UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
A R A G O N

"EL CONJUNTO DE PROTOCOLOS DE COMUNICACIONES TCP/IP Y SU FUNCION EN LA INTERCONEXION DE REDES DE AREA LOCAL ETHERNET"

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICO

P R E S E N T A:
GERARDO OSORNO SAAVEDRA

A S E S O R:
ING. NARCISO ACEVEDO HERNANDEZ

Acompañada de un diskette 3 1/2

E N E P A R A G O N
UNAM

MEXICO, D. F. MAYO 1996

TESIS CON
FALLA DE ORIGEN

Agradecimientos.

A Dios por conducirme en el camino correcto.

A mis padres que me dieron todo su apoyo, comprensión y paciencia durante estos años de esfuerzo.

Cirina Saavedra Ibañez.
Fidel Osorno Cruz.

A mis hermanos por su ayuda y como un ejemplo de lo que se puede lograr.

Angel Osorno Saavedra.
Mauricio Osorno Saavedra.
Luis Osorno Saavedra.
Sonia Osorno Saavedra.

A mi tía María Osorno Cruz que siempre ha creido em mí.

A mi asesor de tesis:
Ing. Narciso Acevedo Rodiguez.

A mis amigos que me apoyaron y ayudaron para lograr esta tesis:

Ing. Eduardo Contreras Zepeda
M. en C. Guillermo Nava Peréz

A mis compañeros y amigos:

Rodolfo Gallardo Luviano.
Jorge López López.
Marcela Palacios Rios.
Adrián Macías Ortíz.
Jorge Angulo Sagrero.

A la Escuela Nacional de Estudios Profesionales Aragón, a mis profesores y muy especialmente y como recuerdo a:

Ing. Juan Méndez Moreno.
Ing. Juan Antonio Galán Carretero.

TESIS

COMPLETA

INDICE

PROLOGO

Para comprender los alcances del presente trabajo es necesario mencionar las etapas de evolución de la comunicación. Antes de 1960, la principal meta era, "¿Cómo puedo transmitir bits a través de un medio de comunicación eficiente y confiable?". Los resultados entregaron el desarrollo de la teoría de la información, el teorema del muestreo, y el procesamiento de señales. A mediados de los 60s surgió la conmutación de paquetes y ahora el objetivo era "¿Cómo puedo transmitir paquetes a través de un medio de comunicación eficiente y confiable?" Los resultados entregaron el desarrollo de tecnologías de conmutación de paquetes, redes de área local y análisis del comportamiento de una red con la carga. A mediados de los 70s y con la diversa variedad de redes, vendedores de equipo y protocolos existentes surgió la pregunta "¿Cómo puedo comunicar a las diferentes redes y proporcionar servicios entre los equipos conectados a las mismas? Una de las respuestas fué el conjunto de protocolos TCP/IP, actualmente la forma más utilizada en el mundo. Cabe mencionar que en México a tenido gran aceptación desde principios de los años 90s y actualmente tiene una tendencia al crecimiento de implantación en instituciones de educación, bancarias, comerciales y de servicios.

El presente trabajo esta dividido en 5 partes descritas a continuación:

En la primera parte (capítulo 1), se tocarán los elementos teóricos sobre el modelo de 7 capas de OSI . Se describirán las funciones de cada una de las capas del modelo de OSI y se explicarán los principales conceptos de comunicación de datos.

En la segunda parte (capítulo 2), se definirá lo que es una red, los diferentes tipos de redes y las topologías de red existentes. Se estudiarán los estándares de redes de área local Ethernet y de área amplia, los elementos que constituyen las redes de área local Ethernet como lo son los concentradores, servidores de archivos, estaciones de trabajo, servidores de terminales, tarjetas de red, transceivers, cableado (par trenzado, cable coaxial etc), los elementos que constituyen una red de área amplia como lo son los módems, los multiplexores y

los diferentes medios de transmisión como las líneas telefónicas y los enlaces digitales E0 de 64 kbit/seg y E1 de 2048 Kbit/seg.

En la tercera parte (capítulo 3) se describen los más importantes dispositivos para interconectar redes de área local como lo son : los repetidores (actuando en la capa 1 de modelo de OSI), los puentes(actuando en las capas 1 y 2 del modelo de OSI), los enrutadores (actuando en las capas 1,2 y 3 del modelo de OSI) y los Gateways (actuando en las capas 4-7 del modelo de OSI). Se mostrarán algunas formas de interconectar estos equipos a las redes de área local y entre sí, con lo que se logra la interconexión de redes.

En la cuarta parte (capítulo 4) se estudiarán los protocolos TCP/IP, su función en la interconexión de redes de área local, las aplicaciones (PING, TELNET Y FTP) que ofrecen para la interconectividad de redes con diferentes sistemas operativos como lo son el sistema operativo DOS y el sistema operativo UNIX. Se estudiará también el esquema de direccionamiento de las diferentes redes interconectadas de acuerdo a TCP/IP.

En la quinta parte (capítulo 5), se desarrollará un programa en lenguaje C para el análisis e interpretación de los resultados obtenidos del monitoreo de una red Ethernet utilizando protocolos TCP/IP. El código del programa se entregará en un disco para PC de 3 1/2.

INTRODUCCION

En la actualidad existen un conjunto de diferentes tipos de redes de computadoras de diferentes tecnologías, diferentes sistemas operativos y diferentes interfaces de hardware. La mayoría de estas redes no cumplen con las especificaciones del modelo OSI y peor aún se siguen fabricando nuevos equipos con tecnologías propias.

Es por lo tanto necesario una forma de poder interconectar todas estas redes diferentes de alguna manera.

El conjunto de protocolos TCP/IP surge como un esfuerzo del departamento de la Defensa Nacional de los Estados Unidos. Dicho esfuerzo iba encaminado a un objetivo principal: Crear un protocolo o un conjunto de protocolos que no estuviera atado a ningún medio físico de transmisión de datos, ni a ningún sistema operativo ni a un hardware en particular pero que, sin embargo, fuera sencillo de implementar para enlazar equipos diversos (desde una PC hasta un mainframe, pasando por todo tipo de minicomputadoras).

Después de ser estándar militar, en la década de los 80's surge como un estándar de mercado. De ser un producto de la defensa y de ahí popularizarse a través de la red ARPANET a multitud de universidades de Estados Unidos, TCP/IP es hoy en día, la solución más interoperable entre cualquier tipo de computadora.

La presente tesis tiene como objetivo presentar un análisis del conjunto de los protocolos TCP/IP. Mostrar como pueden ser usados para comunicarse a través

de un conjunto de redes interconectadas. Señalar como estos protocolos son convenientes para comunicación entre redes de área local y de área amplia.

Se mostrará que aunque los protocolos TCP/IP surgen antes que el modelo de OSI, cumplen con la mayoría de las especificaciones de capa 3 y capa 4 de este modelo. Debido a lo anterior es que este conjunto de protocolos es en la actualidad el más popularmente usado para la interconexión de redes.

Las características que distinguen a TCP/IP son:

Independencia de tecnología de red. Mientras TCP/IP está basado en una tecnología de conmutación de paquetes convencional, es independiente de cualquier vendedor de hardware particular. TCP/IP define una unidad de transmisión de datos llamada datagrama y especifica como transmitir datagramas en una red particular.

Interconexión Universal. TCP/IP permite a dos computadoras en una red, comunicarse a través del uso de una dirección IP en cada máquina. Cada datagrama conduce la dirección de la fuente y del destino. Los dispositivos que interconectan las redes usan la dirección destino del datagrama para tomar decisiones de enrutamiento.

Reconocimientos extremo a extremo. Los protocolos TCP/IP proporcionan reconocimientos entre la fuente y el destino final en lugar de entre máquinas sucesivas en la trayectoria, aún cuando las dos máquinas no estén conectadas a la misma red física.

Estándares de protocolos de aplicación. Además de los servicios de nivel de transporte, los protocolos TCP/IP incluyen estándares para muchas aplicaciones, por ejemplo correo electrónico, transferencia de archivos, terminales virtuales remotas y administración de red.

CAPITULO 1
CONSIDERACIONES TEORICAS

1.1 Consideraciones generales.

En este capítulo se describen el modelo de interconexión de sistemas abiertos OSI y algunos conceptos y protocolos de comunicación de datos como base teórica para la comprensión de los protocolos TCP/IP.

1.2 El modelo de referencia OSI de 7 capas.

La ISO (Organización de Estándares Internacionales) desarrollo el modelo básico de referencia de interconexión de sistemas abiertos (OSI) para definir las interfaces y protocolos de las redes en una estructura de capas. Este modelo fijo como metas lograr la comunicación entre equipos construidos por diferentes manufacturas y hacer a las aplicaciones independientes del hardware en donde operan. Se debe aclarar que es sólo un modelo y que sirve como una organización de estándares que pueden ser implementados por diferentes protocolos.

El modelo de referencia OSI consiste de 7 capas y se muestra en la figura 1.1:

a) Capa Física (capa 1).
b) Capa de Enlace de datos (capa 2).
c) Capa de Red (capa 3).
d) Capa de Transporte (capa 4).
e) Capa de Sesión (capa 5).
f) Capa de Presentación (capa 6).
g) Capa de Aplicación (capa 7).

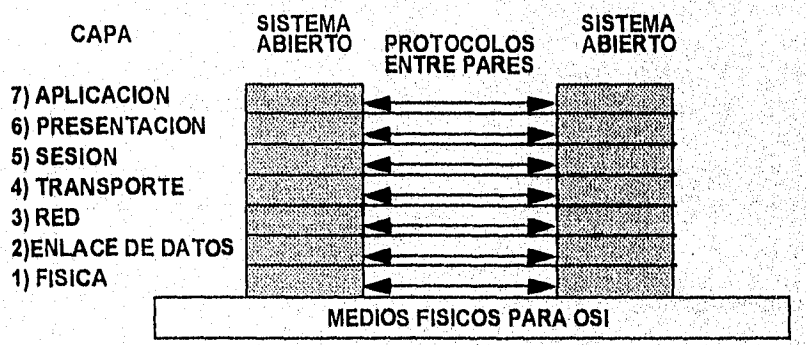


Figura 1.1
Modelo OSI de 7 capas.

No todos los sistemas abiertos comprenden el origen inicial o el destino final de los datos. Cuando los medios físicos de OSI no enlazan directamente a todos los sistemas abiertos, algunos sistemas abiertos actúan solamente como retransmisores, pasando los datos a otros sistemas abiertos. Las funciones y protocolos que permiten la retransmisión de los datos se efectúan en tal caso en las capas inferiores como se ve en la figura 1.2.

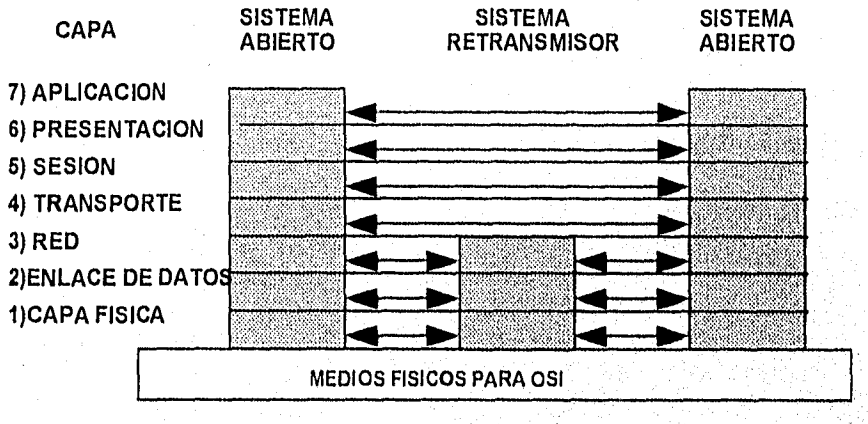


Figura 1.2
Comunicación mediante sistemas abiertos retransmisores.

La ISO define el modelo en el estándar ISO-7498 y el CCITT lo adoptó en la recomendación X.200 y la comunicación entre capas en la recomendación X.210.

1.2.1 Metas del modelo OSI.

- Proporciona normas para la comunicación entre sistemas.
- Elimina cualquier impedimento técnico para lograr la comunicación entre sistemas.
- Elimina todo lo relacionado con el funcionamiento interno de los sistemas.
- Define los puntos de interconexión para el intercambio de información entre sistemas.
- Limita las opciones con el objeto de incrementar la habilidad para comunicarse sin conversiones costosas y adaptaciones entre equipos.

1.2.2 Sistemas abiertos.

Los sistemas abiertos son aquellos que emplean los estándares asociados con el modelo de referencia para la transferencia de información. A la interconexión de éstos se le denomina interconexión de sistemas abiertos.

Un sistema real es un conjunto de una o varias computadoras, el material lógico asociado, periféricos, terminales, operadores humanos, medios de transferencia de información, etcétera; que forman un todo capaz de efectuar procesamiento y/o transferencia de información.

Un sistema real abierto es un sistema real que se ajusta a los requisitos de OSI en su comunicación con otros sistemas reales.

1.2.3 Definiciones básicas del modelo OSI.

Capa (N).

Subdivisión de la arquitectura de OSI constituida por subsistemas del mismo rango (N) como se muestra en la figura 1.3.

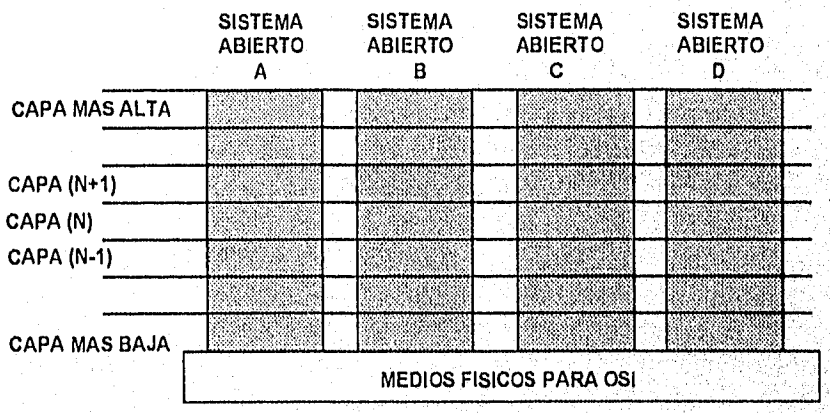


Figura 1.3
Subdivisión del modelo OSI en capas.

Subsistema (N).

Elemento de una división jerárquica de un sistema abierto que sólo interactua directamente con elementos de la división superior siguiente o de la división inferior siguiente.

Entidad (N).

Elemento activo dentro de un subsistema (N) que es capaz de enviar, procesar o recibir información. Por ejemplo un paquete de transferencia de archivos, un sistema de administración de base de datos o una terminal.

Servicio (N).

Capacidad de la capa (N) y de las capas inferiores que se ofrece a las entidades (N+1) en la frontera entre la capa (N) y la capa (N+1).

Función (N).

Parte de la actividad de las entidades (N).

Punto de acceso al servicio SAP(N).

Punto en el cual una entidad (N) ofrece servicios a una entidad (N+1) como se puede apreciar en la figura 1.4.

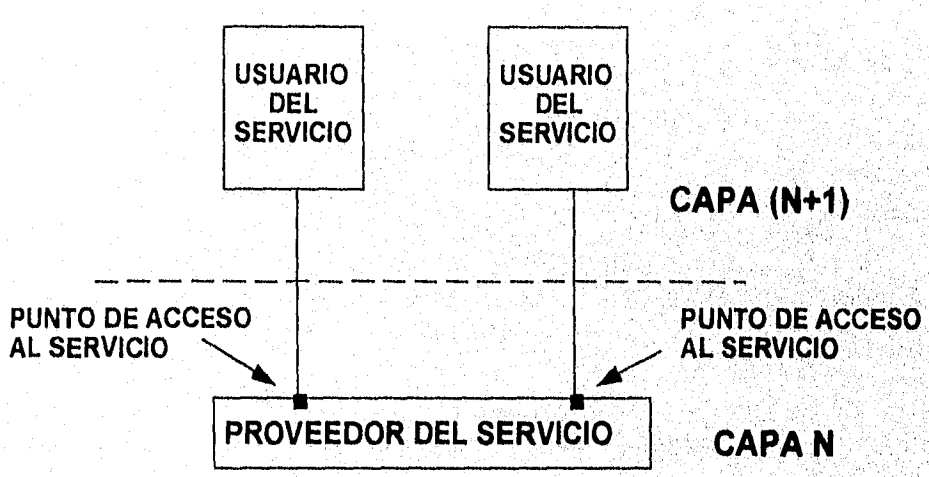


Figura 1.4
Localización de los puntos de acceso al servicio.

Facilidad (N).

Parte de un servicio (N).

Protocolo (N).

Conjunto de reglas y formatos que determina el comportamiento de comunicación en las entidades (N) en la realización de funciones (N).

Con excepción de la capa más alta, cada capa (N) proporciona servicios (N) a las entidades (N+1) de la capa (N+1). Se supone que la capa (N+1) representa todas la utilizaciones posibles de los servicios que proporcionan las capas más bajas.

Cada servicio proporcionado por la capa (N) puede ser caracterizado mediante la elección de una o varias facilidades (N) que determinen los atributos de ese servicio. Cuando una sola entidad (N) no puede dar curso por si misma a todo un servicio pedido por una entidad (N+1), debe solicitar la colaboración de otras entidades (N) para que le ayuden a atender completamente la petición de servicio. Con el objeto de cooperar, las entidades (N) de cualquier capa, excepto las de la capa más baja, se comunican por medio de un conjunto de servicios proporcionados por la capa (N-1). Las entidades de la capa más baja se comunican directamente a través de los medios físicos que las conectan (Ver figura 1.5).

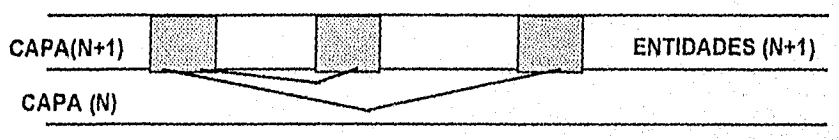


Figura 1.5
Entidades (N+1) que se comunican a través de la capa (N).

Los servicios de una capa (N) se proporcionan a la capa (N+1) utilizando las funciones (N) realizadas dentro de la capa (N) y, de ser necesario los servicios disponibles en la capa (N-1).

La entidad (N) puede proporcionar los servicios a una o varias entidades (N+1) y utilizar los servicios de una o varias entidades (N-1). Un punto de acceso al servicio (N) es el punto en el cual un par de entidades situadas en capas adyacentes utilizan o proporcionan servicios.

1.2.4 Comunicación entre entidades pares.

A las entidades que forman las capas N correspondientes en máquinas diferentes se les denomina entidades pares. Para la comunicación entre estas entidades son necesarias las siguientes definiciones:

Conexión (N).

Asociación establecida por la capa (N) entre dos o más entidades (N+1) para la transferencia de datos.

Punto extremo de conexión.

Terminación en un extremo de la conexión (N) dentro de un punto de acceso al servicio (N).

Para que pueda llevarse a cabo el intercambio de información entre dos o más entidades (N+1), es preciso establecer una asociación entre ellas en la capa (N) utilizando un protocolo (N).

Esta asociación se llama conexión (N). La capa (N) proporciona conexiones (N) entre dos o más puntos de acceso al servicio (N). La terminación de una conexión (N) en un punto de acceso al servicio (N) se llama punto extremo de conexión (N). Una conexión que tiene más de dos puntos terminales de conexión se llama conexión de puntos extremos múltiples (Ver figura 1.6).

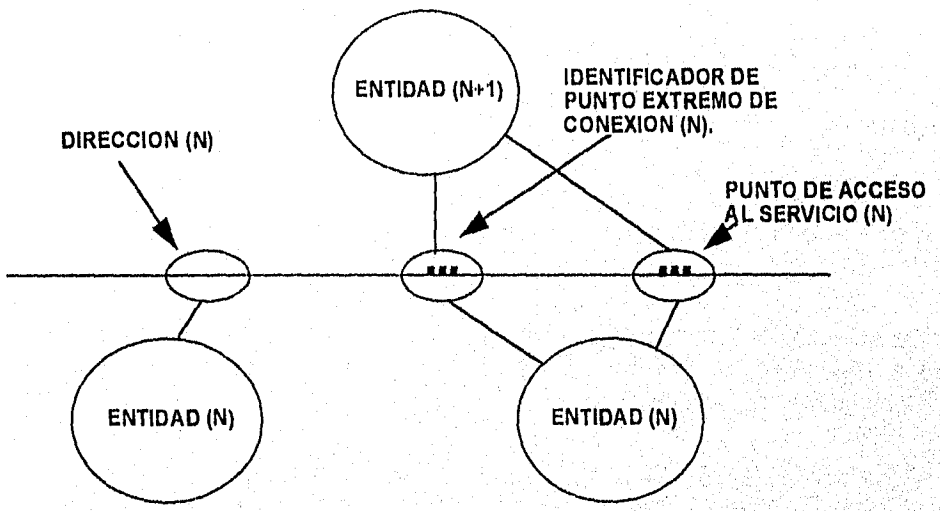


Figura 1.6
Entidades, puntos de acceso al servicio e identificadores.

1.2.5 Comunicación entre capas adyacentes.

Para lograr la comunicación entre capas adyacentes se utilizan cuatro transacciones llamadas "primitivas", las cuales son intercambiadas a través de puntos de acceso al servicio.

Una primitiva o primitiva de servicio se define como una interacción abstracta que define el intercambio lógico de información y control. Esta interacción se realiza entre un usuario y un proveedor de servicio (capas adyacentes).

Los tipos de primitivas son las siguientes:

- Request (Solicitud). Primitiva emitida por el usuario del servicio para solicitar una función.

- Indication (Indicación). Primitiva emitida por el proveedor del servicio para solicitar un procedimiento o para indicar que el usuario del servicio ha solicitado un procedimiento en el punto de acceso al servicio par.

- Response (Respuesta). Primitiva emitida por el usuario del servicio para completar una función previamente solicitada mediante una indicación en ese punto de acceso al servicio.

- Confirm (Confirmación). Primitiva emitida por el proveedor del servicio para completar una función previamente solicitada mediante una petición en ese punto de acceso al servicio.

Como se muestra en la figura 1.7, una aplicación de usuario o una terminal solicita una función al proveedor del servicio emitiendo una petición a la capa inferior. Esta petición de servicio es confirmada por el proveedor del servicio contestando con una confirmación. Si el servicio va a proporcionar una función a otro usuario (en este caso el usuario B), el proveedor del servicio deberá emitir una indicación a B, después de que B es solicitado para proporcionar una respuesta. Considerando que el proveedor del servicio es una capa, ésta conecta a los usuario A y B a través de los puntos de acceso al servicio de la capa. El punto de acceso al servicio contiene la dirección de la función de servicio específica.

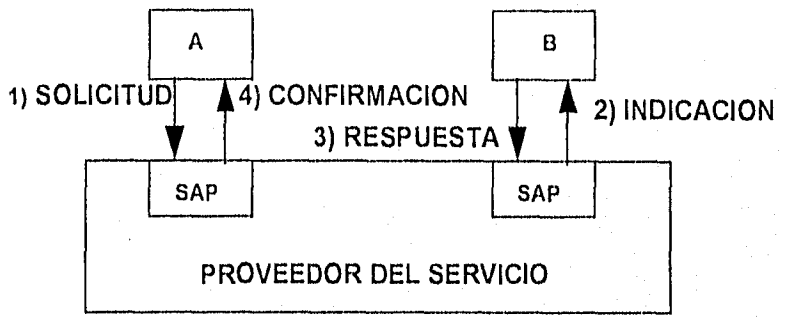
La figura 1.8 proporciona otra vista del proceso. El proveedor del servicio está a la mitad del diagrama, teniendo a los usuarios A y B a cada lado. La petición es enviada al proveedor del servicio, el cual a la vez envía al usuario B una indicación que es transmitida a través del proveedor del servicio como una confirmación al usuario A.

Cabe recordar que el proveedor del servicio puede ser una capa, una función o una entidad dentro de una capa, y el proceso establece un medio de comunicación común entre las capas.

El nombre de cada primitiva comprende 3 elementos:

a) Una inicial o iniciales que especifica la capa.
b) Un nombre que especifica el tipo de servicio.

c) Un nombre que especifica el tipo de primitiva.



SAP=PUNTO DE ACCESO AL SERVICIO.

Figura 1.7

Primitivas entre capas adyacentes.

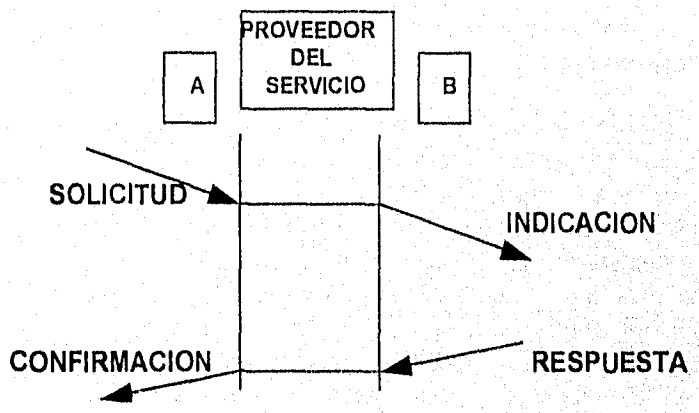


Figura 1.8
Otra vista del proceso de primitivas.

1.2.6 Transmisión de datos en el modelo OSI.

En la figura se muestra un ejemplo de cómo pueden transmitirse los datos mediante el empleo del modelo OSI. El proceso emisor tiene algunos datos que desea enviar al proceso receptor. Este entrega los datos a la capa de aplicación, quien añade un encabezado de aplicación AH (sí existe), a la parte delantera de los mismos y entrega el mensaje resultante a la capa de presentación.

La capa de presentación transforma este mensaje de diversas formas, y tiene la posibilidad de incluir una cabecera en la parte frontal, dando el resultado a la

capa de sesión. Este proceso se sigue repitiendo hasta que los datos alcanzan la capa física, lugar en donde efectivamente se transmiten a la máquina receptora. En la otra máquina, se van quitando uno a otro los encabezados, a medida que los datos se transmiten a las capas superiores, hasta que finalmente llegan al proceso receptor.

La idea fundamental a lo largo de este proceso, es que si bien la transmisión efectiva de datos es vertical, como se muestra en la figura 1.9, cada una de las capas está programada como si fuera una transmisión horizontal.

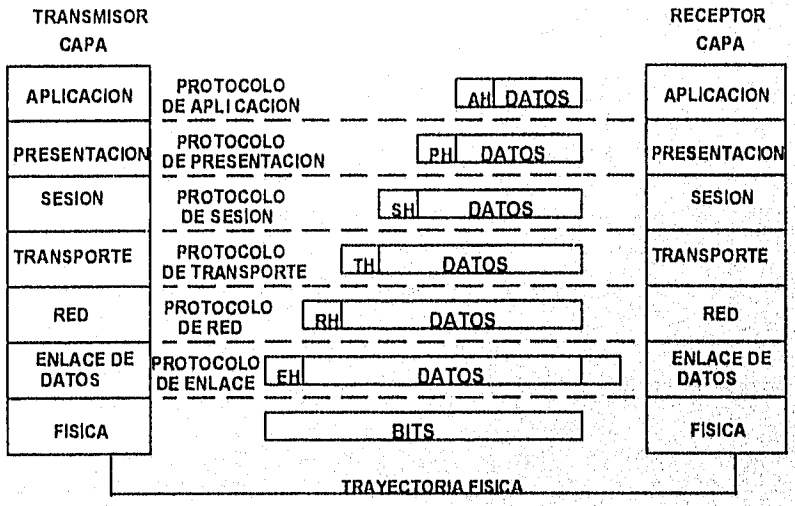


Figura 1.9
Transmisión de datos en el modelo OSI.

