debe principalmente a:

- Es una tecnología madura, bien adaptada a las necesidades que se tenían en los ambientes de oficina de los 70's y 80's.
- Es relativamente simple de implementar. Su protocolo de acceso al medio ofrece un comportamiento aceptable en cargas de trabajo ligeras.
- La política de apertura seguida por Xerox y la gran aceptación de esta tecnología por parte de los fabricantes de equipos, han permitido que Ethernet sea el tipo de red a escoger en ambientes heterogéneos.
- Es sumamente flexible a los cambios en la configuración de la red.

Dentro de las desventajas que presenta Ethernet se encuentran:

- Las redes basadas en CSMA/CD no pueden garantizar cuándo pueden tomar el canal para enviar su trama. Por ello, estas redes no se adecúan a ambientes en tiempo real, es decir, aquellos que necesitan tiempos de respuesta determinísticos.
- El tamaño mínimo de la trama es de 64 octetos. Si lo único que se desea enviar es una señal de reconocimiento, se desperdicia gran parte del ancho de banda del canal.
- El tamaño de la red está limitado a unos cuantos Km. Querer aumentar esa distancia significa aumentar la ventana de colisión y con ello el tamaño de la trama. Por otro lado, si la ventana de colisión está fija a 5.12 μs transmitir a una

velocidad mayor a 10 Mbps requeriría de un tamaño mínimo de la trama mayor. En otras palabras, aumentar el tamaño de la red o aumentar la velocidad de transmisión harán que la red se comporte más ineficientemente. Lo peor es que las aplicaciones de hoy en día, como transmisión de imágenes y video entre nodos, necesita precisamente un tipo de red con velocidades de transmisión mayores, y abarcando áreas geográficas de más de 2 Km.

- La eficiencia de la red está en función del número de sitios que quieren transmitir (tráfico en la red), así como del tamaño de las tramas. En general, cuando la capacidad del canal ha llegado a un 40% del total, la red empieza a presentar numerosas colisiones, situación que es percibida por los usuarios como retrasos considerables de la red.

2.5 Resumen

Ethernet a 10 Mbps es una tecnología madura, económica y sencilla que ha logrado cubrir convenientemente las necesidades de comunicación de las organizaciones. Ethernet ha evolucionado para responder a las necesidades de distintos usuarios como lo muestran las diversas variantes que se han desarrollado de la norma original, en particular 10BaseT se ha hecho muy popular ya que aprovecha las ventajas del cableado estructurado. Todo lo anterior ha provocado que Ethernet sea la tecnología de red local más utilizada.

Ha sido muy criticada en algunos medios debido a sus limitaciones. A pesar de ello, desde los inicios de las redes locales, Ethernet ha dominado el panorama. En 1992 abarcaba un 49% del mercado total, le seguían Token Ring con el 36%, y otras tecnologías como Apple Talk y ARCnet con un 15%, y FDDI con un 0.7%. Hasta hace pocos años las diferencias eran muchos mayores, con Ethernet ocupando el 79 % del total.

3

El conjunto de Protocolos TCP/IP

El conjunto de protocolos TCP/IP ha llegado a ser el estándar para la interconexión de sistemas abiertos, llamados así porque todas sus especificaciones se encuentran al alcance del público. Las computadoras a lo largo del mundo utilizan estos protocolos para comunicarse porque proporcionan el grado más alto de interoperabilidad, abarcan el conjunto más amplio de marcas comerciales y porque se ejecutan sobre más tecnologías de red que cualquier otro conjunto de protocolos.

La mayoría de los institutos de investigación y los centros educativos utilizan esta tecnología como la base de sus sistemas de comunicación de datos, porque les permite intercambiar información y resultados más rápido que aquellos que no lo están, dándole a sus usuarios una ventaja favorable.

Pero a pesar de su popularidad y amplio uso, los detalles de los protocolos TCP/IP y la estructura del software que lo implementa, sigue siendo un misterio para la mayoría de los profesionistas.

Además, esta tecnología oculta los detalles del hardware de red y le permite a las computadoras comunicarse independientemente de su conexión física.

El propósito de este capítulo es mostrar un panorama general de los puntos más sobresalientes de los protocolos TCP/IP. Veremos quién de ellos se encarga de dividir los mensajes, encapsularlos en datagramas y pasarlo a otro protocolo para que se responsabilice de enviarlo por la ruta más adecuada. Se explicará la diferencia entre los distintos tipos de direcciones y la relación que guardan entre ellas.

En resumen, nos daremos cuenta de que:

La tecnología TCP/IP comprende muchos protocolos que interactúan unos con otros. Y para entender totalmente los detalles e implementación de un protocolo, debemos considerar su interacción con el resto de la pila de protocolos.[2]

3.1
La tecnología internet

Un protocolo de red es un estándar que define, entre otras cosas, las "reglas" que les permiten a las computadoras comunicarse; determina cómo éstas deberían identificarse en una red; la forma en que los datos se deben transmitir; establecen los formatos de los mensajes; y cómo la información debería ser procesada una vez que llega a su destino final. Así como los procedimientos para manejar errores u otras condiciones anormales.

Aunque cada protocolo de red es diferente, todos son capaces de compartir el mismo medio físico. Este método común de accesar a la red física le permite a múltiples protocolos coexistir pacíficamente sobre el medio de red, y les permite a los desarrolladores de aplicaciones usar hardware común para una variedad de protocolos. Este concepto es conocido como **independencia de protocolo**, lo que significa que los dispositivos que son compatibles en las capas físicas y de enlace les permiten a los usuarios correr diferentes protocolos sobre el mismo medio.

Los protocolos frecuentemente están agrupados en "familias" (algunas veces llamadas conjuntos o pilas de protocolos), muchas de las cuales son desarrolladas por organizaciones comerciales, por ejemplo AppleTalk fue desarrollada por Apple Computers.

El término genérico TCP/IP es utilizado para referirse a una familia de protocolos, sus iniciales provienen de Protocolo de Control de Transmisión/Protocolo Internet que son dos de los principales protocolos de dicha familia y que analizaremos en forma individual posteriormente. Además de TCP e IP, esta familia incluye otros protocolos y aplicaciones. Un ejemplo de estos protocolos son UDP, ARP e ICMP. Y con respecto a las aplicaciones tenemos a telnet, ftp, rcp, etc. Un término más formal es utilizar **tecnología internet** para referirse a este conjunto de protocolos, y a una red que utiliza esta tecnología internet se le conoce como **internet o red de redes**.

[2] Comer E., Douglas y David L. Stevens. Internetworking with TCP/IP Vol II. Prentice-Hall 1991, pp. 2

Para entender esta tecnología, primero se debe comprender la estructura lógica de los protocolos por capas dentro de una computadora en una internet.

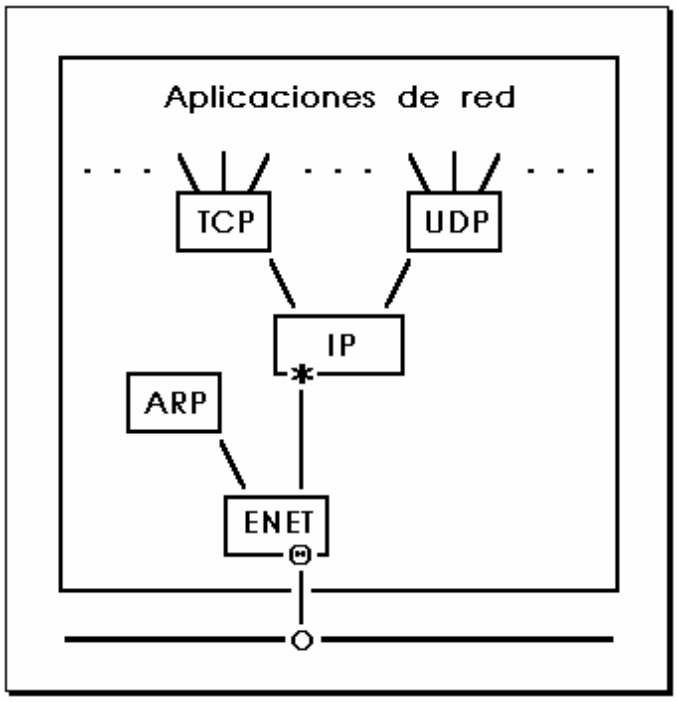


Figura 3.1 Estructura lógica de los protocolos por capas en una estación de red TCP/IP

Cada computadora que utiliza la tecnología internet, tiene una estructura semejante. Cada uno de los módulos (cajas) representan el procesamiento de los datos conforme pasan a través de la computadora; y las líneas que unen los módulos muestran la ruta de los datos. La línea horizontal en la parte inferior representa el cable Ethernet; la **o** es el transceiver, que es el dispositivo que conecta la tarjeta de red a la red de área local; el ***** representa la dirección IP y la **Θ** representa la dirección Ethernet.

Como se puede observar en la figura 3.1, el módulo IP es la base de la tecnología internet. Cada módulo o driver agregará su propio encabezado al mensaje conforme pase descendentemente por la pila de protocolos, y de igual forma le quitará su correspondiente encabezado cuando el mensaje ascienda por la pila hacia la aplicación. EL encabezado IP contiene las direcciones IP, las cuales construyen una simple red lógica de múltiples redes físicas. De aquí surge el nombre de internet.

El nombre de la unidad de datos que fluye a través de una internet depende de su posición dentro de la pila de protocolos. Si se encuentra en el medio físico, y suponiendo que se trata de una red Ethernet, se le denomina trama Ethernet; si está entre el driver Ethernet y el módulo IP se le conoce como datagrama IP; si se ubica entre el módulo IP y el módulo UDP se le conoce como datagrama UDP; si está entre

el módulo IP y el módulo TCP es llamado segmento (o más general, mensaje de transporte); y si está en una aplicación de red, es conocido como mensaje de aplicación.

Como un ejemplo, sigamos la ruta que toman los datos conforme viajan a través de la pila de protocolos. Para una aplicación que utiliza TCP los datos pasan entre la aplicación y el módulo TCP, después pasan al módulo IP y por último al driver Ethernet. El Protocolo de Transferencia de Archivos (FTP) es la aplicación típica que utiliza TCP, de tal manera que su pila de protocolos sería FTP/TCP/IP/ENET. De la misma manera, el Sistema de Archivos de Red (NFS) es una aplicación que utiliza UDP y tendría una pila de la forma NFS/UDP/IP/ENET.

Si observamos la figura 3.1 nos daremos cuenta de que tanto los módulos TCP, UDP, IP como el driver Ethernet son multiplexores n a 1 ya que switchean muchas entradas a una salida cuando una aplicación en una computadora desea enviar información a otra computadora. Y también son demultiplexores 1 a n cuando les llega información a la computadora, ya que switchean una entrada a muchas salidas. Más adelante explicaremos con más detalle las medidas que toma cada protocolo para llevar a cabo esta multiplexación y demultiplexación.

Aunque la tecnología internet soporta muchos medios diferentes de red, nos enfocaremos a la tecnología Ethernet, debido a que la red de esta universidad utiliza dicha tecnología y la meta de esta tesis es implementar un programa de aplicación encaminado a apoyar a la administración de la misma.

El software de Internet está diseñado en torno a 3 conceptos de servicios de red arreglados jerárquicamente; muchos de los éxitos alcanzados se deben a esta arquitectura sorprendentemente robusta y adaptable.[3]

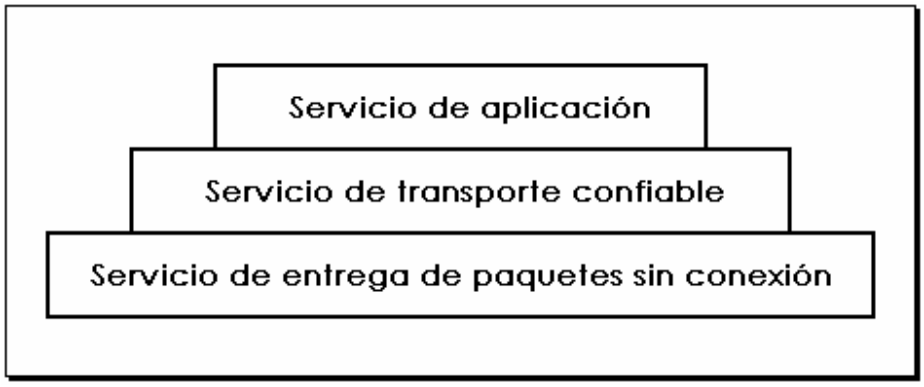


Figura 3.2 Las tres capas conceptuales de los servicios de Internet

Como se muestra en la figura 3.2 los tres conjuntos de servicios que proporciona una red de redes TCP/IP están estrechamente relacionados. A continuación, describiremos los dos servicios inferiores, recordando que el de aplicación se refiere a los programas de aplicación.

[3] Comer E., Douglas. Redes globales de información con Internet y TCP/IP. Prentice-Hall 1996, pp. 93

- Servicio de entrega de paquetes sin conexión. Este servicio forma la base de todos los otros servicios de red de redes. El servicio de comunicación de conmutación de paquetes (o sin conexión), como se explicó en el primer capítulo, simplemente rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Y debido a que este servicio rutea cada paquete por separado, no garantiza una entrega confiable y en orden. Algo muy importante es que tener una entrega de paquetes apoyada en la conmutación de paquetes como la base de todos los sevicios de red de redes, hace que los protocolos TCP/IP sean adaptables a un amplio rango de hardware de red.

- Servicio de transporte confiable. La mayor parte de las aplicaciones necesitan mucho más que sólo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una conexión con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si ésta fuera permanente y directa del hardware. Debajo de todo esto, por supuesto, los protocolos de comunicación dividen el flujo de datos en pequeños mensajes y los envían, uno tras otro, esperando que el receptor proporcione un acuse de recibo de la recepción.

Las principales diferencias de los protocolos TCP/IP con respecto a los demás son:

- Independencia de la tecnología de red. Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van desde redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada **datagrama**, y especifican cómo transmitir los datagramas en una red en particular.

- Interconexión universal. Una red de redes TCP/IP permite que se comuniquen cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de su fuente y su destino. Los nodos intermedios de conmutación utilizan la dirección de destino para tomar decisiones de ruteo.

- Acuse de recibo punto-a-punto. Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aún cuando las dos máquinas no estén conectadas a la misma red física.

- Estándares de protocolos de aplicación. Además de los servicios básicos de nivel de transporte (como las conexiones de flujo confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico,

transferencia de archivos y acceso remoto. Por lo tanto, cuando se diseñan programas de aplicación que utilizan el TCP/IP, los programadores a menudo se encuentran con que el software ya existente proporciona los servicios de comunicación que necesitan.

3.2
El Protocolo de Control de Transmisión (TCP)

Se ha dicho que uno de los servicios que presta TCP/IP es no confiable, debido a que los paquetes se pueden perder, duplicar, retrasar o entregar sin orden, pero el servicio no detectará estas condiciones ni informará al emisor o al receptor. Este tipo de inseguridad les podría causar muchos problemas a los usuarios.

Para evitar esto se desarrolló el Protocolo de Control de Transmisión (TCP). Ubicado sobre el Protocolo Internet, TCP ofrece seguridad y comunicación full-duplex. La ventaja es obvia, los programadores de aplicaciones no necesitan escribir código para manejar pérdidas o datagramas fuera de orden, y debido a que los datos son manejados como un flujo de octetos, el código existente puede ser modificado y adaptarlo para usar TCP.

TCP es conocido como un protocolo orientado a conexión (también conocido como de conmutación de circuitos) por que utiliza ese tipo de comunicación. De acuerdo a lo establecido en la sección 1.5, en una transmisión de conmutación de circuitos antes de que dos programas empiecen a intercambiar datos, deben establecer una conexión entre ellas, por medio de una sincronización donde ambos lados intercambian paquetes y establecen los números de secuencia de los paquetes (el número de secuencia es importante porque, como se mencionó anteriormente, los datagramas pueden llegar fuera de orden y el número de secuencia es utilizado para asegurar que los datos sean acomodados en el orden en que fueron enviados).

TCP es responsable de:

- Fragmentar los mensajes en datagramas cuando sea necesario.
- Volver a enviar los datagramas que se lleguen a perder, y
- Volver a ponerlos en el orden adecuado en el otro extremo.

Como esas funciones son necesarias para muchas aplicaciones, fueron reunidas en TCP, en lugar de formar parte de las especificaciones individuales para enviar los datos de las aplicaciones. Se puede pensar que TCP está formado de librerías de rutinas que las aplicaciones pueden usar cuando necesiten una comunicación que garantice la entrega. Obviamente, esto tiene su costo: TCP requiere más recursos del CPU y más ancho de banda de red.

El Protocolo Internet (IP), como se verá posteriormente, es reponsable de rutear los datagramas uno por uno. Puede parecer que TCP es el que hace todo, y en redes pequeñas esto es cierto. Sin embargo, en Internet (la red de redes), conseguir que un simple datagrama llegue a su destino puede ser una tarea compleja.

Por ejemplo, la conexión puede requerir que el datagrama viaje a través de varias redes, líneas seriales, distintos tipos de tecnologías LANs, etc. Con lo que mantener las rutas de todos esos semidestinos y el procesamiento de medios de transporte totalmente incompatibles hacen que el ruteo sea una tarea compleja.

Antes de que TCP pueda enviar un conjunto de datos a otra computadora en unidades manejables, debe saber el tamaño de los datagramas que las redes a las que pertenecen las estaciones involucradas en la comunicación pueden procesar y, entre otras cosas, esa tarea está a cargo de la sincronización en la comunicación de conmutación de circuitos.

Actualmente, el protocolo TCP en cada extremo de la conexión determina el tamaño adecuado del datagrama a transmitir, en base al tamaño de los datagramas que ambas redes puedan manejar.

Imaginemos que deseamos transferir un archivo de 15000 octetos y como la mayoría de las redes no pueden procesar un datagrama de ese tamaño, TCP fragmentará el archivo en 30 datagramas de 500 octetos cada uno. Cada datagrama será enviado a su destino y ahí serán defragmentados para tener de nuevo el archivo completo. Sin embargo, mientras los datagramas están viajando, la red no sabe que existe alguna relación entre ellos, y es posible que el datagrama número 14 llegue primero que el 13. También es posible que exista un error en la red y algún datagrama no consiga llegar a su destino. En ese caso, esos datagramas tienen que ser enviados nuevamente.

Notemos que la interfaz entre TCP e IP es bastante simple. TCP simplemente envía un datagrama a IP con un destino. IP, por su parte, no sabe como este datagrama se relaciona con los anteriores o los posteriores. Claramente esto no es suficiente para conseguir que un datagrama llegue a su destino final. TCP tiene que saber a qué conexión pertenece el datagrama. A esta tarea se le conoce como demultiplexación.

La información necesaria para realizar esta demultiplexación está contenida en una serie de encabezados. Un encabezado es un conjunto de octetos extras colocados al inicio del datagrama por algún protocolo. De la misma manera que colocamos un envío dentro de una pequeña caja y el servicio de mensajería lo coloca a su vez en una más grande.

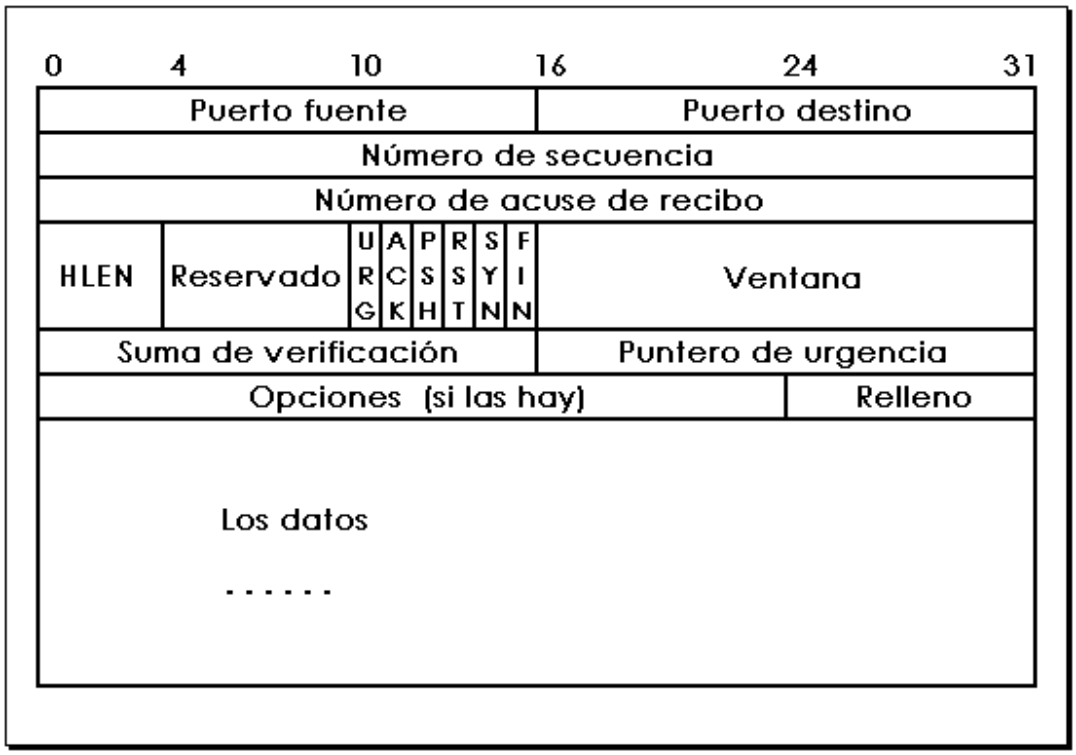


Figura 3.3 Formato del encabezado TCP

TCP coloca su encabezado al inicio de cada datagrama. Este encabezado contiene al menos 20 octetos, pero los más importantes son aquellos que indican el número de puerto fuente y destino, y el número de secuencia. Los números de puerto identifican a los programas de aplicación en los extremos de la conexión. Además de ayudar a diferenciar cuando se tienen varias conversaciones simultáneas. Imagínese que tres usuarios A, B y C están transfiriendo archivos, el TCP les asigna números de puerto 1000, 1001 y 1002 correspondientemente. Cuando A está enviando un datagrama, 1000 es el número de puerto fuente, debido a que es la fuente del datagrama. Por supuesto, el protocolo TCP en el otro extremo tiene asignado otro número de puerto.

El protocolo TCP en la máquina utilizada por el usuario A debe conocer también el número de puerto utilizado por el otro extremo. Esto se lleva a cabo al inicio de la conexión. A su vez esta dirección será colocada en el puerto destino. Por supuesto, si el otro extremo envía un datagrama de regreso al usuario A, los números de puerto fuente y destino estarán invertidos.

Cada datagrama tiene un número de secuencia. Éste es usado para que el protocolo TCP en el destino final pueda colocar los datagramas en el orden correcto, y para asegurarse de que ninguno se perdió. TCP no enumera los datagramas, sólo los octetos. Así, si existen 500 octetos de datos en cada datagrama, el primer datagrama tendrá el número de secuencia 0, el segundo 500, el próximo 1000, etc.

El campo suma de verificación es un número que es calculado sumando los octetos en el datagrama. El protocolo TCP en el extremo destino calculará

nuevamente este valor, y si no coincide con el enviado en el encabezado, indicará que algo le sucedió al datagrama durante la transmisión y será rechazado.

Para asegurarse que el datagrama llegó correctamente a su destino, el receptor debe enviar un datagrama cuyo número de acuse de recibo está ocupado. Por ejemplo, enviar un paquete con un acuse de recibo de 1500 indica que se recibió correctamente el datagrama cuyo número de secuencia es el 1500. El protocolo TCP en el transmisor activa un contador cuando envía un mensaje de transporte, de tal manera que si el mensaje de reconocimiento no se ha recibido y el contador ha expirado, TCP enviará los datos nuevamente. La ventana es utilizada para controlar la cantidad de datos que pueden ser transmitidos en un tiempo dado. No es práctico esperar el mensaje de reconocimiento de cada datagrama enviado para poder mandar el próximo datagrama, provocaría que la comunicación fuera demasiado lenta. Por el contrario, no se puede estar solo enviando datagramas, ya que una computadora muy rápida puede saturar la capacidad de una red lenta. Así, cada extremo indica la cantidad de datos que está preparada para absorber colocando el número de octetos en su campo ventana.

Cuando la computadora recibe datos, la cantidad de espacio a la izquierda de su ventana decrece. Cuando llega a cero, el transmisor debe detenerse. Conforme el receptor procesa los datos, se incrementa su ventana indicando que está listo para aceptar más información. Continuamente, los mismos datagramas utilizados como mensajes de reconocimiento son utilizados para indicar el estado de la ventana en cada extremo de la conexión.

El campo puntero de urgencia le permite a un extremo decirle al otro que le de prioridad a un octeto en particular. Esto es útil para manejar eventos asíncronos, por ejemplo cuando se teclea un caracter de control u otro comando para interrumpir la conexión.

El campo HLEN especifica la longitud del encabezado del segmento, medido en múltiplos de 32 bits. Existen algunas banderas que determinan el propósito y contenido del segmento:

Bandera	Significado si el bit está puesto a 1
URG	El campo de puntero de urgente es válido.
ACK	El campo de acuse de recibo es válido.
PSH	Este segmento solicita una operación push.
RST	Inicio de la conexión.
SYN	Sincronizar números de secuencia.
FIN	El emisor ha llegado al final de su flujo de octetos.

Existen algunos campos en el encabezado TCP que no se describieron. Generalmente están relacionados con el manejo de la conexión, como es el caso de los campos opciones y relleno.

Si se abreviara el encabezado TCP como una "T", el envío de datagramas se parecería a : T... T... T... T...

3.3
El Protocolo Internet (IP)

El protocolo que define el mecanismo de entrega sin conexión (o de conmutación de paquetes) y no confiable es conocido como Protocolo Internet y, por lo general, se le identifica por sus iniciales IP. El protocolo IP proporciona tres definiciones importantes:

- Determina la unidad básica para la transferencia de datos utilizada a través de una red de redes TCP/IP. Es decir, especifica el formato exacto de todos los datos que pasarán a través de una red de redes TCP/IP.
- El software IP realiza la función de ruteo, seleccionando la ruta para la que los datos serán enviados.
- Además de aportar especificaciones formales para el formato de los datos y el ruteo, IP incluye un conjunto de reglas que le dan forma a la idea de entrega de paquetes no confiable. Las reglas caracterizan la forma en la que las estaciones y ruteadores intermedios deben procesar los paquetes; cómo y cuándo se deben generar los mensajes de error y; las condiciones bajo las cuales los paquetes pueden ser descartados.

3.3.1
Ruteo directo e indirecto

El Protocolo Internet es el alma de la tecnología internet, y a su vez, la esencia de IP se encuentra en su tabla de ruteo. A través ésta, IP toma todas las decisiones para rutear un datagrama. Por lo tanto, entender cómo es utilizada la tabla de ruteo equivale a entender la red de redes.

Existen dos formas de ruteo: ruteo directo y ruteo indirecto. El primero se utiliza cuando dos computadoras que pertenecen a la misma red Ethernet desean comunicarse (por ejemplo, si un usuario en la sala de cómputo 1 deseara comunicarse con algún profesor en el edificio de electrónica y computación). Este tipo de ruteo no es muy complicado, cada computadora tendrá asignada una dirección Internet (IP) y su tarjeta de red poseerá una dirección Ethernet. Así, cuando la máquina del usuario de la sala (*U*), que será la fuente del mensaje, le envía la trama al profesor *X*, el encabezado IP contendrá la dirección IP de *U* como fuente y la de *X* como destino; y el encabezado Ethernet poseerá las direcciones Ethernet de *U* y *X* como fuente y destino respectivamente.

Direcciones	Fuente	Destino
Encabezado IP	*U*	*X*
Encabezado Ethernet	*U*	*X*

Por su parte, el ruteo indirecto es más complicado debido a que se utiliza cuando dos computadoras que no pertenecen a la misma red desean comunicarse. Para lograr esto, deben hacer uso de los ruteadores que unen a cada una de sus redes con el resto de Internet. Veamos el siguiente ejemplo.

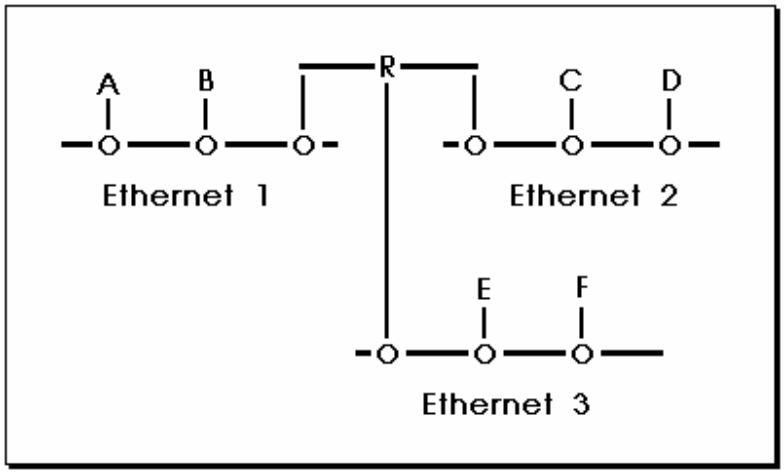


Figura 3.4 Una pequeña internet con tres redes

Cuando las computadoras A y B; A y R; C y D; D y R; E y F; E y R, etc. se comunican, utilizan el ruteo directo. Pero si A desea comunicarse con F, tendrá que utilizar el ruteo indirecto. Para esto, en la trama irán, en su respectivo encabezado, las direcciones IP y Ethernet de A como fuente y la dirección IP de F como destino. Pero como A debe utilizar el ruteador (R) que une a las distintas Ethernets, la dirección Ethernet destino no será la de F, sino la de R.

Direcciones	Fuente	Destino
Encabezado IP	A	F
Encabezado Ethernet	A	R

Una vez que el paquete llega a R, el modulo IP examina la dirección IP destino y dice "esta dirección IP no es la mia", y envía el paquete directamente a F. Esta vez quitando la dirección Ethernet de A como fuente y colocándole la suya.

Direcciones	Fuente	Destino
Encabezado IP	A	F
Encabezado Ethernet	R	F

Este ejemplo es muy simple comparado con el ruteo que se lleva a cabo en Internet, debido a que entran en juego muchos factores, resultado de múltiples ruteadores y redes físicas que se ven involucrados en el manejo de un solo paquete.

Como se mencionó anteriormente, y en base al ejemplo anterior, TCP fragmenta los mensajes en datagramas, les agrega su encabezado y los envía a IP. Por supuesto, tiene que decirle a IP la dirección Internet de la computadora destino y ésto es todo lo concerniente a IP, ya que este protocolo no se preocupa de lo que contiene el datagrama o el encabezado TCP. La tarea de IP es encontrarle una ruta al datagrama para que llegue a su destino final, y para permitirle a los ruteadores u otros sistemas intermedios direccionar al datagrama, IP agrega su propio encabezado.

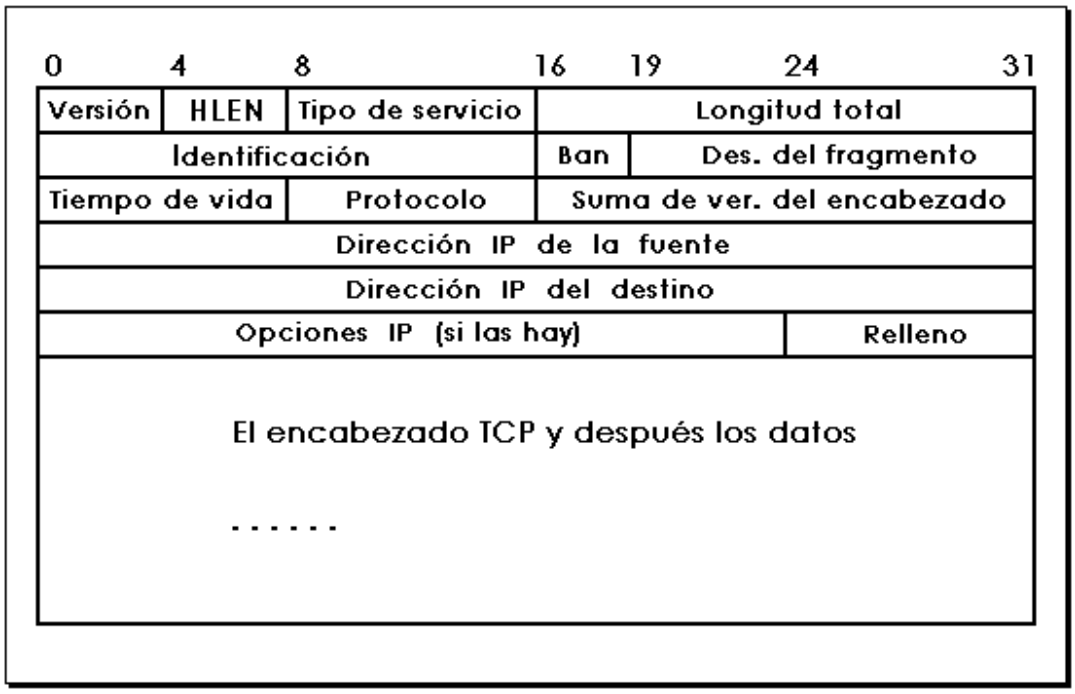


Figura 3.5 Formato del encabezado IP

Los campos principales de este encabezado son las direcciones Internet fuente y destino (direcciones de 32 bits), el número de protocolo y otra suma de verificación. La dirección Internet fuente es la dirección de la máquina que envía el datagrama. Esta es necesaria para que la máquina que reciba el datagrama sepa de quién procede el mismo. La dirección Internet destino es la dirección de la máquina a la que se envía el datagrama. Esta dirección es necesaria para que los ruteadores intermedios sepan a quién entregar el datagrama.

El número de protocolo le dice a IP en el otro extremo a qué protocolo le debe entregar el datagrama (TCP o UDP) en su función de demultiplexor, aunque la mayoría del tráfico IP utiliza TCP, existen otros protocolos que pueden utilizar IP. Finalmente, la suma de verificación le permite a IP comprobar que el encabezado IP no sufrió daño alguno durante el viaje. Observe que TCP e IP tienen sumas de verificación separadas. IP debe ser capaz de verificar que el encabezado no sufrió daño o podría enviar un mensaje al lugar equivocado.

Debido a que el proceso de los datagramas se da en el software, el contenido y el formato no está condicionado por ningún tipo de hardware. El primer campo de 4 bits en un datagrama (versión) contiene la versión del protocolo IP que se utilizó para crear el datagrama. Este campo se emplea para comprobar que el emisor, el receptor y cualquier ruteador entre ellos proceda de acuerdo con el formato del datagrama. Todo software IP debe verificar el campo de versión antes de procesar un datagrama para asegurarse de que el formato corresponde al tipo de formato que espera el software. Si hay un cambio en el estándar, las máquinas rechazarán el datagrama con versiones de protocolo que difieren del estándar, evitando con ello que el contenido de los mismos sea mal interpretado.

El campo longitud de encabezado (HLEN), también de 4 bits, proporciona el encabezado del datagrama con una longitud medida en palabras de 32 bits. Como podemos ver, todos los campos del encabezado tienen longitudes fijas excepto para el campo opciones IP y su correspondiente relleno. El encabezado más común, que no tiene opciones ni relleno, mide 20 octetos y tiene un campo de longitud de encabezado igual a 5.

El campo longitud total proporciona la longitud del datagrama IP medido en octetos, incluyendo los octetos del encabezado y los datos. El tamaño del área de datos se puede calcular restando la longitud del encabezado (HLEN) de longitud total. Dado que este último campo tiene una longitud de 16 bits, el tamaño máximo posible de un datagrama IP es de 2^{16} o 65 535 octetos.

Las banderas y el desplazamiento de fragmento son utilizados cuando un datagrama pasa a través de redes con tamaño de datagrama menor al actual.

El campo tiempo de vida es un número que será decrementado cada vez que el datagrama pase a través de un ruteador. Cuando llega a cero, el datagrama es descargado de la red. Esto se hace para evitar que el datagrama viaje eternamente sobre la red y se formen ciclos. Por supuesto, esto debería ser imposible, pero los diseñadores de la red de redes la crearon para aquellas condiciones imposibles.

Nuevamente, el encabezado contiene algunos campos adicionales que no se discutirán.

Si representaramos el encabezado IP por una "I" y suponiendo que el datagrama IP conlleva un segmento TCP cuyo encabezado está representado por una "T", el mensaje se parecería a IT... IT... IT... IT...

3.3.2 Direcciones Internet

Hasta ahora, hemos analizado la forma en que trabaja el Protocolo Internet y podemos decir que sus diseñadores realizaron un gran esfuerzo. Sin embargo, de todo lo que se ha visto sólo queda una duda, ¿qué es y cómo se asigna una dirección Internet?

Para contestar estas preguntas, recordemos que una dirección nos especifica dónde podemos localizar una estación. Así, en el entorno de redes de computadoras podemos decir que: una dirección le permitirá a cada estación en la red poder ser identificada. En si, una dirección Internet es un número único de 32 bits expresado generalmente en la forma A.B.C.D, donde cada letra representa una cantidad decimal que puede obtenerse de 8 bits (0-255), por ejemplo 192.100.170.60. A esta representación se le conoce como notación decimal con puntos. Cada dirección está conformada por dos piezas: la primera parte es el número de red IP conocido como *netid*, y es la parte de la dirección que diferencía cada red en Internet. La segunda parte de la dirección IP es el número que identifica a cada una de las computadoras dentro de una red, conocido como *hostid.* En otras palabras, cada red en una internet debe tener un número único de red (netid) y, a su vez, cada estación

de esta red debe tener un número único dentro de ella (hostid). Si dos dispositivos en una internet tienen direcciones con el mismo número de red, significa que están localizados en la misma red: 192.100.170.27 y 192.100.170.28.

Para no profundizar mucho, diremos que existen tres tipos de direcciones IP referidas como "A", "B" y "C". Como se puede observar en la figura 3.6, las de tipo A son asignadas a redes que poseen muchos anfitriones o estaciones (entre 2^{16} y 2^{24}), las de tipo B son asignadas a redes de tamaño medio (entre 2^{8} y 2^{16} estaciones), y las de tipo C son asignadas a redes pequeñas (menos de 2^{8} estaciones). Siendo más detallistas se puede contemplar que, en las redes que en su porción netid estén en el rango de 1 a 126 serán de tipo A, las que estén entre 128.1 y 191.254 serán de tipo B y, las que se encuentren en el rango de 192.1.1 y 223.254.254 serán de tipo C. De aquí se desprende que la red de la UTM es de tipo C (192.100.170).

Algunos números como 0 y 255 no se permiten dentro de las direcciones IP porque dichos números tienen un significado especial. Las direcciones por arriba de 223 están reservadas para las clases de redes D y E que no están bien definidas.

Figura 3.6 Las tres formas primarias de direcciones Internet

Debido a que las direcciones IP codifican tanto una red y un anfitrión en dicha red, no especifican una computadora individual, sino una conexión a la red.[4]

Por último, la autoridad que proporciona los número de red IP (netid) es el Centro de Información de Redes (NIC), y los administradores de las redes asignan las direcciones IP a las computadoras (hostid).

3.3.3 Nombres

Ahora sabemos la nomenclatura utilizada para esas direcciones Internet que todo el software de red necesita para abrir conexiones o enviar datagramas. Sin embargo, los usuarios prefieren referirse a las computadoras por su nombre en lugar de utilizar sus direcciones. Por razones obvias, es más fácil recordar un nombre que una

[4] Comer E., Douglas. Internetworking with TCP/IP Vol I. Prentice-Hall 1991, pp. 63

dirección (por ejemplo angel.umar.mx : 200.23.222.17, o itonet2.itox.mx : 200.23.91.20). Para ello, existen bases de datos que le permiten al software buscar un nombre y conseguir su correspondiente dirección numérica.

Cuando Internet era pequeña, ésta base de datos se encontraba en cada computadora. Pero actualmente existen tantas computadoras conectadas a Internet que mantener el mismo esquema sería poco práctico. Por tal motivo, esos archivos se han visto reemplazados por un conjunto de Servidores de Nombres que proporcionan el Servicio de Nombres de Dominio (DNS) que mantienen el nombre de la estación y su correspondiente dirección numérica.

3.4
El nivel Ethernet

Esta sección es una revisión breve de la tecnología Ethernet, pretendiendo dar sólo un panorama general del funcionamiento de las redes Ethernets comentadas en el capítulo anterior. Se estableció que esta tecnología utiliza CSMA/CD que le permite a todos los dispositivos comunicarse a través de un mismo medio, por lo que sólo se permite una transmisión en un momento dado.

La tarjeta Ethernet en una computadora recibe una copia de todos los paquetes que se encuentran en la red, aun cuando estén direccionados hacia otras máquinas. Utiliza el campo de dirección de destino de un paquete como filtro, ignorando los paquetes que están direccionados hacia otras máquinas y selecciona sólo los paquetes direccionados hacia esa máquina. El mecanismo de direccionamiento y filtrado de hardware es necesario para prevenir que una computadora sea abrumada con la entrada de datos.

Aun cuando el procesador central de la computadora podría realizar la verificación, ésta se realiza en la interfaz de la estación haciendo que el tráfico de la red Ethernet sea un proceso menos lento entre todas las computadoras.

La mayoría de la redes utilizan la tecnología Ethernet, que a su vez tiene su propio encabezado y direcciones. Los diseñadores de Ethernet se aseguraron de que dos computadoras no tuvieran la misma dirección Ethernet.

Para asegurarse de que las tarjetas Ethernet nunca tuvieran que modificar su dirección, los diseñadores asignaron 48 bits para la dirección Ethernet. Los fabricantes de equipo Ethernet tienen que registrarse con una autoridad central (IEEE maneja el espacio de direcciones Ethernet y asigna las direcciones conforme se necesitan) de tal manera que los números asignados a ellos no se traslapen con los asignados a otro fabricante.

Las direcciones físicas están asociadas con el hardware de interfaz Ethernet; cambiar el hardware de interfaz a una máquina nueva o reemplazar el hardware de interfaz que ha fallado provocará cambios en la dirección física de la máquina.[5]

[5] Comer E., Douglas. Internetworking with TCP/IP Vol I. Prentice-Hall 1991, pp. 25

Cada paquete Ethernet tiene un encabezado de 14 octetos, ilustrado en la figura 3.7, que incluye las direcciones Ethernet fuente y destino, y un tipo de código. Se supone que cada máquina captura los paquetes cuya dirección destino Ethernet coincida con su propia dirección. Pero es posible configurar a las tarjetas Ethernet de tal manera que se puedan capturar todos los paquetes que viajen por la red, aun cuando no vayan direccionados a esa computadora, lo cual es una de las razones por la que las comunicaciones Ethernet no son seguras.

Esta característica de las tarjetas Ethernet será determinante en el desarrollo de la aplicación final de la presente tesis, ya que permitirá extraer todos y cada uno de los paquetes que viajen a lo largo de la red de la universidad y poder analizar parte de su encabezado.

Observe que no existe una relación entre la dirección Ethernet y la dirección IP, es decir, no existe una fórmula que nos de una dirección IP a partir de la Ethernet o viceversa. Cada máquina debe tener una tabla para determinar a que dirección Ethernet le corresponde la dirección IP. Además de las direcciones, el encabezado contiene un tipo de código, lo que les permite a varias familias de protocolos coexistir en la misma red. Así, se puede utilizar TCP/IP, DECnet, Xerox NS al mismo tiempo. Cada uno de ellos pondrá un valor diferente en el campo tipo.