1.3 Funciones de cada capa del modelo de OSI.

1.3.1 Capa física (CAPA 1).

- Se encarga de las especificaciones mecánicas, eléctricas y procedimientos de funcionamiento de las interfaces de los equipos a conectar (tipos de conector, nivel de las señales y asignación de los pines en el conector).
- Es responsable de la transmisión de bits a través de un particular medio de transmisión físico.
- Maneja voltajes y pulsos eléctricos.
- Establece las velocidades de transmisión.
- Designa cables conectores y componentes.
- Realiza funciones de alineación de trama y temporización.

1.3.2 Capa de enlace (CAPA 2).

- Proporciona una interface de servicio bien definida a la capa de red, para transmisión de datos en unidades de información llamadas tramas, de la máquina origen a la máquina destino.
- Determina como los bits que se enviarán en la capa física están agrupados en tramas.
- Se ocupa de los errores de transmisión.
- Cuenta con mecanismos de retransmisión de tramas para recuperar las tramas perdidas, duplicadas y erróneas.
- Controla el flujo de tramas de modo que los receptores lentos no se vean desbordados por los transmisores rápidos.
- Protocolos de ventana deslizante.
- Retransmisión selectiva.
- Retransmisión no selectiva (GoBack-N).

1.3.2.1 Servicios proporcionados a la capa de red.

a) Servicio sin conexión y sin reconocimiento.

La máquina origen transmite tramas independientes a la máquina destino, sin que ésta proporcione un reconocimiento (Ver figura 1.10).

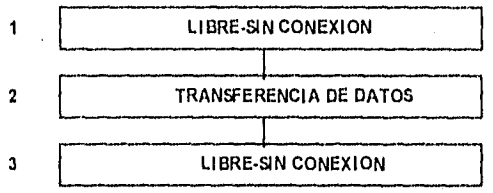


Figura 1.10
Servicio sin conexión.

b) Servicio sin conexión y con reconocimiento.

La máquina origen transmite tramas independientes a la máquina destino, pero cada una de las tramas se reconoce en forma individual (Ver figura 1.11).

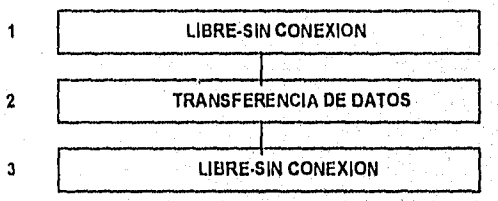


Figura 1.11
Servicio sin conexión y con reconocimiento.

c) Servicio orientado a conexión.

Con este tipo de servicio, las máquinas origen y destino establecen una conexión antes de transmitir algún dato. Cada una de las tramas transmitidas se numera, y la capa de enlace garantiza que cada trama transmitida sea recibida. En este servicio se tienen tres fases distintas. En la primera fase la conexión se establece cuando los dos lados han inicializado las variables y los contadores

necesarios para mantener el seguimiento, de qué tramas se han recibido y cuáles no. En la segunda fase una o más tramas se transmiten. En la tercera fase, la conexión se libera dejando libres a las variables, a las memorias temporales, así como a los otros recursos que se emplean para mantener la conexión (Ver figura 1.12).

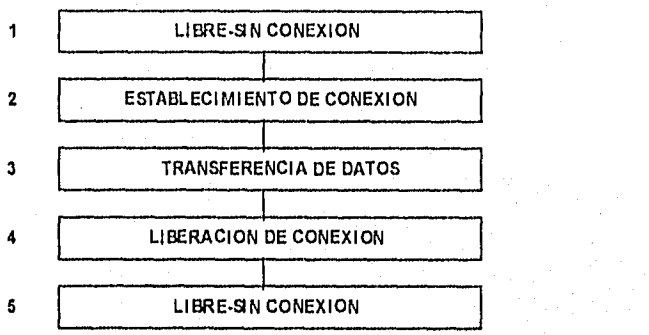


Figura 1.12
Servicio orientado a conexión.

1.3.2.2 Formas de agrupar los bits en tramas.

a) Cuenta de caracteres.

Este método utiliza un campo en la cabecera para especificar el número de caracteres de la trama.

b) Caracteres de inicio y final, con inserción de carácter.

Cada una de las tramas comienza con la secuencia de caracteres ASCII DLE STX (escape de enlace, inicio de texto) y termina con la secuencia de caracteres ASCII DLE ETX (escape de enlace, fin de Texto). Con este método se tiene un problema serio en el momento en que los datos son binarios. Puede suceder con facilidad que los caracteres para las secuencias DLE STX o DLE ETX ocurran en los datos, con lo cual se llegaría a interferir con el proceso de entramado. Una manera de resolver el problema es hacer que la capa de enlace del extremo emisor inserte un carácter ASCII DLE exactamente antes de que ocurra un DLE "accidental" en el flujo de salida de los datos. La capa de enlace en el extremo receptor elimina el carácter DLE antes de que se entreguen los datos en la capa de red. A esta técnica se le conoce como inserción de carácter.

c) Método de banderas de inicio y final con inserción de bit.

Esta técnica permite que las tramas contengan un número arbitrario de bits, y permite un número arbitrario de bits por carácter. Cada trama inicia y termina con un patrón de bits especial, por ejemplo, 01111110. Siempre que la capa de enlace del extremo transmisor encuentre cinco unos consecutivos en los datos, automáticamente insertará un bit con valor 0 en el flujo de salida de datos. Cuando el receptor ve cinco bits de entrada con valor de 1, seguidos por un bit con valor 0, elimina el bit 0.

d) Violaciones de código en la capa física.

Por ejemplo la codificación tipo Manchester codifica cada bit 1 con un par alto-bajo y cada bit 0 con un par bajo-alto. Las combinaciones alto-alto y bajo-bajo no se utilizan para los datos. Sin embargo, algunos protocolos utilizan secuencias inválidas como éstas para el encapsulado de trama.

1.3.2.3 Código de redundancia cíclica.

Existen 2 técnicas relacionadas con el manejo de errores: códigos correctores de errores y códigos detectores de errores.
En la práctica se utiliza un código detector de error conocido como código de redundancia cíclica (CRC).

Cuando se emplea el método del código de redundancia cíclica, el emisor y el receptor deberán estar de acuerdo respecto a un polinomio generador G(x), en forma anticipada. Los bits de orden superior e inferior del polinomio generador deben ser 1. Para calcular el código de redundancia de alguna trama con m bits, que corresponderá al polinomio D(x), la trama deberá ser más grande que el polinomio generador. La idea básica consiste en incluir un código de redundancia al final de la trama, de tal manera que el polinomio representado por la trama con el código de redundancia llamado T(x) sea divisible por el polinomio G(x). Cuando el receptor recibe la trama T(x), intenta dividirla entre G(x). Si existe un residuo habrá ocurrido algún error de transmisión.

El algoritmo para calcular la redundancia es el siguiente:

1) Sea r el grado de G(x). Agregar r bits con valor de cero de menor valor significativo de la trama, de tal manera que ahora contenga m+r bits, y corresponda al polinomio F(x).

2) Dividir la serie de bits correspondientes a F(x) entre la serie de bits correspondientes a G(x), empleando la división en módulo 2, es decir F(x)/G(x).

3) Restar el residuo obtenido de la división anterior a la serie de bits correspondientes a F(x), empleando la resta en módulo 2. El resultado es la trama lista para transmitir T(x).

4) En el lado receptor se realiza la división T(x)/G(x), y si la trama está libre de error, el residuo debe ser cero.

Ejemplo de cálculo de código de redundancia cíclica.

Trama de datos D(x) 1101011011 10 bits=m bits

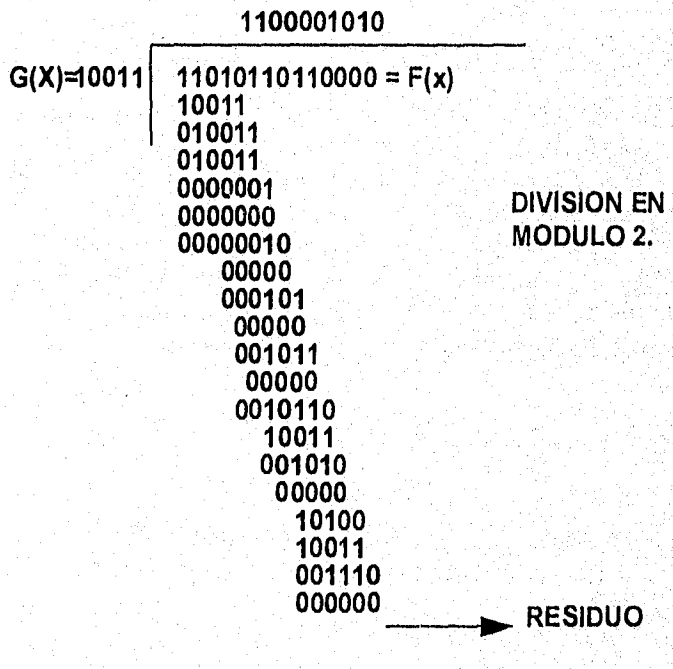
Polinomio Generador 10011 . Grado del polinomio 4 (r=4 bits).

Primer paso:

F(x)=m+r= 11010110110000

Segundo Paso:

F(x)/G(x) en módulo 2.



Tercer paso:

Realizar la resta F(x)- residuo en módulo 2.

11010110110000 = F(X)
- 1110 = RESIDUO

11010110111110= T(x) Trama a transmitir

1.3.2.4 Ventanas deslizantes (Continuos ARQ).

Esta técnica es nombrada así por que a una estación le es permitido solicitar automáticamente una retransmisión a otras estaciones en caso de detección de error. Esta técnica usa transmisión full dúplex.

Los dispositivos continuos ARQ usan el concepto de ventanas de tranmisión y recepción. Una ventana es establecida en cada enlace para proporcionar una reserva de recursos en ambos DTE's. En muchos sistemas, la ventana proporciona espacio de buffer y reglas de secuenciamiento. Durante el inicio de una sesión de enlace entre los DTE's una ventana es establecida. Si un DTE A y un DTE B quieren comunicarse, el DTE A reserva una ventana para B y B reserva una ventana para A. El concepto de ventanas es necesario para protocolos full dúplex por que ellos mantienen un flujo de tramas continuo sin los reconocimientos de los protocolos de parada y espera. Como consecuencia el receptor debe tener una asignación de espacio para manejar el tráfico entrante continuo.

Las ventanas en el lado transmisor y el lado receptor son controladas por variables de estado, que en realidad es otro nombre para un contador. El lado transmisor mantiene una variable de estado de envío V[S], **éste es el número de secuencia de la siguiente trama a ser transmitida.** El lado receptor mantiene una variable de estado de recepción V[R], **que contiene un número que se espera esté contenido en el número de secuencia de la siguiente trama**. V[S] es incrementado con cada trama transmitida y colocado en el campo de secuencia de envío de la trama. Cuando llega la trama al lado receptor se checan los errores de transmisión, además de checarse el número de secuencia de envío con el V[R]. Si la trama es aceptada, el receptor incrementa V[R] en uno, coloca este número en un campo de secuencia de recepción en una trama de reconocimiento, y envía la trama al lado transmisor para completar la transmisión.

Si el número de secuencia de envío de la trama no es igual al V[R] o se detecta un error, después de transcurrido un tiempo, un NACK (no reconocimiento con el número de secuencia de V[R]) es enviado al transmisor. Muchos protocolos

llaman a este NACK un Reject o Select Reject. Una vez que el transmisor recibe el NACK se da cuenta que hubo un error en la trama transmitida por lo que resetea su V[S] y retransmite la trama con el número de secuencia que indica V[R].

Muchos sistemas usan números de 0 a 7 para V[S], V[R] y los números de secuencia en la trama. Una vez que las variables de estado son incrementadas hasta 7, entonces los números son utilizados nuevamente comenzando en cero. Debido a que los números son utilizados nuevamente a los DTE's no se le permite enviar una trama con un número de secuencia que no ha sido reconocido. Por ejemplo el protocolo debe esperar que una trama con V[S] igual a 6 sea reconocida antes de usar V[S] de 6 de nuevo en otra trama. En la figura 1.13 se muestran las tramas de 6 hasta 4 que no han sido reconocidas. Si una trama con número V[S] igual a 6 fuera enviada, el ACK correspondiente de la trama 6 no indicaría cual trama es reconocida.

El uso de números de 0 a 7 permite 7 tramas pendientes de reconocimiento antes de que la ventana sea cerrada y abierta nuevamente. Aunque 0-7 da 8 números de secuencia, el V[R] contiene el valor de la siguiente trama esperada.

El tamaño de la ventana es una importante consideración de diseño. Entre más grande sea la ventana más tramas pueden ser transmitidas sin un reconocimiento del receptor, aunque esto también significa que el receptor debe asignar más recursos para buffers que alojen los datos recibidos.

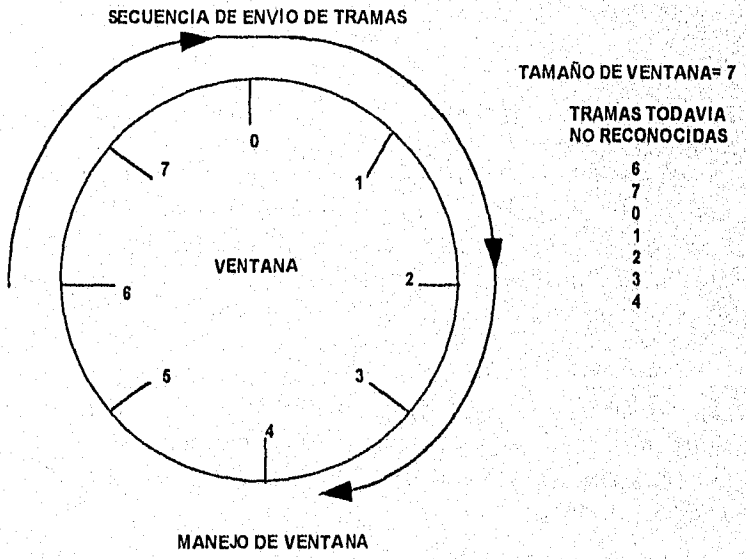


Figura 1.13
Protocolo de ventana deslizante.

Una ventaja del protocolo de ventana deslizante es el reconocimiento de todas las tramas enviadas con un sólo reconocimiento de la última trama. Por ejemplo, si se enviaron las tramas 1,2,3 y 4, un reconocimiento con V[R]= 5 indicará que la siguiente trama debe ser 5 y que ha recibido y reconocido todas las tramas hasta la 4.

Los protocolos de poleo ARQ son usados extensamente en redes de área amplia WAN. ARQ usa dos métodos para la retransmisión de tramas erróneas. Retransmisión selectiva que únicamente retransmite la trama errónea y Go-Back-N que retransmite todas las tramas que fueron transmitidas después de la trama errónea incluyendo ésta.

1.3.2.5 Retransmisión selectiva.

La retransmisión selectiva proporciona una buena utilización de línea, puesto que la trama errónea es la única retransmisión. Sin embargo, como se muestra en la figura 1.14, la estación receptora debe mantener las tramas 3, 4 y 5 esperando la retransmisión de la trama 2. A la llegada de la trama 2 al receptor, ésta debe ser insertada en la secuencia correcta antes de que los datos sean pasados a la aplicación de usuario. Las tramas guardadas en el receptor pueden consumir valioso espacio de buffer especialmente si el DTE tiene limitado espacio de memoria y diversos enlaces activos.

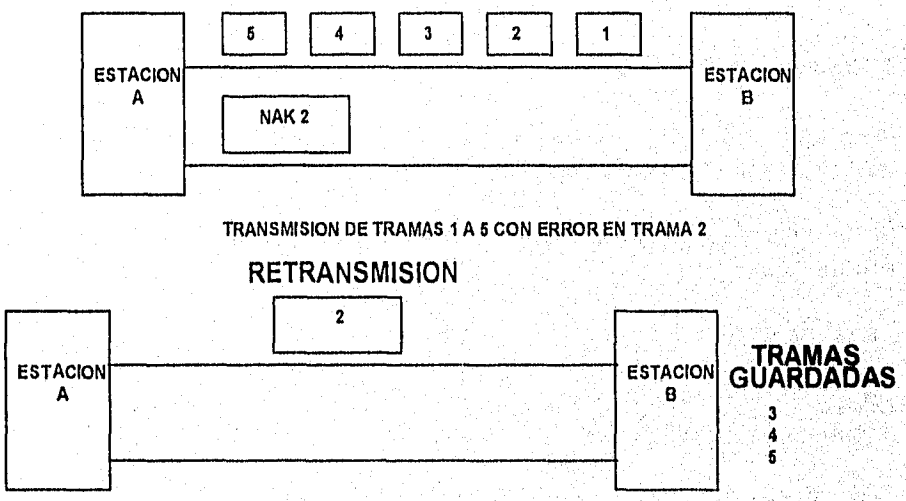
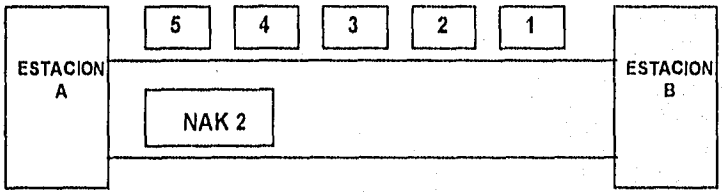


Figura 1.14
Esquema de retransmisión selectiva.

1.3.2.6 Retransmisión no selectiva (GO-BACK-N).

GO-BACK-N es una técnica más simple. Una vez que la trama errónea es detectada, la estación receptora descarta todas las tramas subsecuentes en la sesión hasta que ésta recibe la retransmisión correcta. GO-BACK-N no requiere cola de tramas y resecuensiamiento de tramas en el receptor (Ver figura 1.15).



TRANSMISION DE TRAMAS 1 A 5 CON ERROR EN TRAMA 2

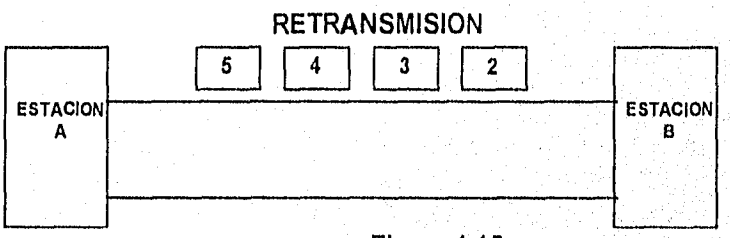


Figura 1.15
Esquema de retransmisión no selectiva (GO-BACK-N).

1.3.3 Capa de red (CAPA 3).

- Se ocupa de obtener los paquetes de la fuente y de encaminarlos durante toda la trayectoria hasta alcanzar su destino.
- Es la capa más baja del modelo de OSI que se ocupa de la transmisión extremo a extremo.
- Proporciona servicios orientados a conexión y sin conexión.
- Puede desensamblar mensajes de la capa de transporte en paquetes y después reensamblarlos en la estación destino.
- Realiza el enrutamiento de paquetes a través de la red.
- Realiza interconexión de redes.
  (Este tema se describirá a detalle en el capítulo 4).
- Realiza control de congestión.

1.3.3.1 Circuito virtual.

A una conexión en la capa de red se le conoce con el nombre de circuito virtual. En un circuito virtual se selecciona una ruta que va desde la máquina origen hasta la máquina destino como parte del proceso de conexión. Esta ruta se utiliza para todo el tráfico que circule por la conexión. Cuando se libera la conexión, se desecha el circuito virtual. Si los paquetes que circulan por un circuito virtual dado siguen siempre la misma ruta, cada nodo de conmutación debe recordar hacia donde expedir paquetes, para cada uno de los circuitos virtuales abiertos que pasan a través de él. Cada nodo de conmutación deberá mantener una tabla, con una entrada por cada circuito virtual abierto. Cada paquete que viaja a través de la red, deberá contener un campo con el número de circuito virtual en su cabecera, además de los números de secuencia, los códigos de redundancia, etc. Existen 2 tipos de circuitos virtuales conmutados y permanentes.

1.3.3.2 Datagrama.

Un datagrama es un agrupamiento lógico de información que se envía por la capa de red sin previo establecimiento de un circuito virtual. El datagrama contiene los datos de usuario, y la información necesaria para su enrutamiento como la dirección origen y destino del mismo. Cada datagrama enviado se enruta independientemente de sus predecesores. Los datagrama sucesivos pueden seguir rutas diferentes.

1.3.3.3 Enrutamiento.

Para el enrutamiento de paquetes existen algoritmos de software, que son los responsables de decidir sobre qué línea de salida se debe transmitir un paquete que llega. Si la red utiliza datagramas, esta decisión deberá tomarse con cada paquete de datos que llega. Si la red utiliza circuitos virtuales, las decisiones de enrutamiento sólo se tomarán cuando se establezca un circuito virtual nuevo. Al último caso se le conoce como enrutamiento de sesión.

1.3.3.4 Control de congestión.

Cuando se tiene la presencia de muchos paquetes en la red o en parte de ella, el rendimiento se degrada. Esta situación se conoce con el nombre de congestión. El control de la congestión tiene que ver con la seguridad de que la red sea capaz de transportar el tráfico ofrecido. Éste es un asunto global, que toma en cuenta el comportamiento de todas las máquinas, de todos los nodos (enrutadores o swiches), el procesamiento de almacenamiento y reenvío dentro de los nodos y todos los demás factores que tienden a disminuir la capacidad de transporte de la red.

Existen algunos algoritmos para el control de la congestión como lo son:
a) Preasignación de buffers.

Si se manejan Circuitos Virtuales es posible resolver el problema de la congestión con está técnica. Cuando se establece un circuito virtual el paquete de solicitud de llamada sigue su camino a través de la subred, produciendo entradas en las tablas de los enrutadores según avanza. En el momento que llega a su destino, la ruta que deberá seguir todo el tráfico subsiguiente ya se ha determinado, así como se han hecho entradas en las tablas de enrutamiento de todos los enrutadores intermedios. Normalmente el paquete de solicitud de llamada no reserva ningún espacio de memoria en los enrutadores intermedios. Sin embargo, una sencilla modificación del algoritmo de establecimiento podría hacer que cada uno de los paquetes de solicitud de llamada reserve, también buffers para datos. Si llega un paquete de solicitud de llamada a un enrutador y todos los buffers fueron reservados con anticipación, se deberá proceder a buscar una ruta alterna para el proceso o bien una señal de ocupado al extremo que llama.

b) Descarte de paquetes.

Este algoritmo en lugar de reservar buffers en los enrutadores, no reserva absolutamente nada. Si llega un paquete y no hay espacio para colocarlo, el enrutador sencillamente lo descarta.

c) Control isarítmico de la congestión.

Este método se llama isarítmico, debido a que se mantiene constante el número de paquetes, existen permisos que circulan dentro de la subred. Siempre que un enrutador desee transmitir un paquete recién llegado apenas de una estación, primero deberá capturar un permiso y después destruirlo. Cuando, finalmente, el enrutador destino recibe el paquete, regenera el permiso. Estas reglas aseguran que el número de paquetes de la subred nunca exceda al número de permisos que originalmente están presentes.

d) Control de flujo.

Algunas redes han intentado utilizar mecanismos de control de flujo para eliminar la congestión. Aunque la capa de transporte puede llegar a utilizar esquemas de control de flujo para impedir que una estación sature a otra y, además, los esquemas de control de flujo pueden utilizarse para evitar que un enrutador sature a sus vecinos, es extremadamente difícil controlar la cantidad de tráfico en la red empleando reglas de control de flujo de extremo a extremo. Más todavía, si las estaciones se ven forzadas a detener la transmisión debido a las estrictas reglas de control de flujo, la subred no llegará a estar suficientemente cargada.

e) Paquetes reguladores.

Esta idea consiste en que cada enrutador supervise el porcentaje de uso de sus líneas de salida. Cada que la línea sobrepase un límite de porcentaje de uso, la línea entra a un estado de "alerta". Cada uno de los nuevos paquetes que llegan al enrutador se examinan para ver si su línea de salida está en estado de alerta. Si es el caso, el enrutador transmite un paquete regulador, de vuelta a la estación de origen, tomando el destino del paquete mismo.

Cuando la estación origen recibe el paquete regulador se le solicita que se reduzca el tráfico, enviando al destino especificado, de acuerdo con un porcentaje X durante un intervalo de tiempo específico. Si no llega ningún paquete regulador durante el intervalo de tiempo mencionado anteriormente, la estación puede aumentar el flujo de datos nuevamente.

f) Bloqueos.

La congestión máxima es un bloqueo, al que también se le conoce como estancamiento. El primer enrutador no puede proseguir hasta que el segundo enrutador lleve a cabo una acción, y el segundo enrutador tampoco puede continuar porque está esperando que el primero haga algo.

Para solucionar el problema Merlyn y Schweitzer presentaron una solución al problema.

En este esquema se construye un grafo dirigido, en el cual los buffers son los nodos del grafo. Los arcos conectan a pares de buffers localizados en el mismo enrutador o en enrutadores adyacentes. El grafo se construye de tal manera que si todos los paquetes se mueven de un buffer a otro a lo largo de los arcos del grafo, entonces no se presentaran bloqueos.

1.3.4 Capa de transporte (CAPA 4).

- Su objetivo es proporcionar un servicio eficiente, fiable y económico a sus usuarios, normalmente entidades de la capa de sesión.
- Proporciona dos tipos de servicio de transporte orientado a conexión y sin conexión.
- Supervisa la calidad del servicio.
- Realiza control de Flujo.
- Realiza multiplexaje y funciones de ensamblado y desensamblado.

1.3.4.1 Servicios de la capa de transporte.

El servicio orientado a conexión en la capa de transporte tiene una fase de establecimiento, de transferencia de datos y de liberación.

De la misma manera como hay dos tipos de servicio de red, también hay dos tipos de servicio de transporte: es decir, orientado a conexión y sin conexión. El servicio de transporte orientado a conexión es similar al servicio de red orientado a conexión. En los 2 casos, las conexiones tienen tres fases: establecimiento, transferencia de datos y la liberación. Si las 2 capas son similares, cuál es la razón de tener 2 capas. La razón es que los usuarios no tienen control sobre los nodos de conmutación proporcionantes del servicio de red, por lo que si el servicio es deficiente, entonces los usuarios no podrían resolver los problemas que se les presenten. La única solución posible es colocar otra capa arriba de la capa de red, que mejore la calidad del servicio. Si a una entidad de transporte se le informa, a la mitad de una larga transmisión, que se ha interrumpido repentinamente su conexión de red, sin ninguna indicación respecto a lo que sucedió con respecto a los datos que se encontraban en tráfico, ésta puede establecer una nueva conexión con la entidad de transporte remota. Utilizando esta nueva conexión, la entidad de transporte puede enviar una pregunta a la otra entidad de transporte, para averiguar qué datos llegaron y cuáles no, y después reiniciar la transmisión a partir del primer dato que se perdió.

1.3.4.2 Calidad de servicio.

Otra manera de ver la capa de transporte consiste en considerar que su función primordial es la de enriquecer la calidad del servicio suministrada por la capa de red de acuerdo a varios parámetros.

a) Retardo en el establecimiento de la conexión.

Es el tiempo que transcurre entre una solicitud de conexión de transporte y la confirmación que recibe del usuario del servicio de transporte. Cuanto más corto sea éste, mejor será el servicio suministrado.

b) La probabilidad de fallo de establecimiento de la conexión.

Es el riesgo de que no se pueda establecer una conexión dentro del máximo tiempo de retardo permitido, por ejemplo, debido a la congestión de la red, a la falta de espacio en las tablas de los enrutadores, o bien, a otros problemas internos.

c) Caudal.

El parámetro de caudal mide el número de octetos de datos del usuario que se transfieren cada segundo.

d) El retardo de tránsito.

El retardo de tránsito mide el tiempo que transcurre entre el envío de un mensaje por la máquina fuente y la recepción de éste en la máquina destino.

e) La tasa de error residual.

La tasa de error residual mide el número de mensajes perdidos o dañados, como una fracción del total de mensajes transmitidos, en el periodo de muestreo.

f) La probabilidad de fallo de transferencia.

La probabilidad de fallo de transferencia mide la manera en la cual el servicio de transporte está actuando, de acuerdo con lo prometido. Cuando se establece una conexión de transporte, se llega a un acuerdo con respecto a un nivel dado de caudal, de retardo de tráfico y de tasa de error residual. La probabilidad de fallo de transferencia indica la fracción de veces que estos objetivos acordados no se llegaron a satisfacer, durante algún periodo de observación.

g) El retardo en la liberación de la conexión.

El retardo en la liberación de conexión es el tiempo que transcurre entre el inicio de la liberación de una conexión por alguno de los extremos comunicándose y el momento en que se logra ésta.

h) La probabilidad de fallo en la liberación de la conexión.

Es la fracción de intentos de liberación de conexión que no se completaron durante el intervalo de retardo acordado para la liberación de la conexión.

i) Prioridad.

El parámetro prioridad brinda una forma al usuario de transporte para indicar que algunas de sus conexiones son más importantes que otras, y en caso de existir congestión, tenga la seguridad de que las conexiones con alta prioridad obtendrán servicio, antes que las de menos prioridad.

j) Resistencia.

El parámetro resistencia proporciona la probabilidad de que la misma capa de transporte termine espontáneamente una conexión, ya sea por problemas internos o por congestión.

1.3.4.3 Protocolos de transporte.

Cuanto más malo sea el servicio de red, será más complejo el protocolo de transporte. OSI ha considerado el problema con 5 clases de protocolos de transporte.

a) La clase 0 establece una conexión de red para cada conexión de transporte que se haya solicitado, y al mismo tiempo supone que la conexión de red no comete errores. El protocolo de transporte no realiza control de flujo, sin embargo, si proporciona los mecanismos para el establecimiento y liberación de las conexiones de transporte.

b) La clase 1 se ha diseñado para recuperarse de los fallos de la conexión de red, las dos entidades de transporte se resincronizan y continúan a partir del punto en que habían quedado. Para lograr la resincronización deberán guardar números de secuencia. No proporciona control de error ni control de flujo.

c) La clase 2 supone que la conexión de red no comete errores, pero dos o más conexiones de transporte pueden transmitirse multiplexadas sobre la misma conexión de red.

d) La clase 3 combina las características de las clases 1 y 2. Permite multiplexión y también puede recuperarse de los fallos de la conexión de red. Además, utiliza control de flujo.

e) La clase 4 es capaz de manejar paquetes que se hayan perdido, duplicado o dañado y además es capaz de recuperarse de los fallos de la conexión de red.

1.3.4.4 Elementos de los protocolos de transporte.

a) Establecimiento de conexión.

Todos los protocolos orientados a conexión deben proporcionar un mecanismo para el establecimiento de conexiones.

En la figura 1.16a por medio de las flechas se denotan las unidades de datos del protocolo de transporte (TPDU'S) enviadas y recibidas por las entidades de

transporte. De alguna manera, A selecciona un número de secuencia, X por ejemplo, y lo envía a B en una TPDU de solicitud de conexión (SC); B contesta con una TPDU de confirmación de conexión (CC), reconociendo a X y anunciando su propio número de secuencia inicial Y. Por último A reconoce la elección que hizo B, del número de secuencia inicial, en su primera TPDU de datos.

El funcionamiento de una comunicación ida y vuelta en presencia de TPDU's duplicadas y retardadas se muestra en la figura 1.16b. La primera TPDU es un duplicado de solicitud de conexión (SC) retardado, procedente de una conexión que ya se liberó. Esta TPDU llega a B sin que A se llegue a enterar. Ante esta TPDU, B reacciona mediante la transmisión de una TPDU CC para A, a través de la cual se le pide que verifique que está tratando de establecer una nueva conexión. En el momento en que A rechaza el intento de establecimiento de B, ésta comprende que fue engañada por un duplicado retardado y abandona la conexión.

El peor caso se tiene cuando una solicitud de conexión retardada y un reconocimiento para una confirmación de conexión, se encuentran flotando dentro de la subred; situación que se muestra en la figura 1.16c. Como en el ejemplo anterior, B recibe una solicitud de conexión retardada y la contesta. En este momento, resulta crucial entender que B ha propuesto utilizar a Y como el número de secuencia inicial para el tráfico que va de B hacia A, sabiendo muy bien que todavía no existe ninguna TPDU que contenga un número de secuencia Y o un reconocimiento para Y. Cuando llega a B la segunda TPDU retardada, el hecho de que Z haya sido asentido en lugar de Y, le indica a B que éste también es un duplicado antiguo y abandona la conexión.

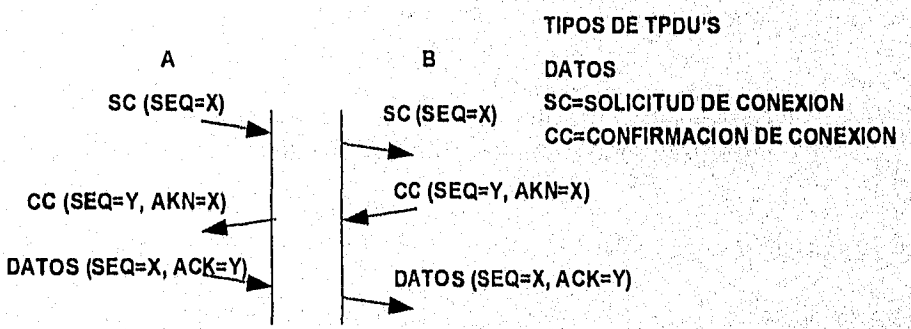


Figura 1.16a
Operación normal.

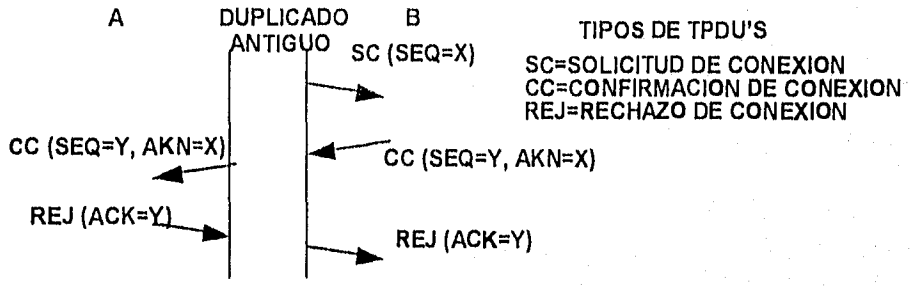


Figura 1.16b
Duplicado antiguo.

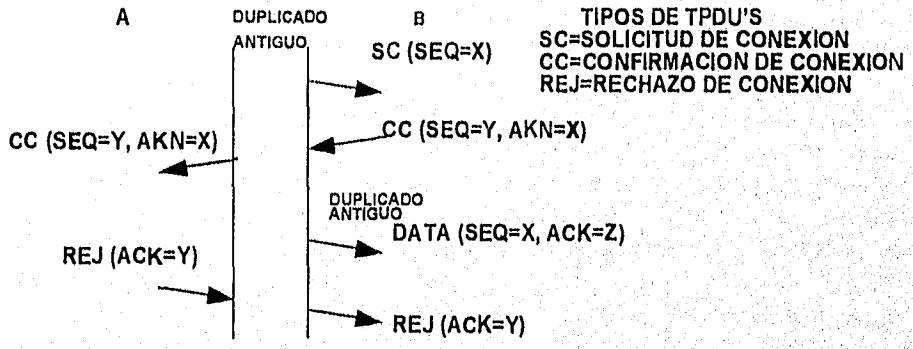


Figura 1.16c
Duplicado de solicitud de conexión y duplicado de reconocimiento.

Figura 1.16.
Tres escenarios para el establecimiento de una conexión mediante una comunicación ida y vuelta.

b) Liberación de conexión.

En la figura 1.17 se ilustran cuatro escenarios de liberación utilizando el protocolo de ida y vuelta.

En la figura 1.17a se presenta el caso normal, en el que uno de los usuarios transmite una solicitud de desconexión (SD), para indicar la liberación de la conexión. En el momento que ésta llega, el emisor devuelve una confirmación de desconexión (CD) y arranca un temporizador, por si acaso se pierde la CD. En el momento que la CD llega, el emisor original devuelve una TPDU ACK y

elimina la conexión. Por último, cuando llega este ACK, el receptor también elimina la conexión.

Si se llegará a perder el último ACK, como se muestra en la figura 1.17b, la situación queda protegida por el temporizador. Cuando el plazo de éste se termina, la conexión de todos modos se elimina.

Ahora considérese el caso en el que se pierde un CD o SD. El usuario que inicia la desconexión no recibirá el CD, pero al término de una temporización comenzará todo de nuevo. En la figura 1.17c, se observa cómo funciona esto, suponiendo que en una segunda ocasión no se llegan a perder las TPDU's.

El último escenario mostrado en la figura 1.17d, es el mismo que el mostrado en la figura 1.17c, con la única excepción de que ahora se supone que todos los intentos de repetición, para transmitir la SD, también son infructuosos como consecuencia de la pérdida de las TPDU's. Después de intentar hacerlo n veces, el transmisor se da por vencido y elimina la conexión. Mientras tanto, el receptor, al término de una temporización, también elimina la conexión.

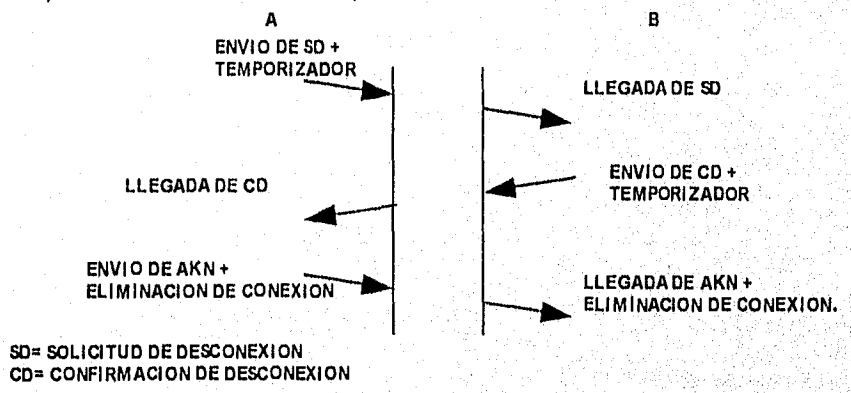


Figura 1.17a
Caso normal de desconexión.

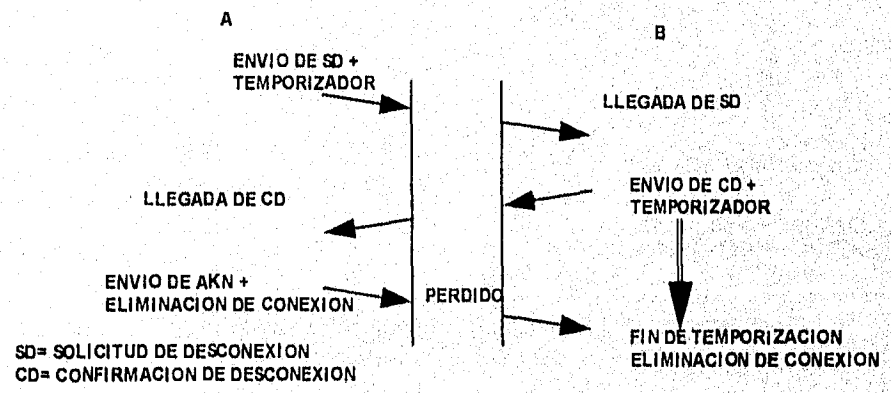


Figura 1.17b
Pérdida del último reconocimiento de desconexión.

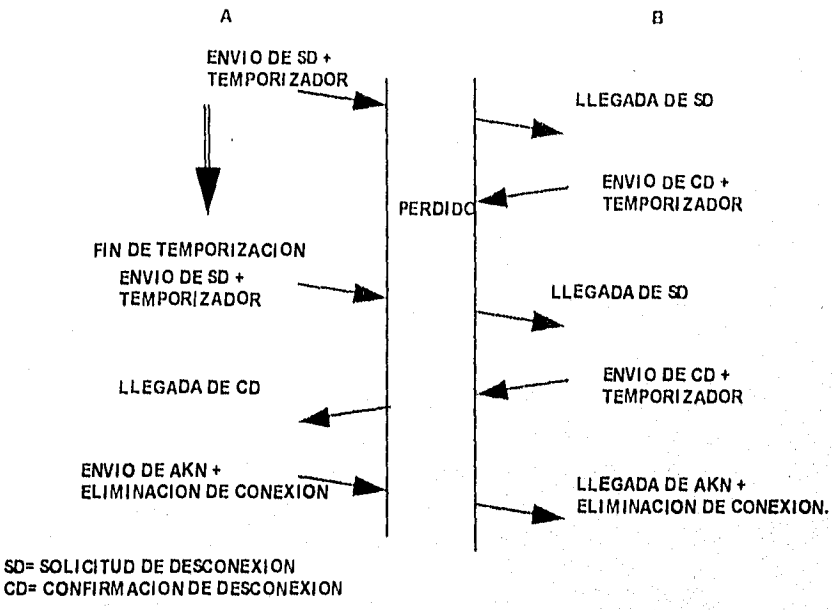


Figura 1.17c
Confirmación de desconexión perdido.

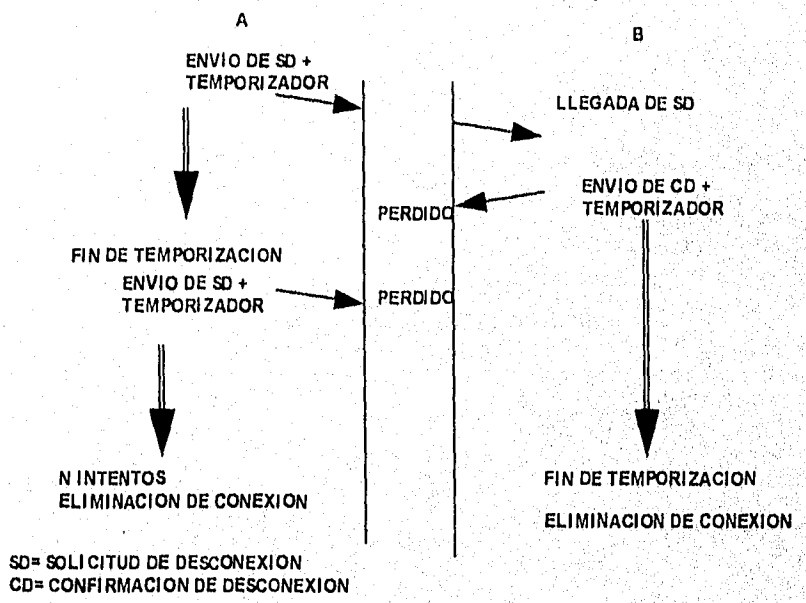


Figura 1.17d
confirmación de desconexión perdido y pérdida de las siguientes solicitudes de desconexión.

Figura 1.17
Cuatro escenarios para la liberación de conexión.

c) Rechazo de conexión.

Todos los protocolos deben tener alguna forma para que la parte llamada acepte o rechace la conexión solicitada.

d) Asignación a conexión de red.

Las entidades de transporte normalmente establecen una conexión de red y mantienen el seguimiento de la correlación que se lleva a cabo entre las conexiones de transporte y de red. Sin embargo, también es posible que las entidades de transporte utilicen un protocolo de red sin conexión para el transporte de datos, asegurándose de que el protocolo de transporte sea de clase 4.

e) División de grandes mensajes en varias unidades de datos del protocolo de transporte (TPDU).

Los mensajes que se desean transmitir pueden tener cualquier longitud, por lo que dependerá de la capa de transporte el dividirlos en varias TPDU's del tamaño que el protocolo usa para poderlos transportar, y después rearmar las piezas del mensaje de una manera transparente.

f) Asociación de TPDU con conexión.

Si hay múltiples conexiones abiertas en una máquina, las entidades de transporte tendrán que atribuir un número a cada una de la conexiones, y poner los números de conexión en cada una de las TPDU.

g) Transferencia de TPDU'S

Es una característica de todos los protocolos de transporte.

h) Liberación normal.

La liberación de la conexión se hace mediante intercambio de TPDU'S de control de transporte. En caso de tener TPDU's inválidas, el protocolo debe saber que hacer.

i) Concatenación de TPDU's para el usuario.

Esta característica permite que la entidad de transporte colecte varias TPDU's y las transmita juntas, como si fueran un sólo paquete.

j) Liberación por error.

Para las clases de protocolo 0 y 2 la conexión se libera automáticamente en caso de error.

k) Numeración de TPDU's.

Con la asignación de los números de secuencia consecutivamente mayores, es posible tener un control de flujo y de reconocimientos, y habrá una forma de determinar, después de que ocurre una falla, cuál fué la última TPDU que se recibió.

l) Transferencia de datos acelerados.

m) Control de flujo en la capa de transporte.

El control de flujo de la capa de transporte consiste en tener una parte explícita del protocolo de transporte que se ocupe del número de TPDU que se puede transmitir en cualquier instante. Se puede usar el esquema de ventana deslizante.

n) Resincronización posterior a un reset.

Se realiza en cada uno de los extremos de transporte para descubrir cuales de las TPDU que se enviaron ya fueron recibidas.

o) Retención de una TPDU hasta un reconocimiento.

Es necesario que se retengan copias de las TPDU's enviadas hasta que se obtenga un reconocimiento, de tal forma que se puedan retransmitir en caso de que se presente una falla.

p) Reasignación después de una desconexión de red.

Si la conexión de red libera y no es posible lograr la resincronización, entonces dependerá de la capa de transporte el establecer una nueva conexión sobre la cual pueda trabajar.

q) Referencias congeladas.

La idea es evitar que se de a una TPDU un identificador que sea igual al de una antigua TPDU, que todavía existe.

r) Multiplexaje.

Multiplexaje ascendente: Es el proceso de multiplexaje de diferentes conexiones de transporte en una misma conexión de red.

Multiplexaje descendente: Múltiples conexiones de red multiplexadas en una conexión de transporte.

s) Uso de conexiones múltiples de red.

t) Retransmisión después de una temporización.

Esto sólo es necesario en protocolos clase 4, por que es la única clase en la que la pérdida de paquetes es común como para requerir un control de error en la capa de transporte.

u) Resecuenciamiento de TPDU's.

El extremo destino puede recibir las TPDU's en un orden distinto al enviado, por lo que es su responsabilidad juntarlas y ordenarlas.

v) Temporizador de inactividad.

Se utiliza para detectar una conexión muerta en la red.

1.3.5 Capa de sesión (CAPA 5).

- La función principal de la capa de sesión consiste en proporcionar una manera por medio de la cual los usuarios de la capa de sesión (por ejemplo entidades de la capa de presentación, o en algunas ocasiones procesos de usuario común y corrientes) establezcan conexiones llamadas sesiones y transfieran datos sobre ellas en forma ordenada. Una sesión podría utilizarse para un acceso remoto desde una terminal a un servidor remoto, o para una transferencia de archivos.

- Realiza administración de diálogos.
- Maneja la sincronización.
- Lleva a cabo la administración de actividades.
- Se encarga del mapeo de direcciones.

1.3.5.1 Administración de diálogos.

El hecho de mantener un seguimiento de a quién le corresponde el turno de transmitir (y hacerlo cumplir), cuanto tiempo el usuario puede tener la línea, y si la transmisión es simplex, half-dúplex o full-dúplex, se denomina administración de diálogos.

La administración de diálogo se realiza mediante el empleo de un token de datos. En el momento que se establece la sesión, el funcionamiento full-dúplex es una de las opciones a elegir. Si se selecciona el funcionamiento half-dúplex, la negociación inicial también determina qué extremo poseerá primero el token. Solamente el usuario que tiene el token puede transmitir datos, el otro deberá permanecer en silencio.

1.3.5.2 Sincronización.

La sincronización se utiliza para llevar a las entidades de sesión de vuelta a un estado conocido, en caso de que haya algún error o falla. Para lograr lo anterior se introducen puntos de sincronización en el flujo de datos.

Existen dos tipos diferentes de puntos de sincronización, llamados puntos de sincronización mayor y menor. Las unidades delimitadas por los puntos de sincronización mayores se llaman unidades de diálogo, y generalmente representan partes del trabajo lógicamente significativas.

Los puntos de sincronización mayores y menores son diferentes en varios aspectos. En el momento que se realiza una resincronización, es posible sólo volver al punto de sincronización mayor más reciente. Los puntos de sincronización mayores son tan importantes, que cada uno que se inserte en el flujo de datos deberá confirmarse explícitamente con un reconocimiento. Los puntos de sincronización menores son reconocidos opcionalmente y sirven para que una aplicación se recupere de errores ocurridos en capas arriba de la capa sesión. Por ejemplo los datos que se pierden por falta de papel en una impresora que está trabajando en línea.

1.3.5.3 Administración de actividades.

La idea de administración de actividades es la de permitir que el usuario divida el flujo de mensajes en unidades lógicas denominadas actividades. Cada actividad puede ser considerada como una transferencia de datos distinta, con un inicio y fin indicados específicamente. Las actividades pueden ser suspendidas, reanudadas y rechazadas.

1.3.6 Capa de presentación (CAPA 6).

- Se encarga de la preservación del significado de la información transportada.
- Realiza compresión de datos
- Realiza criptografía.

La capa de presentación trata con los problemas relacionados con la representación de los datos transmitidos incluyendo los aspectos de conversión, cifrado y compresión de datos.

La capa de presentación se encarga de la preservación del significado de la información transportada. Cada dispositivo en la red (PC's, máquinas IBM, SUN) puede tener su propia forma de representación interna de los datos, por lo que es necesario tener acuerdos y conversiones para poder asegurar el entendimiento entre dispositivos diferentes en la red. El trabajo de la capa de presentación consiste precisamente en codificar los datos estructurados del formato interno utilizado en la máquina transmisora, a un flujo de bits adecuado para la transmisión y, después decodificarlos para representarlos en el formato del extremo destinatario.

1.3.6.1 Técnicas de Compresión de datos.

a) Codificación de un conjunto finito de símbolos igualmente probables.

Esta codificación sugiere asignar un código corto totalmente diferente a la información por transmitir. En este esquema tanto el transmisor como el receptor deben saber las equivalencias entre el código de la información y el código de transmisión.

b) Codificación dependiente de la frecuencia.

En casi todos los textos, algunos símbolos aparecen con mayor frecuencia que otros. Esta observación sugiere un esquema de codificación en la que, a los símbolos comunes se les asignan códigos cortos y a los símbolos ocasionales códigos largos.

c) Codificación dependiente del contexto.

Un ejemplo de codificación dependiente del contexto consiste en comprimir series de símbolos repetidos en una cuenta, más el símbolo. Las series de caracteres en blanco, de avance de línea y de ceros no significativos, son los candidatos más probables para aplicar este método.

1.3.6.2 Criptografía.

Criptografía es el proceso de poner en clave la información por medio de un codificador o cifrador.

Cifrador de sustitución.

En un cifrador de sustitución, cada letra o grupo de letras se sustituye por otra letra o grupo de letras para disfrazarlas.

Cifrador de transposición.

Los cifradores de transposición, reordenan las letras pero no las disfrazan.

1.3.7 Capa de aplicación (capa 7).

La capa de aplicación contiene los programas del usuario, que hacen el trabajo real para lo cual se adquieren las computadoras.

Algunos ejemplos de aplicaciones son:

- Correo electrónico
- Servicio de terminal virtual
- Solicitud y transmisión de archivos
- Creación de gráficas y pantallas
- Procesamiento de textos

1.3.8 Conceptos de comunicación de datos.

1.3.8.1 Definiciones Generales.

Información.

La información puede ser voz, imágenes, datos de computadora, mediciones de temperatura etc..

La transferencia de información entre dos puntos sobre un sistema de comunicaciones requiere primero que la información primero sea codificada en datos y entonces se usen señales para representar los datos transmitidos.

Como todos los sistemas de comunicaciones transmiten, en una u otra forma información, y como se desea tener algún tipo de medida del contenido de información de los mensajes que se van a transmitir, es importante establecer primero lo que se entiende por información.

Desde el punto de vista de las comunicaciones, información son señales eléctricas que se modifican con el tiempo y cuyo cambio es, además, impredecible. Las secuencias de unos y ceros son desconocidas de antemano y corresponderán al mensaje transmitido.

Por cantidad de información transmitida en T segundos se entiende el número de combinaciones diferentes y distinguibles de amplitudes de la señal que pueden transmitirse en ese mismo tiempo. Lo anterior expresado matemáticamente es igual a:

Información = T/τ log2 n. bits

Donde:

T=Tiempo en segundos.

τ= Intervalos de τ segundos
(Mínimo intervalo en que pueden cambiar de valor las señales)

n= Número de niveles de amplitud distinguibles.

Datos.

Son una representación de eventos, conceptos o instrucciones de una manera conveniente para comunicación, interpretación o procesamiento de las

máquinas. Los datos son los símbolos intercambiados por las máquinas. Los datos pueden ser analógicos y digitales.

Señal.

Es una forma de energía que puede representar datos que se transfieren. Esta puede ser luz, electricidad o cualquier otro tipo de energía.

El empleo de las señales eléctricas (en el más amplio sentido, debe considerarse a la luz perteneciente a esta clase, dado que está en el espectro electromagnético) ha reemplazado completamente a las otras formas de transmisión de información a grandes distancias. Esto se debe, principalmente a que las señales eléctricas son relativamente fáciles de controlar y viajan con velocidades como la de la luz o cercanas.

Hay dos tipos de señales eléctricas usados en comunicación:

Señales Analógicas.

Las señales analógicas pueden tomar cualquier valor a través del tiempo y cambian suavemente de un valor al siguiente. Una señal analógica periódica varia regularmente entre valores sobre el tiempo y puede representarse gráficamente como una onda. Las señales analógicas pueden ser descritas en términos de los siguientes tres parámetros: Amplitud, Frecuencia y Fase.

Señales Digitales.

Las señales digitales tienen dos propiedades distintivas. Primero ellas pueden tomar sólo un número limitado de valores discretos, frecuentemente dos. Segundo, los valores de la señal realizan la transición casi instantáneamente de un estado a otro.
La información en una señal digital depende del estado de la señal durante un cierto tiempo. Por lo tanto las estaciones transmisora y receptora deben tener señales de reloj que estén sincronizadas.

Transmisión.

Es la actividad de mover información a través de un sistema de comunicación.

En telecomunicación hay dos formas de transmisión: Transmisión Analógica y Transmisión Digital. Ver figuras 1.18 y 1.19.