Finalmente, existe una suma de verificación. El controlador Ethernet calcula ésta suma del paquete entero y lo coloca al final del mismo. Cuando el receptor obtiene el paquete, vuelve a calcular este valor y rechaza el paquete cuando no concuerda con el valor original enviado con el paquete.

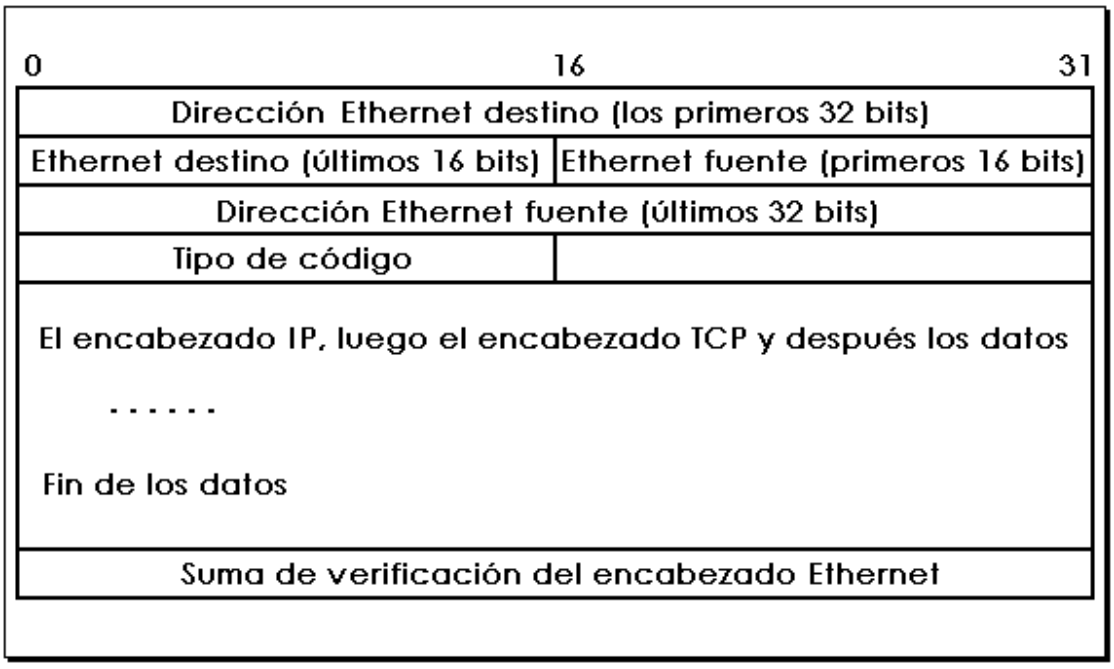


Figura 3.7 Formato del encabezado Ethernet

Si representáramos el encabezado Ethernet con una "E" y la suma de verificación con una "S", el archivo se parecería a EIT...S EIT...S EIT...S.

Cuando los paquetes son recibidos en el destino final, cada uno de los protocolos se encarga de remover su correspondiente encabezado. La interfaz Ethernet remueve el encabezado Ethernet y la suma de verificación, y observa el campo tipo de código. Si este campo indica que los datos pertenecen al protocolo IP, el driver del dispositivo Ethernet pasa el datagrama a IP, el cual remueve su encabezado y a su vez revisa el campo de protocolo. Si dicho campo indica que los datos deben ser entregados a TCP, IP pasa el datagrama a TCP, quien elimina su encabezado y al mismo tiempo observa el número de secuencia y junto con otra información, combina los datagramas, construye el archivo original y lo envía al programa de aplicación correspondiente.

3.5
El Protocolo de Resolución de Direcciones (ARP)

Este protocolo es utilizado para traducir direcciones IP en direcciones Ethernet. La conversión sólo se realiza para aquellos paquetes que van de salida debido a que es cuando los encabezados IP y Ethernet ya han sido creados. Para llevar a cabo esta tarea, se hace uso de una tabla de búsqueda, llamada tabla ARP que está almacenada en memoria y contiene un renglón para cada computadora. Existe una columna para la dirección IP y una para su correspondiente dirección Ethernet, de modo que cuando se tiene una dirección IP, se busca dentro de la tabla para encontrar su correspondiente dirección Ethernet.

Recordemos que las direcciones IP se escriben en notación decimal con puntos. Por su parte, las direcciones Ethernet se representan agrupando sus bits en colecciones de 4 y representándolos en forma hexadecimal. Una vez que se tiene esta representación, se juntan dos números consecutivos y se separan del resto por un guión o por dos puntos. Por ejemplo 00:60:97:2D:48:D0.

El protocolo ARP es necesario porque tanto la dirección IP como la Ethernet son seleccionadas independientemente una de la otra. La primera es asignada por el administrador de la red de acuerdo a la localización de la computadora en la red, y la dirección Ethernet es seleccionada por el fabricante de acuerdo al espacio que se le ha asignado. De tal manera que cuando la computadora es cambiada de lugar dentro de la red, su dirección IP cambia. O bien cuando la tarjeta de red de la máquina es sustituída por otra, su dirección Ethernet se modifica.

Durante la operación normal, una aplicación de red (llámese telnet, ftp, correo electrónico, etc.), envía un mensaje de aplicación a TCP y TCP envía el correspondiente mensaje al módulo IP. Hasta aquí, la dirección IP destino es conocida por la aplicación y por los módulos TCP e IP. El datagrama IP ha sido construído y está listo para pasarlo al driver Ethernet, pero primero se debe determinar la dirección Ethernet destino. Si dentro de la tabla ARP de dicha máquina se encuentra la respuesta, se coloca la dirección Ethernet destino en el encabezado Ethernet y se envía la trama. Pero si no es así, se llevan a cabo dos acciones:

- El datagrama IP se coloca en estado de espera, y

- Se envía una petición ARP con una dirección Ethernet destino de difusión para que sea escuchada por todas las computadoras de la red.

Cada una de las tarjetas de red de las máquinas reciben la petición y examinan el campo tipo del encabezado Ethernet, pasándolo al módulo ARP. Esta petición dice "si tu dirección IP coincide con esta otra, entonces dime tu dirección Ethernet". Cada módulo ARP examina la dirección IP que se le ha enviado, y si coincide con su propia dirección IP, envía la respuesta directamente a la máquina que hizo la solicitud ya que conoce su dirección Ethernet. Esta respuesta dice "si, esa dirección IP es mía, aquí está mi dirección Ethernet". La respuesta es recibida por la máquina que realizó la solicitud y su driver Ethernet examina el campo tipo de la trama Ethernet y pasa el paquete al módulo ARP. Éste a su vez revisa el paquete y agrega las direcciones IP y Ethernet a su tabla ARP. Posteriormente, se le agrega el encabezado Ethernet al datagrama que estaba esperando y se envía a su destino.

En el caso de que no exista la computadora cuya dirección Ethernet se desea conocer, no habrá respuesta ARP y el módulo IP descargará todos los datagramas dirigidos a esa dirección.

Algunas implementaciones de IP y ARP no almacenan los datagramas IP mientras esperan la respuesta ARP. En lugar de ello, descargan dichos datagramas y más tarde será enviado nuevamente debido a que TCP no recibió el mensaje de reconocimiento en el tiempo establecido. Para ese entonces, lo más probable es que la respuesta ARP ya haya llegado y por consiguiente, la tabla ARP ya posea la dirección deseada.

3.6
El Protocolo de Datagrama de Usuario (UDP)

Hasta ahora hemos discutido las conexiones que utilizan TCP, que es el responsable de fragmentar los mensajes en datagramas y reensamblarlos apropiadamente. Sin embargo, en muchas aplicaciones los mensajes alcanzarán en un solo datagrama. Un ejemplo es buscar la dirección de una máquina dada. Cuando un usuario intenta conectarse a un sistema, generalmente se referirá al sistema por su nombre en lugar de su dirección. El sistema del usuario tiene que trasladar el nombre a una dirección antes de que pueda hacer algo.

Generalmente, solo unas pocas estaciones tienen la base de datos necesaria para trasladar los nombres a direcciones. Así que el sistema del usuario tendrá que enviar una petición a uno de los sistemas que posee esa base de datos (DNS). Esta petición es muy corta y alcanzará en un datagrama, del mismo modo que la respuesta. De este modo no es necesario utilizar TCP. Por supuesto que TCP hace más que fragmentar mensajes en datagramas, se asegura de que los datos lleguen correctamente, volviendo a enviar los datagramas perdidos. Pero para cuestiones de enviar un solo datagrama, no necesitamos toda la complejidad que envuelve TCP. Si no obtenemos una respuesta después de algunos minutos, volvemos a preguntar nuevamente. Para aplicaciones parecidas, existen alternativas a TCP.

La alternativa más común es el Protocolo de Datagramas de Usuario (UDP). Este protocolo está diseñado para aplicaciones donde no se necesitan poner secuencias de datagramas juntos. Funciona de forma muy parecida a TCP. Existe un encabezado UDP que el software de la red lo coloca al inicio de los datos, entonces el protocolo UDP envía los datos a IP, el cual agrega su encabezado IP, colocando el campo de número de protocolo de UDP en lugar de TCP.

UDP no divide los datos en múltiples datagramas, ni mantiene algún registro de lo que ha enviado, así que puede volver a enviar los datos si es necesario. Los números de puerto UDP son usados de la misma manera que TCP, existen números de puerto bien conocidos para servidores que usan UDP. Por su parte, el encabezado UDP es más pequeño que el de TCP, sólo posee número de puerto fuente y destino, y una suma de verificación. UDP es usado por el protocolo que procesa la búsqueda de nombres y por un número de protocolos similares.

Es así que UDP es referido algunas veces como protocolo no confiable, porque cuando un programa envía un datagrama UDP sobre la red, no hay forma de saber si llegó a su destino final. Esto significa que tanto el que envía como el que recibe deben implementar sus propias medidas de seguridad en los protocolos de aplicación que utilicen UDP. Mucho del trabajo que TCP realiza transparentemente (como generar la suma de verificación, reconocimiento de llegada de paquetes, retransmisión de paquetes perdidos, etc.) debe ser realizado por la aplicación misma cuando utilice UDP.

Sin embargo, UDP tiene la ventaja sobre TCP en dos áreas críticas: velocidad y sobreencabezados de paquetes. Debido a que TCP es un protocolo confiable, maneja grandes longitudes de paquetes para asegurar que los datos lleguen a su destino final intactos, lo que resulta en una gran cantidad de paquetes sobre la red. UDP no tiene este sobreencabezado de paquetes, y por consiguiente es considerablemente más rápido que TCP. Así, en aquellos lugares donde la velocidad es importante, o donde el número de paquetes enviados sobre la red debe ser mínimo, UDP es la solución.

3.7
El Protocolo de Control de Mensajes Internet (ICMP)

Otra alternativa es el Protocolo de Control de Mensajes Internet (ICMP). ICMP es utilizado para mensajes de error, y otros mensajes relacionados con el software TCP/IP, en lugar de un programa de usuario particular. Por ejemplo, si se intenta conectar a una estación, el sistema puede mostrar un mensaje ICMP diciendo que dicha estación es inalcanzable. ICMP también es utilizado para encontrar información acerca de la red. Al igual que UDP, ICMP procesa mensajes que alcanzan en un solo datagrama, pero es más simple que UDP ya que no tiene números de puertos en su encabezado. Desde que todos los mensajes ICMP son interceptados por el mismo software de red, no son necesarios los números de puerto que le diga a dónde pertenece dicho mensaje ICMP.

3.8
El packet driver

En la mayoría de las implementaciones de red, el software de los protocolos TCP/IP reside en el sistema operativo de las computadoras. Por lo tanto, un programa de aplicación que utilice TCP/IP para comunicarse, debe interactuar con el sistema operativo para la petición del servicio deseado. Desde el punto de vista del programador, las rutinas que proporciona el sistema operativo definen la interfaz entre la aplicación y el software de los protocolos, lo que se conoce como la interfaz de aplicación.

Entre las funciones operacionales que debe soportar una interfaz se encuentran:

- Reservar recursos locales para la comunicación.
- Especificar los puntos extremos de la comunicación.
- Enviar y recibir datos.
- Manejar las condiciones de error o un aborto de la conexión.
- Terminar una comunicación exitósamente.
- Liberar los recursos locales cuando se termine la conexión.

Cuando una aplicación invoca una llamada al sistema, el control pasa desde la aplicación a la interfaz de la aplicación, quien hace la llamada al sistema, y finalmente llega al sistema operativo. Éste direcciona dicha llamada a un procedimiento interno que realiza la operación requerida. Una vez que el procedimiento interno termina, el control regresa a través de la interfaz de la aplicación a la misma aplicación, la cual continúa la ejecución. En pocas palabras, cuando un programa de aplicación necesita los servicios del sistema operativo, el proceso que ejecuta la aplicación salta al sistema operativo, realiza la operación necesaria y regresa de nuevo a la aplicación. Sin embargo, el sistema operativo no puede comunicarse directamente con la tarjeta de red que conecta la PC a la red. Como resultado, las aplicaciones de red deben usar un driver como intermediario para comunicarse con la tarjeta.

Un packet driver es una pieza de software que proporciona una interfaz entre una aplicación de red y una tarjeta de red (NIC), generalmente una tarjeta Ethernet.

Antes de los packet drivers, las aplicaciones de red se comunicaban directamente con la tarjeta y tomaban el control de ella. Con esto, la tarjeta sólo podía soportar un protocolo de red (TCP/IP, IPX, XNS, etc.) en un momento dado. Por ejemplo, si se había cargado el software necesario para accesar al servidor de una red local Novell, la tarjeta sólo sería capaz de enviar y recibir paquetes Novell (IPX). De tal manera que para correr una aplicación que utilizara TCP/IP se debería reiniciar la máquina y cargar el software TCP/IP para que se comunicara directamente con la tarjeta, y por consiguiente no se tendría acceso al servidor Novell.

Por otra parte, los programadores de aplicaciones de red tenían que proveerse del software de soporte de muchas marcas y modelos de tarjetas de red. Ésto

significaba actualizar y desarrollar nuevo software cada vez que surgía una nueva tarjeta en el mercado.

Así, antes de los packets drivers existían dos problemas:

- Una interfaz de red sólo podía soportar una aplicación de red en un momento dado, y
- Los programadores de aplicaciones de red continuamente tenían que proveerse de software actualizado que soportara nuevas tarjetas de red.

Los packets drivers proporcionaron la solución a ambos problemas. Debido a que funcionan como intermediario, las aplicaciones de red se comunican con el packet driver y éste a su vez se comunica con la tarjeta de red. Así las aplicaciones ya no necesitan saber cómo comunicarse con cientos de tarjetas de red diferentes; sólo necesitan saber cómo comunicarse con una pieza de software que conforma el packet driver.

Los packet drivers, como se muestra en la figura 3.8, también les permiten a diferentes aplicaciones de red identificarse ellos mismos con el driver (registrarse) y poder mantener el contacto para el envío y recepción de datos. Más de una aplicación puede comunicarse con el packet driver al mismo tiempo, así que es posible correr múltiples aplicaciones de red (tanto tiempo como puedan utilizar diferentes pilas de protocolos) sin tomar el control de la tarjeta de red. Ésto significa que potencialmente se puede accesar a un servidor o a una LAN que corra Novell y al mismo tiempo correr aplicaciones que utilicen TCP/IP.

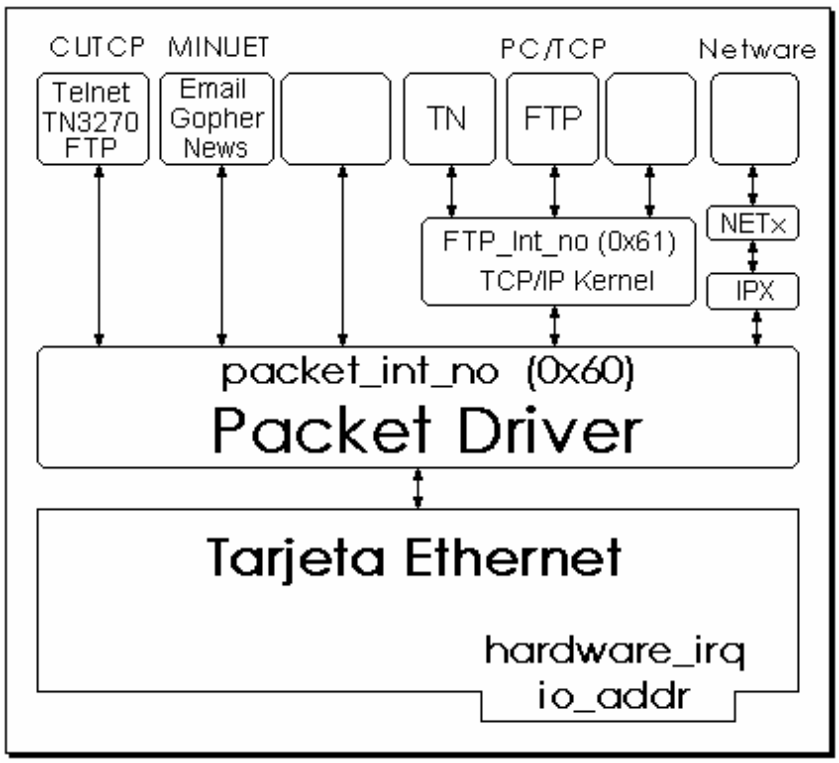


Figura 3.8 Ubicación del packet driver

Los packets drivers son escritos de acuerdo a la especificación Packet Drivers Interface PC/TCP desarrollado por FTP Software Inc., que es un documento que consiste en la especificación de una intefaz a nivel de programación que define cómo comunicarse con los packet drivers para correr, de forma independiente del hardware, los protocolos propios de la pila TCP/IP.

Cuando un distribuidor de una aplicación establece que ésta corre sobre un packet driver, significa que ha escrito e integrado en su aplicación un programa capaz de usar las funciones que ofrece el packet driver interface.

De este modo, si en una PC se tiene instalada una tarjeta Ethernet del fabricante 3Com y se sustituye por otra de Western Digital, bastará con cambiar el packet driver de la primera tarjeta por otro escrito para la segunda para que sigan funcionando los protocolos de la familia TCP/IP que ya lo hacían.

De esta forma, podemos decir que:

- Un packet driver (PD) es un programa escrito para un hardware de comunicaciones concreto y de un fabricante concreto que ofrece unas funciones normalizadas sobre ese hardware, y
- El Packet Driver Interface PC/TCP es un conjunto de funciones normalizadas que debe ofrece cualquier packet driver.

Como se mencionó anteriormente, el uso de un packet driver permite que varias aplicaciones utilicen simultáneamente el mismo acceso al medio (la misma tarjeta de red). Para ello es necesario que el packet driver demultiplexe los paquetes que lleguen entregándolos a la aplicación correspondiente, y multiplexe los paquetes que están por salir.

Como estamos considerando el caso de la tecnología Ethernet propia de la red de la UTM, el campo tipo, de dos octetos, del encabezado Ethernet se reserva precisamente para funciones de multiplexación/demultiplexación, y es el que utilizan los packet drivers para conocer la aplicación a la que un paquete recibido debe entregarse. Esta entrega será realizada sin interrumpir el acceso a la tarjeta por cualquier otro protocolo de la pila.

El packet driver trabaja como un programa TSR (termina y permanece residente) o device driver, cargándose en el vector de interrupciones por software. De esta manera se carga en memoria, se establece y regresa el control al sistema operativo. Así, cualquier programa de aplicación puede accesar a él llamándolo a través de su interrupción por software.

Al cargarlo, la línea de comando tiene la siguiente apariencia:

packet_driver [opciones] < packet_int_no > < hardware_irq >
< io_addr > < base_addr >

donde:

[opciones] indica las distintas formas en que puede trabajar una tarjeta Ethernet, las cuales pueden ser:

-d, para inicialización retardada de la tarjeta Ethernet hasta que el packet driver sea utilizado por vez primera. Esta opción se emplea para computadoras que no cuentan con disco duro.

-n, conversión Netware. Convierte los paquetes 802.3 (Ethernet) en paquetes Novell (IPX).

-w, se utiliza esta opción para correr el packet driver sobre Microsoft Windows.

-u, para descargar el packet driver y liberar la interrupción que estaba ocupando.

< packet_int_no >, indica el número de interrupción por software con el que se podrá accesar al packet driver. Esta interrupción debe configurarse correctamente para evitar conflictos con otro software que también utilice el vector de interrupciones.

< hardware_irq >, establece el número de interrupción por hardware de la tarjeta de red.

<io_addr >, establece el número de puerto de E/S de la tarjeta de red.

<base_addr >, es la dirección de memoria base en la RAM que ocupará la tarjeta.

La mayoría de las aplicaciones basadas en TCP/IP para PC que son del dominio público, utilizan packet drivers. De la misma manera existen algunos programas especiales que les permiten a los packet drivers coexistir con Microsoft Windows y otras dos bien conocidas especificaciones de interfaz de red: NDIS (un estándar desarrollado por Microsoft y 3Com) y ODI (desarrollado por Novell y Apple).

Es necesario aclarar que los packet drivers fueron la primera opción para tratar de estandarizar el software de red y por consiguiente fueron apareciendo versiones más complejas pero más fácil de instalar. Por ejemplo los usuarios de Windows trabajan con software de red más moderno que los simples packet drivers como Microsoft TCP/IP-32 o Novell LAN Workplace.