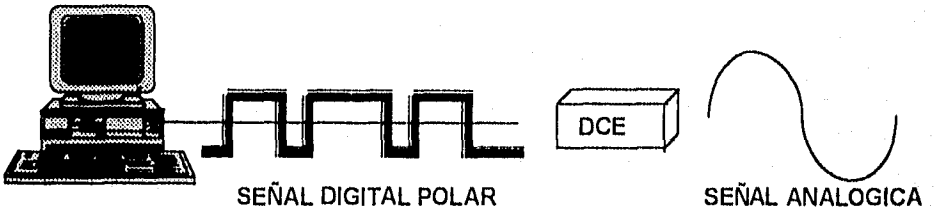


Figura 1.18
Transmisión analógica.

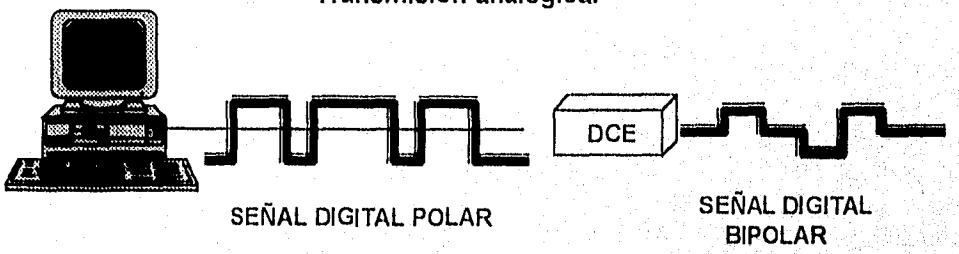


Figura 1.19
Transmisión digital.

Comunicación.

Es la conducción o transmisión de información de un lugar y/o tiempo a otro.

Telecomunicaciones.

Se refiere a la transmisión electrónica de alguna clase de información electrónica, incluyendo llamadas telefónicas, señales de televisión, datos de computadoras, correo electrónico, fax y telemetría.

Teleprocesamiento.

Este término se refiere al acceso de archivos de datos y poder de computación a distancia. Generalmente usando terminales y facilidades de telecomunicación.

Sistema de Teleprocesamiento.

Computadoras, terminales, líneas de comunicación y hardware y software usado para implementar una aplicación completa de procesamiento de datos.

Comunicación de datos.

Se refiere a la transmisión electrónica de datos. Transmisión de datos es un sinónimo. Ambos términos son generalmente usados para referenciar datos que son manipulados por computadoras. Sin embargo, en el sentido estricto, comunicación de datos también abarca telegrafía, telemetría y formas similares de transmisión electrónica de datos.

Sistema de Comunicación de datos.

Son aquellas partes del sistema que están involucradas en la transmisión de datos de un extremo a otro.
Hoy el más común sistema de transmisión de datos toma la forma de personas en terminales comunicándose con una computadora a distancia. La computadora usualmente responde rápidamente.

En los sistemas de comunicación de datos modernos, las funciones de transmisión de datos de cada estación conectada a la línea de comunicación son realizadas por software o firmware instalado en las estaciones de comunicación. Las funciones realizadas por el software o firmware son divididas en capas independientes.

En cada capa, un conjunto de reglas debe ser acordado y seguido por ambas partes para que la comunicación sea exitosa. Las reglas que gobiernan la comunicación en cada capa son llamadas protocolos.

Un sistema de comunicación de datos puede ser visto como un número de niveles. En cada nivel, una capa de software trabaja junto con el hardware para proporcionar un conjunto útil de funciones.

Todos los sistemas de comunicación tienen al menos 2 capas en común: la capa física y la capa de enlace de datos.

La figura 1.20 ilustra un sistema de comunicación de datos simple. Los procesos de aplicación (aplicación de usuario). La aplicación de usuario usualmente consiste de software como un programa de computadora, programas de control de inventario, reservación de líneas aéreas, etc..

Como se observa la aplicación reside en el equipo terminal de datos o DTE. DTE es un término genérico usado para describir máquinas de usuario como computadoras o terminales, aunque un DTE también puede ser una minicomputadora o mainframe.

La función del sistema de comunicaciones es interconectar DTE's de manera que ellos puedan compartir recursos, intercambiar datos, proporcionarse respaldo uno con respecto del otro, etc..

La figura 1.20 muestra el canal de comunicaciones que se usa para realizar comunicaciones lógicas entre los DTE's. Además, también muestra el equipo de terminación de circuito de datos, o DCE (también llamado equipo de comunicación de datos). Su función es conectar los DTE's en la línea o canal de comunicaciones.

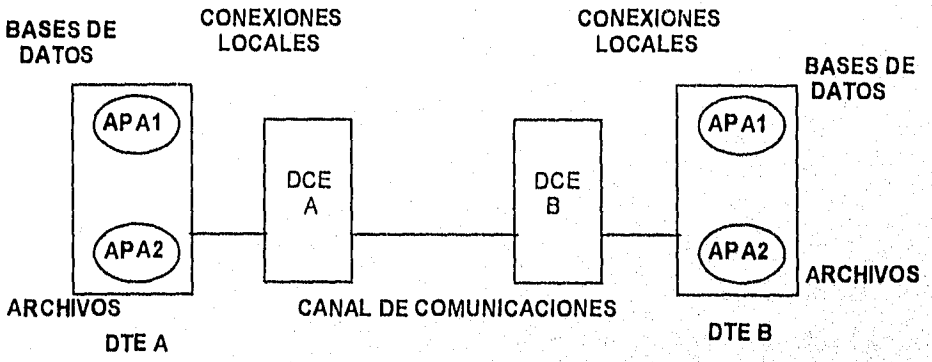


Figura 1.20
Sistema de comunicación de datos simple.

1.3.8.2 Componentes de un sistema de comunicación.

La fuente, que origina el mensaje, como una voz humana, una imagen de televisión, un mensaje de teletipo, o simplemente datos. Si los datos no son eléctricos, deben convertirse mediante un transductor de entrada en una forma de onda eléctrica que se conoce como señal de banda base o mensaje.

El transmisor, que modifica la señal de banda base a una señal eficiente para transmisión.

El canal, que es un medio tal como alambre un cable coaxial, una guía de ondas, una fibra óptica, o un enlace de radio, a través del cual se envía la salida del transmisor.

El receptor, que reprocesa la señal proveniente del canal y elimina las modificaciones introducidas por el transmisor y el canal. La salida del receptor alimenta el transductor de salida, que convierte la señal eléctrica a su forma original, el mensaje.

El destinatario, que es la unidad a la que se le comunica el mensaje (Ver figura 1.21).

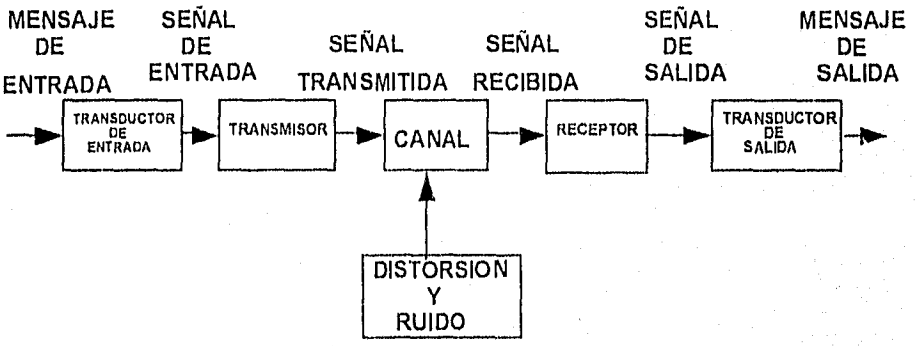


Figura 1.21
Componentes de un Sistema de Comunicación.

1.3.8.3 Canal de Comunicaciones.

Es el medio por el cual nosotros queremos tomar una cadena de bits de una máquina de procesamiento de datos en un extremo, y transmitir esa cadena de bits sin que haya errores a otra máquina de procesamiento de datos en un extremo distante.

Capacidad de Canal.

La capacidad de un canal de comunicaciones se define como la máxima cantidad de información que éste puede transmitir, sin error. Para propósitos de comunicación de datos, ésta es frecuentemente medida en bits por segundo.

Claude Shannon proporciono una ecuación para determinar la capacidad de un canal ideal cuyas únicas limitaciones son el ancho de banda y el ruido aleatorio:

C=Blog(1+SNR) bps.
Donde B=1/ τ El ancho de banda del canal
SNR= S/N Relación señal a ruido.
S= Potencia de la señal a través del canal en watts
N= Potencia del ruido a través del canal en watts.

La ecuación de Shannon proporciona un límite teórico superior para un canal binario.

Canales de comunicación analógicos.

Desafortunadamente la mayoría de las líneas que son usadas para transmitir datos no son digitales. El canal de comunicación de datos más común es el circuito telefónico ordinario.

Ancho de banda.

Las líneas analógicas son diseñadas para conducir rangos específicos de frecuencias. La capacidad de una línea analógica es medida por el rango de frecuencias que la línea puede conducir, es decir su ancho de banda.

El ancho de banda de un canal analógico es siempre la diferencia entre los límites inferior y superior de las frecuencias que este es capaz de conducir.

Los canales telefónicos están diseñados para transmitir de 300 a 3300 Hz y la diferencia entre estas cantidades es 3000 Hz. Actualmente el ancho de banda de un canal Telefónico es de 4000 Hz, pero parte del ancho de banda es usado para proporcionar adecuada separación entre los canales cuando múltiples canales comparten el mismo medio de transmisión.

Enviando datos a través de la línea telefónica.

Cuando los datos son enviados sobre canales telefónicos ordinarios, los datos digitales deben ser convertidos a señales analógicas que deben ajustarse al ancho de banda del canal telefónico a través de un proceso de modulación.

Módem.

Para usar una línea telefónica analógica en la transmisión de niveles de voltaje discreto que máquinas de procesamiento de datos usan, los bits primero deben ser convertidos a un rango de frecuencias. El proceso de realizar la conversión de la cadena de bits digital a una señal analógica es una forma de modulación. El proceso de realizar la conversión opuesta es llamado demodulación. El dispositivo que realiza estas conversiones es llamado módem.

Formas de Compartir un canal de comunicación.

En muchos sistemas que utilizan la transmisión de datos, el costo de los canales de comunicación representa un gran porcentaje del costo total del

sistema. Los canales deben ser compartidos tanto como sea posible, para asegurar que su capacidad sea completamente utilizada.

Para poder compartir un canal existen técnicas de multiplexaje y de conmutación de paquetes que se explicarán posteriormente.

Mensaje Digital o Binario.

Un mensaje digital o binario se entiende como una secuencia de dos tipos de pulsos o formas de onda conocidas, que se presentan a intervalos regularmente espaciados en el tiempo.

Se considera un mensaje digital a causa de que esta forma se está convirtiendo rápidamente en la más usual en transmisión de señales, ya sea por que el mensaje se encuentra directamente en forma digital, como en el caso de la salida de una computadora, o por que es necesario convertirlo a una forma digital como en el caso de las comunicaciones telefónicas de audio.

1.3.8.4 Sincronización de los componentes de la red.

Para que las computadoras y las terminales se comuniquen, ellas primero necesitan avisarse una a otra que son capaces de comunicarse. Segundo, una vez que ellas están comunicándose, deben proporcionar un método que mantenga ambos dispositivos consientes de las transmisiones que vengan.

En el primer punto un transmisor, tal como una terminal o computadora, debe transmitir su señal de modo que el dispositivo receptor sepa cuando buscar y reconocer los datos cuando éstos llegan. En esencia el receptor debe saber el tiempo exacto en el que llega cada elemento binario a través del canal de comunicaciones. Este requerimiento significa que una base de tiempo mutuo o un reloj común es necesario entre los dispositivos transmisor y receptor.

Una máquina debe primero enviar a la máquina receptora una indicación de que quiere "hablar" con ésta.

Este proceso es parte del protocolo de comunicaciones y es generalmente conocido como sincronización. Conexiones a corta distancia frecuentemente usan un canal separado, o línea para proporcionar la sincronización. Esta línea transmite un señal que es encendida, apagada o variada de acuerdo con convenciones preestablecidas. Cuando la señal de reloj cambia, notifica al receptor para que examine la línea de datos. Esta señal de reloj también puede resincronizar al receptor para mantener los relojes alineados.

La temporización o sincronización puede ser una función orientada a carácter, como en la transmisión asíncrona, donde el receptor se sincroniza con el bit de inicio y fin de cada carácter.

La temporización también puede ser una función orientada a bloque, como en la transmisión síncrona donde el receptor se sincroniza con la bandera de inicio y final de cada bloque de datos.

En cualquier evento, la sincronización asegura la recepción de los datos tal como fueron transmitidos y ayuda en la detección y corrección de errores.

Códigos de sincronización.

Cuando hay grandes distancias entre computadoras y terminales es más económico incorporar la señal de temporización (reloj) en la señal de datos, en lugar de usar un canal de reloj separado. Esto es conocido como código de self-clocking.

Un código self-clocking es un código en el que el dispositivo receptor puede checar periódicamente si está muestreando la línea en el tiempo exacto de llegada de cada bit. Estos códigos hacen que la línea cambie de estado muy frecuentemente. Los mejores códigos de reloj son aquellos en los cuales el estado de la línea cambia frecuentemente, debido a que este cambio de estado permite al receptor reajustar continuamente su señal.

El reloj simplemente proporciona una referencia para los 1's y 0's binarios individuales. La idea es tener un código con transiciones de nivel frecuentes y regulares en el canal. Las transiciones delinean las celdas de datos binarios en el receptor. El muestreo del receptor ocurre a más alta velocidad que la velocidad de los datos para definir con mayor precisión las celdas de bits.

1.3.8.5 Formato de las señales digitales.

En el mundo de hoy, la mayoría de los dispositivos terminales de datos o DTE's son dispositivos digitales. Esto significa que ellos mueven la información con señales digitales. Internamente la información es movida de un circuito a otro sobre alambres que son relativamente cortos y la información se mueve rápidamente. Una vez que la información sale del DTE, ésta debe moverse sobre una gran distancia, pero no se mueve tan rápido. Debido a que las necesidades cambian, diferentes formatos de señal se usan en diferentes posiciones de la trayectoria de comunicación de datos. Aunque hay muchos formatos de señales digitales en uso, los tres más comunes formatos de señales digitales son los que se mencionan a continuación:

Señales digitales de formato polar.

El formato polar es encontrado en la parte de la trayectoria de comunicación de datos llamado "interface" la cual esta localizada entre el DTE y el DCE (equipo terminal del circuito de datos). El puerto serial de la mayoría de las computadoras utiliza el formato polar. Las señales polares transmiten datos usando uno de los dos niveles de voltaje, un voltaje positivo para indicar "0" y un nivel de voltaje negativo para indicar "1".

Señales digitales de formato unipolar.

El formato unipolar es frecuentemente usado en forma interna en el DTE o computadora. Usando este formato, un 1 es representado por un nivel de voltaje positivo y un "0" por ausencia de voltaje.

Señales digitales de formato Bipolar.

Este formato utiliza voltajes positivos y voltajes negativos. Pero a diferencia de otros formatos, se utilizan voltajes positivos y negativos para transmitir un bit "1", los bits "0" son indicados por un nivel de voltaje cero. El formato Bipolar cambia la polaridad de los "1's" transmitidos. Esto es, el primer "1" es transmitido con un voltaje positivo, el siguiente "1" es transmitido con un voltaje negativo.

Código de inversión de marcas alternadas (AMI).

Usa pulsos de polaridad alternada para codificar 1's binarios.

La figura 1.22 muestra un código de no retorno a cero (NRZ). Puede observarse que el nivel de la señal permanece estable a través de toda la celda. En este caso el nivel de señal permanece en bajo para un bit 1 y va a alto para un bit 0 (voltajes opuestos son usados en muchos dispositivos). NRZ es un esquema de codificación de comunicación de datos usados ampliamente, debido a su relativa simplicidad y bajo costo. El código de NRZ puede ser polar o bipolar.

El código de retorno a cero (RZ) usualmente ocasiona un cambio del estado de la señal en cada bit representado como se observa en la figura. Puesto que los códigos de retorno a cero proporcionan una transición en cada bit representado, ellos tienen muy buenas características de sincronización. Sin embargo, una desventaja del código de retorno a cero es que este requiere de dos transiciones de señal en cada bit, lo que ocasiona que un código de retorno a cero necesite 2 veces el ancho de banda con respecto al ancho de banda de un código de no retorno a cero.

La figura 1.22 ilustra otro código muy popular encontrado en muchos sistemas de comunicación de hoy, el código Manchester. Este código se usa en el grabado de cintas magnéticas, enlaces de fibra óptica, líneas coaxiales y redes de área local.

La figura 1.22 muestra una ilustración de diversos esquemas de codificación binaria usados en la industria.

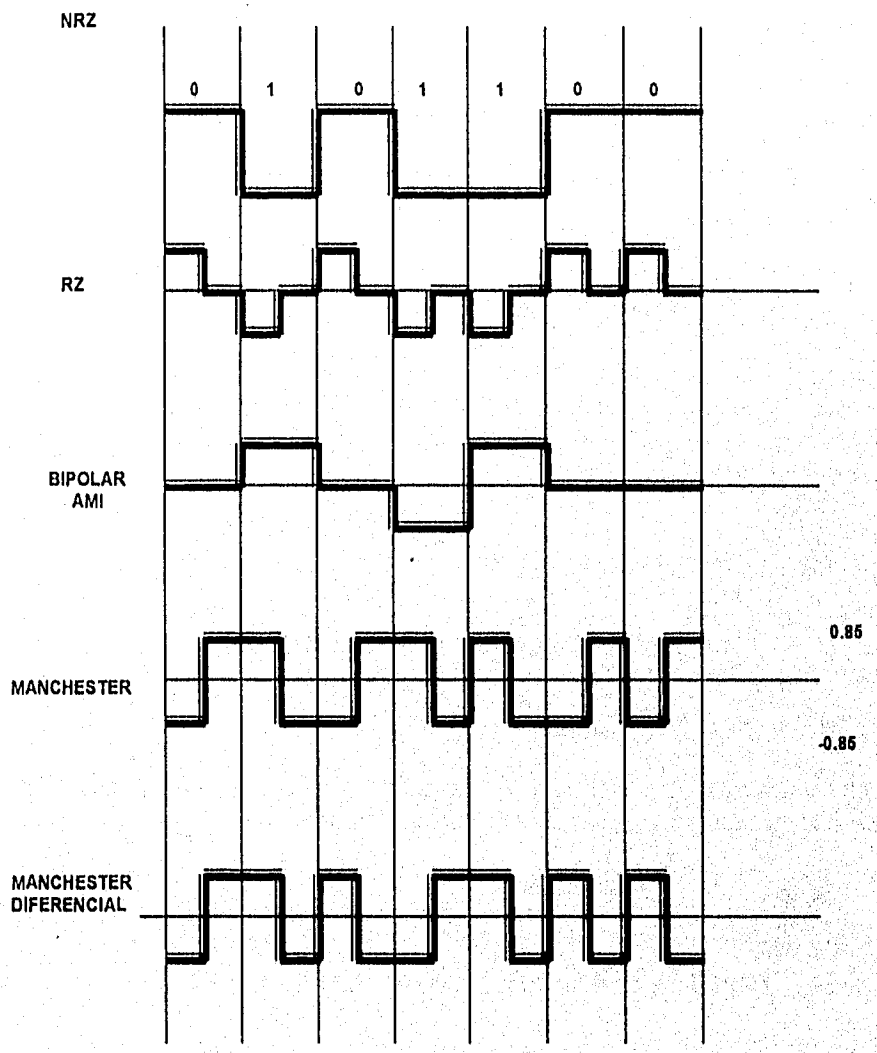


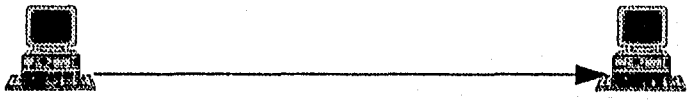
Figura 1.22
Códigos Digitales.

1.3.8.6 Métodos de intercambio de información.

Hay tres diferentes formas de intercambio de información entre dispositivos comunicándose. Las tres formas son:

Modo de comunicación Simplex.

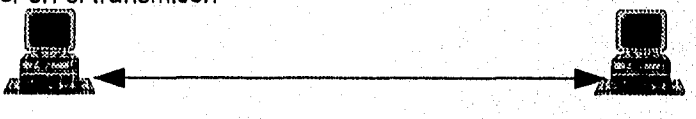
En este modo, la comunicación es en una sola dirección. No hay comunicación en dirección opuesta. El inconveniente es que no es posible verificar si los datos son recibidos correctamente.



MODO DE COMUNICACION SIMPLEX

Modo de comunicación Half Dúplex.

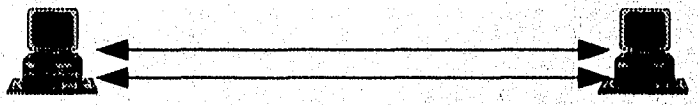
En este modo, la comunicación es en ambas direcciones, pero únicamente una dirección a la vez. Un dispositivo puede transmitir y el otro recibir. Cuando el transmisor termina de enviar su información se convierte en el receptor y el receptor en el transmisor.



MODO DE COMUNICACION HALF/DUPLEX

Modo de comunicación Full Dúplex.

En este modo, la comunicación es en ambas direcciones simultáneamente. ambos dispositivos pueden transmitir y recibir al mismo tiempo.



MODO DE COMUNICACION FULL/DUPLEX

1.3.8.7 Transmisión asíncrona.

Cuando se tiene comunicación asíncrona, los bits que representan un byte, conocidos como bits de datos, son precedidos y seguidos por bits de inicio, paro y paridad (Ver figura 1.23).

El número de bits representando un carácter varia de acuerdo al protocolo de comunicaciones en uso. Este es conocido como el número de bits de datos o longitud de palabra. Normalmente es de 7 u 8 bits. Cada carácter es enviado en un grupo consistiendo de un bit de inicio, el carácter (bits de datos), un bit de paridad opcional y uno o más bits de paro.

Bit de Inicio.

Un bit de inicio es siempre agregado al inicio de una trama para alertar al dispositivo receptor que los datos están llegando y para sincronizar al mecanismo que separa los bits individuales. Un bit de inicio es un espacio o bit binario cero. Un cero es transmitido como un voltaje positivo. El voltaje entre caracteres es negativo, por lo que el bit de inicio cambia de negativo a positivo.

Bits de datos.

Los estándares de comunicación permiten la transmisión de diferentes longitudes de caracteres o palabras. Cuando un software de comunicaciones pregunta por la longitud de palabra nos indica si queremos enviar caracteres de 7 u 8 bits. Si todos los datos a transmitir están en forma ASCII, caracteres de 7 bits son suficientes. Si los datos a ser transmitidos no son ASCII se necesitan usar caracteres de 8 bits. Los bits de datos se transmiten empezando por el bit menos significativo.

Bit de Paridad.

El chequeo de paridad es un método para probar si la transmisión está siendo recibida correctamente. El dispositivo enviante agrega un bit de paridad que es calculado de acuerdo al contenido de los bits de datos. El dispositivo receptor checa que el bit de paridad lleve efectivamente la relación correcta con los otros bits. La paridad puede ser calculada de la siguiente manera:

Paridad Par (Even).

Paridad par significa que sumando los bits de datos y el bit de paridad debe resultar en un número par. Por ejemplo la letra A cuya representación es 01000001. Cuando se suman los bits se obtiene como resultado 2 que es un número par, por lo que el bit de paridad agregado en la transmisión debe tener un valor de 0.

Paridad Impar (Odd).

Paridad impar significa que el total de bits de datos más la paridad debe resultar en un número impar. Usando el ejemplo de la letra A, el bit de paridad debe ser 1 para obtener un numero impar.

Sin Paridad (No Parity).

Sin paridad significa que no se utiliza bit de paridad.

Paridad Espacio (Space).

El bit de paridad se usa siempre establecido a cero.

Paridad Marca (Mark).

El bit de paridad se usa siempre establecido a uno.

Bits de Paro.

Al final del carácter y después del bit de paridad se envian los bits de paro. Estos pueden ser uno, uno y medio o dos bits de paro. Un bit y medio significa que la longitud del bit es más grande que la longitud del bit normal. Los bits de paro forzan a cierto espacio mínimo entre caracteres transmitidos. Ellos son enviados como 1's binarios o niveles de voltaje negativo.

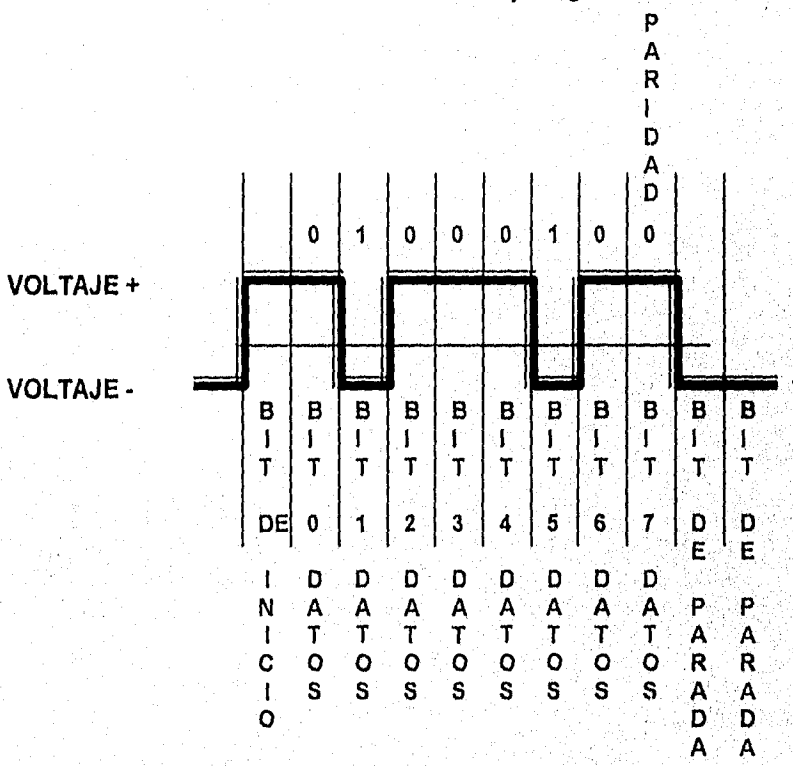


Figura 1.23
Protocolo de transmisión asíncrona.

1.3.8.8 Transmisión síncrona.

Cuando las máquinas transmiten una a otra continuamente, la transmisión síncrona puede dar la más eficiente utilización de línea. Aquí los bits de un carácter son seguidos inmediatamente por los bits del siguiente. No hay bits de inicio ni de alto, ni pausas entre caracteres. La cadena de caracteres es dividida en bloques. Todos los bits del bloque son transmitidos en iguales intervalos de tiempo. Las máquinas transmisora y receptora deben estar exactamente en sincronización por la duración del bloque de modo que la máquina receptora sabe cual es el primer bloque de datos.

La sincronización de las máquinas transmisora y receptora es controlada por osciladores en muchos sistemas. Antes de que un bloque sea enviado, el oscilador de la máquina receptora debe ser puesto exactamente en fase con el oscilador de la máquina transmisora. Esto se hace enviando un patrón o carácter de sincronización en el inicio del bloque. Una vez que los osciladores son sincronizados permanecen así hasta el fin del bloque.