Windows para trabajo en grupo, por poner un ejemplo, carga su driver de red con la línea de comando "net start" en el archivo autoexec.bat, y utiliza los archivos \windows\system.ini y \windows\protocol.ini para controlar y configurar su enlace a la red. Y todo se lleva a cabo desde la aplicación "configuración de red", que a través de ventanas y menús hacen de la configuración manual algo obsoleto, o simplemente con el popular shareware Trumpet Winsock. Windows 95 tiene su propia pila de protocolos TCP/IP "Dial-Up networking" en la opción de comunicaciones cuando se instala Windows.

Las nuevas tarjetas de red son totalmente compatibles con los dispositivos Plug and Play, por lo que al encender la PC los parámetros son colocados automáticamente de acuerdo a las características de la máquina y ya no es necesaria la configuración manual de la dirección de E/S base para la tarjeta, ni del número de interrupción. Además, los drivers son cada vez más completos ya que ellos mismos determinan, al inicio de su operación, el tipo de medio que está siendo utilizado para conectar la tarjeta a la red.

Sin embargo, la ventaja de seguir utilizando la configuración manual con respecto a las facilidades que proporciona el nuevo software como Windows 95, es el mayor control que se tiene sobre el packet driver y la seguridad de que sabemos que números de interrupciones se están utilizando. Además de que Windows 95 esconde los packet drivers y su acceso lo lleva a cabo a través de librerías dinámicas (DLL) o drivers virtuales (VxD).

Dentro de las características que sólo poseen algunas tarjetas de red, se encuentra aquella que será de vital importancia para el desarrollo de nuestro software: **el modo promiscuo**. Alrededor de esta característica girará el desempeño y el éxito de la aplicación.

3.9
El modo promiscuo

El modo promiscuo es el estado en el cual muchas tarjetas para redes de área local pueden ser configuradas para permitirles capturar todos los paquetes que viajan por la LAN. Prácticamente todas las tarjetas Ethernet (802.3) para todos los sistemas aceptan el modo promiscuo, así como algunas para la tecnología token ring (802.5), y algunas otras para redes MAN.

Dicho modo es habilitado por el programador colocando ciertos valores en los registros de la tarjeta, forzándola para que acepte todos los paquetes que se encuentran en la red, incluyendo los destinados para otras estaciones. El software puede direccionar los paquetes a un archivo, desplegarlos, o muchas otras cosas más. El número de paquetes que pueden ser capturados depende del buffer del controlador, de la velocidad del sistema, de la velocidad del bus, y de otras tantas condiciones. Además, también depende de la eficacia del programa escrito para manejar el estado promiscuo de la tarjeta, ya que debe ser lo suficientemente inteligente y rápido para proveer información útil conforme ésta llegue de la tarjeta.

Debido a que la mayoría de los protocolos no encriptan los datos en los paquetes, el contenido de los paquetes capturados puede ser fácilmente examinado. En la mayoría de las situaciones, observar los paquetes en código ASCII es suficiente para descubrir user IDs y passwords, además de otro tipo de información importante. En algunos casos, conociendo los algoritmos de compresión o codificación de datos (tales como Radix-50, TASCII, ASCII, EBCDIC, etc.) y, junto con el modo promiscuo, se puede obtener información de la red que solo el administrador de la misma tiene derecho a saber. Ésto, junto con el hecho de que se pueden obtener las especificaciones de la mayoría de los protocolos de red a través de los vendedores o

vía dominio público en una gran variedad de fuentes, permiten que sea realmente atractivo y fácil de capturar y analizar un paquete para los programadores.

Probablemente uno de los problemas que representa el modo promiscuo es su gran potencial para explotar los recursos de las redes. Muchas veces los desarrolladores de los programas no los hacen con la intención de entrometerse, pero si un paquete puede ser capturado y analizado, este será explotado.

El modo promicuo en pocas palabras es algo peligroso, aunque a veces puede ser útil. Todos los analizadores de red y los monitores de red utilizan el modo promiscuo en una forma u otra, ya que no puede ser detectado en la red cuando está habilitado en una estación dada. Es semejante a alguien que esta escuchando una conversación telefónica en una extensión telefónica con el micrófono deshabilitado, de tal manera que nadie sabe que alguien está en la extensión y que todas las conversaciones pueden ser escuchadas. Desafortunadamente, en muchos aspectos, el modo promiscuo es un malechor necesario si ciertos aspectos en el manejo de la red son alcanzados.

3.10 Resumen

La importancia de la comunicación de datos se ha visto reflejada en las redes de computadoras. A medida que se desarrolla una, la otra tiende a mejorar y a alcanzar nuevas metas. Pero todo debe estar regido bajo ciertas reglas que faciliten el desempeño y el mejor manejo de los recursos. Por algo la tecnología internet ha llegado a ser el pilar sobre el que descansan millones de redes a lo largo de todo el mundo. Conocida comúnmente como TCP/IP, esta tecnología se ha visto beneficiada por la preferencia de la mayoría de los especialistas, y no es difícil imaginar esta reacción si tomamos en cuenta que los protocolos que conforman este conjunto realmente están diseñados para las condiciones más adversas. Mientras que TCP se dedica a acondicionar los datos, dividiendo los mensajes cuando es necesario, a enviarlos nuevamente cuando no han alcanzado su destino y a agruparlos para su entrega final, el protocolo IP se dedica exclusivamente a buscar la mejor ruta para ellos. Pareciera que son entidades altamente independientes, y lo son, porque cada protocolo se dedica únicamente a sus funciones. Pero al mismo tiempo se encuentran estrechamente relacionados, ya que uno depende en gran medida de los demás para lograr sus objetivos.

Aprovechando las ventajas que representa tener una tecnología Ethernet como base de la red de computadoras de la UTM, empezaremos a desarrollar en el capítulo 5 un programa de aplicación que nos permita explotar las características de los distintos encabezados para analizarlos y separar ciertos campo de los mismos, sin caer en el área dedicada a los datos y mantener segura la integridad de los mismos.

4

Internet

Internet es uno de los hechos más importantes de este fin de milenio, es una fuente inagotable de recursos que constituye una base del conocimiento que engloba a todo el planeta. Es una red mundial formada por redes de computadoras de diferente topología, las cuales pueden intercambiar mensajes, programas y todo tipo de información entre si. Es una revolución en el campo de la comunicación interpersonal y del trabajo en grupo, ya que permite compartir ideas y conocimientos tanto a nivel personal como entre los miembros de las comunidades con intereses comunes, distribuidas por toda la tierra.

La rapidez con la que se pueden llevar a cabo todo esto a nivel mundial ha dado lugar al nombre de autopista de la información.

La definición que mejor se ajusta a lo que hoy es Internet viene dada por la expresión "Red de redes" y ha llegado a ser un instrumento decisivo en nuestra civilización, puesto que ha transformado la forma de vivir y de trabajar.

Algunas fuentes citan que cubre más de 200 países con 500 redes separadas, conteniendo más de 10 millones de estaciones y más de 80 millones de usuarios.

Algunos dicen que Internet debió tener sus orígenes desde 1957 después de que la ex Unión Soviética lanzó su primer satélite artificial "Sputnik". Los Estados Unidos en respuesta formaron la Agencia de Investigación de Proyectos Avanzados (ARPA), en el Departamento de Defensa para establecer un equilibrio comparable en ciencia y tecnología, ambos al servicio de la milicia.

Otros proponen que Internet se inició durante la Guerra Fría, a principios de los 60's, con la pregunta de "¿cómo podrían las autoridades estadounidenses comunicarse una con otra en caso de un ataque nuclear por parte de los soviéticos?".

A principios de los 60's la configuración de red que se utilizaba era un protocolo punto-a-punto, parecido a una red de anillo, donde las computadoras están conectadas en serie dependiendo una de la otra y, debido a que si un nodo de la red se descompone, los demás nodos se verán afectados.

En respuesta a este problema de las redes de los 60's, Paul Baran concibió la idea de un nuevo tipo de tecnología de red denominada de conmutación de paquetes, una red parecida a un telaraña. Se apoyaría en un protocolo de red que le permitiría a la información encontrar su propia ruta a través de la red aun si uno o más nodos de la misma no funcionaran.

La visión de Paul Baran llegó a ser la idea central para la creación de una pequeña WAN que conectaba las computadoras de 4 universidades estadounidenses, la cual creció para llegar a ser la supercarretera de la información con millones de nodos en millones de redes alrededor del mundo.

4.1 Historia

A principios de 1960 los Estados Unidos de América enfrentaron un extraño problema, ¿cómo harían para comunicarse durante y después de una guerra mundial?, puesto que hasta el momento ningún tipo de blindaje podría proteger las redes de comunicación entre las ciudades y estados. Se pretendía construír una red donde ninguna estación de control o centro de mando de la misma fuera un blanco inmediato para un misil enemigo.

Este problema fue encargado a RAND Corporation, quien estudió el caso durante meses hasta que un hombre, Paul Baran, propuso un ingenioso plan donde ofrecía una red diseñada para funcionar aun cuando se estuviera desbaratando, de tal manera que no estuviera estructurada sobre las condiciones normales que se habían manejado hasta la fecha, dando la sensación de ser insegura.

Las principales características de esta red eran:

- Los diferentes nodos o centros de control se diseñarían para comunicarse en una forma fortuita: un nodo podría enviar un mensaje a cualquier otro nodo aleatorio de la red en una dirección tal que pudiera llegar a su destino final. Este nodo debería enviar el mensaje a otro nodo hasta que, eventualmente, el mensaje lograra llegar

a su destino final. Si alguna parte de la red estuviera dañada, los paquetes deberían evadirla y tomar rutas alternas. Este sistema parecía ser muy ineficiente comparado con las redes existentes (sistema telefónico), pero sería prácticamente indestructible.
- Todos los nodos de la red tendrían el mismo estatus, y cada uno de ellos podría originar, enviar y recibir mensajes.
- Los mensajes estarían divididos en paquetes, donde cada uno de ellos se direccionaría separadamente.
- Cada paquete tendría su origen en algún nodo específico y su destino en otro, y cada paquete se responsabilizaría de su ruta a través de las redes.

La tarea de llevar a cabo este proyecto fue encargado a ARPA, quien decidió implementar una red descentralizada de paquetes conmutados en los E.U. A esta red experimental se le denominó ARPAnet que podía, entre otras cosas:

- Resistir daños parciales y aún asi funcionar.
- Trabajar aunque una parte de la red desapareciera en cualquier momento.
- Requerir el mínimo de información de las computadoras que formaban parte de ella.
- Cada computadora de la red podía comunicarse con cualquier otra computadora.

Esas características que suponían una red poco confiable sonaron extraño, pero la historia ha demostrado que la mayoría de ellas estuvieron correctas.

Los primeros nodos de esta red fueron supercomputadoras de alta velocidad y estuvieron instalados en la UCLA (Universidad de California de Los Ángeles), el Instituto de Investigación de Stanford, la Universidad de Santa Barbara en California y la Universidad de Utah. Estas cuatro computadoras podían transferir datos a través de líneas de transmisión dedicadas a altas velocidades. Los científicos e investigadores podían enlazarse y utilizar las facilidades prestadas por otras computadoras.

Por el segundo año de operación de ARPAnet, un extraño hecho llegó a ser claro. El principal tráfico de ARPAnet no fue el cómputo a larga distancia, fueron noticias y mensajes personales. Los investigadores y académicos que tuvieron acceso a ARPAnet utilizaron la red para colaborar en proyectos, para intercambiar notas de trabajo y para enviarse recados a través de su cuenta personal (e-mail) que los acreditaba como usuarios en las computadoras de ARPAnet. Así, apareció la primera lista de correo (mecanismo a través del cual se puede envíar un mismo mensaje a un conjunto de suscriptores interesados en un tema particular). Sorprendentemente, una de las primeras grandes listas fue "SF-LOVERS", para los fanáticos de la ciencia ficción.

La gente no podía esperar y los diseñadores de Internet en Estados Unidos, Inglaterra y Escandinavia, en respuesta a las presiones del mercado, empezaron a colocar el software de IP en todo tipo de computadoras. Se llegó a convertir en el único método práctico para comunicar computadoras de diferentes fabricantes, lo que resultó muy atractivo para el gobierno y las universidades, quienes no tenían la política de comprar una determinada marca de computadoras. Todos compraron las computadoras que mejor les convenía y esperaban poder comunicarse con otras en la red.

Al mismo tiempo que Internet se consolidaba, las redes locales Ethernet eran desarrolladas. La tecnología de redes locales maduró hasta 1983, cuando aparecieron las primeras estaciones de trabajo para escritorio y las redes locales se multiplicaron. La mayor parte de las estaciones de trabajo tenían el sistema UNIX de Berkeley instalado que incluía el software de red IP. Esto creó una nueva demanda: en lugar de conectar una computadora de tiempo compartido en un centro de cómputo, las organizaciones requerían conectar toda su red local a ARPAnet, lo cual permitía que todas las computadoras que estuvieran en la red usaran los servicios de ARPAnet. De igual forma, muchas compañías y otras organizaciones empezaron a construír redes privadas usando los mismos protocolos de comunicación de ARPAnet. Parecía obvio que si estas redes podían comunicarse entre sí, los usuarios de una red podrían comunicarse con usuarios de otra y todo mundo saldría beneficiado.

De estas nuevas redes, una de las más importantes fue la NSFNET, auspiciada por la Fundación Nacional de la Ciencia, una agencia del gobierno estadounidense. A finales de los 80's la NSF creó cinco centros de supercómputo en universidades importantes. Hasta entonces, las computadoras más rápidas del mundo sólo estaban a disposición de los fabricantes de armamento y de algunos investigadores de compañías muy grandes. Con la creación de estos centros, la NSF ponía estas fuentes a disposición de cualquier investigación escolar. Sólo se crearon cinco centros porque su costo era muy elevado y fue necesario compartirlos, lo que provocó un problema de comunicación: se necesitaba interconectar a los centros y permitir a los usuarios tener acceso a ellos. Al principio, la NSF trató de utilizar la red ARPAnet para la comunicación de los centros, pero esta estrategia falló debido a problemas burocráticos.

En respuesta a esto, la NSF decidió construír su propia red basada en la tecnología IP de ARPAnet. Esta red conectaba los centros mediante enlaces telefónicos de 56 Kbps. Sin embargo, era obvio que si se trataba de conectar cada universidad a los centros de supercómputo, el proyecto se podría venir abajo. Por esta razón, se decidió crear redes regionales, y en cada región del país las escuelas podían conectarse a su vecino más próximo. Cada cadena estaba conectada a un centro de supercómputo en un solo punto. Con esta configuración, cualquier computadora podría comunicarse con otra.

Repentinamente las escuelas que participaban en la red contaron con un amplio universo de información y colaboradores al alcance de sus manos. El tráfico en la red se incrementó con el tiempo hasta que las computadoras que la formaban lo controlaban y las líneas de teléfono conectadas a ellas se saturaron. En 1987 se celebró un contrato para administrar y actualizar la red, con la compañía Merit Netowork Inc., que operaba la red educacional de Michigan, en colaboración con IBM y MCI. La vieja red fue mejorada con líneas telefónicas de mayor velocidad (por un factor de 20) y con computadoras más poderosas.

El aspecto más importante del esfuerzo de conectividad de NSF fue el hecho de permitirle a todos el acceso a la red que hasta entonces, sólo estaba autorizado a investigadores en ciencias computacionales, empleados y contratistas del gobierno. La NSF promovió el acceso universal a las instituciones educativas, financiando

conexiones en las universidades únicamente si éstas tenían un plan para permitir el acceso en la zona.

4.2
Desarrollo cronológico

1962
- Paul Barand de RAND Corporation inicia las investigaciones en redes de comunicación distribuída para controlar y comandar puestos militares estadounidenses.
- Se publica el reportaje "introducción a las redes de conmutación de paquetes".

1965
- ARPA es responsabilizada del estudio e investigación en "redes de computadoras cooperativas de tiempo compartido".

1967
- Algunos delegados reunidos en un coloquio de la Asociación para la Maquinaria Computacional en Galinberg, Tennesse, discutieron el primer plan de ARPAnet y sus principios operacionales.
- Fueron presentados algunos planes para las redes de conmutación de paquetes.
- El Laboratorio Nacional de Física (NPL) en Middlesex, Inglaterra desarrolló la red de datos NPL.

1968
- La red de conmutación de paquetes le fue presentada a ARPA.

1969
- ARPA fue comisionada para la investigación en redes de computadoras. Algunos centros de investigación de cuatro campus universitarios en los Estados Unidos fueron los primeros nodos de ARPAnet, siendo el primero de ellos la UCLA, después el Instituto de Investigación de Stanford, Santa Barbara y la Universidad de Utah.
- Bolt Beranek y Newman, Inc. (BBN) desarrollaron la Honeywel 516, una minicomputadora con 12 K de memoria.
- El primer RFC (Request For Comments) "Host Software" fue presentado por Steve Croker, y sigue siendo uno de los fundamentos de la programación ISP.
- La Universidad de Michigan, en Estados Unidos, y las Universidades Wayne States establecieron una red basada en X.25 para académicos y estudiantes.
- ARPAnet fue un éxito desde sus inicios, pero aunque originalmente fue diseñada para permitirle a los científicos y estudiantes compartir datos y acceso remoto a las computadoras, el correo electrónico llegó a ser y sigue siendo la aplicación de red más importante. ARPAnet llegó a ser una oficina postal digital muy veloz, debido a que la gente la utilizó para colaborar y discutir proyectos de investigación de variado interés y algunos tópicos.

1970
- Los nodos de ARPAnet empezaron a utilizar el Protocolo de Control de Red (NCP).
- En la Universidad de Hawaii, se desarrolló la ALOHnet por Norman Abrahamson, pero no llegó a conectarse a ARPAnet hasta 1972.

1971
- De 15 nodos que tenía ARPAnet llegó a 23, conectando universidades, fuentes gubernamentales y algunos establecimientos a lo largo de Estados Unidos.
- Ray Tomlinson de BBN inventó el altamente conocido programa de correo electrónico para enviar mensajes a través de una red distribuída. El programa original se derivó de otros dos: un programa de correo electrónico entre máquinas (SNDMSG) y un programa de transferencia de archivos experimental (CPVNET).

1972
- Se llevó a cabo una conferencia internacional sobre comunicaciones de computadoras, donde se dio una demostración de ARPAnet entre 40 computadoras y el Procesador Terminal de Interfaz (TIP), organizado por Bob Khan y en donde el Grupo de trabajo de InterNetWorking (INWG) fue creado para establecer estándares que gobernaran el crecimiento de la red. Vinton Cerf fue electo presidente de dicho grupo, y más tarde se le llegó a conocer como el "padre de Internet".
- Se estableció la especificación de Telnet (RFC 318).

1973
- ARPAnet se internacionalizó con conexiones a la Universidad College de Londres, Inglaterra y a la Royal Rada en Noruega.
- El Dr. Bob Metcalfe presentó su idea de Ethernet en su tesis de doctorado en la Universidad de Harvard.
- Vinton Cerf esquematizó una arquitectura de redes utilizando ruteadores (antes gateways) en el mes de Marzo, al reverso de un sobre en un lobby de un hotel en San Francisco.
- Cerf y Khan presentaron las ideas básicas de Internet al INWG en la Universidad de Sussex, Brighton, Inglaterra.
- Fue creada la especificación para la transferencia de archivos (RFC 454).

1974
- El público obtiene su primer idea sobre cómo pueden ser utilizadas las redes de computadoras.
- ARPAnet empieza a desviarse de sus raíces y valores originales de investigación militar.
- BBN da cabida a las versiones comerciales al público de Telnet a través del servicio de conmutación de paquetes.
- Vinton Cerf y Bob Khan publican "Un Protocolo para la Intercomunicación con Conmutación de Paquetes", la cual especifica en detalle el diseño de un Protocolo de Control de Transmisión (TCP).

1975
- El manejo operacional de Internet es transferido a DCA, actualmente la Agencia de Información de Sistemas de Defensa (DISA).

1976
- La Reina Elizabeth II de Inglaterra deseó estar en línea y enviar su primer mensaje real.
- Los laboratorios Bell de AT&T desarrollan UUCP (Unix-to-Unix CoPy).

1977
- THEORYNET, creado por Larry Landweber en la Universidad de Wisconsin provee correo electrónico a más de 100 investigadores en ciencias de la computación utilizando un sistema desarrollado localmente y Telnet para accesar al servidor.
- Es creada la especificación de correo electrónico (RFC 733).
- Se realizó la primera demostración de comunicación utilizando paquetes de radio NET/SATNET.

1979
- Tom Truscott y Jim Ellis de la Universidad de Duke, junto con Steve Bellovin de la Universidad de Carolina del Norte establecieron el primer grupo de noticias USENET entre la Universidad de Duke y la de Carolina del Norte. Los usuarios de todo el mundo se unen a esos grupos de discusión para hablar sobre redes, política, religión, etc.
- La red experimental de paquetes de radio (PRnet) inició sus experimentos con la fundación DARPA. La mayoría de las comunicaciones se realizaron entre automóviles que utilizaban la conexión ARPAnet a través del Instituto de Investigación de Stanford.

1981
- Las estaciones de ARPAnet llegaron a 213, y cada nueva estación era agregada cada 20 días.
- BITNET (Because It's Time NETwork) se inició como una red corporativa en la Ciudad Universitaria de New York, con la primera conexión a la Universidad de Yale, y proveía correo electrónico y una lista de servidores para distribuír información, como también transferencia de archivos.
- La CSNET (Computer Science NETwork) fue construída con la colaboración de científicos en ciencias computacionales de las universidades de Delawere, Purdue, Wisconsin, RAND Corporation y BBN, con fondos de la NSF para proveer servicios de red, especialmente correo electrónico, a universidades científicas sin acceso a ARPAnet. CSNET después se llegó a conocer como la Red de Ciencia y Computación.
- Minitel (Teletel) se distribuyó en Francia por Telecom de Francia.