Un bloque de bits enviado por transmisión síncrona debe tener ciertas características. Éste debe comenzar con el patrón o carácter de sincronización. Normalmente finalizará con el patrón o carácter de chequeo de error. La longitud del bloque puede ser fija o variable. Frecuentemente la longitud variable permite mejor utilización de línea. Si se usa un bloque de longitud fija será necesario agregar 0's para rellenar paquetes que contengan pocos datos. Si el bloque es de longitud variable, un patrón de fin de bloque debe ser usado para decirle a la máquina receptora que inicie las acciones necesarias para cuando el bloque finalice. Este patrón será enviado antes del patrón de chequeo de error.

Frecuentemente los datos son enviados en forma de caracteres o grupos de 6,7 u 8 bits (usualmente). Los patrones anteriores pueden ser de 1, 2 o más caracteres. Un esquema de transmisión, por ejemplo de caracteres de 6 bits, debe comenzar con los siguientes caracteres: 111111, 111110. Esto constituye el patrón de sincronización. Un circuito en la máquina receptora pasa todo el tiempo explorando la entrada de este patrón. Cuando el circuito detecta la entrada de este patrón, entonces el dispositivo sabe que el siguiente bit que reciba es el primer bit de datos. La codificación de caracteres debe ser tal que este patrón no se presente en ningún lugar de los datos del bloque.

El bloque finalizará con un patrón de fin de mensaje e inmediatamente después el patrón de chequeo de error de 6 bits. Cuando el texto esta siendo transmitido, el dispositivo receptor esta generando su propio patrón de chequeo de error, el cual es calculado de los caracteres recibidos. Al mismo tiempo, es examinado cada carácter recibido para ver si éste es el carácter de fin de mensaje. Cuando

este carácter es recibido, la máquina sabe que el siguiente carácter recibido es el patrón de chequeo de error y entonces compara éste con el patrón que había calculado. Si hay una diferencia, la máquina receptora envía un mensaje a la máquina transmisora solicitando retransmisión del mensaje.

La figura 1.24 muestra el formato de un bloque de texto transmitido en forma síncrona.

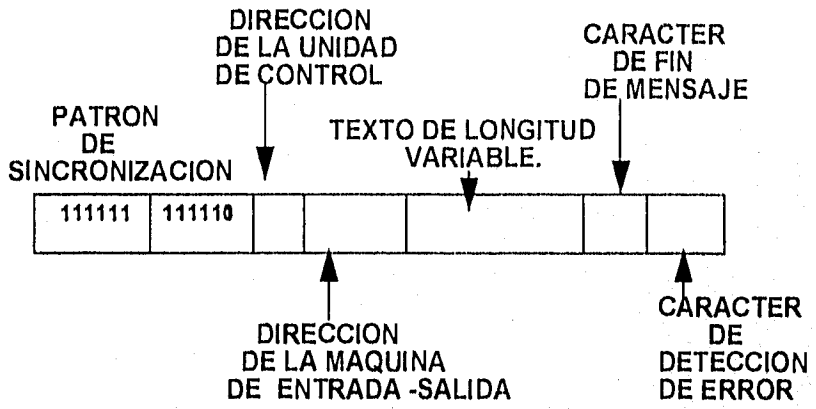


Figura 1.24
Formato típico de un bloque de transmisión síncrona.

Éste está diseñado para una línea en la cual muchas máquinas de entrada-salida están conectadas.

Estas máquinas están arregladas en grupos. Cada grupo está conectado a una unidad de control, la cual también está conectada a la línea por la cual se transmiten datos para y de la computadora. Después del patrón de sincronización en cada bloque viene la dirección de la unidad de control y la dirección de la máquina de entrada-salida para la cual el mensaje va o de la cual el mensaje viene. Es posible que mensajes transmitidos a la computadora puedan ser más largos que la máxima longitud de un bloque. En este caso son divididos en los bloques que sea necesario y un carácter es usado como identificador de segmento para enlazar éstos. La unidad de control coloca este identificador antes del los datos. El texto es de 6 caracteres y puede ser de una longitud hasta de 98 caracteres.

La transmisión síncrona es un método de transmisión orientada a bloque. Esto significa que la transmisión síncrona está relacionada con el envío y recepción de bloques de datos. El tamaño del bloque es dependiente del protocolo, dispositivos y facilidades usados.

El transmisor inicia la transmisión del bloque con un patrón de bits de preámbulo y usualmente termina con un patrón de bits. Los patrones de bits son información de control. Otra información de control es incluida, tal como caracteres de chequeo de bloque para detección y corrección de errores. Los datos más toda la información de control es llamada trama. El formato de la trama depende de si el modo de transmisión es orientado a carácter o a bit.

La transmisión orientada a carácter trata el bloque de datos como una secuencia de caracteres, usualmente caracteres de 8 bits y cuenta con códigos de control especiales que se utilizan durante la transmisión (Ver figura 1.25).

PAD	PAD	SYN	SYN	STX	MENSAJE DE TEXTO	ETX	BCC	PAD	PAD

Figura 1.25.
Trama de protocolo orientado a carácter.

Los protocolos orientados a bit operan siempre en modo transparente y cualquier valor deseado de bits puede ser enviado en el campo de información de la trama.
La transparencia es más fácil de lograr con protocolos orientados a bit que con protocolos orientados a carácter, debido a que los valores de bits de control siempre aparecen en un lugar fijo en la trama. Por lo tanto, cualquier configuración de bits deseado puede aparecer en cualquiera de los campos de la trama sin confusión (Ver figura 1.26).

BAN-DERA	DIRECCION	CONTROL	INFORMACION	SECUENCIA DE CHEQUEO DE TRAMA	BAN-DERA

Figura 1.26
Trama de protocolo orientado a bit.

1.3.8.9 Transmisión Isócrona.

Normalmente, un dispositivo que usa un formato de datos asíncrono esta conectado a un módem asíncrono. Sin embargo muchas aplicaciones de hoy tienen un dispositivo asíncrono, tal como una PC, conectada a un módem

síncrono. La combinación de un dispositivo usando formato orientado a carácter y un módem usando formato orientado a bloque es llamado isócrono.
Un ejemplo de Transmisión Isócrona es un dispositivo asíncrono conectado a un módem síncrono en un extremo del sistema de comunicaciones y un módem síncrono y un dispositivo síncrono en el otro extremo del sistema de comunicaciones.

Otro ejemplo de transmisión isócrona es un dispositivo asíncrono conectado a un módem síncrono en un extremo del sistema de comunicaciones y un módem síncrono y un dispositivo asíncrono en el otro extremo del sistema de comunicaciones.

1.3.8.10 DCE para un canal digital.

Los canales de comunicaciones digitales están creciendo muy rápidamente. Ellos pueden proporcionar fácil conectividad para diversos negocios o incluso nuestras propias casas. La meta es proporcionar una red global capaz de manejar voz, vídeo, y datos con conectividad total.

Sin embargo, los canales digitales no utilizan el mismo tipo de señal digital usada dentro de las computadoras o la proporcionada por el puerto serial de las computadoras. Es necesario por lo tanto un dispositivo DCE para cambiar la señal digital polar que sale del puerto serial de la computadora a una señal bipolar que sea compatible con el canal digital.

Hay tres dispositivos que pueden hacer a la señal compatible. Ellos son la Unidad de Servicio de Datos DSU, la Unidad de Servicio de Canal CSU y un dispositivo combinado de los dos anteriores DSU/CSU.

El DSU es un dispositivo que básicamente toma la señal digital polar que sale del puerto serial de la computadora y la convierte a una señal bipolar. El DSU o DSU/CSU es la interface entre los usuarios DTE y la red digital. El DSU contiene la circuiteria necesaria para proporcionar RS232-D o V.35.

Las funciones suministradas por el DSU son:

- Convierte la señal polar del DTE a señal bipolar para la red y el pulso bipolar de la red a pulso polar para el DTE.
- Reconoce violaciones del código bipolar.
- Recuperación de temporización de la red.
- Tiene la capacidad de proporcionar un loop o lazo cerrado para pruebas con la red.

CAPITULO II
REDES DE AREA LOCAL Y DE AREA AMPLIA

2.1 Consideraciones generales.

En los años 50's surge la computadora electrónica: grandes máquinas centrales (mainframes) que utilizan terminales tontas. En los 60's y 70's las minicomputadoras que siguen utilizando una computadora central y terminales tontas, y en los 80's las microcomputadoras.

Con el éxito de las microcomputadoras personales y desarrollos de software más elaborados, surgen las redes de computadoras.

2.2 Redes de área local.

¿Qué es una red de área local?

Una red de área local es un sistema de comunicación y transmisión de datos que permite a un número de dispositivos físicos independientes intercambiar información con una probabilidad de error pequeña.

¿Qué puede una red de área local conectar?
Computadoras personales, servidores de red, minicomputadoras, recursos compartidos, impresoras, plotters y otras redes.

Características de una red de área local.

- Compuesta por un conjunto de dispositivos que realizan tareas independientes.
- Compuesta por un conjunto de dispositivos que se comunican unos con otros.
- Limitada geográficamente hasta aproximadamente 10 km.
- Localizada en una sola oficina, un sólo edificio o muchos edificios dentro de una limitada área geográfica.
- Capaz de enviar un alto volumen de información a relativamente altas velocidades de 1 a 100 Mbits.
- Conectada por un medio continuo.
- Con mecanismo de broadcast.

2.3 Elementos que constituyen a las redes de área local.

a) Concentrador de cableado (HUB).

El concentrador es un equipo que sirve como nodo central para las redes de cable de par torcido (UTP). Este equipo contiene un conjunto de puertos jack

RJ45 en donde se conectan las estaciones de trabajo, el servidor de archivos y cualquier equipo que cumpla con el estándar IEEE802.3. La mayoría de los concentradores también tienen un puerto AUI (DB15) que es una interface adicional para poder incorporar el concentrador a una red con medio físico diferente al UTP con la ayuda de un transceiver.

b) Servidor de archivos (File Server).

El servidor de archivos es una máquina de computo cuyos recursos son dedicados para servir a estaciones de trabajo formando una red. El servidor contiene las aplicaciones tales como correo electrónico, bases de datos, procesadores de palabras y los archivos que los clientes crean. Cuando una estación de trabajo quiere hacer uso de estos recursos, tiene que conectarse al sistema de red que el servidor está corriendo y cargar las imágenes de las aplicaciones que necesita.

c) Estaciones de trabajo.

El término estación de trabajo es usado para PC's que tienen alguna conexión a recursos de computación fuera de ellos mismos. No importa si un módem de línea conmutada, un enlace de microondas o una tarjeta de red LAN proporciona la conexión.

d) Tarjetas de red (Network Interface Card NIC).

Las tarjetas de red son primordiales para la conexión de PC's como estaciones de trabajo, así como para la conexión de impresoras en red.

Una tarjeta de red se instala en una PC en una de las ranuras de expansión de la tarjeta madre. Una vez que se encuentra instalada se procede a la configuración por software de parámetros necesarios en la tarjeta para su interacción con la PC (Ver figura 2.1).

Los parámetros a configurar en la tarjeta de red son:

Dirección base de entrada-salida (I/O BASE ADDRESS).

La tarjeta requiere 32 contiguas direcciones de entrada-salida. La dirección base se usa para asignar el inicio de este espacio de direcciones. Este espacio de direcciones se utiliza para la comunicación entre la computadora y la tarjeta de red y poder accesar a los diferentes registros internos de la tarjeta para configuración del envío y recepción de datos. El rango de direcciones que es posible usar es de 200-3E0.

Dirección base de RAM (RAM BASE ADDRESS).

Es un espacio de memoria RAM de 16 KB comprendida en el área de memoria superior y que sirve como buffer de datos para la tarjeta. El rango de direcciones normalmente permitido es de la C8000 a la DFFFF.

Nivel de interrupción (IRQ).

A cada dispositivo o periférico en una computadora se le asocia un nivel de interrupción que le permite solicitar atención del CPU o microprocesador. Los valores posibles son 2,3,4,5,7,10,11 y 15. Debe notarse que algunas de las interrupciones mencionadas se usan por dispositivos de la PC y hay que elegir un valor que no tenga conflicto.

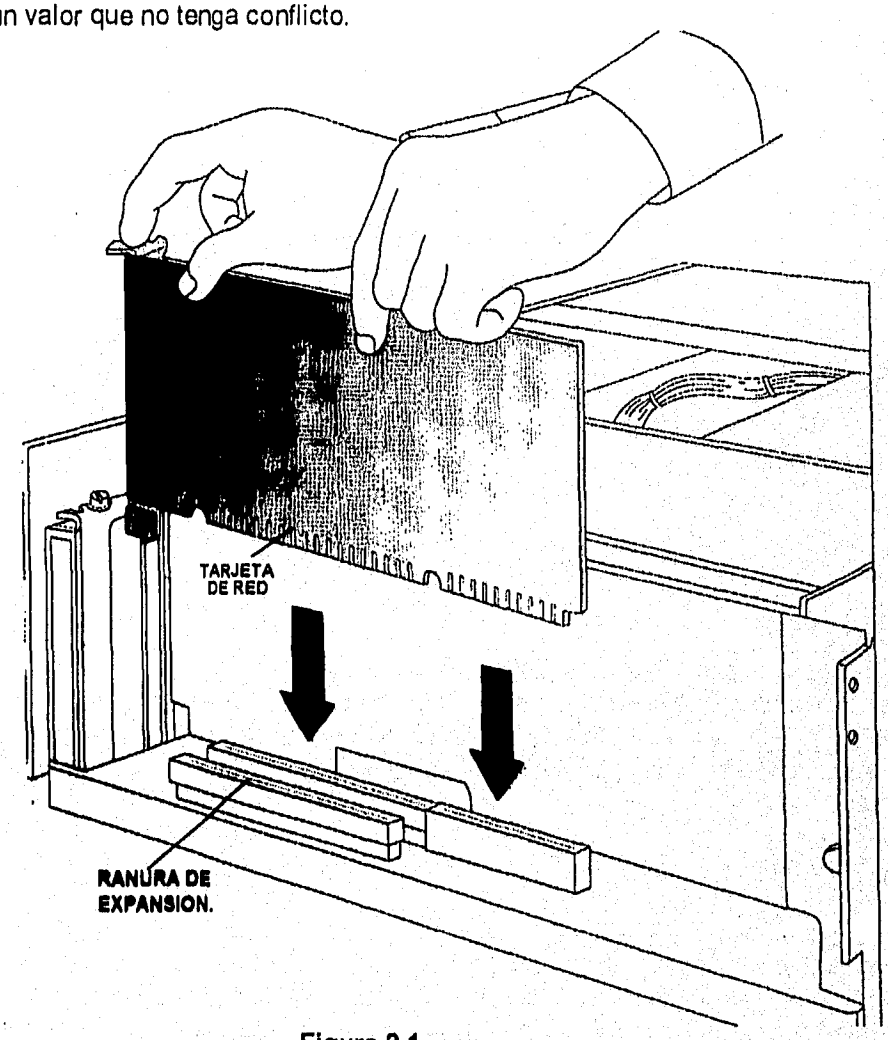


Figura 2.1
Colocación de una tarjeta de red en una PC.

e) Cableado.

Cable de par torcido no blindado (UTP).

Un par de alambres de cobre aislados torcidos uno respecto del otro forman un par torcido. Dos o más pares torcidos forman un cable de par torcido. El cable de par torcido se encuentra protegido por una cubierta exterior aislante. El conector más usado para la conexión de cables de par torcido es el RJ45 de 4 pares que es el conector que se implementa en las tarjetas de red (Ver figura 2.2).

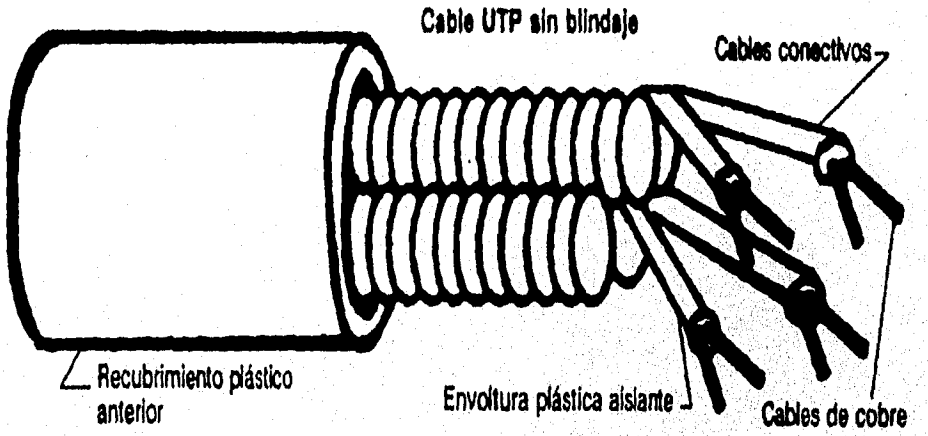


Figura 2.2
Cable de par torcido UTP.

Cable de par torcido blindado (STP). Los cables de conductores gruesos y muy bien cubiertos por el jacket son denominados del tipo STP. Estos son más caros que los UTP y menos flexibles . Deben tener una impedancia entre 85 y 112 Ohms a 10 MHZ. Deben presentar una atenuación máxima de 11db/110m a 10 MHZ.

Cable coaxial.

El cable coaxial se forma por un alambre conductor básico y una cubierta formada por una malla de alambre que actúa como tierra. El alambre conductor y la tierra se encuentran separados por un aislante plástico y, finalmente todo el conjunto está protegido por una cubierta exterior aislante llamada jacket (Ver figura 2.3).

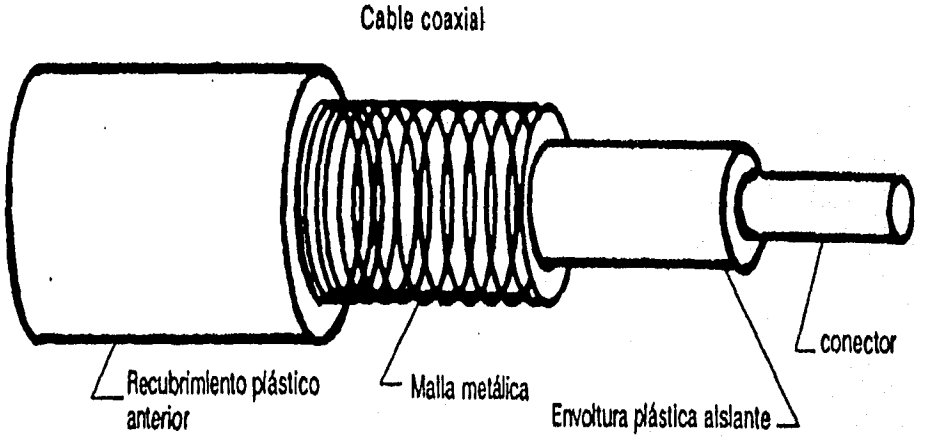


Figura 2.3
Constitución de un cable Coaxial.

Los cables coaxiales pueden ser de varios tipos y anchos. Sin embargo, su principal característica es que pueden transportar una señal eléctrica a mayor distancia entre más grueso es el conductor. El tipo de conector más usado para la conexión de estos cables es el BNC. Diversos estándares de cable coaxial son usados en redes, los más conocidos son los siguientes:- RG8 y RG11 son Ethernet cable grueso de 50 ohms.- RG-58 es cable delgado Ethernet de 50 Ohms.- RG-59 es usado para televisión por cable y enlaces digitales E0 y E1 de RDI en México.- RG-62 es usado para Arcnet de 93 ohms.

Cable de fibra óptica.

La tercera tecnología de cables que se utiliza en las redes locales es la fibra óptica. Normalmente se emplea por tres razones básicas: para aquellos casos en los que las grandes distancias son un factor determinante para la implantación de una red local; cuando se requiere una alta capacidad de aplicaciones de comunicación y cuando el ruido o cualquier tipo de interferencia son factores a considerar. El cable de fibra óptica se compone de una fibra muy delgada elaborada de dos tipos de vidrio con diferentes índices de refracción, uno para la parte interior y otro para la parte exterior. Esta diferencia en la refracción previene que la luz penetre en una parte de la fibra óptica hasta la parte exterior evitando así la pérdida de la información. La fibra óptica a su vez, se encuentra cubierta por una placa aislante y protectora en la parte más exterior para darle más integridad estructural al cable. Es sin embargo, extremadamente flexible ya que se pueden realizar giros hasta de 360 grados sin problemas de afectación en el cable (Ver figura 2.4).

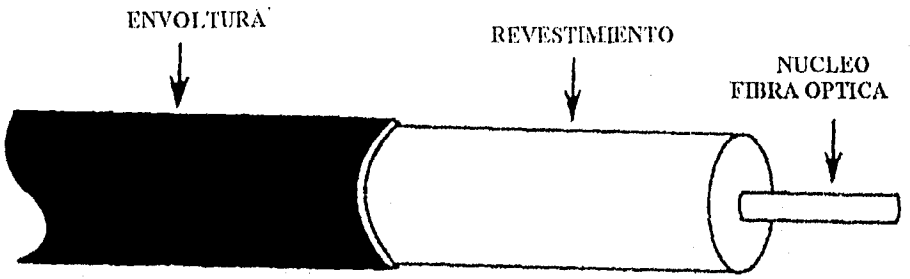


Figura 2.4
Cable de fibra óptica.

El diámetro de la fibra interior más comúnmente usado es de 62.5 micras y el de la fibra exterior de 125 micras (fibra multimodo).

Para la transmisión de información en redes locales vía fibra óptica se utiliza una fibra como transmisor y otra como receptor. Es por esto que se producen en conjuntos de mínimo dos fibras por cable. El tipo de conector de uso más común es el conector tipo ST.

Las distancia máximas obtenidas para las redes locales son de 2000 metros de nodo a nodo sin el uso de amplificadores.

f) Transceivers.

Son pequeños dispositivos que nos permiten convertir de una interface Ethernet con conector DB15 (conector AUI) a una interface con conector RJ45 para UTP, BNC para coaxial y ST para fibra óptica.

Entre las tareas de los transceivers se encuentra la de permitir conectar una estación de trabajo al medio físico.

Los transceivers generan las señales respectivas para los bits de salida, reciben los bits de las tramas de entrada, detectan la presencia de portadora en el medio y detectan colisiones en el medio.

g) Minicomputadoras.

Están diseñadas para proporcionar un proceso centralizado. Todos los usuarios comparten el poder de un procesador central, y una sola copia de software de aplicación corre en el CPU central. Fueron hechas para manejar de decenas a cientos de usuarios con terminal a la vez.

h) Mainframes.

El mainframe es una computadora diseñada para conversar con cientos o miles de terminales a la vez. Las terminales tontas enlazadas que necesitan usar la aplicación deben compartir una copia del CPU central. Los Mainframes se caracterizan por tener gran cantidad de almacenaje de disco y de cinta magnética. Fueron construidos para servir a grandes WAN, aunque en los días de hoy pueden ser encontrados sirviendo grandes LAN.

i) PC's.

Computadoras personales con tarjeta de red que les permite conectarse a una red de área local.

j) Servidores de terminales.

Los servidores de terminales son equipo con puertos seriales asíncronos con interfaces RS232 o RS423 que nos permiten conectar terminales asíncronas (tontas). El servidor de terminales tiene además un puerto que nos permite conectarnos a una red Ethernet, normalmente un puerto AUI (DB15). En resumen la función del servidor de terminales es la de permitir la comunicación de una minicomputadora o mainframe con las terminales asíncronas usando la red de área local.

k) Sistema operativo de red.

El sistema operativo de red es el corazón y alma de la red. El hardware del sistema proporciona las trayectorias de datos y las plataformas en la red, pero el sistema operativo es el encargado de controlar todo lo demás. La funcionalidad, la facilidad de uso, el rendimiento, la administración, la seguridad de los datos y la seguridad de acceso, dependen del sistema operativo.

Actualmente existen en el mercado varios sistemas operativos de red, en los que se destacan Netware de Novell, LAN Server de IBM, LAN MANAGER de Microsoft, 3+OPEN de 3COM, VINES de BANAYAN y APPLESHARE de APPLE.

Componentes del sistema operativo.

El sistema operativo de la red se engloba en dos componentes básicos. El sistema operativo del servidor y el sistema de la estación de trabajo. El sistema operativo del servidor de red se ejecuta dentro de la máquina del servidor y procesa todos los servicios. Los componentes de la estación de trabajo se ejecutan en ésta, y establecen la conexión con la red y el servidor, y controlan el flujo de las comunicaciones. Estos componentes pueden ser proporcionados por

el fabricante de las tarjetas de interface que se instalan en las estaciones de trabajo o por el sistema operativo de red, o por una combinación de ambos.

l) Equipos de interconexión de redes.

Repetidores, Puentes, Enrutadores y Gateway's.

Estos equipos permiten interconectar redes de área local y de área amplia y se describen ampliamente en el capítulo de interconexión de redes.

2.4 Estándares de redes de área local.

En 1980 el Instituto de Ingenieros Eléctricos y Electrónicos mejor conocido como IEEE, tomó la tarea de definir los estándares de redes de área local (LAN). En 1985 el IEEE publico 4 estándares separados. El IEEE802.2, IEEE802.3, IEEE802.4 e IEEE802.5 (Ver figura 2.5).

MODELO OSI	MODELO IEEE802	ESTANDARES IEEE802				
RED	IEEE802.1 RELACION DE ESTANDARES IEEE, ADMINISTRACION					E
CAPA DE ENLACE	CONTROL DE ENLACE LOGICO. LLC	IEEE802.2			OTROS ESTANDARES 802	I N T E R C O N E X I O N
	CONTROL DE ACCESO AL MEDIO MAC	IEEE802.3 CSMA/CD	IEEE802.4 TOKEN BUS	IEEE802.5 TOKEN RING		
CAPA FISICA	CAPA FISICA	CAPA FISICA 802.3	CAPA FISICA 802.4	CAPA FISICA 802.5		

Figura 2.5
Cuadro de estándares de redes de área local.

Las especificaciones del proyecto IEEE 802 principalmente relacionan las capa uno y dos del modelo de OSI. Una característica distintiva es que el IEEE divide la capa dos en dos subcapas. Una parte define control de acceso al medio (generalmente llamada la subcapa MAC), mientras que la otra parte

(generalmente llamada la subcapa LLC) define todas las otras funciones de capa 2.

Desde 1985 el IEEE ha seguido investigando para agregar más estándares de redes que a continuación se mencionan:

IEEE802.1 Administración de sistemas e interconexión.
IEEE802.2 Control de enlace lógico.
IEEE802.3 Red usando acceso CSMA/CD para Ethernet.
IEEE802.4 Red de bus (Arcnet) usando acceso Token Passing.
IEEE802.5 Red de anillo (Token Ring) usando acceso Token Passing.
IEEE802.6 Redes de área metropolitana.
IEEE802.7 Tecnología de banda ancha.
IEEE802.8 Tecnología de fibra óptica.
IEEE802.9 Voz integrada y datos.
IEEE802.10 Seguridad de LAN.
IEEE802.11 Redes inalámbricas.
IEEE802.12 Fast Ethernet.
IEEE802.14 Ethernet 100Base-VG.