1982
- Bob Khan y Vinton Cerf crearon TCP/IP, el lenguaje común para todas las computadoras de Internet y fue aprobado por el Departamento de Defensa estadounidense como un estándar adecuado. Por primera vez a las redes basadas en el modelo ARPAnet se les conoció como "internet", y nació la Internet que conocemos actualmente.
- La combinación de máquinas de escritorio baratas y poderosas y los servidores de red les permitieron a las compañías unirse a ARPAnet por vez primera. Las corporaciones empezaron a usar Internet para comunicarse una con otra, con sus clientes y proveedores.
- EUNET (European UNIX Network) fue creada por EUUG para proporcionar correo electrónico y servicios de noticias (USENET).
- Los países bajos se conectan: Dinamarca, Suecia e Inglaterra.
- La especificación del Protocolo de Gateway Externo (RFC 827) es utilizada para gateways (ahora ruteadores) entre redes.

1983
- NCP es sustituído por TCP/IP y el Servidor de Nombres es desarrollado en la Universidad de Wisconsin para no requerir un conocimiento extenso de la ruta para enlazarse a otros sistemas.
- Las estaciones de trabajo de escritorio incluyeron el UNIX de Berkeley, que poseía el software TCP/IP de red.
- CSNET y ARPAnet se unen a través de un ruteador.
- ARPAnet se divide en ARPAnet y MILnet, esta última se integra a la red del Departamento de Defensa creada anteriormente.

1984
- Es introducido el Servicio de Nombres de Dominio (DNS) y el número de estaciones llega a 1000.
- Se establece JUNET (Japan UNIX Network) utilizando UUCP.
- En Inglaterra se establece JANET (Joint Academic NETwork).

1985
- Se conecta la universidad más alejada de Canadá a BITNET en un esfuerzo por crear una conexión de costa a costa.

1986
- Case Western Reserve University en Clevelan, Ohio crea la primera sociedad "FreeNET" para acceso al público.
- NSFNET creó un backbone a una velocidad de 56 Kbps.
- Se desarrolla el Protocolo de Transferencia de Noticias (NNTP), diseñado para realzar el desempeño sobre TCP/IP.
- Los registros Mail Exchange (MX) son desarrollados por Craig Portridge. Estos le permitieron a las estaciones de red que no poseían el Protocolo Internet, poseer una dirección de dominio.

1987
- El número de estaciones en Internet excedió los 10, 000.
- La guía de referencia "Request For Comments" fue aprobada por ARPAnet, existiendo cerca de 1000 RFCs.

1988
- Internet fue una herramienta esencial para comunicaciones, pero también empezó a crear conciencia acerca de la privacidad y la seguridad en el mundo digital.
- Aparecieron nuevos términos como "Hacker, Hackin" y "Electronic Breakin". Estos términos fueron demostrados dramáticamente el primero de Noviembre de este año cuando un programa malicioso denominado "el gusano Internet" deshabilitó temporalmente aproximadamente 6 000 de las 60 000 estaciones de Internet.
- El CERT (Equipo de Respuesta a Emergencias Computacionales) fue formado para salvaguardar la red en respuesta al gusano de Internet.
- El Internet Relay Chat (IRC) fue desarrollado por Jarkko Olkarinen de Finlandia.
- Se crean las primeras redes regionales enlazadas a NSFNET en Canadá, Dinamarca, Finlandia, Islandia, Noruega y Suecia.

1989
- Se lleva a cabo la primera transmisión entre un servicio de correo eletrónico comercial e Internet: entre MCI a través de la Corporación para la Iniciativa de Investigación Nacional (CNRI) y Compuserv a través de la Universidad del Estado de Ohio.
- Se crea AARNET (Australian Academic Research Network) por AVCC y CSIRO.

1990
- Una víctima feliz de su éxito inesperado y no planeado: desaparece ARPAnet dejando a sus espaldas la red de redes.
- Con la desaparición de ARPAnet los proveedores comerciales de hardware y software de red surgen a una velocidad exponencial.
- El número de estaciones ha crecido a 300 000 alrededor del mundo.
- Peter Deutschi, Alan Emtage y Bill Heelan de la Universidad McGill en Montreal Canadá desarrollan Archie.
- Aparece CA*net, el backbone canadiense formado por 10 redes regionales con conexión directa a NSFNET.

1991
- En este año, Tim Berners-Lee del CERN en Suiza posteó el primer código del World Wide Web (WWW). La habilidad para combinar palabras, imágenes y sonidos en las páginas del Web exitaron a muchos programadores quienes vieron el potencial de publicar información en Internet en una forma tan fácil como utilizar un procesador de palabras.
- Marc Hendreesen y un grupo de estudiantes en NCSA de la Universidad de Illinois desarrollaron un visualizador denominado Mosaico.
- El tráfico de NSFNET sobrepasó el trillón de octetos/mensuales, 10 billones de paquetes/mensuales.

1992
- La primera difusión de audio y video tomó lugar sobre una porción de Internet denominada "MBONE".
- Las herramientas de búsqueda, Veronica y Gopher, fueron desarrolladas en la Universidad de Nevada.
- El Banco Mundial se pone en línea.

1993
- Fue creado InterNIC por la NSF para proveer servicios específicos de Internet como directorio, bases de datos, registro, Nombres de Dominio y de información.
- Mosaico, el visualizador de Web estuvo disponible al público.
- La primera y la segunda familia estadounidenses (Clinton/Gore) se pusieron en línea. Lo mismo que la ONU.

1994
- El comercio esta en línea, y el primer CyberBanco abre sus puertas para los negocios. Los Rolling Stones difunden su música sobre el MBONE. Cualquiera que tenga acceso a Internet puede ordenar su pizza a Pizza Hut.
- El Primer Ministro Japonés se pone en línea.

1995
- La red NSFNET regresa a los proyectos de investigación abandonando la senda comercial del Web en Internet que ahora comprende el grueso del tráfico en la red de redes.
- Un equipo de programadores de Sun Microsystems investigan en un nuevo lenguaje de programación denominado "Java", el cual cambia radicalmente la forma de las aplicaciones y de la información en que puede ser desplegada y utilizada la información sobre Internet.

1996
- Los usuarios en casi 150 países alrededor del mundo están conectados a Internet y el número de estaciones es de aproximadamente 10 millones.

1997
- Todos los continentes del globo están conectados en un progreso sin precedente, llegando a 235 países.

Actualmente, las diferentes piezas de Internet están conectadas por un conjunto de computadoras llamadas ruteadores, las cuales conectan a las redes unas con otras. Esas redes pueden ser Ethernets, Token Rings o simplemente líneas telefónicas.

Los ruteadores toman decisiones acerca de cómo rutear los datos o paquetes de datos. Debido a que los ruteadores no tienen una conexión con cada uno de los demás ruteadores, cada paquete de datos es enviado al ruteador más cercano del destino del paquete. Para esto Internet utiliza el protocolo Internet que observa la dirección de un paquete y se asegura de que los ruteadores sepan qué hacer con él cuando les llegue.

4.3 Resumen

Internet es una gigantesca red de redes. Cuando se habla de Internet se refiere a computadoras interconectadas entre sí a nivel mundial para comunicación de datos.

Los usuarios forman parte de todo tipo de instituciones, ya sea de investigación, docencia, comerciales o gubernamentales. Internet es la red de computadoras más grande del mundo.

También conocida como la "Red" es una red de redes donde se intercambia información sin restricciones. Estas redes van desde las grandes y formales como las redes corporativas de AT&T, Digital Equipment y Hewlett Packard, hasta las pequeñas e informales.

Para comunicarse entre sí, las computadoras necesitan "hablar" un mismo lenguaje (protocolo). En Internet, los protocolos utilizados son TCP/IP. Por lo tanto, para conectar una computadora a Internet, además de la conexión física, se requiere que los protocolos TCP/IP estén instalados en dicha computadora. A diferencia de otros protocolos de comunicación, existen implementaciones de TCP/IP para prácticamente todas las marcas y modelos de computadoras, lo que explica su aceptación y utilización en todo el mundo. Internet está presente en más de 235 países.

5

Implementación del Monitor de Enlaces IP

En los capítulos anteriores se han visto los conceptos y las ideas básicas de la comunicación de datos, así como una pequeña introducción a los protocolos TCP/IP. En este capítulo, se llevará a cabo el desarrollo de un monitor de enlaces a nivel del protocolo IP, haciendo uso del conocimiento que se tiene acerca de los encabezados que acompañan a los datos.

Dicho monitor tiene como finalidad básica la captura de los paquetes Ethernet que se encuentren viajando sobre la red de la universidad, de tal manera que nos permita analizar sus encabezados para estudiar los campos que nos interesan, como sus direcciones IP fuente y destino, cantidad de datos, etc., y llevar un control estadístico de las conexiones realizadas en nuestra red.

A lo largo de este capítulo se analizarán los algoritmos e ideas sobre el diseño del software, y las técnicas de programación utilizadas. Se proporcionará un panorama general sobre la interacción interna del software, por ejemplo cómo cada módulo y los diferentes elementos se relacionan unos con otros, las E/S tanto del usuario (preferencias) como de las interfaces (resultados). Se describirán las principales funciones del programa y todos sus niveles de interconectividad.

Cabe mencionar que no se describirán los detalles de las llamadas al sistema operativo, solo la forma en que cada módulo o componente trabajará, sus funciones, entradas y salidas.

Nuestro software de aplicación se divide en dos partes: la primera, denominada Monitor, se ejecuta sobre MS-DOS y es la encargada de la captura de los paquetes de información Ethernet que se encuentran en la red de la UTM, el análisis de sus encabezados y almacenamiento de la información. Sin embargo, esta primera parte lo único que realiza es separar las direcciones IP fuente y destino, la fecha y hora del enlace y la cantidad de información intercambiada. Lo que obligó a desarrollar una segunda parte, denominada Nslookup, que tomará dichas direcciones numéricas del archivo creado por Monitor y, utilizando el Servidor del Servicio de Nombres de Dominio (DNS) que se encuentra en mixteco.utm.mx, transformará dichas direcciones en nombres de dominio. Esta parte se ejecuta sobre un ambiente windows.

A continuación se explicará el desarrollo de la primera parte que se elaboró en lenguaje de programación C. La razón por haberla creado para ejecutarse sobre MS-DOS se debe al mayor control que se tendría sobre la tarjeta en cuanto a su dirección base de E/S, ya que se utiliza su packet driver. El inconveniente que se tiene es que la tarjeta, al entrar en un modo de operación especial (promiscuo), no podrá comunicarse con ninguna otra máquina, sólo podrá recibir información. Por consiguiente se optó por utilizar dos computadoras, una dedicada especialmente a ejecutar Monitor y en otra estará Nslookup. El archivo dado por Monitor tendrá que almacenarse en un dispositivo que pueda intercambiarse entre las máquinas.

5.1
La familia EtherLink III de 3Com

Es importante destacar que el software se realizó para las tarjetas 3Com de la familia EtherLink III, especialmente para las que utilizan bus tipo ISA, debido a que se logró conseguir su manual técnico donde vienen indicados sus registros y principales comandos, y por que se contaba con tarjetas de este tipo y de su correspondiente packet driver. Para poder entender el desarrollo del software, revisemos las características más importantes de esta familia, que está integrada por las tarjetas que se muestran en la tabla 5.1.

Tipo de Bus	Tarjeta	Número de conectores por tarjeta	Especificación de cable	Tipo de conector
ISA	3C509-TPO 3C509B-TPO	uno	10BASE-T	RJ-45
	3C509-TP 3C509B-TP	dos	10BASE-T coaxial delgado	RJ-45 AUI

Tabla 5.1 Tarjetas 3Com de la familia EtherLink III

Tipo de Bus	Tarjeta	Número de conectores por tarjeta	Especificación de cable	Tipo de conector
ISA	3C509-Coax 3C509B-Coax	dos	coaxial delgado coaxial grueso	AUI BNC
	3C509-COMBO 3C509B-COMBO	tres	10BASE-T coaxial delgado coaxial grueso	RJ-45 AUI BNC
EISA	3C579	dos	coaxial delgado coaxial grueso	AUI BNC
	3C579-TP	dos	10BASE-T coaxial delgado	RJ-45 AUI
MCA	3C529	dos	coaxial delgado coaxial grueso	AUI BNC
	3C529-TP	dos	10BASE-T coaxial delgado	RJ-45 AUI
PCMCIA	3C589-TP 3C589B-TP	uno	10BASE-T	RJ-45
	3C589-COMBO 3C589B-COMBO	dos	10BASE-T coaxial grueso	RJ-45 BNC

Tabla 5.1 Tarjetas 3Com de la familia EtherLink III (continuación)[6]

Esta familia de tarjetas posee una memoria RAM organizada en dos pilas FIFO (primero en entrar, primero en salir), una para transmitir (TX FIFO) y otra para recibir (RX FIFO).

Los paquetes Ethernet que se estén recibiendo serán almacenados en RX FIFO por la tarjeta, y el software de red de la estación se encargará de leer la información de esa pila. Por su parte, los paquetes Ethernet que se transmitirán serán escritos por el software de red a la pila TX FIFO de la tarjeta, y ésta se encargará de enviarlos a su destino. Se pueden conservar múltiples paquetes en ambas FIFOs, lo que depende del tamaño de los paquetes y de la memoria RAM de la tarjeta.

Observemos la disposición de los registros dentro de la tarjeta 3C509B-TP, figura 5.1, que utiliza un bus tipo ISA, y posee dos tipos de conectores (RJ-45 y AUI). De aquí en adelante tomaremos como referencia dicha tarjeta para explicar los registros y comandos que soportan el resto de las tarjetas, salvo algunas variaciones muy pequeñas.

[6] 3Com. EtherLink® III Parallel Tasking™ ISA, EISA, Micro Channel®, and PCMCIA Adapter Driver Technical Reference. 1994, pp. 1-1

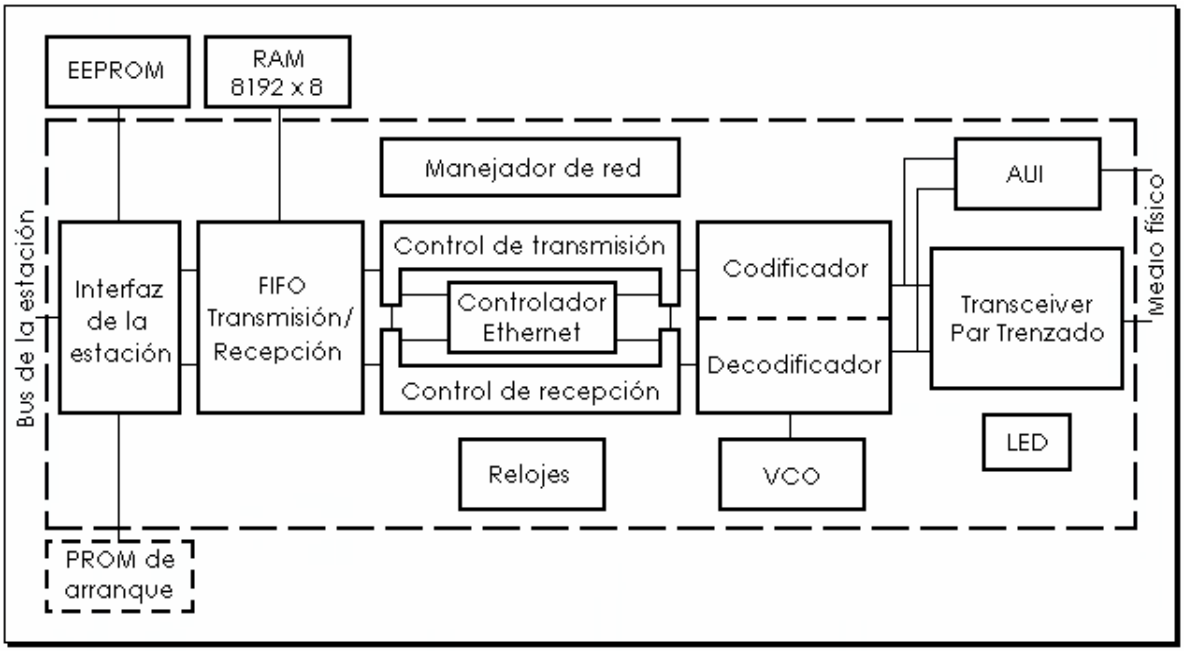


Figura 5.1 Tarjeta 3C509B-TP

Debido a que la tarea principal de nuestra aplicación consistirá en el análisis de los encabezados en los paquetes Ethernet recibidos, centraremos nuestra atención en los registros y comandos referentes a la recepción de información.

5.1.1
Descripción de operación de las tarjetas 3Com

El modo en que las tarjetas de esta familia transfieren los datos está programada (PIO). Conforme son recibidos los datos desde el cable, se van acumulando en la RX FIFO. Similarmente, la transmisión de datos se lleva a cabo escribiendo a la tarjeta ocho o 16 bits al mismo tiempo, y acumulándolos en TX FIFO, para que la tarjeta se encargue de enviar el paquete por el cable. Una vez que los datos son leídos o transmitidos, el espacio que ocupaban en su correspondiente FIFO estará disponible.

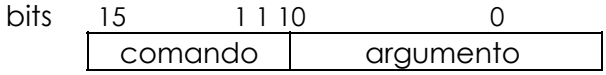
Uno de los registros que más se utilizará en la aplicación es el registro de estado de recepción (RX S), que contendrá la información referente al estado del paquete que se encuentra en la cima de la pila RX FIFO. Por ejemplo, su tamaño, el progreso en la recepción, las fallas en la tarjeta, algunos errores ocurridos durante la recepción, etc.

El conjunto de registros en la tarjeta está organizado en 7 ventanas con 8 registros cada una. Las ventanas 2, 4 y 5 contienen registros responsables del desempeño de la tarjeta; mientras que la ventana 0 contiene los registros de configuración de la EEPROM; la ventana 1 se considera como crucial por que en ella

se encuentran los registros estándares que incluyen los registros usados en la ruta del driver de la tarjeta, además de aquellos referentes al estado de los paquetes recibidos (RX S) y transmitidos (TX S), los registros de entrada y salida programada (TX PIO y RX PIO).

Pero por cuestiones de interés, las ventanas 3 y 6 serán las de mayor importancia. La primera contiene registros responsables del manejo de la FIFO, y la segunda contiene los registros de estadísticas como el total de octetos recibidos correctamente, las colisiones detectadas, los errores detectados durante la recepción, etc.

A continuación veremos las principales instrucciones que soportan las tarjetas 3Com en el modo de recepción. Dichos comandos tendrán una longitud de 16 bits, donde los 11 bits menos significativos representarán el argumento, y los 5 bits más significativos el comando o instrucción.



Reseteo global

0000 0	000 00XX XXXX

El argumento de este comando enmascarará el reseteo del módulo deseado, de acuerdo a:

Bit	Acción
0	Reseteará el transceiver de 10Base-T y AUI.
1	Reseteará el codificador/decodificador interno.
2	Reseteará el módulo de red, incluyendo el controlador Ethernet.
3	Reseteará el módulo FIFO.
4	Reseteará el estado de la máquina para autoinicializarse.
5	Reseteará la interfaz del bus.

Si se utiliza un argumento de valor 0, se resetearán todos los módulos.

Selección de la ventana de registros

0000 1	000 0000 0XXX

Este comando seleccionará la ventana de registros XXX para poder accesar a los registros en ella. El registro de estado mantendrá el número de la ventana actual. Después de un reseteo global, la ventana 0 será la ventana activa.

Deshabilitar la recepción

0001 1	000 0000 0000

Este comando deshabilita la recepción del controlador Ethernet. Si un paquete está en proceso de recepción, será recibido y posteriormente se deshabilitará completamente la recepción.

Habilitar la recepción

0010 0	000 0000 0000

Habilita la recepción del controlador Ethernet. Si un paquete, durante la habilitación, se encuentra en el cable y está destinado para la tarjeta, no será recibido. Se puede utilizar el comando anterior para deshabilitar la recepción o bien, se puede resetear la recepción para el mismo fin.

Resetear la recepción

0010 1	000 0000 XXXX

Se recomienda utilizar este comando solo en casos muy necesarios.

Bit	Acción
0	Reseteará el transceiver lógico 10Base-T y AUI.
1	Reseteará el receptor lógico codificador/decodificador .
2	Reseteará el receptor lógico de red, incluyendo el controlador Ethernet y el receptor. Abortará cualquier recepción del paquete actual.
3	Reseteará el receptor lógico FIFO.

Descargar el paquete RX

0100 0	000 0000 0000

Descargará el paquete que se encuentra en la cima de la pila RX FIFO cuando ya no sea necesario o porque se ha detectado algún error en él. Si el paquete no ha sido completamente recibido y se utiliza esta instrucción, se ignorará el resto del paquete.

Este comando automáticamente carga el próximo paquete del FIFO y actualiza el estado RX con el estado del nuevo paquete.

Filtros de recepción

1000 0	000 0000 XXXX

Este comando permite determinar el tipo de paquetes Ethernet, de acuerdo a su dirección destino, que puede leer la tarjeta de acuerdo a:

Bits	Acción
0001	Solo aceptará los paquetes destinados a esa estación.
0010	Podrá aceptar paquetes con direcciones de grupo (multidifusión).
0100	Aceptará paquetes con direcciones de difusión.
1000	**Aceptará todos los paquetes (modo promiscuo).**

Habilitación de estadísticas

1010 1	000 0000 0000

Este comando habilita la captura de las estadísticas que serán almacenadas en los registros de la ventana 6. Al iniciar la sesión de la tarjeta, este comando está deshabilitado, y una vez que esté habilitado y se desee leer cualquier estadística desde la ventana 6, se deberá deshabilitar la recepción de estadísticas temporalmente.