Además de la estandarización de la organización IEEE, la ISO ha adoptado los estándares de redes de área local como se muestra en la tabla siguiente:

IEEE	Descripción	Equivalente ISO
802	Introducción y arquitectura.	
802.1a	Metodología de prueba de conformidad.	
802.1b	Administración LAN.	
802.1d	Puentes MAC.	
802.1e	Protocolo de carga del sistema.	
802.1i	Suplemento de puente MAC para FDDI.	
802.2	Control de enlace lógico.	8802-2
802.3	10base5 CSMA/CD.	8802-3
802.3a	10base2 CSMA/CD.	8802-3
802.3c	Repetidores para 10 Mbps.	8802-3
802.3d	Repetidor de fibra óptica FOIRL.	8802-3
802.3e	1base5.	8802-3
802.3h	Administración de capa para 10 baseT.	
802.3i	Consideraciones del sistema para 10 baseT.	
802.3k	Administración de capa para repetidores de 10 Mps.	
802.3l	Protocolo MAU 10baseT.	
802.4	Redes en bus Token Passing.	8802-4
802.5	Redes en anillo Token Ring.	8802-5

2.4.1 Estándar IEEE802.2 (subcapa LLC).

La subcapa de control de enlace lógico LLC es responsable de proporcionar una trayectoria de transmisión libre de error a la capa de red. Dentro de la estructura IEEE, estas funciones son proporcionadas por la especificación del protocolo IEEE 802.2.

a) Formato de la unidad de datos del protocolo LLC.

La trama consiste de hasta 4 campos. Como todos los protocolos de la capa de enlace, IEEE 802.2. ofrece varios servicios a la capa de red. Estos servicios son obtenidos en lugares llamados puntos de acceso al servicio (SAP). Los SAP's son como cajas, cada SAP tiene una dirección. Para LLC, los SAP's únicamente identifican un proceso de la capa de red. Para procesos de la capa de red, los SAP's son lugares para dejar mensajes acerca del servicio deseado (Ver figura 2.6).

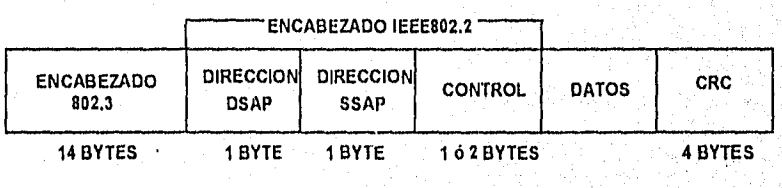


Figura 2.6
Formato de la unidad de datos LLC.

El primer campo de la trama es el punto de acceso al servicio destino (DSAP) y tiene una longitud de un byte. El DSAP especifica el proceso de la capa de red receptor.
El segundo campo es el punto de acceso al servicio fuente (SSAP) y tiene una longitud de un byte. El SSAP especifica el proceso de capa de red fuente.

Los DSAP's y SSAP's son asignados por la oficina de estándares del IEEE. Actualmente sólo 7 bits son usados para el DSAP y SSAP el bit menos significativo tiene una función especial. El bit menos significativo del DSAP indica si el destino es una dirección individual o un grupo. El bit menos significativo del SSAP indica si la unidad de datos LLC contiene una solicitud o una respuesta. LLC usa estos bits para indicar como procesar ciertos bits en el campo de control.

b) Valores de los puntos de acceso al servicio más comunes (SAP'S).

NUMERO DE SAP	*VALOR DEL SAP*
00	IEEE NULL SAP
02	IEEE MANAGEMENT ISAP (INDIVIDUAL)

NUMERO DE SAP	*VALOR DEL SAP*
03	IEEE MANAGEMENT GSAP (GRUPO)
04	SNA
05	SNA
06	IP
07	IP
08	SNA
09	SNA
0C	SNA
0D	SNA
OE	PROWAY_2B
10	NETWARE
42	BPDU (BRIDGE PROTOCOL DATA UNIT)
43	BPDU (BRIDGE PROTOCOL DATA UNIT)
4E	EIA RS511
7E	ISO_8202(X.25)
80	XNS
81	XNS
86	LLC
87	LLC
8E	PROWAY
AA	SNAP
AB	SNAP
BC	VINES IP (VIP)
BD	VINES IP (VIP)
E0	XNS
E1	XNS
FO	NETBIOS
F1	NETBIOS
F4	IBM NM
FE	ISO TRANPORT LAYER

c) El campo de control puede contener uno o dos bytes, dependiendo del servicio suministrado o solicitado.

d) El cuarto campo que puede o no estar presente es el campo de información procedente de la capa de red.

e) Tipos de servicio LLC.

El protocolo LLC proporciona tres tipos de servicio.

Servicio sin conexión y sin reconocimiento (Tipo 1).
Servicio sin conexión y con reconocimiento (Tipo 3).
Servicio orientado a conexión (Tipo 2).

Todas las redes 802 deben proporcionar servicio sin conexión y se clasifican como redes tipo 1. Opcionalmente el servicio orientado a conexión puede ser proporcionado y las redes se clasifican como tipo 2. Las redes del tipo 1 no proporcionan reconocimientos, control de flujo y recuperación de errores. La mayoría de las redes del tipo 1 usan un protocolo de alguna capa del modelo de OSI más alta (por ejemplo la capa de transporte). Las redes tipo 2 proporcionan reconocimientos, control de flujo y recuperación de errores.

Las estaciones individuales pueden soportar más de un servicio.

f) Control de flujo.

Técnica de alto y espera.
Técnica de ventanas deslizantes

g) Comandos y respuestas LLC.

Los comandos y respuestas establecidos en el campo de control LLC, dependen de si la LAN es del tipo 1 o del tipo 2 y se muestran a continuación:

Redes LAN Tipo 1.

Comandos	Respuestas
UI	
XID	XID
TEST	TEST

Redes LAN tipo 2.

Comandos	Respuestas	
I	I	FORMATO Información
RR	RR	FORMATO Supervisión
RNR	RNR	
REJ	REJ	
SABME	UA,FRMR	FORMATO no numerado
DISC	UA,DM	

Trama de información (I).

Se usa para transmitir información de usuario entre dos dispositivos. La trama de información puede también reconocer recepción de datos de la estación transmisora.

Receive Ready (RR).

Es usado por la estación primaria o secundaria para indicar que está lista para recibir una trama de información y/o para reconocer tramas recibidas anteriormente usando el campo N(R). Si la estación había indicado estado de ocupado con un comando Receive Not Ready, entonces usa el comando RR para indicar que ahora está libre para recibir datos.

Receive Not Ready (RNR).

Es usado por una estación para indicar una condición de ocupado. Éste le dice a la estación transmisora que la estación receptora no es capaz de recibir datos entrantes adicionales. La trama RNR puede reconocer tramas previamente transmitidas usando el campo N(R). La condición de ocupado puede ser limpiada enviando la trama RR.

REJ (Reject).

Trama de rechazo o solicitud de retransmisión (tipo de servicio 2). Comando o respuesta.

SABME (Set Asynchronous Balanced Mode Extended).

Trama de establecimiento de modo balanceado asíncrono extendido, o solicitud para conexión de enlace de datos entre dos nodos usando LLC (tipo de servicio 2). Comando únicamente.

DISC (Disconnect).

Trama de desconexión, termina una conexión de enlace de datos (tipo de servicio 2). Comando únicamente

DM (Disconnect Mode).

Trama de modo desconectado, respuesta negativa a un SABME, indicando que un nodo no puede establecer la solicitud de conexión de enlace de datos (tipo de servicio 2). Respuesta únicamente.

UA (Unnumbered Acknowledgment).

Trama de reconocimiento no numerada, una respuesta positiva a una trama SABME, indicando que un nodo acepta la solicitud de conexión de enlace de datos (tipo de sevicio 2). Respuesta únicamente.

FRMR (Frame Reject).

Trama de indicación de rechazo de trama, la cual ocurre cuando una trama LLC invalida es recibida. El nodo que la recibe emite ya sea un DISC o SABME en respuesta. (tipo de servicio 2). Respuesta únicamente.

UI (Unnumbered Information).

Trama de información no numerada, usada para envío de datos a otros nodos usando LLC, basado en DSAP (tipo de servicio 1). Comando únicamente.

XID (Exchange Station Identification).

Trama de identificación de estación, usada para intercambio de información de dos nodos sin importar que tipos de servicios ellos soporten (tipo de servicio 1). Comando o respuesta.

TEST.

Una trama de prueba, con un campo de información opcional para calificar la trayectoria de transmisión LLC-LLC (tipo de servicio 1). Comando o respuesta.

2.4.2 Estárdar IEE802.3 y ETHERNET.

Ethernet fué inventado en 1970. La versión 1.0 fué liberada por Digital, Intel y Xerox en 1980. La versión 2.0 de Ethernet apareció en 1982 y como se mencionó la especificación IEEE 802.3 surgió en 1985.

Estos estándares cubren los protocolos de capa física y de la subcapa MAC.

Definen el control de acceso al medio por CSMA/CD.
Definen la estructura de la trama.
Definen las características del medio físico.

IEEE 802.3 esta basado en Ethernet, pero define opciones de múltiples capas físicas. En redes cumpliendo el estándar del IEEE, los servicios de enlace son generalmente proporcionados por la especificación IEE802.2. Hoy el término Ethernet es frecuentemente usado para aplicarse a todas las redes LAN con acceso al medio CSMA/CD.

a) Ethernet e IEEE802.3 utilizan control de acceso al medio CSMA/CD.

El algoritmo CSMA/CD funciona como sigue:

Si una estación no está transmitiendo, ésta monitorea la línea. Si la línea está ocupada espera. Una vez que la línea está libre la estación espera 9.6 microsegundos (para proporcionar espaciamiento entre tramas) y comienza la transmisión de una trama. Durante la transmisión de la trama, la línea es monitoreada por la estación transmisora para detectar si hay colisiones.

Las colisiones pueden únicamente ocurrir durante una ventana de colisión que existe durante la parte inicial de la transmisión. La ventana de colisión es el resultado de un tiempo finito que es requerido por la señal a ser propagada a través de la red. Durante este periodo otra estación puede considerar que la línea está libre y por lo tanto comenzar a transmitir.
Cuando una colisión es detectada la transmisión prosigue por entre 32 y 48 bits más antes de que ésta es abortada. Esta continuación conocida como señal de tráfico, garantiza que la duración de la colisión es suficiente para garantizar que todas las estaciones transmisoras en la red están consientes de esto.

Para cualquier configuración de red el retardo de ida y vuelta debe de ser menor a 46.4 microsegundos.

En Ethernet una colisión ocurre únicamente si dos estaciones comienzan a transmitir dentro de un intervalo de tiempo igual al retardo de propagación entre dos estaciones. La máxima distancia entre transceivers es 2500 mts, la ventana de colisión está limitada a 23 microsegundos.
Una estación puede estar segura de que no hubo colisión si no detecta nada dentro de un tiempo de propagación de ida y vuelta de 46.4 microsegundos. El tiempo de un bit es de 0.1 microsegundos, la decisión de detección de colisión es hecha dentro de los primeros 464 bits de una trama. La máxima longitud de una trama es 12,144 bits.

Antes de transmitir una trama de datos la capa física debe insertar un preámbulo de 64 bits de modo que los receptores en la red puedan sincronizarse. El preámbulo consiste de 1's y 0's finalizando en dos 1's para indicar el inicio de trama.

Preámbulo.

10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010 (AAAAAAAAAAAAAAAA Hex.).

Delimitador de inicio de trama.

10101011 (AB Hex.).

El retardo tiene un efecto muy importante en el comportamiento del protocolo. Existe una pequeña posibilidad de que, justo después de que una estación empiece a transmitir otra estación llegue a estar lista para hacerlo y escuche el canal. Si la señal correspondiente a la primera estación todavía no ha alcanzado a la segunda, esta última detectara un canal desocupado y también empezará a transmitir dando como resultado una colisión. Cuanto mayor sea el retardo de propagación más importante llegará a ser el efecto y, por consiguiente el protocolo tendrá un rendimiento peor.

b) Codificación Manchester (capa física).

Este tipo de codificación es usado por las redes Ethernet e IEEE 802.3 y se muestra en la figura 2.7.

En esta codificación digital cada periodo de bit se divide en dos intervalos iguales. Un bit binario con valor de 1 se envía con un voltaje alto durante el primer intervalo y bajo durante el segundo. Un bit binario de valor de 0 es precisamente lo contrario: es decir, primero se tiene un voltaje bajo y después uno alto. Con este esquema se asegura que todos los periodos de bit tengan una transición en la parte media propiciando así una excelente sincronización entre el receptor y transmisor. Una desventaja de la codificación Manchester es que requiere el doble de ancho de banda del necesario para una codificación binaria directa, dado que los pulsos tienen la mitad de ancho.

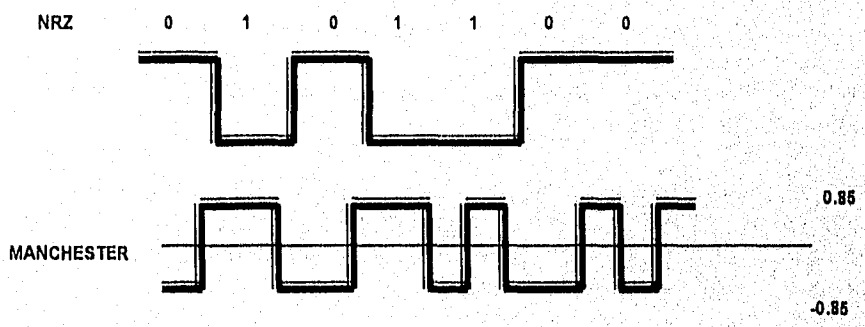
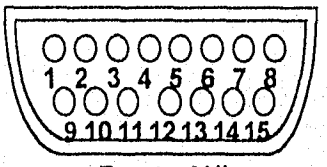


Figura 2.7
Codificación Manchester.

Las interfaces disponibles en la capa física de los equipos conectados a una red de área local Ethernet, pueden ser AUI, RJ45, BNC y F.O.

Descripción de señales del puerto AUI (Attachment Unit Interface).

1 Blindaje para el par torcido de control (GND).
2 Presencia de colisión +.
3 Transmisión +.
4 Blindaje para el par torcido de recepción (GND).
5 Recepción +.
6 Referencia de alimentación.
7 No conectado.
8 No conectado o GND.
9 Presencia de colisión -.
10 Transmisión -.
11 Blindaje para el par torcido de Transmisión (GND).
12 Recepción -.
13 Alimentación (11V a 16V).
14 Blindaje para el par torcido de alimentación (GND).
15 No conectado o GND.



Puerto AUI.

Descripción del puerto RJ45.

El conector físico utilizado para las redes de área local de par torcido es el conector subminiatura de 8 pines RJ45 que se toma de la especificación ISO 8877desarrollada para la Red Digital de Servicios Integrados ISDN y que la recomendación I.430 del CCITT adopta también.

El EIA/TIA - 568 ha adoptado dos esquemas de alambrado definidos por el TIA e AT&T. Estos son similares pero los pares 2 y 3 están invertidos. Ambos esquemas soportan aplicaciones ISDN.

EIA 568A (TIA)

Identificador de par	Polaridad	Pin	Código de colores.
T1	+	5	Blanco-Azúl (Par 1)
R1	-	4	Azúl (Par 1)
T2	+	3	Blanco-Naranja (Par 2)
R2	-	6	Naranja (Par2)

T3	+	2	Blanco-Verde (Par 3)
R3	-	7	Verde (Par 3)
T4	+	1	Blanco-Café (Par 4)
R4	-	8	Café (Par 4)

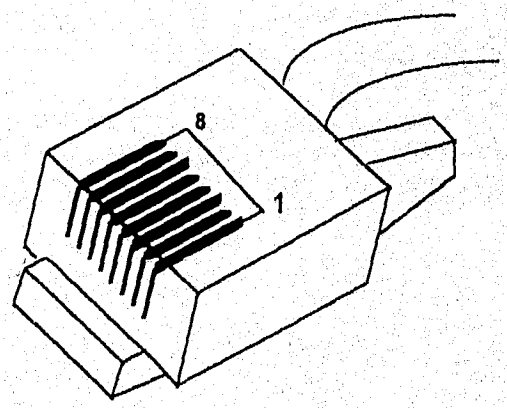
EIA 568 B (AT&T).

Identificador de par	Polaridad	Pin	Código de colores.
T1	+	5	Blanco-Azúl (Par 1)
R1	-	4	Azúl (Par 1)
T2	+	1	Blanco-Naranja (Par 2)
R2	-	2	Naranja (Par2)
T3	+	3	Blanco-Verde (Par 3)
R3	-	6	Verde (Par 3)
T4	+	7	Blanco-Café (Par 4)
R4	-	8	Café (Par 4)

10 BASET (IEEE802.3)

El esquema de alambrado 10 BASE-T especifica un Jack RJ45 de 8 posiciones usando 2 pares del esquema de alambrado EIA/TIA 568. Estos son los pares 2 y 3 de los esquemas AT&T y TIA.

Identificador de par	Pin	Código de colores.
T1	1	Blanco-Azúl (Par 1)
R1	2	Azúl (Par 1)
T2	3	Blanco-Naranja (Par 2)
R2	6	Naranja (Par2)



Conector RJ45 para cable UTP.

La interface BNC sólo tiene el centro que es la Tx/Rx y la malla que corresponde a la señal GND.

La fibra óptica consta de una fibra óptica para la transmisión Tx y una fibra óptica para la recepción Rx.

2.4.3 Formatos de las tramas Ethernet e IEEE 802.3.

Los formatos para la tramas Ethernet e IEEE802.3 se muestran en las figuras 2.8a y 2.8b respectivamente y sus campos se describen a continuación.

FORMATO DE TRAMA PARA ETHERNET

PREAMBULO	DIRECCION DESTINO	DIRECCION FUENTE	TIPO	DATOS	CHEQUEO DE REDUN-DANCIA CI-CLICA.
8 BYTES	6 BYTES	6 BYTES	2 BYTES	46-1500 BYTES	4 BYTES

a)

FORMATO DE TRAMA PARA IEEE802.3

PREAMBULO	DELIMITADOR DE INICIO DE TRAMA	DIRECCION DESTINO	DIRECCION FUENTE	LONGITUD	ENCABEZADO 802.2 Y DATOS	CHEQUEO DE REDUN-DANCIA CI-CLICA.
7 BYTES	1 BYTE	2 ó 6 BYTES	2 ó 6 BYTES	2 BYTES	46-1500 BYTES	4 BYTES

b)

Figura 2.8
Formatos de tramas Ethernet e IEEE802.3.

a) Preámbulo y delimitador de inicio de trama.

Para iniciar una trama, el MAU/Transceiver transmite un preámbulo de 8 bytes en Ethernet y el IEEE802.3 un preámbulo de 7 bytes, consistiendo de unos y ceros alternativos. El siguiente byte de IEEE802.3 es el delimitador de inicio de trama que es como el preámbulo, excepto que éste finaliza con dos unos consecutivos. Estos bits anuncian que viene una trama y sincronizan a todos los receptores en la LAN.

b) Dirección de destino.

Esta dirección es de 6 bytes para Ethernet y de 2 o 6 bytes para IEEE802.3 e indica el destino donde debe ser entregada la información de la trama.

c) Dirección fuente.

Es la dirección de quien envía la trama, como la dirección destino, esta dirección es de la misma longitud para cada estándar. IEEE es responsable de asignar los primeros 3 bytes para cada vendedor. La dirección se encuentra en la ROM de las tarjetas de red en los puertos de los equipos de comunicación de redes y cada vendedor asigna 3 bytes adicionales a los asignados por el IEEE para formar un número de 6 Bytes.

Ejemplos de direcciones de hardware Ethernet para diferentes vendedores (3 octetos).

00000C DIRECCION DE HARDWARE 00000C, EQUIPO CISCO
00001B DIRECCION DE HARDWARE 00001B, EQUIPO NOVELL
00001D DIRECCION DE HARDWARE 0000ID, EQUIPO CABLETRON
000093 DIRECCION DE HARDWARE 000093, EQUIPO PROTEON
0000A2 DIRECCION DE HARDWARE 0000A2, EQUIPO WELLFLEET
0000AA DIRECCION DE HARDWARE 0000AA, EQUIPO XEROX
0000C0 DIRECCION DE HARDWARE 0000C0, EQUIPO WESTERN DIGITAL
0000D8 DIRECCION DE HARDWARE 0000D8, EQUIPO 3COM
080002 DIRECCION DE HARDWARE 080002, EQUIPO 3COM
080009 DIRECCION DE HARDWARE 080009, EQUIPO HP
08000A DIRECCION DE HARDWARE 08000A, EQUIPO NESTAR
08000B DIRECCION DE HARDWARE 08000B, EQUIPO UNISYS
080010 DIRECCION DE HARDWARE 080010, EQUIPO AT&T
08001E DIRECCION DE HARDWARE 08001E, EQUIPO APOLO
080020 DIRECCION DE HARDWARE 080020, EQUIPO SUN
08002B DIRECCION DE HARDWARE 08002B, EQUIPO DEC
080038 DIRECCION DE HARDWARE 080038, EQUIPO BULL
08005A DIRECCION DE HARDWARE 08005A, EQUIPO IBM
08006E DIRECCION DE HARDWARE 08006E, EQUIPO EXCELAN

d) Longitud de datos.

El campo de longitud de 2 bytes indica el número de bytes de datos que se encuentran antes del chequeo de secuencia de trama. Este número dice cuantos bytes de datos están en la trama. Este número no incluye los bytes de relleno que pueden existir dentro del campo de datos. La capa de MAC usa este número para delinear el paquete IEEE802.2.

e) Tipos de datos.

Las tramas Ethernet utilizan este campo, en lugar del campo de longitud, para indicar el protocolo de capa superior contenido en el campo de datos de la trama.

Ejemplos del campo de tipo de redes Ethernet.

0000-05DC CAMPO DE LONGITUD IEEE802.3
0800 CAMPO DE TIPO 0800 INFORMACION IP
0805 CAMPO DE TIPO 0805 INFORMACION X.25 CAPA 3
0806 CAMPO DE TIPO 0806 INFORMACION ARP
0A00 CAMPO DE TIPO 0A00 INFORMACION IEEE 802.3 XEROX
6003 CAMPO DE TIPO 6003 INFORMACION DECNET FASE 4
8019 CAMPO DE TIPO 8019 INFORMACION COMPUTADORAS APOLO
809D CAMPO DE TIPO 809D INFORMACION APPLETALK
814C CAMPO DE TIPO 814C INFORMACION SNMP

f) Campo de datos.

Contiene los datos de la trama. El número de bytes citados en el campo de longitud constituyen el paquete IEEE802.2. Los bytes de relleno incluyen cualquier número de bytes antes del chequeo de secuencia de trama.

El IEEE802.3 tiene algoritmos que detectan tramas defectuosas y colisiones. Estos algoritmos requieren que cada trama sea lo suficientemente grande para que el inicio de la trama se propague a través de la LAN y una señal de detección de colisión sea transmitida de regreso al transmisor antes de que el transmisor finalice la transmisión de la trama. El mínimo tamaño del paquete es de 64 bytes. Cuando pocos datos son transmitidos, el transmisor agrega caracteres de relleno. El receptor descarta las tramas más pequeñas a 64 bytes.

g) Secuencia de chequeo de trama (FCS).

Este campo de la trama contiene un código de chequeo de redundancia cíclica de 32 bits (4 Bytes) que calcula el emisor antes de la transmisión y confirma el receptor en la recepción.

El chequeo de redundancia cíclica (CRC) se calcula sobre los campos de dirección fuente, dirección destino, longitud o tipo, datos y campos de relleno de la trama. El receptor calcula el CRC con la información recibida y compara éste con el CRC en el campo FCS. El receptor descarta cualquier trama con un CRC que no cumpla con ser igual al CRC calculado por el emisor.

$$G(x) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^{8} + X^{7} + X^{5} + X^{4} + X^{2} + X + 1$$

Polinomio generador para CRC-32 de redes LAN.

Se tienen algunas variantes a la trama IEEE802.3 cuando se utiliza el sistema operativo Novell que usa el protocolo IPX y se muestran en la figura 2.8a y 2.8b.

FORMATO DE TRAMA PARA IEEE802.3

PREAMBULO	DELIMITADOR DE INICIO DE TRAMA	DIRECCION DESTINO	DIRECCION FUENTE	LONGITUD	IPX	CHEQUEO DE REDUN-DANCIA CI-CLICA.
7 BYTES	1 BYTE	6 BYTES	6 BYTES	2 BYTES	46-1500 BYTES	4 BYTES

Figura 2.8a.
Formato de trama IEEE802.3 sin IEEE802.2 y con IPX para Novell.

FORMATO DE TRAMA PARA IEEE802.3

PREAMBULO	DELIMITADOR DE INICIO DE TRAMA	DIRECCION DESTINO	DIRECCION FUENTE	LONGITUD	ENCABEZADO 802.2, SNAP, IPX	CHEQUEO DE REDUN-DANCIA CI-CLICA.
7 BYTES	1 BYTE	6 BYTES	6 BYTES	2 BYTES	46-1500 BYTES	4 BYTES

Figura 2.8b.
Formato de trama IEEE802.3 con IEEE802.2 y SNAP con IPX para Novell.

2.5 Protocolo SNAP (Protocolo de acceso a la subred (RFC 1042)).

En una red IEEE 802.3 utilizando LLC (IEEE802.2) para reconocer y proporcionar información acerca de ciertos protocolos de capa alta, se usa un protocolo intermedio llamado SNAP. LLC indica que está utilizando SNAP cuando el valor del DSAP es AA o AB hexadecimal. El protocolo SNAP le indica a LLC el tipo de protocolo de capa alta encapsulado, en la misma forma en que el campo de tipo Ethernet lo hace. La tabla de campo de tipo Ethernet es la misma para SNAP. Este protocolo inventado por Internet sirve para encapsular datagramas del protocolo IP y las solicitudes y respuestas de ARP, dentro de una trama de 802.3 y 802.5 (Ver figura 2.8c). El identificador de protocolo normalmente vale cero.

FORMATO DE TRAMA PARA IEEE802.3 CON SNAP.

		PROTOCOLO SNAP			
ENCABEZADO 802.3	ENCABEZADO 802.2	IDENTIFICADOR DE PROTOCOLO	TIPO ETHERNET	DATOS	CHEQUEO DE REDUN-DANCIA CI-CLICA.
14 BYTES	3 ó 4 BYTES	3 BYTES	2 BYTES		4 BYTES

Figura 2.8c.
Utilización del protocolo SNAP en una trama IEEE802.3.

2.6 Topología de redes.

La topología de la red es la forma geométrica de interconexión de los nodos de la red. De la topología dependen varias características de la red, tales como: seguridad, costo, velocidad de operación, facilidad de instalación y mantenimiento.

Antes de las topologías de las redes actuales, los enlaces de comunicación consistían solamente de enlaces punto a punto o enlaces punto a multipunto.

Un enlace punto a punto es una conexión directa entre dos dispositivos. Un ejemplo es una conexión de una computadora a una impresora o una terminal a un mainframe.
Un enlace multipunto es una conexión entre tres o más puntos en un enlace. Los enlaces multipunto se usan para conectar un equipo maestro con una serie de equipos esclavos.

a) Estrella.

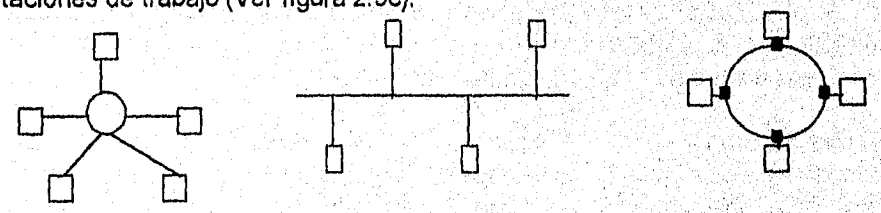
Esta topología consiste de un nodo central que enlaza a todas las estaciones de trabajo con un enlace punto a punto para formar una red. El nodo central controla la conmutación y enrutamiento de tráfico de mensajes de red. Las estaciones de trabajo pueden comunicarse una con otra pasando por el nodo central (Ver figura 2.9a).

b) Anillo.