Deshabilitación de estadísticas

1011 0	000 0000 0000

Deshabilitará la recolección de estadísticas.

5.2
Desarrollo del software

Contamos ya con todas las herramientas para implementar nuestro software, ya que sabemos la estructura interna que guardan cada uno de los encabezados, la forma en que se comunicará el packet driver con la tarjeta. Pero sobre todo, la forma en que debemos activar y manejar el modo promiscuo y cada uno de los registros de la tarjeta para obtener la información deseada. Ahora estamos en condiciones de dar un panorama general sobre las actividades que llevará a cabo el software.

Lo que se ha hecho es comunicarse directamente con la tarjeta Ethernet y tomar la información que nos interesa desde ella. Ésto quiere decir que el sistema operativo no podrá accesar a la tarjeta y por lo tanto recibir o transmitir información. Esta alternativa se debe a que si el sistema operativo recoge los paquetes Ethernet, entonces ya no se podrán recuperar para ser analizados por el programa. Por otra parte, si el programa los captura ya nadie más podrá accesar a ellos. Ésto se apoya en la manera en que están elaboradas las tarjetas Ethernet. Una vez que se lea un octeto de información, éste será borrado de su memoria interna (FIFO).

Para lograr que el sistema operativo no intervenga en el proceso de recolección, se tiene que esconder la tarjeta de red de él. El sistema operativo recibe paquetes Ethernet cuando la tarjeta hace una interrupción (interrumpe al CPU) utilizando su número de interrupción por hardware. Si podemos desactivar dicha interrupción, el sistema operativo no recibirá nada y los paquetes se quedarán en la tarjeta.

Cuando se haya logrado lo anterior, tendremos que configurar la tarjeta en modo promiscuo para que pueda recibir todo tipo de paquetes Ethernet que viajen por la red aún cuando no vayan destinados para nuestra estación. Logrando ésto, podremos descomponer, analizar y presentar la información que nos interesa por cualquier medio, ya sea visual (por pantalla), impreso o guardarlo en un archivo.

En resumen, el software cambia en primer instancia la configuración de la tarjeta Ethernet para que no haga interrupciones, y la configura a modo promiscuo. Después monitorea el registro que indica cuando se ha recibido un paquete, y decodifica la información de interés para después desplegarla por pantalla y almacenarla en un archivo. Cuando se de por terminada la ejecución del software, se configura nuevamente la tarjeta para que trabaje en modo normal.

5.2.1 Monitor

Para empezar, la siguiente figura muestra las principales entradas y salidas que poseerá nuestra aplicación.

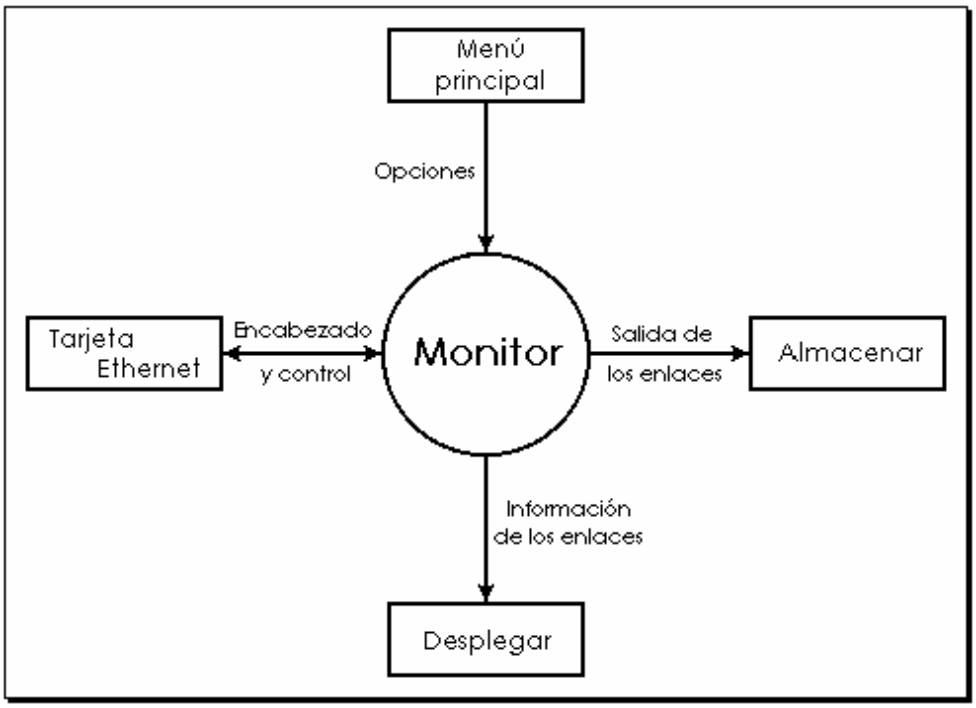


Figura 5.2 Descripción general de Monitor

Las entradas estarán indicadas por el usuario a través del menú principal y por la información proveniente de la tarjeta Ethernet (encabezados); y las salidas que proporcionará Monitor serán: el desplegado de la información por pantalla, hacia un archivo o bien, información de control que permitirá comunicarse con la tarjeta.

A continuación se muestra la descomposición de la aplicación por módulos, donde se observa la interrelación que guardan cada una de las partes principales del programa.

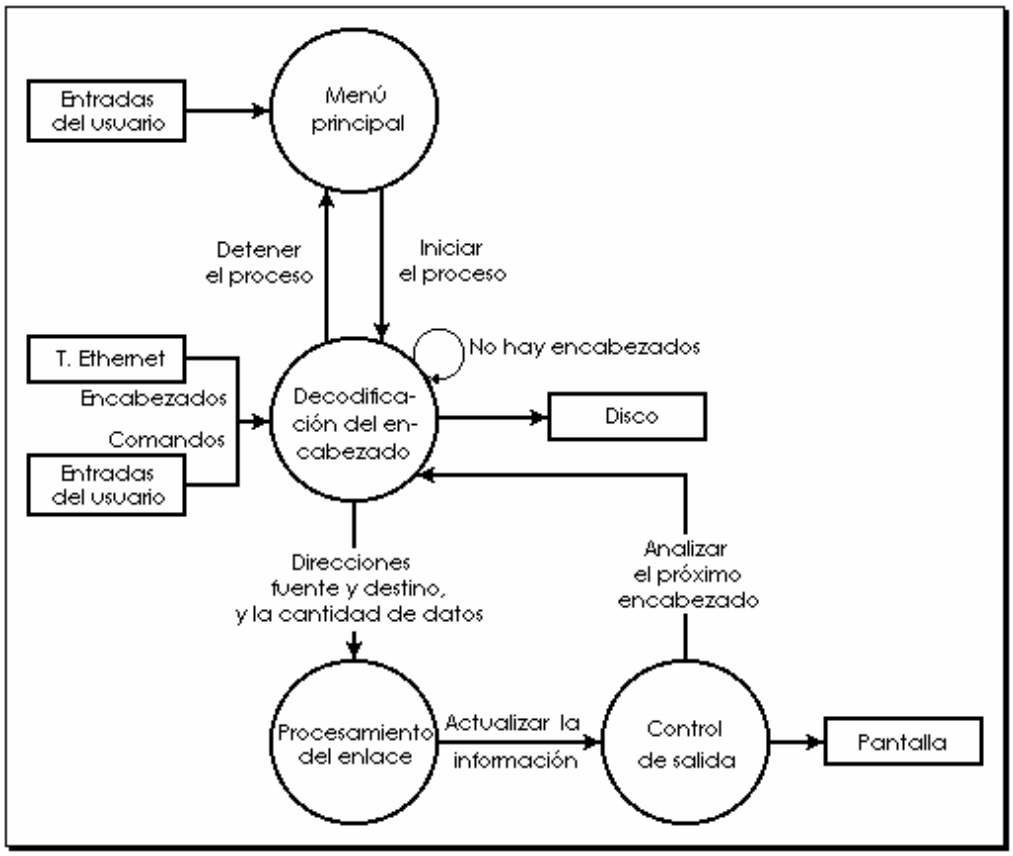


Figura 5.3 Descomposición por módulos

5.2.1.1
Descripción por módulos

Modulo menú principal

Este módulo le permitirá al usuario colocar los principales parámetros para el despliegue de la tabla de enlaces. Estos parámetros podrán ser:

- Tipo de flujo a desplegar: flujo total o flujo promedio.
- Actualizar la pantalla cada x lecturas.
- El factor exponencial que podrá ser 1000 ó 1024.
- Le permitirá seleccionar el nombre del archivo de salida.
- Iniciar el proceso o continuarlo en el caso de haberlo detenido temporalmente.
- Resetear todos los enlaces existentes en memoria, y
- Salir del proceso.

Este módulo no hará ningún proceso, sólo regresará una estructura que contendrá las preferencias seleccionadas por el usuario, como se muestra a continuación:

```
struct preferencias{
        doble factor;    // factor exponencial
```

```
int actualizar;   // actualizar la pantalla
short tipo_flujo // 0 para promedio, 1 para total
}
```

El nombre del archivo de salida estará contenido en una variable global denominada arch_salida, y la detección temporal del proceso regresará a este módulo.

Módulo decodificador del encabezado

Este proceso decodificará y analizará la información del encabezado capturado por la tarjeta. También revisará el buffer del teclado para posibles entradas por parte del usuario tratando de: enviar la tabla de enlaces a un archivo, refrescando la tabla en la pantalla o simplemente deteniendo el proceso.

El encabezado será leído desde la memoria interna de la tarjeta (FIFO). Los elementos del encabezado serán decodificados y solo las direcciones fuente y destino, y la longitud del paquete Ethernet serán de importancia. Este proceso estará en un ciclo mientras no existan paquetes Ethernet presentes en la FIFO, hasta que llegue uno nuevo. No tendrá subordinados y únicamente deberá iniciar hasta que todas las preferencias del usuario se encuentren establecidas, o el proceso de control de salida termine sus funciones.

Necesitará de la capacidad de memoria interna de la tarjeta, y la información enviada por ella y no contendrá ningún paquete que resulte colisionado o con errores detectados en el CRC, incluyendo los paquetes incompletos.

Los datos del encabezado recibidos desde la tarjeta de red serán almacenados en la siguiente estructura:

```
struct encabezado{
        unsigned char ip_fuente[4];
        unsigned char  ip_destino[4];
        int longitud;
        }
```

El pseudocódigo de este módulo es:

leer las preferencias del usuario
inicio
    mientras (existan encabezados) **hacer**
        leer encabezado
        si (tecla presionada) **entonces**
            si (tecla ‘d’ o ‘D’) **entonces** ir al menú principal
            otro si (tecla ‘a’ o ‘A’) **entonces escribe** a archivo
        otro si (se leyó un encabezado) **entonces**
            leer direcciones IP
            leer cantidad de información

ir a procesamiento del enlace
fin_mientras
fin

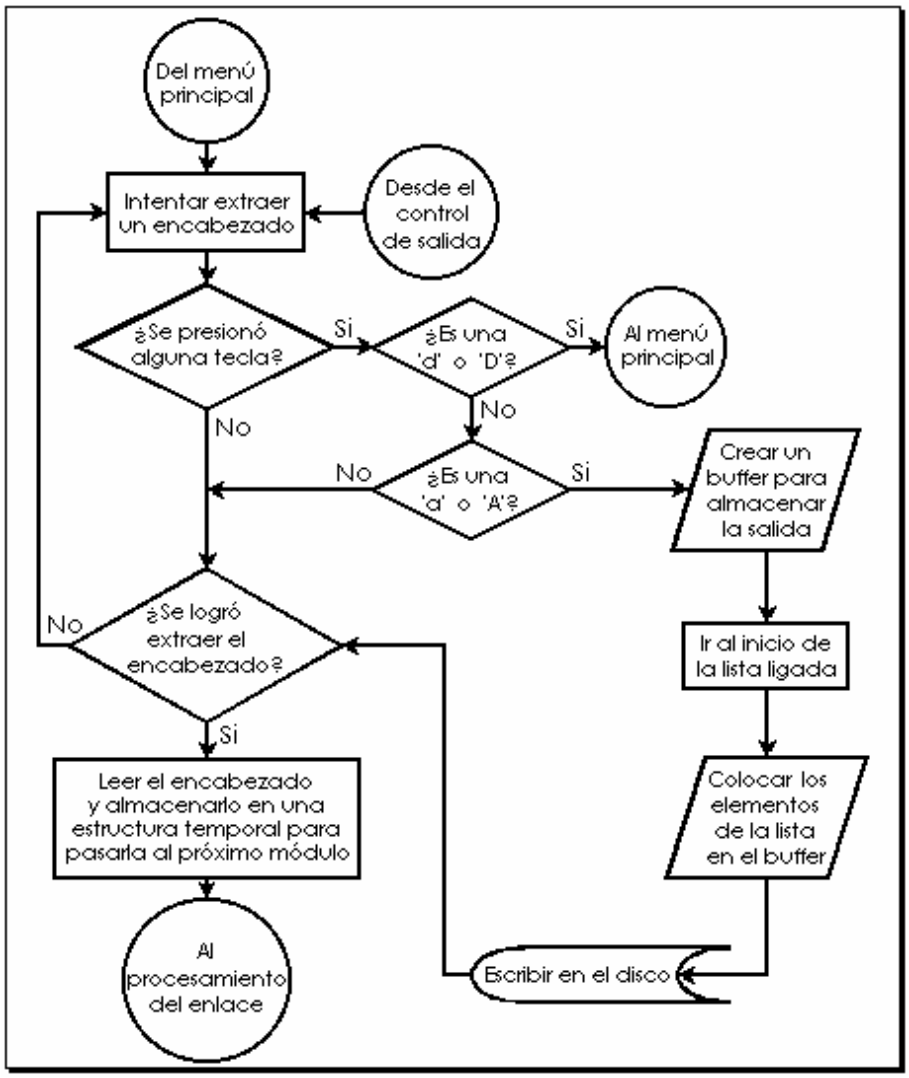


Figura 5.4 Diagrama de flujo del módulo decodificador del encabezado

Módulo procesamiento del enlace

Este módulo se encargará del procesado de los enlaces y los almacenará en memoria. Identificará la ruta indicada por la información obtenida en el módulo decodificador del encabezado y la comparará con los otros enlaces usando las direcciones fuente y destino. Si el enlace en cuestión no está presente en la tabla de enlaces, el módulo lo agregará a la tabla y le asignará el próximo índice disponible; en caso contrario, utilizará el índice asignado a dicho enlace para modificar únicamente la cantidad de flujo intercambiado. Este módulo también informará al módulo control de salida de cualquier cambio en la tabla usando el número de índice para ello.

Las actividades realizadas por esta parte del programa no poseerán ningún proceso subordinado y su desempeño dependerá de la información obtenida por el módulo decodificador del encabezado, el cual pasa el nuevo enlace a este módulo. Por lo tanto, este módulo no podrá iniciar hasta que el módulo decodificador del encabezado haya finalizado.

Es importante destacar que se requerirá de una gran cantidad de memoria disponible, debido a que se utilizará una lista ligada para almacenar los enlaces en ella. La estructura de los enlaces, como se define más adelante, contendrá la información necesaria acerca de las direcciones del transmisor y del receptor del paquete Ethernet, y la hora en que fue descubierto el enlace por el programa. El índice indicará la posición del enlace en la lista ligada. Además será usado por el módulo control de salida para buscar el enlace y así facilitar la salida por pantalla.

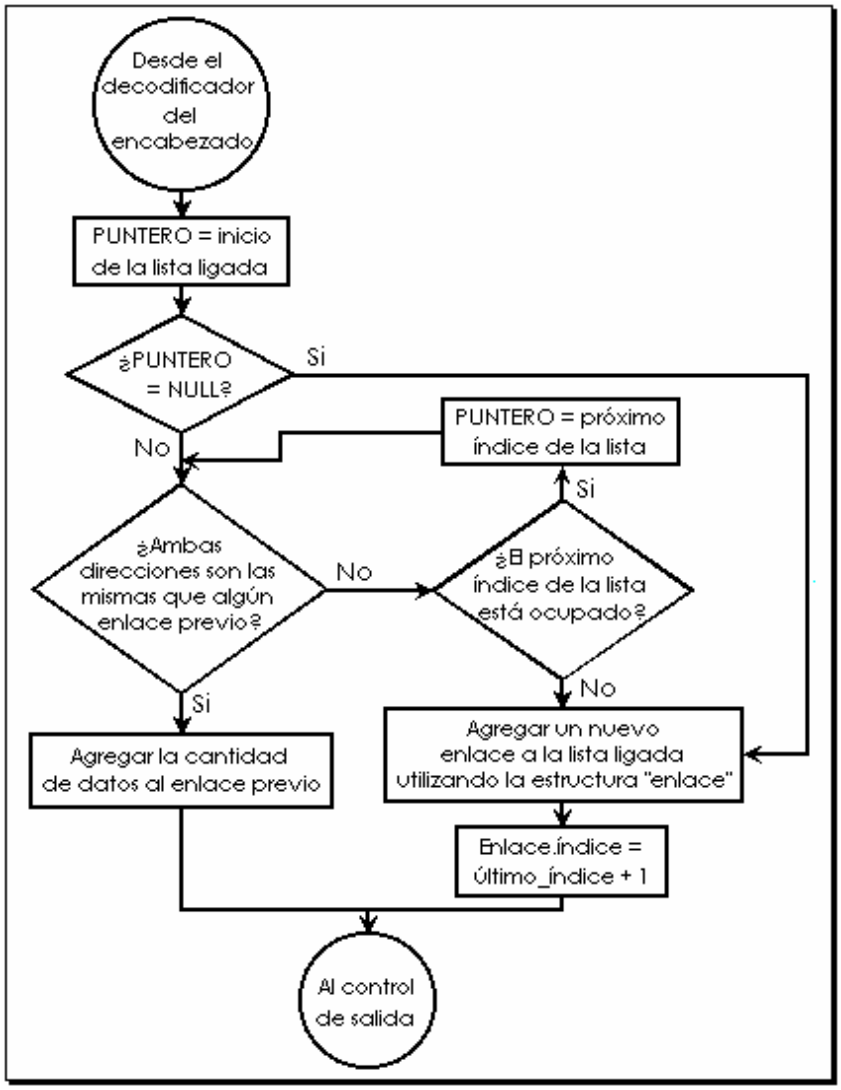


Figura 5.5 Diagrama de flujo del módulo procesamiento del enlace

```
struct enlace {
        unsigned char direcciones[2][4];
```

```
long double datos;
time_t hora;
int indice;
struct enlace *proximo;
}
```

El pseudocódigo es:

```
PUNTERO=inicio de la lista ligada
inicio
    si (PUNTERO=NULL) entonces
        incrementar ultimo_indice
        agregar el nuevo enlace a la lista ligada
        ir al control de salida
    otro mientras (no se termine la lista y enlace_encontrado=0) hacer
        si (ya existe el enlace) entonces
            agregarle la cantidad de información
            ir al control de salida
            bandera enlace_encontrado=1
        otro avanzar PUNTERO
      fin_mientras
    si (enlace_encontrado=0) entonces
        agregar el nuevo enlace a la lista ligada
fin
```

Módulo control de salida

Este proceso será el responsable de actualizar y desplegar la tabla por pantalla, y le permitirá al usuario la salida de la misma hacia un archivo.

Formateará la tabla y la desplegará de acuerdo a las preferencias indicadas por el usuario. La pantalla contendrá todo lo necesario, las direcciones fuente y destino, la hora en que fue descubierto el enlace, la cantidad de datos intercambiados, la hora en que el programa inició sus operaciones. La pantalla será actualizada usando el índice de los enlaces, los cuales serán ordenados en la pantalla utilizando el mismo índice. Solo la línea del enlace a actualizar será modificada, el resto permanecerá intacto.

Para ello, necesitará del número de índice del enlace que ha cambiado o, si es nuevo, del último índice para desplegarlo, que le será proporcionado por el módulo procesamiento del enlace.

5.2.2
Nslookup

Nslookup, semejante en el nombre al comando que en el sistema operativo UNIX lleva a cabo la conversión de direcciones IP en nombres de dominio, utiliza la abstracción socket, que es la base de la E/S de red en BSD de UNIX, para comunicarse con el Servidor del Servicio de Nombres de Dominio. El socket es una generalización del mecanismo de acceso a archivos de UNIX que proporciona un punto final para la comunicación. Los programas de aplicación requieren que el sistema operativo cree un socket cuando se necesita. El sistema devuelve un entero pequeño que utiliza el programa de aplicación para hacer referencia al socket creado recientemente. La aplicación puede elegir abastecer una dirección de destino cada vez que utiliza el socket (cuando se envían datagramas) o elegir enlazar la dirección de destino a un socket y evadir la especificación de destino repetidamente (cuando se hace una conexión TCP).

En este caso se utiliza la segunda opción, utilizando una conexión TCP, es decir, el programa realiza una petición al servidor DNS y espera hasta que se lleva a cabo la conexión. Si no obtiene respuesta vuelve a insistir hasta que es atendido. Una vez realizado esto, va leyendo las direcciones a traducir desde el archivo creado por Monitor y le solicita a DNS la conversión de dirección IP a nombre de dominio (ejemplo: 192.100.170.60 -> iec50.utm.mx). La respuesta puede ser exitosa cuando se logra la conversión o bien, puede ser lo contrario en el caso de no existir un nombre de dominio para alguna dirección particular, o bien porque en el transcurso de la búsqueda se consumió el tiempo predeterminado para ella, que viene siendo aproximadamente de un minuto.