En la topología de anillo cada nodo es conectado uno al lado del otro hasta que el primer nodo es conectado con el último para formar una trayectoria cerrada llamada anillo (Ver figura 2.9b).

c) Bus.

La topología de bus es una estructura de red donde un sólo cable conecta a todas las estaciones de trabajo sin brincos y sin múltiples trayectorias entre estaciones de trabajo (Ver figura 2.9c).



A) TOPOLOGIA DE ESTRELLA C) TOPOLOGIA DE BUS B) TOPOLOGIA DE ANILLO

Figura 2.9
Topología de redes.

2.7 Diferentes tipos de redes IEEE802.3.

IEEE802.3 especifica diversas capas físicas, por el contrario Ethernet sólo define una. Cada capa física de IEEE802.3 tiene un nombre que resume sus características.

Para fácil identificación de un tipo de red IEEE802.3 en particular, se utiliza una abreviación formada por los tres parámetros básicos de la red.

1) Su velocidad de transmisión (Mbps).

2) La técnica de codificación (banda base, banda ancha).

3) El tamaño del segmento en unidades de cientos de metros.

Por ejemplo

VELOCIDAD EN MEGABITS	BANDA BASE O BANDA ANCHA	LONGITUD DEL SEGMENTO EN MULTIPLOS DE 100 MTS
10	BASE	5

2.7.1 Ethernet 10base5 (Thick Ethernet).

Las estaciones de trabajo se conectan al medio vía tarjetas de red, de la tarjeta de red sale un cable AUI con conector de 15 pines, que lleva 5 pares de hilos blindados hacia el MAU (Unidad de Acoplamiento al Medio). Estos hilos transportan:

- Los datos de entrada.
- Los datos de salida.
- Las señales de control.
- Los voltajes entre la tarjeta de red y el transceiver.

En el MAU se utiliza un conector tipo vampiro con el cual se perfora la protección del cable hasta tocar su núcleo. De esta manera se pueden conectar estaciones adicionales, sin que el cable de red se dañe.

Medio de transmisión: Cable coaxial de 50 Ohms con un centímetro de diámetro de color amarillo con marcas cada 2.5 metros, que indica los lugares donde se pueden conectar la estaciones de trabajo.

Velocidad de transmisión: 10 Mbps en banda base.

Codificación: Manchester.

Longitud máxima de cualquier segmento: 500 Mts.
Cada segmento debe tener resistencias de terminación para evitar el eco.

Aunque el segmento tiene 200 marcas no se pueden tener más de 100 estaciones en él.

Máximo 1024 estaciones por red.

La máxima longitud del cable AUI es de 50 mts.

La máxima cantidad de repetidores es de 4 para formar 5 segmentos.

Aún con repetidores la red no debe de pasar de 2500 mts.

Este tipo de red se muestra en las figuras 2.10 a y 2.10b.

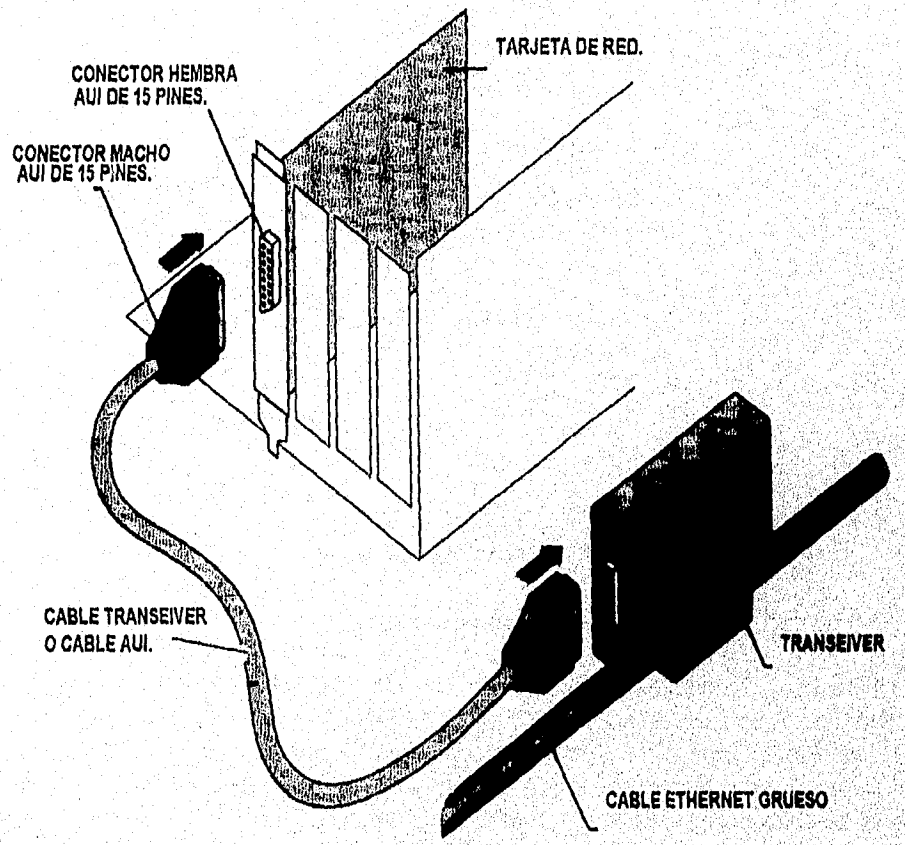


Figura 2.10a
Conexión de un equipo a una red 10base 5.

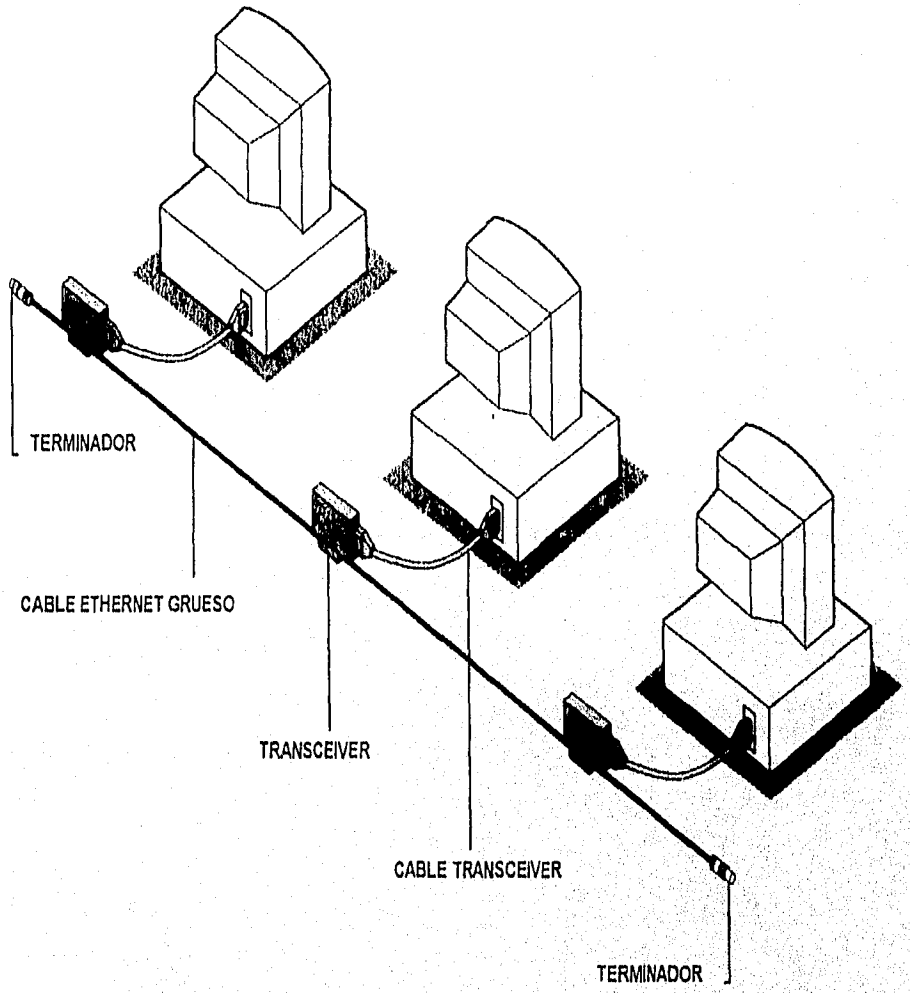


Figura 2.10b
Red 10base 5.

2.7.2 La red Ethernet 10base2 (Thin Ethernet).

Utiliza cable coaxial delgado de 5 mm de diámetro (código RG-58 50 ohms). La longitud máxima de los segmentos es de 185 mts.
El número máximo de nodos en un segmento de red se reduce a 30 y pueden colocarse con una separación de 0.5 mts. Debido a que el cable es más flexible que el cable para 10base5, éste puede llegar al dispositivo que se quiere conectar sin necesidad del cable AUI, o sea la tarjeta de red proporciona un conector BNC hembra donde se conecta el cable vía un conector tipo-T (conector de dos entradas BNC hembra y un BNC macho).

Velocidad de transmisión: 10 Mbps.

Longitud máxima del segmento: 185 mts.

Tamaño máximo de la red: 925 mts.

Nodos por segmento: 30.

Nodos por red: 1024.

Distancia entre nodos: 0.5 mts.

Codificación: Manchester.

4 Repetidores máximo.

Medio de comunicación: Cable coaxial con impedancia de 50 Ohms (Ver figuras 2.11a y 2.11b).

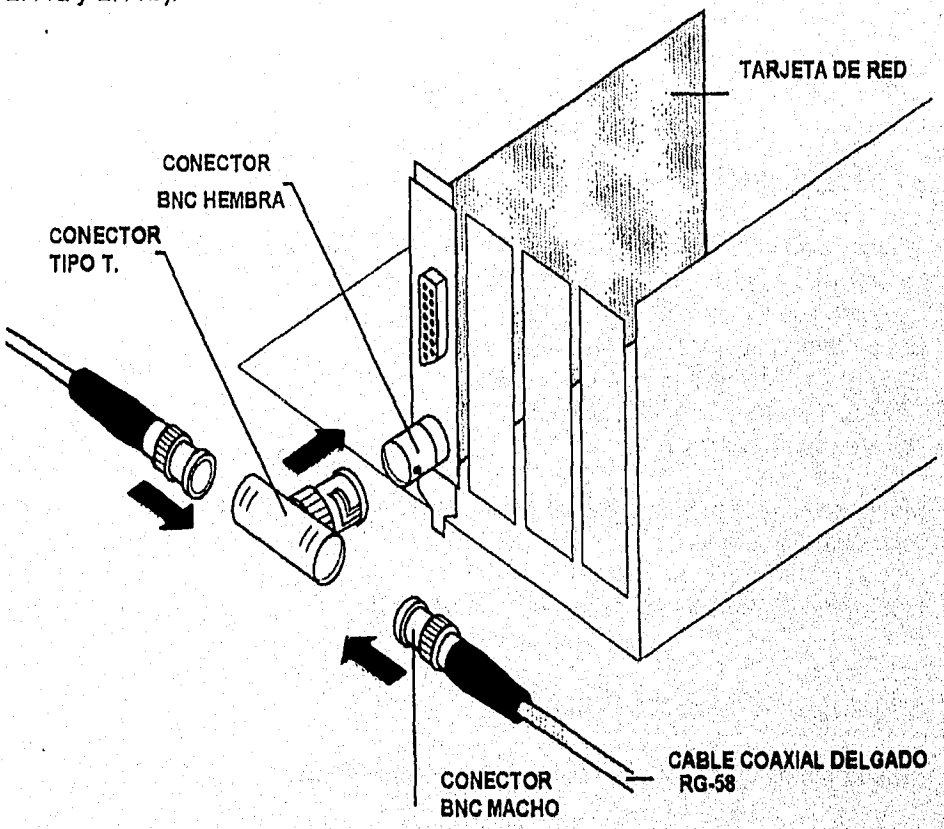
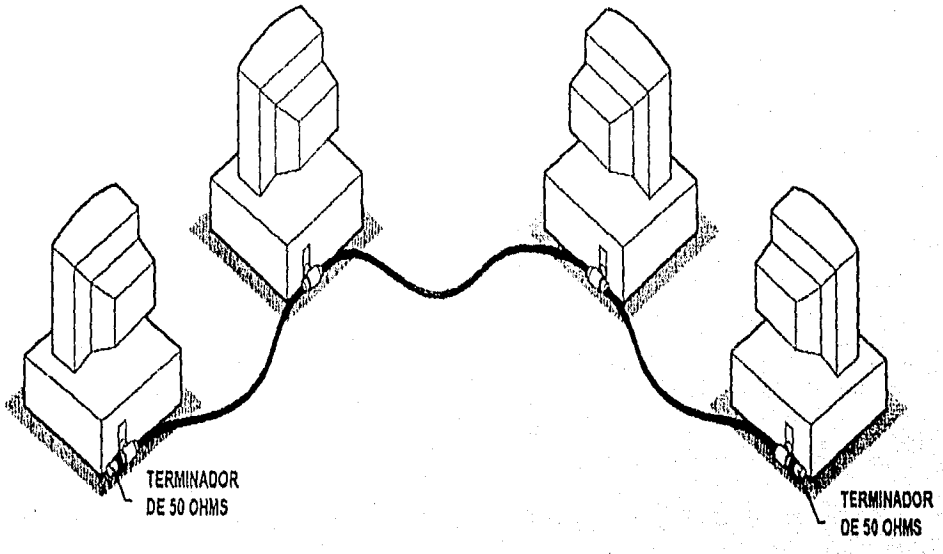


Figura 2.11a
Conexión de un equipo a una red 10 base2.



2.11b
Red 10base 2.

2.7.3 Ethernet 10 baseT.

Este tipo de red necesita un concentrador (Hub) para poder conectar el servidor de archivos y las estaciones de trabajo.
Velocidad de transmisión: 10 Mbps.
Código de transmisión: Manchester.
Longitud máxima del segmento: 100 mts.
Tamaño máximo de la red: 500 mts.
Número de repetidores: 4.

Medio de comunicación: cable de par trenzado no blindado (UTP).
Topología : Estrella.

Las figuras 2.12a y 2.12b muestran una red 10 baseT.

2.7.4 Ethernet 1base5 (STARLAN).

Topología de árbol estrella que se comporta como bus.

Código de Transmisión: Manchester.
Velocidad de transmisión: 1 Mbps.

Longitud de los segmentos: 250 mts.

Nodos por segmento: 50.

Medio de transmisión: Par trenzado.

Cada dispositivo se conecta a un concentrador por medio de dos pares trenzados, uno para transmisión y otro para recepción usando un conector RJ45. Los concentradores se pueden conectar en cascada hasta 5 niveles. Ver figuras 2.12a y 2.12b que son las mismas para 10 base T.

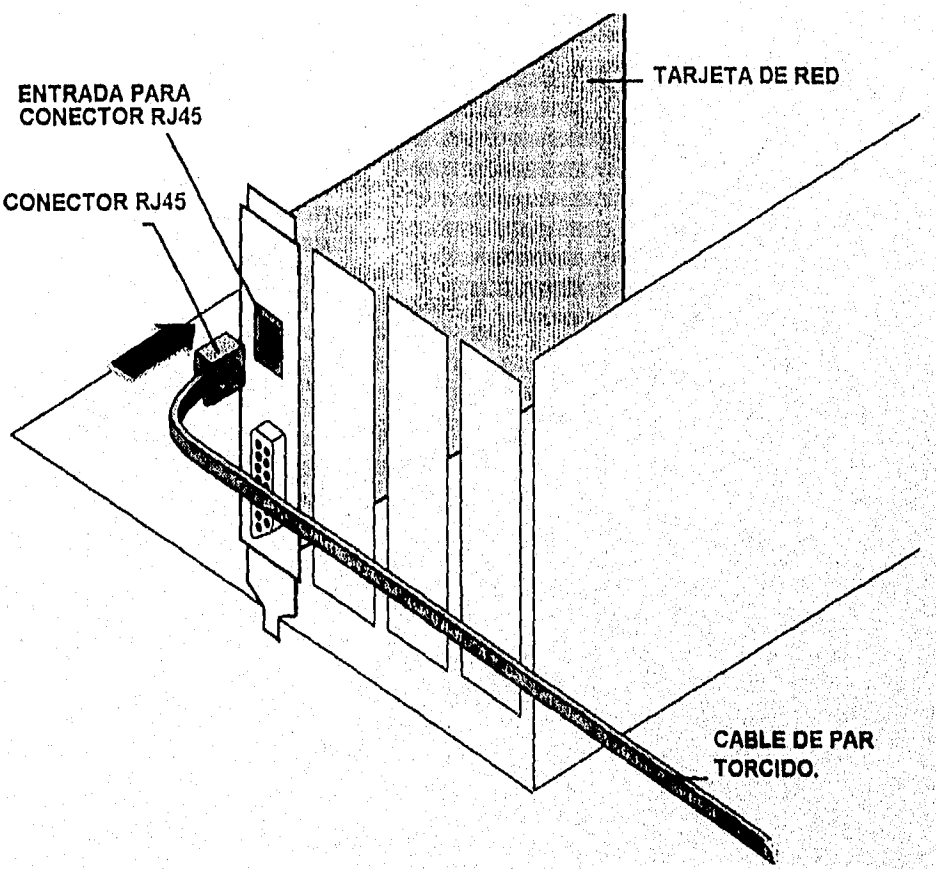


Figura 2.12a
Conexión de un equipo a una red 10 baseT.

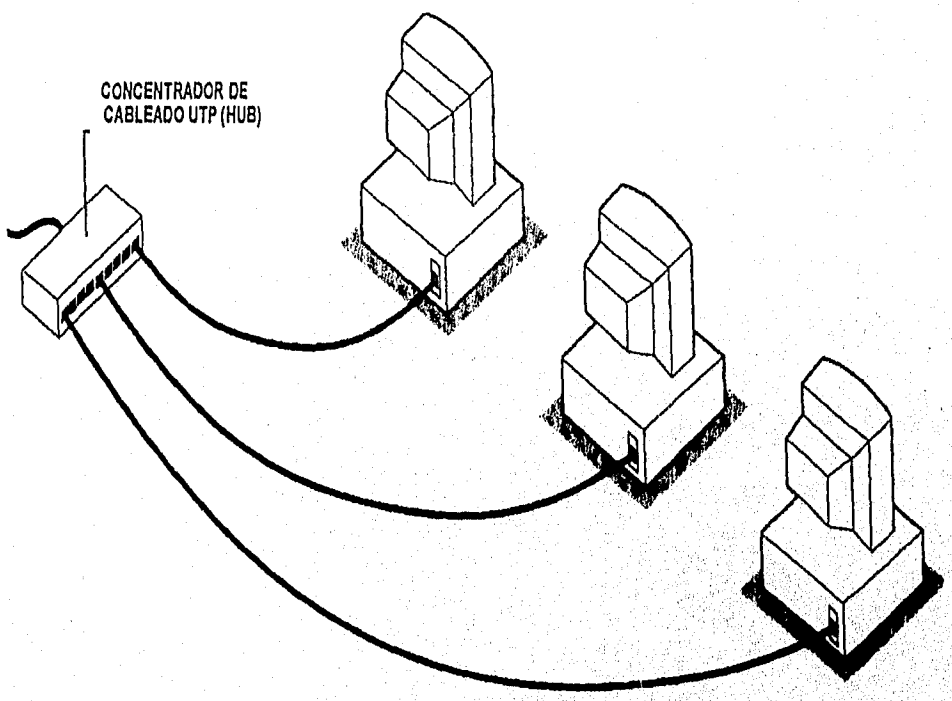


Figura 2.12b
Red 10 Base T.

2.8 Redes de área amplia (WAN).

2.8.1 Consideraciones generales.

Conforme las redes de área local van creciendo en tamaño y complejidad, y conforme las instituciones van confiando en estas redes labores cada día más críticas, surge la necesidad de comunicarlas entre sí en una misma ciudad o en ciudades distintas. Así se forma lo que comúnmente se denomina redes de área amplia WAN.

En sentido estricto, una red de área amplia es una red de redes, en la que se conectan varias redes locales mediante dispositivos que permiten su conectividad local o remota, a pesar de que tengan diferente topología. Estos dispositivos pueden usar o no líneas telefónicas y servicios públicos de transmisión de datos.

Características de una red de área amplia.

- Cubren grandes distancias geográficas.
- Soportan velocidades de transmisión bajas.
- Interconectan redes de área local LAN.

Las redes de área amplia son manejadas actualmente por tecnologías de multiplexores, conmutación de paquetes e interconexión de redes. Éstas además están evolucionando hacia tecnologías de conmutación de paquetes rápida y protocolos tales como: Frame Relay, Cell Relay y ATM.

Junto con las tecnologías mencionadas, el módem juega un papel aún importante en las redes actuales, debido a que permite dar acceso a sitios que sólo cuentan con líneas telefónicas como medio de transmisión.

2.9 Elementos que constituyen una red de área amplia.

2.9.1 Módem.

Un módem es un dispositivo DCE instalado entre un DTE y un medio de transmisión analógico tal como una línea telefónica. Un módem modula datos digitales de un DTE dentro de portadoras analógicas. Un módem en el extremo

receptor demodula la señal analógica, extrayendo los datos digitales para el DTE destino.

2.9.2 Tecnologías de multiplexores.

Multiplexores.

Antes de describir a los multiplexores es útil mencionar que multiplexar es la técnica que permite compartir un único enlace de comunicaciones entre varios usuarios simultáneos.

Hay 3 tipos de multiplexores que son el de FDM, el TDM y STDM.

a) Los multiplexores FDM.

En estos multiplexores el espectro de frecuencia total se subdivide entre los canales lógicos, donde cada uno de los usuarios posee una banda de frecuencia en exclusiva.

b) Los multiplexores TDM.

En estos multiplexores se le asigna un tiempo a cada uno de los usuarios, de modo que utilizan el ancho de banda total del medio físico durante un periodo de tiempo hasta que les vuelve a tocar su turno en orden secuencial y cíclico.

c) Los multiplexores STDM.

En estos equipos el tiempo de uso del ancho de banda total es compartido en proporción directa a la demanda de cada subcanal.

2.9.3 Tecnologías de conmutación de paquetes.

Las tecnologías de conmutación de paquetes utilizan nodos intermedios para enviar la información entre la máquina fuente y la máquina destino. Estos nodos no participan en el proceso de la información, sino únicamente en la tarea de conmutación de la información hacia la máquina destino.
Las tecnologías de conmutación de paquetes dividen la información a enviar en unidades con un límite en el tamaño llamadas paquetes.

Dentro de las tecnologías de conmutación de paquetes se encuentran las redes X.25 y las redes TCP/IP .

2.9.4 Tecnologías de interconexión de redes.

Esta tecnología será discutida en detalle en el capítulo III.

2.9.5 Tecnología de Conmutación de paquetes rápida (Fast-Packet Switching).

Cubre un rango de tecnologías y protocolos que buscan solucionar problemas de bajas velocidades y datos excesivos de los protocolos de capa alta. Ésta incluye Frame Relay, Cell relay, así como ATM.

a) Frame Relay.

Es un protocolo de la capa de enlace de datos que proporciona un rendimiento alto y soporta altas velocidades. Frame Relay es una derivación del protocolo de acceso de enlace al canal-D ISDN del CCITT.

Éste minimiza control de flujo y error, garantizando que las tramas lleguen libres de error al destino y que éstas tramas lleguen en el orden correcto.

Frame Relay no trata de recuperar tramas perdidas o dañadas. El control de errores es dejado a protocolos de nivel más alto.

Una trama está compuesta de 4 componentes básicos: Un identificador de conexión de enlace de datos (DLCI); tres bits de manejo de congestión; un campo de carga de longitud variable; y un campo de dos octetos de chequeo de secuencia de trama. El DLCI describe una conexión en lugar de una dirección destino.

Este uso del DLCI, en lugar de una dirección, muestra la forma en que Frame Relay opera: los circuitos virtuales son establecidos entre dos nodos finales a través de nodos de conmutación. Las tramas siguen este circuito virtual a través de la red.

Frame Relay está definido para trabajar a velocidades de 64 kbps hasta 2 Mbps, pero se espera sea conveniente para velocidades hasta de 100 Mbps.

b) Tecnología de redes de área metropolitana IEEE802.6.

La tecnología de redes de área metropolitana está generando un interés creciente como medio de transporte de tráfico de datos de velocidad alta y en ráfaga dentro de un área de una ciudad. Las implementaciones MAN caen

dentro de las tecnologías siguientes: Colas Distribuidas, Bus Dual (DQDB), y tecnología de LAN de 100 Mbps.

c) SMDS (Switched Multi-Megabit Data Services).

Es un servicio público basado en el servicio de datagrama sin conexión. Está diseñado para permitir la interconexión de LAN's y otras aplicaciones de datos de velocidad alta sobre áreas metropolitanas.

d) Cell Relay y ATM (Asynchronous Transmition Mode).

ATM es una forma estandarizada de Cell Relay. Cell Relay es una forma de conmutación de paquetes rápida para transferencia digital. Ésta hace uso de paquetes de longitud fija cortos, conocidos comúnmente como celdas. La longitud de los paquetes ha sido optimizada para conducir una mezcla de tipos de tráfico: voz, datos e imágenes.

Las definiciones de ATM que existen hoy, definen un formato de paquete de 53 bytes que contiene un campo de carga de 48 bytes y 5 bytes de información de direccionamiento. ATM trabaja bajo el principio de que es posible variar el número de celdas que son puestas en la red por un nodo particular. Este proceso que es conocido como división de tiempo asíncrono, permite que el ancho de banda asignado a una particular transmisión varíe de acuerdo a las necesidades del usuario. El pequeño tamaño de las celdas significa que la granularidad del ancho de banda es pequeño.

ATM es un protocolo de circuito virtual orientado a conexión. Cuando una llamada se inicia, una ruta predeterminada es calculada de extremo a extremo.

ATM ha sido diseñada para hacer uso de sistemas de transmisión de muy alta velocidad, con enlaces operando a 33 Mbps o más altos.

2.10 Líneas de comunicación.

- Líneas telefónicas conmutadas.
- Líneas telefónicas privadas.
- Enlaces digitales E0 de la red digital integrada.
- Enlaces digitales E1 de la red digital integrada.
- Enlaces digitales DS0 sobre 2 hilos.

Se discutirán con detalle en el Apéndice A.

2.11 Interfaces para redes WAN.

Las interfaces que permiten la conexión de equipos de transmisión de datos a una red WAN son las siguientes; y algunas de ellas se explicarán con mayor detalle en el apéndice B.

RS-232, RS-449, V.24, V.35, etc.

2.12 Protocolos de la capa de enlace de datos en redes WAN.

Entre los protocolos de la capa de enlace de datos que se utilizan con mayor frecuencia en redes WAN están: HDLC, PPP, SDLC, LAPB y en el punto 2.13 se describe uno de los más importantes.

2.13 El Protocolo HDLC.

HDLC (High Level Data Link Control) es un protocolo orientado a bit y es un estándar publicado por ISO con los estándares 3309,4335,6154 y 6256.

HDLC soporta transmisión Half Dúplex y Full Dúplex.

Una estación HDLC es clasificada en uno de los tipos mostrados en la figura 2.13 y se describen a continuación:

1) Estación primaria.

La estación primaria es responsable del enlace de datos. Esta estación transmite tramas de comandos a las estaciones secundarias en el canal. En turno, ésta recibe tramas de respuestas de las estaciones secundarias. Si el enlace es multipunto, la estación primaria es responsable de mantener una sesión separada con cada estación conectada al enlace.