Esta parte creará un archivo para cada una de las estaciones involucradas en la actividad de la red de la universidad registrada en el archivo proporcionado por el programa Monitor. En cada archivo nuevo se depositarán los nuevos formatos de las direcciones y se seguirán conservando los demás datos como la hora y la cantidad de información intercambiada. Por ejemplo, si dentro del archivo dado por Monitor se encuentran las siguientes líneas:

[Dirección IP 1]	[Dirección IP 2]	[Activo desde]	[Flujo de datos]
192.100.170.60	192.100.170.4	19/12/97 08:05	116471.00 B
192.100.170.60	192.100.170.1	19/12/97 08:05	212963.00 B

Se creará un archivo para la estación 60 de la red, en donde se almacenarán las distintas conexiones que realizó dicha estación, de tal suerte que dicho archivo tendrá un parecido a:

La actividad de la estación iec50.utm.mx (192.100.170.60) el día 19/12/97 fue la siguiente.

Hora	Dirección IP	Nombre de dominio	Cantidad de flujo
08:05	192.100.170.4	nuyoo.utm.mx	116471.00 B
08:05	192.100.170.1	mixteco.utm.mx	212963.00 B

De igual forma se creará un archivo para las estaciones 1 y 4.

Además de la conversión de las direcciones IP en nombres de dominio y de la creación de los distintos archivos, Nslookup le permitirá al usuario graficar la actividad de la red.

Esta parte se desarrolló en Visual Basic debido a la flexibilidad que presenta este paquete en cuanto a interfaz y facilidad en su manejo. Además de que se utilizó un shareware denominado Catalyst Software que permite, a través de herramientas complementarias a Visual Basic, la creación de sockets.

El pseudocódigo de Nslookup es el siguiente:

```
Seleccionar archivo_entrada
Seleccionar carpeta_de_salida
Seleccionar tipo_visualizador
inicio
        conectarse con el servidor DNS
        IP = ' '
        N = ' '
        mientras (!fin archivo_entrada) hacer
                N = ' '
                leer IP de archivo_entrada
                solicitar la conversión y guardarla en N
                leer la cantidad de flujo y almacenarla en el área correspondiente
                Si (N == ' ')  entonces
                                desplegar mensaje "No encontrado"
                                N = IP
                escribir N en archivo
        fin_mientras
        desconectarse del servidor DNS
graficar
fin
```

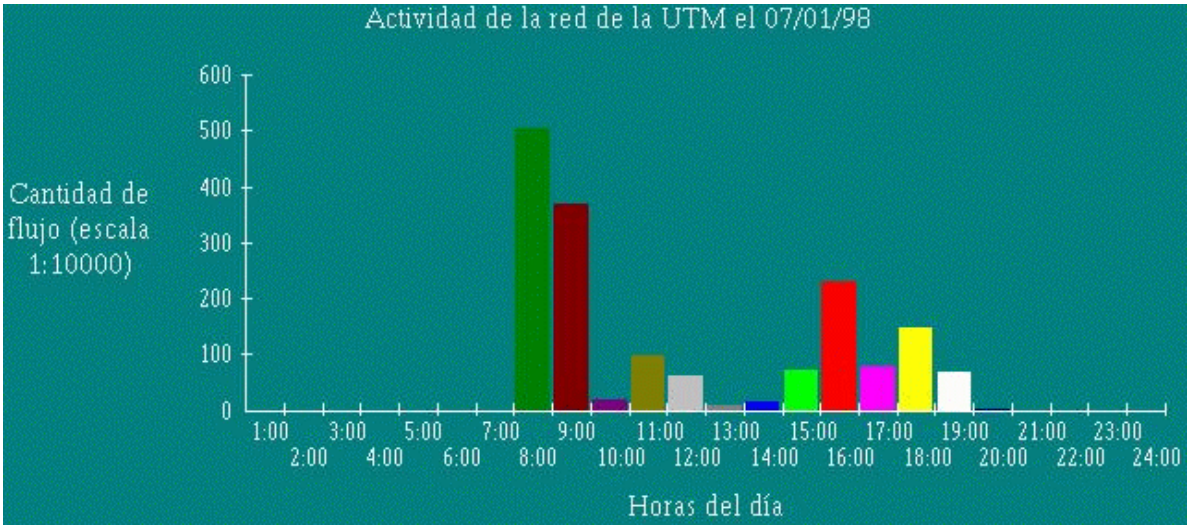
Conclusiones

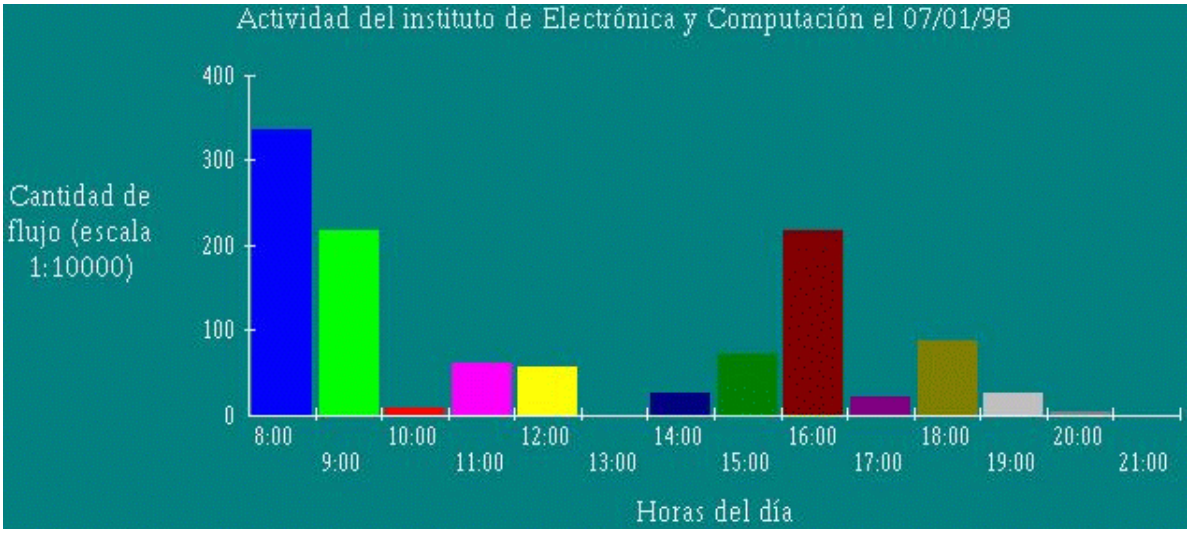
La aplicación Monitor de Enlaces IP es el resultado de una inquietud basada en el constante incremento en el tráfico de la red y por consiguiente baja productividad de la misma.

Monitor de Enlaces IP es el producto de la combinación de dos programas que se ejecutan sobre plataformas diferentes: Monitor y Nslookup. Mientras el primero corre en un ambiente de sistema operativo DOS, encargado de la captura y análisis de los paquetes Ethernet que se encuentran presentes en la red de la universidad, Nslookup, en un ambiente windows, se responsabiliza de estudiar y generar cada uno de los reportes pertenecientes a cada estación involucrada en la actividad de la red. Para ello aprovecha las ventajas que presenta Visual Basic de comunicarse con herramientas tan poderosas y sencillas como Notepad y Wordpad.

De acuerdo al objetivo planteado, podemos asegurar que Monitor de Enlaces IP cumple con las perspectivas para las que fue propuesto, ya que ha permitido observar el gran número de enlaces que se presentan en nuestra red; y a partir de los reportes generados por la aplicación, se pueden determinar las horas de mayor demanda de los servicios de red en cada una de las jornadas. Además, en base a las gráficas presentadas, podemos observar que la cantidad de información intercambiada es considerable.

Como una muestra de lo expresado se presentan algunas gráfica de las generadas por Nslookup, donde se logra observar tanto las horas de mayor demanda, como el correspondiente flujo de información involucrado en la red.





En base a esto, Monitor de Enlaces IP no sólo sirve para obtener estadísticas y generar reportes, también es un instrumento que puede ser aprovechado para tener un seguimiento de las posibles tendencias en la actividad de la red, y en base a ello, sugerir tanto a académicos como a alumnos, acerca de los mejores horarios para un uso más eficiente y mejor de los servicios de red.

Es recomendable destinar una máquina lo suficientemente rápida para la ejecución del programa Monitor, debido a que como se indicó en la sección 3.9, el número de paquetes que pueden ser capturados por la tarjeta Ethernet en modo promiscuo depende en gran medida de la velocidad de la máquina. Además, debido a la presencia del etherswitch instalado en nuestra red, Monitor no llega a registrar la actividad de toda la red. Esto se debe a que el etherswitch divide una red

Ethernet en segmentos, de tal manera que determina cuáles paquetes pueden pasar entre dichos segmentos apoyándose en las direcciones fuente y destino del paquete. Si éstas pertenecen a estaciones ubicadas en un mismo segmento, entonces no será necesario que el paquete esté presente en los demás. Si el transmisor y el receptor pertenecen a segmentos distintos, el paquete estará en esos segmentos solamente. Así el etherswitch evita la presencia innecesaria de paquetes en toda la red, reduciendo con esto las probabilidad de colisiones. Lo más recomendable en este caso sería colocar una copia de Monitor en cada área para tener resultados más precisos.

Mejoras

La aplicación presenta algunas características que pueden mejorarse entre las cuales, y quizá la que salta más a la vista, es la carencia de ejecución en tiempo real, y el inconveniente de tener que utilizar dos computadoras para su ejecución. Lo más conveniente sería poder realizar todo el trabajo (captura y análisis de los paquetes Ethernet) en el menor tiempo posible, o en su defecto también sería aceptable desechar una computadora y realizar todo el trabajo en una misma máquina. Pero como se explicó en el capítulo 5, al entrar en modo promiscuo la tarjeta Ethernet, no nos permite utilizar los servicios de red, razón por la cual se optó por utilizar dos máquinas.

Otro detalle que podría mejorarse sería el generalizar la aplicación Monitor para un mayor número de tarjetas de red Ethernet, debido a que sólo está elaborada para tarjetas 3Com de la familia EtherLink III. Por desgracia, para lograr esto se deben conseguir la mayoría de las hojas técnicas de las tarjetas para poder ampliar el rango de aceptación.

Hasta el momento, Nslookup se preocupa por generar archivos relacionados con las estaciones involucradas en cada reporte entregado por Monitor, y esos archivos se eliminan cada vez que el reporte de Monitor es cambiado, a no ser que se especifique otra carpeta de destino, lo que resultaría poco práctico y un poco riesgoso puesto que se vería en peligro la capacidad de almacenamiento del driver utilizado. Por esto, es recomendable agregarle a la aplicación alguna técnica de compresión y descompresión de datos que facilitaran el almacenamiento de gran cantidad de archivos en poco espacio, logrando con ello dos avances: una mejor administración del espacio disponible y al mismo tiempo generar una especie de base de datos que le permitiría al usuario un análisis posterior de la información.

Perspectivas

Los beneficios del presente trabajo puede ser el principio de una serie de implementaciones que favorezcan un mejor manejo y control de los recursos de red. La gran variedad de alternativas está abierta, desde la creación de un paquete que no sólo realice estadísticas de conexiones sino también ayude a determinar las áreas de mayor congestión, detectar aquellos enlaces que sólo están desperdiciando el

ancho de banda, registrar condiciones anormales o intentos de violar la seguridad de la red, y otras aplicaciones más.

Apéndice A
Manual de usuario de Monitor

Instalación y configuración

Para utilizar el software de Monitor, se recomienda tener los siguientes componentes:

- Computadora IBM PC o compatible
- Procesador 286 o superior.
- Monitor VGA a color.
- Por lo menos 8 MB de memoria RAM.
- Sistema Operativo MS-DOS versión 6.0 o superior.
- Tarjeta de red 3Com EtherLink III y conexión a la red.

El programa utiliza un archivo denominado instalar.exe, el cual al ejecutarse, instala el software de Monitor en la unidad que se desee, creando el subdirectorio MONITOR por omisión, y copia los siguientes archivos:

- 3C5x9pd.com packet driver de las tarjetas 3Com EtherLink III.
- Moni.exe archivo ejecutable.
- monitor.bat archivo que carga al packet driver y al ejecutable.

Después de la instalación, sólo se necesitará ejecutar el archivo monitor.bat para que empiece a correr el software.

Guía de usuario

Hacemos hincapie en que dicha máquina al poseer una conexión de red no necesitará que tenga asignada una dirección IP, debido a que no la requerirá, salvo que aparte de correr Monitor se utilice para enlazarse y hace uso de los servicios de red. En este último caso, mientras se esté ejecutando Monitor no se tendrá acceso a los servicios de red debido a que se configura la tarjeta sólo para la recepción de los paquetes Ethernet. Para poder trabajar normalmente con la tarjeta, sólo será necesario detener la ejecución de Monitor, o en el caso de que durante su ejecución ocurra algún problema o termine en forma anormal, será necesario resetear la PC.

Si existe algún problema al ejecutar el programa, aparecerán cualquiera de las siguientes ventanas, indicando el motivo de la falla:

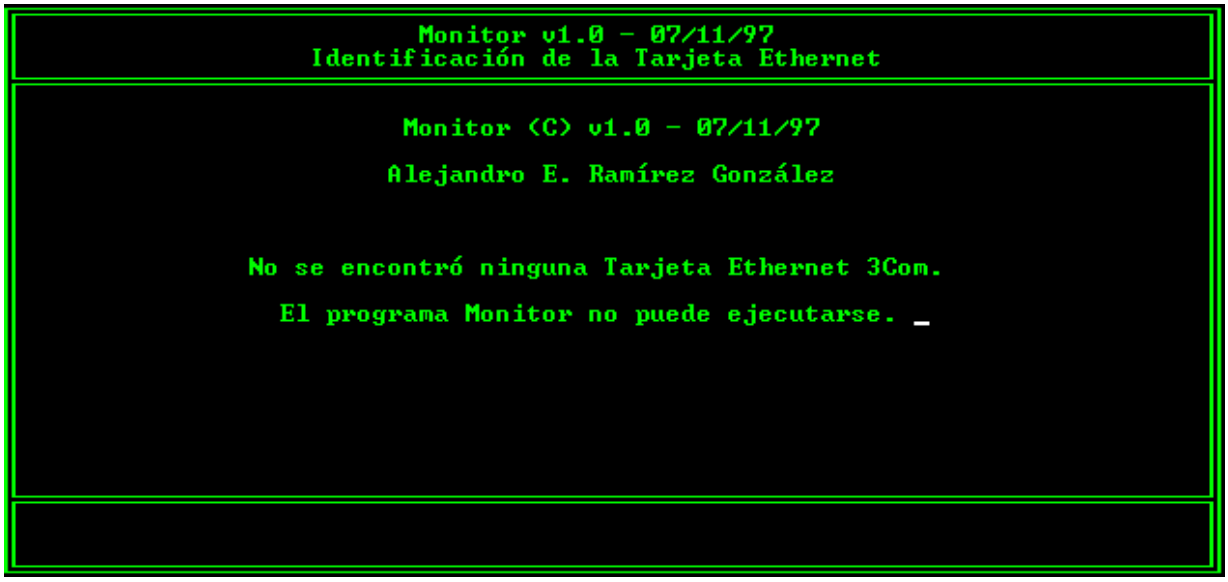


Figura A-1 Pantalla de identificación de la tarjeta Ethernet

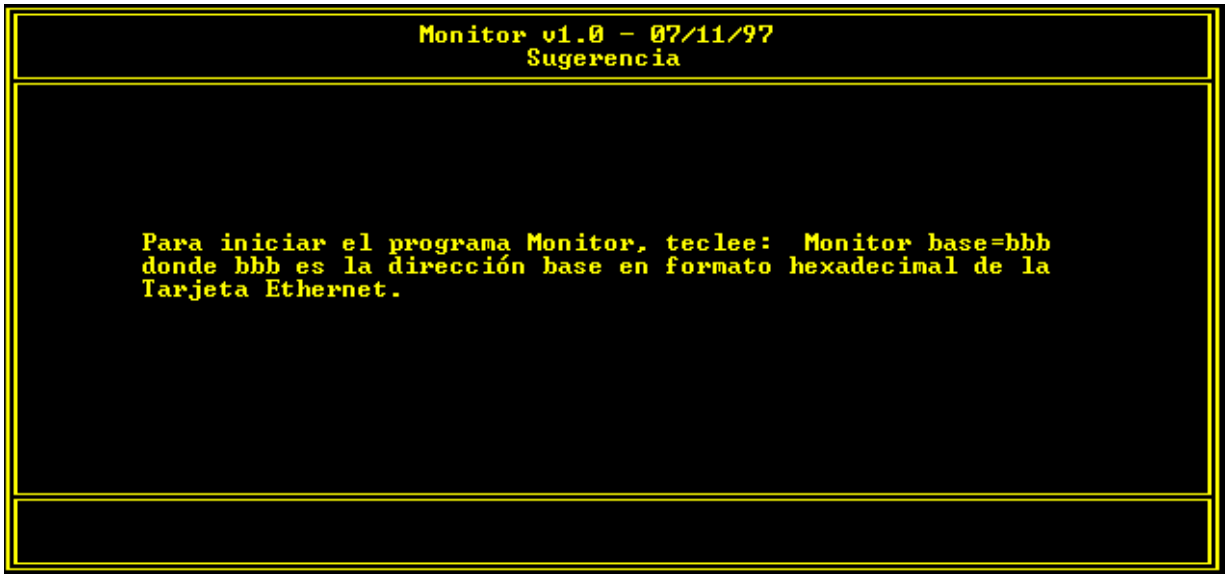


Figura A-2 Pantalla de sugerencia

En caso contrario, aparecerá una pantalla de presentación que tendrá la siguiente apariencia:

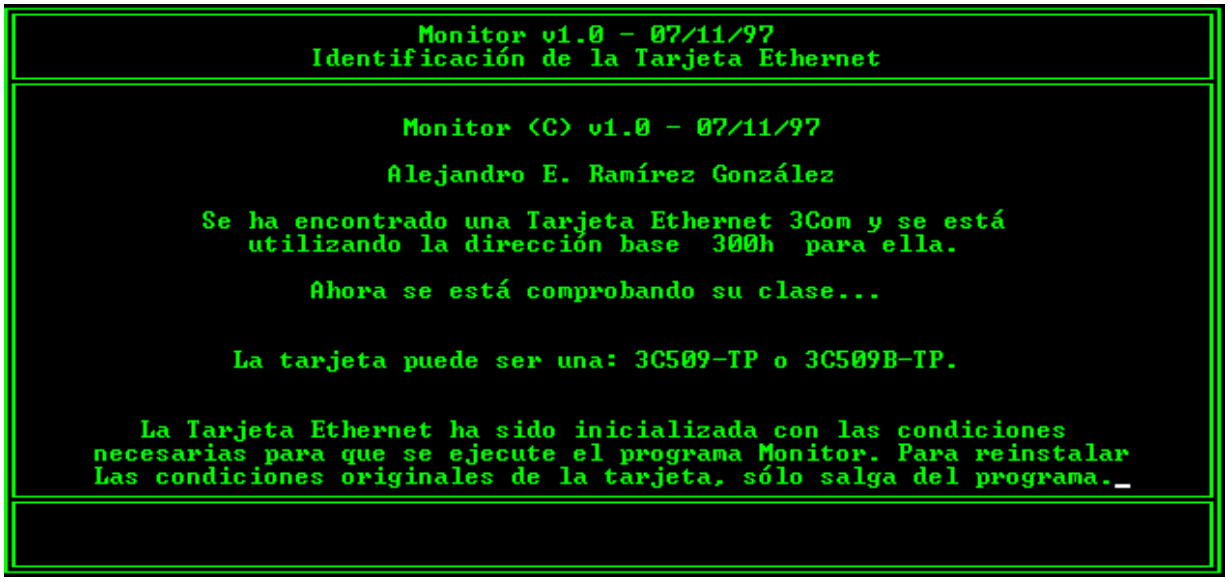


Figura A-3 Pantalla de presentación de Monitor

Después de algunos segundos, esta pantalla desaparecerá y dará lugar a la pantalla del menú principal:

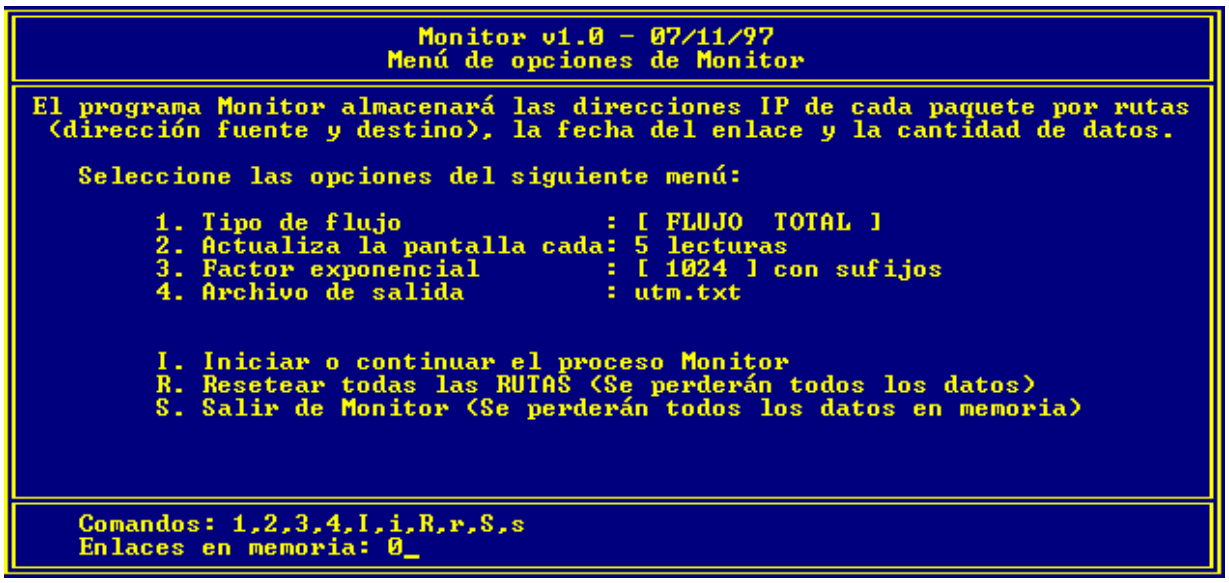


Figura A-4 Pantalla del menú de Monitor

Como se observa, son pocas las opciones que soporta Monitor, siendo éstas:

- El tipo de flujo que se desplegará: flujo total o flujo promedio. El primero indica la cantidad tal y cual se transfiere, mientras que el segundo indica la cantidad transferida por unidad de tiempo.
- Cada cuantas lecturas se actualizará la pantalla.
- El factor exponencial que se manejará: 1000 ó 1024.
- El nombre por omisión del archivo de salida será **utm.txt**, pero podrá modificarse en caso de desearlo.
- Iniciar el proceso Monitor o continuarlo en caso de haberlo detenido temporalmente.
- Se podrán resetear todos los enlaces presentes en memoria.
- Salir de la aplicación, lo que permitirá la configuración de la tarjeta para uso normal.

Si se decide iniciar el proceso, se presentará una pantalla semejante a la de la figura 5.10, donde se irán mostrando cada uno de los enlaces descubiertos.

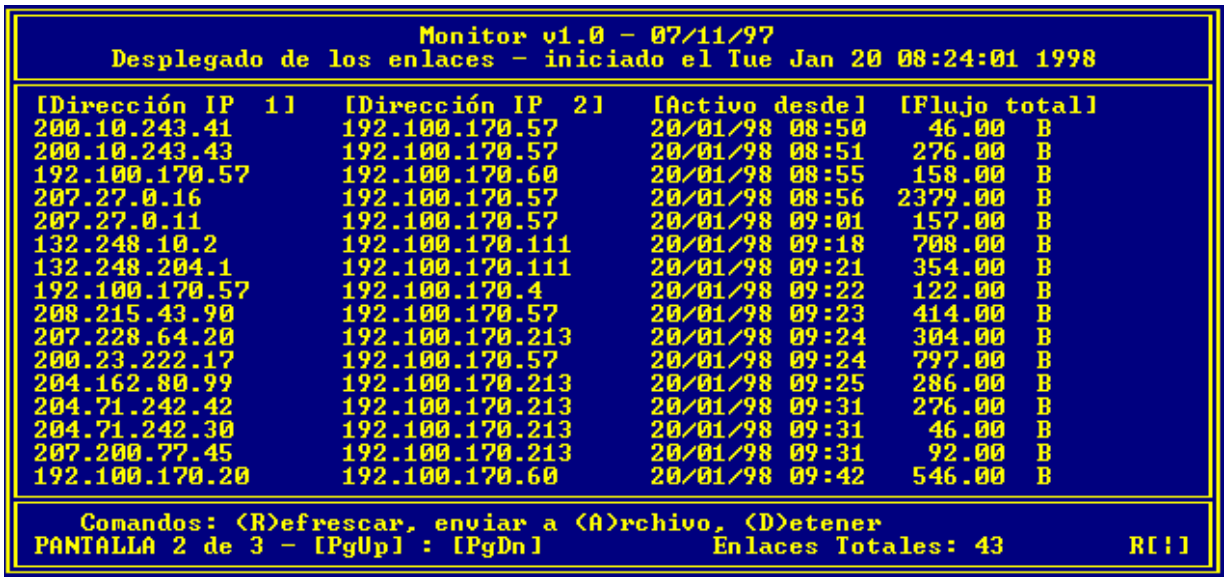


Figura A-5 Pantalla de enlaces de Monitor

En la parte superior se muestra la identificación del programa e información de interés como la fecha y hora en que se inicio la ejecución del mismo. La parte central es el espacio destinado al despliegue de los enlaces presentados de acuerdo a como fueron descubiertos.

En la parte inferior de la pantalla se encuentran los comando permitidos en esta sección que pueden ser:

Comandos: (R)efrescar, enviar a (A)rchivo, (D)etener

- (R)efrescar, permite actualizar los datos de la pantalla en un momento dado.

- (A)rchivo, permite enviar la información de las pantallas al archivo de salida.
- (D)etener, permite detener momentáneamente la adquisición de datos y regresar al menú principal.

Las teclas PgUp y PgDn permiten moverse a través de las distintas pantallas que contienen el total de enlaces descubiertos y cuya posición en un momento dado esta señalada por:

```
PANTALLA 1 de 3 - [     ] : [PgDn]
PANTALLA 2 de 3 - [PgUp] : [PgDn]
PANTALLA 3 de 3 - [PgUp] : [     ]
```

Además, se indica la cantidad de enlaces presentes en todo momento de la ejecución de Monitor

```
Enlaces Totales: 43
```

Apéndice B
Manual de usuario de Nslookup

Instalación y configuración

Por su parte, para utilizar el software de Nslookup se recomienda tener los siguientes componentes:

- Computadora IBM PC o compatible.
- Procesador 486 o superior.
- Monitor VGA a color.
- 16 MB de memoria RAM.
- Ambiente Windows 95.
- Conexión a la red.
- Ratón.

El programa utiliza un archivo de configuración denominado setup.exe, el cual al ejecutarse, instala el software de Nslookup en la unidad que se desee, creando el subdirectorio NSLOOKUP por omisión, y copia los siguientes archivos:

- Nslookup.exe archivo ejecutable.
- Nslookup.hlp archivo de ayuda.

El mismo programa de instalación creará automáticamente un acceso directo en el menú de programas en el ambiente windows.

Guía de usuario

Si el programa se instaló correctamente, podrá ejecutarse simplemente invocándolo. Al principio aparecerá una pantalla de presentación como se muestra en la figura B-1. Posteriormente aparecerá la interfaz de la aplicación, que tiene la apariencia de la figura B-2.

Es importante destacar que la aplicación no soporta resoluciones muy bajas ni muy elevadas en píxeles, por lo que se recomienda utilizar resoluciones cercanas a 800 x 600 píxeles, siendo ésta la más óptima. De usar resoluciones distintas, se distorcionarían las imágenes que posee y en la interfaz gráfica no se apreciarían completamente las gráficas.

Figura B-1 Pantalla de presentación de Nslookup

Figura B-2 Interfaz de Nslookup

Las distintas opciones podrán activarse con el ratón, y en el caso de carecer de él, se podrá utilizar la combinación de teclas Alt+letra_subrayada, como se trabaja normalmente en el ambiente de windows.

En la parte superior, aparece la barra de título, que muestra la leyenda Nslookup.

Abajo de la barra de título se presenta la barra de menú, con los siguientes comandos:

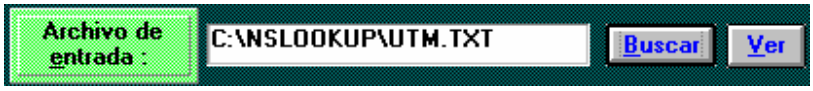
Al seleccionar el menú de Archivo, se desplegará la opción Salir, con lo que se da por terminada la sesión de Nslookup.

El menú de Opciones permitirá escoger el visualizador para los archivos. Esto es, permite seleccionar el programa a utilizar para analizar los archivos. Los visualizadores recomendados son Notepad y Wordpad.

El menú Ayuda desplegará dos opciones:

- Cómo funciona NSLOOKUP. Esta opción desplegará la ayuda del programa, la cual también podrá ser invocada al presionar la tecla F1.
- Acerca de NSLOOKUP. Mostrará la pantalla que aparece al principio con el logo de la UTM.

La interfaz, presenta dos cajas de textos precedidas por sus correspondientes etiquetas. La primera, Archivo de entrada, contendrá la ruta donde se encuentra el archivo que se analizará y que fue creado por el programa Monitor.

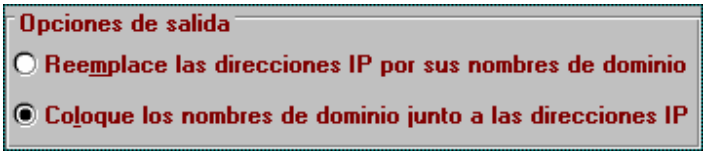


La segunda caja de texto indicará la ruta donde se ubicarán los archivos creados por Nslookup. El usuario debe colocar la ruta adecuada de dicha carpeta si es distinta a la indicada por omisión por Nslookup, además de asegurarse de que la misma carpeta ya fue creada.

Además, la caja de texto correspondiente a Archivo de entrada poseerá dos botones de comando con las leyendas Buscar y Ver. El primero botón le permitirá al usuario consultar los drivers de la PC para buscar el archivo deseado en el caso de no recordar su ubicación, y el segundo comando le permitirá visualizar el contenido del archivo seleccionado en formato de texto.

Más abajo se encuentran dos opciones que permitirán formatear la presentación de los archivos de salida:

- Reemplace las direcciones IP por sus nombres de dominio. Esta opción toma la dirección IP del archivo proporcionado por Monitor y simplemente la sustituye por su nombre de dominio cuando sea proporcionado por el Servidor DNS, en caso contrario, coloca la misma dirección IP.
- Coloque los nombres de dominio junto a las direcciones IP. Esta opción coloca juntos tanto la dirección IP como su correspondiente nombre de dominio en el archivo de salida. En caso de que el Servidor DNS no proporcione el nombre de dominio, se sustituye por la leyenda "No encontrado".



A la derecha de estas opciones se encuentran tres botones de comandos que facilitan el inicio de la ejecución de Nslookup, la presentación de los datos en forma gráfica, y la finalización de Nslookup:

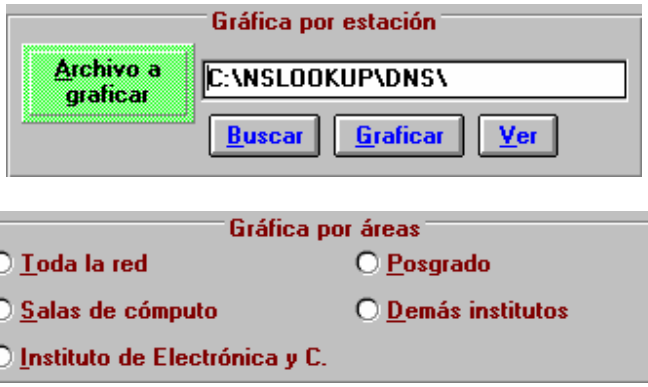
Posteriormente se presentan dos ventanas donde irán apareciendo, en la izquierda, cada una de las direcciones IP a traducir y a su derecha, su nombre de dominio. Cuando Nslookup no pueda resolver alguna dirección, mostrará un mensaje indicando que no logró resolver dicha dirección.

Dirección IP	Nombres de dominio
192.100.170.60	iec50.utm.mx

Dirección IP	Nombres de dominio
204.91.242.90	No encontrado

Por último se presentan dos indicadores del avance en el progreso de Nslookup. En el indicador de la izquierda se muestra el porcentaje de avance y cuando finalice mostrará la leyenda "- Terminado -". Por su parte, el indicador de la derecha muestra el tiempo aproximado que tardará Nslookup para resolver las direcciones contenidas en el archivo proporcionado por Monitor, y cuando termine mostrará el tiempo que tardó en ejecución.

Cuando se decida utilizar el comando Graficar, dará lugar a una nueva interfaz, donde se mostrarán las gráficas de acuerdo a dos criterios, como se muestra a continuación:



La selección gráfica por estación permitirá visualizar la actividad que presentó cada una de las estaciones involucradas en la actividad de la red. Para ello hará uso de los archivos creados por Nslookup. Nuevamente, esta selección presentará una caja de texto que contendrá la ruta de ubicación del archivo que se desea graficar, acompañada de tres comandos: Buscar, que le permitirá al usuario seleccionar el archivo deseado; Graficar, que mostrará los datos del archivo gráficamente y; Ver, que le mostrará al usuario el archivo con sus detalles en forma de texto.

El segundo criterio, gráfica por áreas, le facilitará al usuario analizar la actividad de la red por áreas, permitiéndole ver el desempeño de la red en base a las cinco divisiones marcadas:

- Toda la red.
- Salas de cómputo.
- Instituto de Electrónica y Computación.
- Posgrado.
- Demás institutos.

Se realizó esta división en base a que las salas de cómputo, el Instituto de Electrónica y Computación y Posgrado se consideran las áreas de mayor actividad en los servicios de red.

Cabe mencionar que esta segunda opción sólo estará disponible cuando se analice algún archivo proporcionado por Monitor, ya que utiliza esa información general para estas gráficas. En el caso de invocar a Nslookup e inmediatamente se decida emplear la interfaz gráfica, sólo aparecerá el criterio gráfica por estación, que permitirá estudiar gráficamente los archivos creados anteriormente.

Si se decide abandonar esta interfaz, aparecerá nuevamente la interfaz principal de Nslookup, donde se podrá analizar un nuevo archivo proporcionado por Monitor o abandonar definitivamente Nslookup.

Glosario

Ancho de banda
Técnicamente, es la diferencia en Hertz (Hz) entre la frecuencia más alta y la más baja que un canal puede transmitir. Sin embargo, típicamente se utiliza como la cantidad de datos que pueden ser enviados a través de un circuito de comunicación dado.

Banda ancha
Es un medio de transmisión capaz de soportar un amplio rango de frecuencias. Puede transmitir múltiples señales dividiendo la capacidad total del medio en diversos canales con ancho de banda independientes, donde cada canal opera sólo en un rango específico de frecuencias. La ventaja de la banda ancha es que se emplea menos cable y la desventaja es el alto costo de los equipos de conexión.

Banda base
Es un medio de transmisión a través del cual las señales digitales son enviadas sin cambio en su frecuencia. Sólo se permite un canal de comunicación en un momento dado. Ethernet es un ejemplo de red en banda base.

Circuito virtual
Abstracción básica proporcionada por un protocolo orientado como TCP. Una vez que un circuito virtual se ha creado, se establece un efecto hasta que se desactiva explícitamente.

Chequeo por Redundancia Cíclica (CRC)
Número entero calculado a partir de una secuencia de octetos utilizado para detectar errores que aparecen cuando esa secuencia de octetos se transmite de una máquina a otra. Por lo general, el hardware de red de comunicación de paquetes calcula un CRC y lo añade a un paquete cuando lo transmite. Durante la recepción, el hardware verifica el contenido del paquete recalculando el CRC y comparándolo con el valor enviado.

CSMA/CD
Característica del hardware de red que al operar permite que varias estaciones compitan por el acceso a un medio de transmisión escuchando para saber si el medio está ocupado, y mecanismo que permite al hardware detectar cuando dos estaciones intentan transmitir simultáneamente. Ethernet utiliza CSMA/CD.

Datagrama IP
Unidad básica de información autoidentificable que pasa a través de una red de redes TCP/IP. Un datagrama IP es a una red de redes lo que un paquete de hardware es a una red física.

Difusión
Sistema de entrega que proporciona la copia de un paquete dado a todas las estaciones conectadas para la difusión del paquete.

Dirección de hardware (dirección MAC o dirección física)
Dirección de bajo nivel utilizada por las redes físicas. Cada tipo de hardware de red tiene su propio esquema de direccionamiento. Por ejemplo, en una Ethernet las direcciones son de 48 bits.

Dirección IP
Dirección de 32 bits asignada a cada estación que participa en la red de redes TCP/IP. Cada dirección IP se divide en parte de red y en parte anfitrión y se representa en notación decimal con puntos (ejemplo: 192.100.170.60).

Fragmentación
Proceso de dividir un datagrama IP en pequeñas piezas cuando deben viajar a través de una red que no puede manejar el tamaño del datagrama original. Cada fragmento tienen el mismo formato que un datagrama; los campos en el encabezado IP especifican si un datagrama es un fragmento y, de ser así, el desplazamiento del fragmento con respecto al datagrama original. El software IP en el receptor final debe reensamblar los fragmentos para obtener el datagrama original.

Multidifusión
Técnica que permite que copias de un solo paquete se transfieran a un subconjunto seleccionado de todos los posibles destinos. Algunos tipos de hardware (como Ethernet) soportan la multidifusión y permiten que una interfaz de red pertenezca a uno o más grupos de multidifusión.

Octeto
El término octeto es usado en la documentación de Internet para representar secciones de 8 bits. No se utiliza el término byte debido a que TCP/IP es soportado por algunas computadoras que tienen tamaño de bytes distintos de 8 bits.

Organización Internacional de Estándares (ISO)
Organización no comercial y voluntaria, fundada en 1946, responsable de discutir, proponer y especificar estándares en muchas áreas, incluyendo computación y comunicaciones.

Packet driver
Es una pieza de software que proporciona una interfaz entre una aplicación de red y una tarjeta de red.

Paquete
Es la unidad de datos enviados a través de una red. En términos genéricos, un paquete es usado para describir la unidad de datos en todos los niveles de la pila de protocolos, pero es más correcto usarlo para describir unidades de datos de aplicación.

Pila de protocolos
Conjunto de protocolos por capas que trabajan juntos para proveer una combinación de funciones de red.

Protocolo
Es una descripción formal del formato de los mensajes y las reglas que dos computadoras deben seguir para intercambiar esos mensajes. Los protocolos pueden describir detalles de bajo nivel de las interfaces de máquina a máquina (el orden en que los bits de un octeto son enviados a través de un cable) o el intercambio entre programas de aplicación (la forma en que un programa transfiere un archivo a través de una red de redes).

Reconocimiento o acuse de recibo (ACK)
Es la respuesta enviada por un receptor para indicar que la información que le fue enviada llegó sin errores. Se puede implementar en cualquier nivel, incluyendo el nivel físico, en el de enlace o en niveles elevados.

Reensamblado
Proceso IP de unir todos los fragmentos de un datagrama IP y crear una copia del datagrama original. El destino final lleva a cabo esto.

Ruta
Es la trayectoria que el tráfico de red toma desde su fuente hasta su destino.

Ruteador (router)
Computadora dedicada, de propósito especial, que se conecta a dos o más redes y envía paquetes de una red a otra. En particular, un ruteador IP envía datagramas IP entre las redes a las que está conectado. Un ruteador utiliza las direcciones de destino en un datagrama para decidir el próximo salto al que enviará el datagrama.

Servicio de Nombres de Dominio (DNS)
Sistema de base de datos distribuida en línea y utilizado para transformar nombres de máquinas en direcciones IP y viceversa.

Servicio sin conexión
Característica del servicio de entrega de paquetes ofrecida por la mayor parte del hardware y por el Protocolo de Internet (IP). Este servicio trata a cada paquete o datagrama como entidades separadas que pueden tomar diferentes rutas para llegar a su destino.

Socket
Abstracción proporcionada por el sistema operativo UNIX que permite a un programa de aplicación, accesar a los protocolos TCP/IP.

Trama
Término que deriva de los protocolos orientados a carácter que añaden caracteres especiales de comienzo de trama y de fin de trama cuando transmiten paquetes.

Winsock
Es un programa que conforma un conjunto de estándares llamados Windows Socket API. Winsock implementa software de Windows con una pila de protocolos TCP/IP. En otras palabras, winsock permite a un programa que utiliza sockets llamar a Windows para correr.

Bibliografía

Arnett Flint, Mathew; "INSIDE TCP/IP", 2ª Ed., New Riders 1995.

Black, U.; "Redes de Computadoras: Protocolos, Normas e Interfaces", Macrobit 1990.

Catalyst Software; "An Introduction To TCP/IP Programming With SocketWrench/VB™", 1995.

Comer E., Douglas; "Internetworking With TCP/IP Vol I: Principles, Protocols, and Arquitecture", 2ª Ed., Prentice-Hall 1991.

Comer E., Douglas; "Internetworking With TCP/IP Vol II: Design, Implementation, and Internals", Prentice-Hall 1991.

Comer E., Douglas; "Internetworking With TCP/IP Vol III: Client-Server Programming And Applications BSD Socket Version", Prentice-Hall 1993.

Comer E., Douglas; "REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IP Principios básicos, protocolos y arquitectura", 3ª Ed., Prentice-Hall 1996.

Farmer, W. D., and Newhall, E. E.; "An Experimental Distributed Switching System to Handle Bursty Computer Traffic, Proceedings of the ACM Sysmposium Problems on the Optimization of Data Communications Systems", October 1969.

FTP Software, Inc.; "PC/TCP Versión 1.11 Packet Driver Specification", June 1994.

IEEE Standards for Local and Metropolitan Area Networks; "ANSI/IEEE Std. 802.3 CSMA/CD", 1990.

Krol, Ed; "CONECTATE AL MUNDO DE INTERNET", McGraw-Hill 1994.

Mejía Olvera, Marcelo; "Conceptos generales sobre redes locales, Soluciones Avanzadas", Abril-Mayo 1993.

Minoli, D.; "Telecommunications Technology Handbook", Artech House, 1991.

National Instruments; "Instrumentation REFERENCE AND CATALOGUE", 1994.

Scolofsky T, and Kale C.; "RFC 1180: A TCP/IP Tutorial", January 1991.

Soto Sumuano Leonardo; "Introducción a redes de computadoras", Soluciones Avanzadas, Enero-Febrero 1993.

Stallings, William; "Data and Computer Communications", 4ª Ed., Macmillan 1994.

Stremler G., Ferrel; "SISTEMAS DE COMUNICACIÓN", Alfaomega 1989.

Tanenbaum S., Andrew; "REDES DE ORDENADORES", 2ª Ed., Prentice-Hall 1994.

Universidad Politécnica de Madrid; "PROGRAMA DE POSTGRADO EN SISTEMAS Y REDES DE COMUNICACIONES: REDES LOCALES Y METROPOLITANAS", Departamento de Ingeniería Telemática.

3Com; "EtherLink® III Parallel Tasking™ ISA, EISA, Micro Channel®, and PCMCIA Adapter Driver Technical Reference", 1994.