2) Estación secundaria.

La estación secundaria actúa como una esclava de la estación primaria. Ésta responde a los comandos de la estación primaria en forma de tramas de respuesta, y mantiene únicamente una sesión, que es con la estación primaria, además no es responsable del control del enlace.

3) Estación combinada.

La estación combinada transmite comandos y respuestas y recibe comandos y respuestas de otra estación combinada. Ésta mantiene una sesión con otra estación combinada.

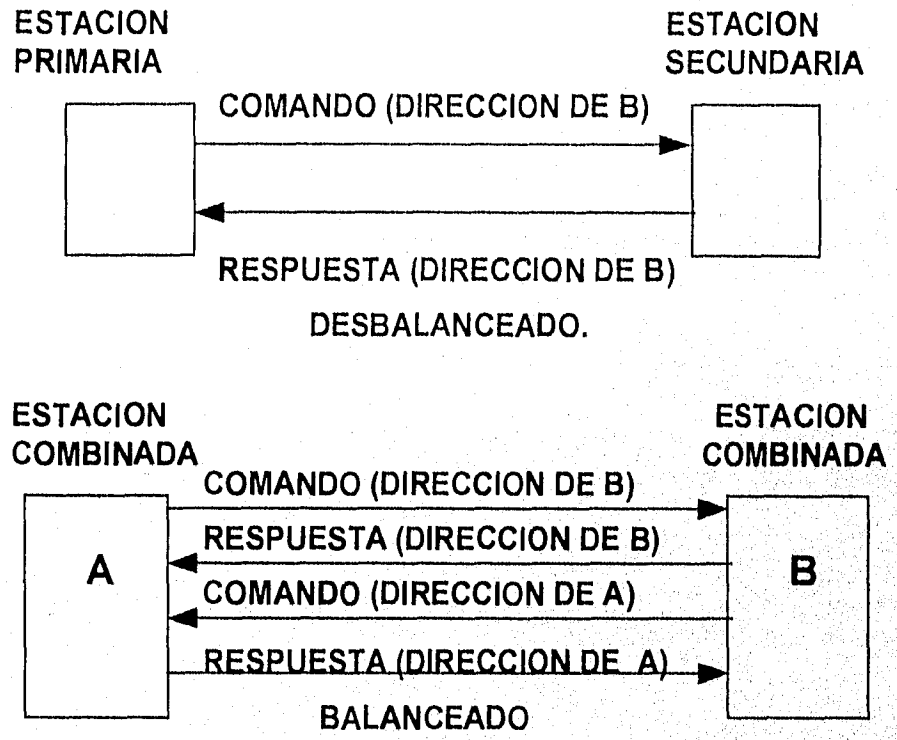


Figura 2.13
Diferentes tipos de estaciones y reglas de direccionamiento HDLC.

Las estaciones se comunican una con otra a través de uno de tres estados lógicos.

1) El estado de desconectado lógicamente.

El estado de desconectado lógicamente (LDS), prohibe a una estación transmitir o recibir información. Si la estación secundaria esta bajo el modo desconectado normal, ésta puede transmitir una trama únicamente después de recibir permiso explícito de una estación primaria. Si la estación secundaria está bajo el modo desconectado asíncrono, la estación secundaria puede iniciar una

transmisión sin recibir permiso explícito, pero la trama debe ser sólo una trama, indicando el status de la estación secundaria.

2) El estado de inicialización.

Definido por el vendedor de equipo implementando HDLC y está fuera de los estándares HDLC.

3) El estado de transferencia de información.

EL estado de transferencia de información (ITS) permite a las estaciones primaria, secundaria y combinada, transmitir y recibir información de usuario. El estado de transferencia de información puede ser cambiado emitiendo comandos DISC.

Mientras las estaciones están en el estado de transferencia de información, se les permite estar en uno de tres modos de operación. Estos modos pueden ser establecidos y reseteados en cualquier momento durante la sesión.

1) Modo de respuesta normal (NRM).

En el modo de respuesta normal se requiere que la estación secundaria reciba permiso explícito de la estación primaria antes de transmitir. Después de recibir permiso, la estación secundaria inicia una transmisión de respuesta que contiene datos. La transmisión puede consistir de una o más tramas mientras el canal está siendo usado por la estación secundaria. Después de transmitir la última trama la estación secundaria debe esperar de nuevo permiso para volver a transmitir.

2) Modo de respuesta asíncrono (ARM).

En el modo de respuesta asíncrono se permite que una estación secundaria inicie transmisiones sin recibir permiso explícito de la estación primaria (usualmente cuando el canal está libre). La transmisión puede contener una o múltiples tramas de datos, o puede contener información de control reflejando cambios de estado de la estación secundaria. ARM puede decrementar el overhead debido a que la estación secundaria no necesita secuencia de poll en orden a enviar datos.

3) Modo balanceado asíncrono (ABM).

El modo balanceado asíncrono usa estaciones combinadas. Una estación combinada puede iniciar transmisiones sin recibir permiso previo de otra estación combinada.

HDLC proporciona dos formas de configurar el canal para uso de estaciones primaria, secundaria y combinada.

1) Configuración desbalanceada.

Una configuración desbalanceada (UN), se forma de una estación primaria y una o más estaciones secundarias para operar en configuración punto a punto o punto a multipunto, half dúplex o full dúplex. La configuración es llamada desbalanceada por que la estación primaria es responsable de controlar a cada estación secundaria y de emitir los comandos de establecimiento de modo.

2) Configuración balanceada.

La configuración balanceada (BA), consiste de 2 estaciones combinadas conectadas punto a punto únicamente, half dúplex o full dúplex. Las estaciones combinadas tienen igual status en el canal y pueden enviar tráfico, no solicitado, una a la otra. Cada estación tiene igual responsabilidad del control del enlace.

2.13.1 Formato de la trama HDLC.

HDLC usa el término trama para indicar una entidad independiente de datos transmitidos a través del enlace de una estación a otra.

Tres tipos de tramas son permitidas:

- Trama de información.

Se usa para transmitir información de usuario entre dos dispositivos. La trama de información puede también reconocer recepción de datos de la estación transmisora.

- Trama de supervisión.

Realiza funciones de control tales como el reconocimiento de tramas, la solicitud de retransmisión de tramas y la solicitud de la suspensión temporal de la transmisión de tramas. Su utilidad es dependiente del modo operacional del enlace (NRM, ABM y ARM).

- Trama no numerada.

Es también usada para propósitos de control. La trama es usada para inicialización o desconexión del enlace. La trama contiene posiciones de 5 bits que permiten acomodar uno de 32 comandos y 32 respuestas.

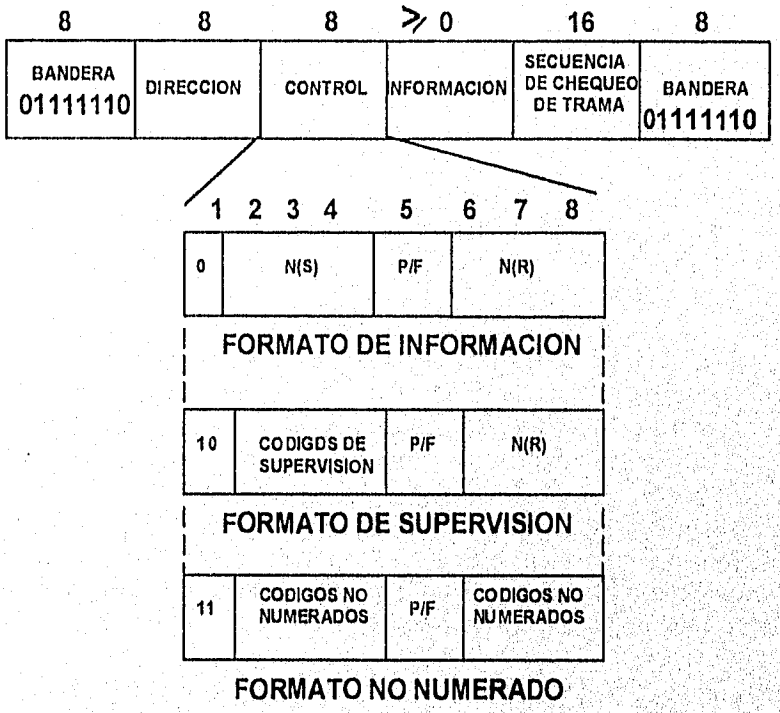


Figura 2.14
Formato de la trama HDLC.

La trama consiste de 5 ó 6 campos como muestra la figura 3.14. Todas las tramas deben comenzar y finalizar con un campo de banderas. Las estaciones conectadas al enlace de datos deben monitorear continuamente la secuencia de bandera. La secuencia de bandera consiste de 01111110. Las banderas pueden ser continuamente transmitidas en el enlace entre tramas HDLC. Siete unos continuos pueden ser enviados para indicar una problema en el enlace. Quince o más unos mantienen el canal en el estado de libre. Una vez que la estación receptora ve una secuencia que no es una bandera, ésta sabe que ha encontrado el inicio de la trama, una condición de problema o una condición de canal libre. Cuando encuentra la siguiente secuencia de bandera, la estación sabe que ya tiene la trama completa.

El campo de dirección identifica la estación primaria o secundaria involucrada en la transmisión de una trama en particular. Una única dirección es asociada con cada estación. En una configuración desbalanceada, los campos de direcciones en comandos y respuestas contienen la dirección de la estación secundaria. En configuraciones balanceadas, una trama de comando contiene la dirección destino y una trama de respuesta contiene la dirección de la estación emisora.

El campo de control contiene los comandos y respuestas, así como los números de secuencia usados para mantener la contabilidad del flujo de datos del enlace entre la estación primaria y secundaria. El formato y el contenido del campo de control varía, dependiendo del uso de la trama HDLC.

El campo de control define la función de la trama, y por lo tanto invoca la lógica para controlar el movimiento de tráfico entre las estaciones emisora y receptora. El campo de control identifica los comandos y respuestas usados para controlar el flujo de tráfico en el enlace.

El más simple formato del campo de control es el de la trama de información. Este campo de control contiene dos números de secuencia. El número N(S) indica el número de secuencia asociado con la trama transmitida. El número N(R) indica el siguiente número de secuencia que es esperado en el receptor. El N(R) sirve como un reconocimiento de las tramas anteriores. Por ejemplo, si el campo N(R) es establecido a 4, la estación que recibe N(R)=4, comprenderá que sus transmisiones de tramas 0,1,2,3 han sido recibidas correctamente, y que la estación con la que se comunica está esperando que la siguiente trama tenga un número de secuencia de envío de 4.

El bit de la quinta posición, el bit P/F o bit Poll/Final, es reconocido únicamente cuando es establecido a 1 y es usado por las estaciones primaria y secundaria para proporcionar las siguientes funciones:

La estación primaria usa el bit P para solicitar una respuesta de status de una estación secundaria. El bit P puede también significar un Poll.

La estación secundaria responde a un bit P con datos o una trama de status y un bit F. El bit F puede también significar el fin de transmisión de la estación secundaria bajo modo de respuesta normal.

El bit P/F es llamado P cuando es usado por la estación primaria, y un bit F cuando es usado por la estación secundaria. Únicamente un bit P (esperando un bit F de respuesta) debe ser enviado en un enlace. Un bit P establecido a 1 puede ser usado como punto de chequeo. Esto es P=1 dice: respóndeme estación secundaria por que quiero saber tu status.

El bit P/F es usado e interpretado en diversas formas :

En NRM, la estación secundaria no puede transmitir hasta que un comando con el bit P puesto a 1 es recibido. La estación primaria puede solicitar tramas de información enviando una trama con el bit P puesto a 1, o enviando ciertas tramas de supervisión (RR, REJ, SREJ) con el bit P puesto a 1.

En ARM y ABM, tramas de información pueden ser transmitidas sin ser solicitadas por un comando con el bit P puesto a 1. El bit P puesto a 1 es usado para solicitar una respuesta en la oportunidad más cercana con el bit F puesto a 1.

En ARM y ABM, enseguida de la recepción de un comando con el bit P puesto a 1, una trama con el bit F puesto a 1 es transmitida.

En transmisión full-dúplex, donde la estación secundaria está transmitiendo cuando el comando con el bit P establecido en 1 es recibido, el bit F es establecido a 1 en la más cercana oportunidad de respuesta.

La transmisión de una trama con el bit F en 1 no requiere que la estación secundaria detenga la transmisión. Tramas adicionales pueden ser transmitidas siguiendo la trama que tenía el bit F en 1. En ARM y ABM, el bit F no es interpretado como el fin de la transmisión por la estación secundaria; esto es únicamente interpretado como indicativo de respuesta de la trama anterior.

El campo de información contiene los datos de usuario actuales. El campo de información reside en las tramas bajo el formato de información y en algunos comandos y respuestas del formato no numerado.

La secuencia de chequeo de trama (FCS) es usada para checar errores de transmisión entre 2 estaciones en un enlace de datos.
La estación transmisora realiza un cálculo en la cadena de datos del usuario y agrega la respuesta como el campo FCS. La estación receptora realiza el mismo cálculo y compara su resultado con el campo FCS. El campo FCS es llamado chequeo de redundancia cíclica y para su cálculo se utiliza un polinomio generador definido en la recomendación CCITT V.41.

$$G(x) = X^{16} + X^{12} + X^{5} + 1$$

Polinomio generador para HDLC.

2.13.2 Comandos y respuestas HDLC.

El diagrama y cuadro 2.15 muestran los comandos y respuestas para HDLC.

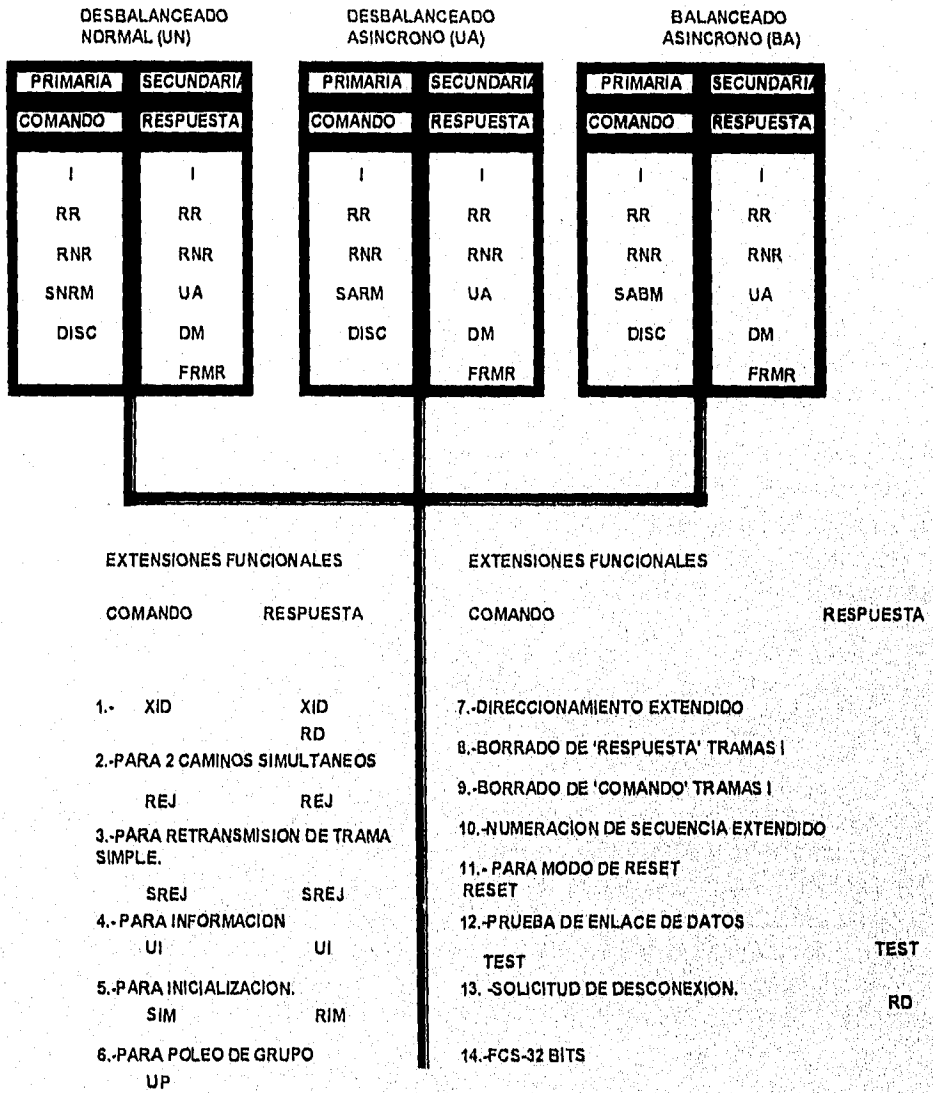


Diagrama 2.15
Comandos y respuestas HDLC.

TRAMA	BITS CAMPO DE CONTROL								NOMBRE DE COMANDO O RESPUESTA HDLC	COMANDO	RESPUESTA
FORMATO	1	2	3	4	5	6	7	8			
INFORMACION	0	N(S)			*	N(R)			I INFORMACION	X	X
SUPERVISION	1	0	0	0	*	N(R)			RR	X	X
	1	0	0	1	*	N(R)			REJ	X	X
	1	0	1	0	*	N(R)			RNR	X	X
	1	0	1	1	*	N(R)			SREJ	X	X
NO NUMERADO	1	1	0	0	*	0	0	0	UI	X	X
	1	1	0	0	*	0	0	1	SNRM	X	
	1	1	0	0	*	0	1	0	DISC	X	X COMO RD
	1	1	0	0	*	1	0	0	UP	X	
	1	1	0	0	*	1	1	0	UA		X
	1	1	0	0	*	1	1	1	TEST	X	X
	1	1	1	0	*	0	0	0	SIM	X	X COMO RIM
	1	1	1	0	*	0	0	1	FRMR		X
	1	1	1	1	*	0	0	0	SARM	X	X COMO DM
	1	1	1	1	*	0	0	1	RSET	X	
	1	1	1	1	*	0	1	0	SARME	X	
	1	1	1	1	*	0	1	1	SNRME	X	
	1	1	1	1	*	1	0	0	SABM	X	
	1	1	1	1	*	1	0	1	XID	X	X
	1	1	1	1	*	1	1	0	SABME	X	

* bit P/F

Cuadro 2.15
Comandos y Respuestas HDLC.

- El formato de la trama de supervisión se usa con 4 comandos que son: Receive Ready (RR), Reject (REJ), Receive not Ready (RNR), Selective Reject (SREJ).

El propósito de este formato y de los 4 comandos y respuestas es realizar funciones de supervisión numerada, tales como reconocimiento, poleo, suspensión temporal de transferencia de datos, y recuperación de errores. Las tramas del formato de supervisión no contienen un campo de información, como consecuencia estas tramas no contienen en el campo de control un número de secuencia de transmisión. El formato de supervisión puede ser usado para reconocer las tramas recibidas de la estación transmisora.

Receive Ready (RR).

Es usado por la estación primaria o secundaria para indicar que está lista para recibir una trama de información y/o para reconocer tramas recibidas

anteriormente usando el campo N(R). Si una estación indico un estado de ocupado con un comando Receive Not Ready, entonces usa el comando RR para indicar que ahora está libre para recibir datos. La estación primaria puede usar un comando RR con P=1 para poleo de una estación secundaria.

Receive Not Ready (RNR).

Es usado por una estación para indicar una condición de ocupado. Éste le dice a la estación transmisora que la estación receptora no es capaz de recibir datos entrantes adicionales. La trama RNR puede reconocer tramas previamente transmitidas usando el campo N(R). La condición de ocupado puede ser limpiada enviando la trama RR.

Selective Reject (SREJ).

Es usado por una estación para solicitar la retransmisión de una sola trama indicando su número en el campo N(R). Como con reconocimiento inclusivo, todas las tramas numeradas de N(R)-1. Select Reject proporciona capacidad de retransmisión selectiva.

Reject (REJ).

Es usado para solicitar la retransmisión de tramas comenzando con la trama numerada en el campo N(R). Tramas numeradas N(R)-1 son todas desconocidas. La trama REJ puede ser usada para implementar la técnica de retransmisión no selectiva GO-BACK-N.

- Comandos y respuestas no numerados.

El formato de trama no numerado es usado para enviar la mayoría de comandos y respuestas de HDLC.

Los comandos y respuestas no numerados son agrupados por la función que realizan:

⇒ Comandos de establecimiento de modo.

SNRM, SARM, SABM, SNRME, SARME, SABME, SIM, DISC, RIM, DM Y UA.

⇒ Comandos de transferencia de información.

UI, UP.

⇒ Comandos de recuperación.

RESET (RSET).

⇒ Comandos misceláneos.

XID, TEST, FRMR, RD.

Los comandos y respuestas del formato de trama no numerado tienen el siguiente significado:

SNRM (Set Normal Response Mode).

Este comando coloca a la estación secundaria en modo de respuesta normal. La estación primaria controla todo el flujo en la línea.

SARM (Set Asynchronous Response Mode).

Establece el modo para permitir que la estación secundaria transmita sin un poleo de la estación primaria. Esta trama coloca a la estación secundaria en el estado de transferencia de información ITS de ARM. Debido a que SARM establece 2 estaciones desbalanceadas, SARM debe ser emitido en ambas direcciones del enlace.

SABM (Set Asynchronous Balanced Mode).

Establece el modo balanceado asíncrono, donde las estaciones pueden transmitir y recibir cuando lo deseen.

SNRME (Set Normal Response Mode Extended).

Establece el Modo de respuesta normal extendido con 2 bytes en el campo de control.

SARME (Set Asynchronous Response Mode Extended Command)
Establece el modo de respuesta asíncrono extendido con 2 bytes en el centro de control.

SABME (Set Asynchronous Balanced Mode Extended).

Establece SABM con 2 bytes en el campo de control.

SIM (Set Initialization Mode).

Este comando es usado para inicializar la sesión primario/secundario. UA es la respuesta esperada.

DISC (Disconnect).

Este comando de la estación primaria coloca a la estación secundaria en modo desconectado. UA es la respuesta esperada.

RIM (Request Initialization Mode).

La trama RIM es una solicitud de una estación secundaria a una estación primaria para un comando SIM.

DM (Disconnect Mode).

Esta trama es transmitida de una estación secundaria para indicar que está en el modo de desconectado.

UA (Unnumbered Acknowledgment).

Este es un comando para reconocimiento no numerado de comandos de establecimiento de modo y para SIM, DISC y RESET. También es usado para reportar el fin de la condición de ocupado de una estación.

UI (Unnumbered Information).

Este comando permite transmisión de datos de usuario en tramas no numeradas.

UP (Unnumbered Polls).

Trama de poleo no numerado usada para solicitar información de control.

RSET (Reset).

La estación transmisora resetea su N(S) y la estación receptora resetea su N(R). Este comando es utilizado para recuperación.

XID (Exchange Station Identification).

Trama de identificación de estación, usada para intercambio de información de dos nodos sin importar que tipos de servicios ellos soporten.

TEST

Una trama de prueba, con un campo de información opcional para calificar la trayectoria de transmisión de enlace de datos (tipo de servicio 1). Comando o respuesta.

FRMR (Frame Reject).

La estación secundaria envía esta trama cuando recibe una trama inválida. Esto no es usado como error de bit indicado en el chequeo de secuencia de trama, sino para condiciones más inusuales. El campo de información contiene la razón. Esta trama de respuesta es usada en las siguientes condiciones:

1) Recepción de un campo de control, de un comando o respuesta inválido.
2) Recepción de un campo de información muy largo.
3) Recepción de un campo N(R) inválido.
4) Recepción de un campo de información no permitido.
5) Recepción de una trama de supervisión o no numerada de una longitud incorrecta.

HDLC proporciona considerable información de status con la trama FRMR. El campo de información es usado para proporcionar lo siguiente:

- Campo de control rechazado.

- La trama rechazada fué un comando o respuesta.

- El campo de control es inválido.

- La trama fué transmitida con un campo de información no permitido.

- El campo de información es demasiado largo.

- Los números de secuencia son inválidos.

RD (Request Disconnect).

Esta es una solicitud de una estación secundaria para ser desconectada y colocada en el estado desconectada lógicamente.

HDLC utiliza el temporizador T1 que arranca con la transmisión de cada trama. T1 es usado para iniciar la retransmisión si éste expira. HDLC utiliza también un contador N2 que determina el máximo número de retransmisiones a ser realizadas antes de que expire el temporizador T1.

2.13.3 Procesos de Transmisión HDLC.

Modo balanceado Asíncrono con flujo de datos half dúplex.
Modo balanceado Asíncrono con flujo de datos full dúplex.
Recuperación de error Go-Back-N (punto de chequeo).
Recuperación de error Go-Back-N (Reject).
Recuperación de error Selective Reject.

Ejemplo de Modo Balanceado Asíncrono con flujo de datos half dúplex (Ver figura 2.16).

TIME SLOT	0	1	2	3	4	5	6	7	8
ESTACION A TRANSMITE	B,SABM P		B,I N(S)=0 N(R)=0	B,I,P N(S)=1 N(R)=0				A,RR,F N(R)=2	
ESTACION B TRANSMITE		B,UA,F			B,RR,F N(R)=2	A,I N(S)=0 N(R)=2	A,I,P N(S)=1 N(R)=2		B,RR,F N(R)=2

Figura 2.16
Tramas transmitidas en modo balanceado asíncrono Half Dúplex.

En el time slot 0, la estación A transmite un comando SABM con el bit P=1 y la dirección de la estación B.

En el time slot 1, la estación B responde con un UA con el bit F=1 y la dirección de la estación B.

En el time slot 2 y 3, la estación A envía tramas de información 0 y 1 con N(S)=0 y N(S)=1 respectivamente y con el bit P=1 en la trama 1. Las tramas contienen la dirección de B.

En los time slots 4, 5, 6, la estación B reconoce la transmisión de A con un RR y poniendo N(R)=2 y F=1.

La estación B también transmite tramas de información 0 y 1.

Las tramas de información tienen N(R)=2. En la trama de información 1 el bit P es puesto a 1. La trama del time slot 4 contiene la dirección de B y la 5 y 6 la dirección de A.

En el time slot 7, la estación A reconoce las tramas 0 y 1 de B con un RR, N(R)=2 y un bit F=1. La trama contiene la dirección de A.

En el time slot 8, la estación B también reconoce la última transmisión de A con RR, el bit F=1 y N(R) aún en 2.

Ejemplo de modo balanceado asíncrono con flujo de datos full dúplex (Ver figura 2.17).

TIME SLOT	0	1	2	3	4	5	6	7	8
ESTACION A TRANSMITE	B,I N(S)=0 N(R)=0	B,I,P N(S)=1 N(R)=1			B,I N(S)=2 N(R)=3	B,RR,P N(R)=4		B,I N(S)=3 N(R)=5	B,RR,P N(R)=6
ESTACION B TRANSMITE	A,I N(S)=0 N(R)=0	A,I N(S)=1 N(R)=1	B,RR,F N(R)=2	A,I N(S)=2 N(R)=2	A,I N(S)=3 N(R)=2	A,I N(S)=4 N(R)=3	B,RR,F N(R)=3	A,I N(S)=5 N(R)=3	A,RR,P N(R)=4

Figura 2.17
Tramas transmitidas en modo balanceado asíncrono Full Dúplex.

En el time slot 0, las estaciones A y B transmiten una trama de información con N(S)=0.

En el time slot 1, las estaciones A y B envían reconocimientos de recepción de las tramas 0 con N(R)=1 en tramas de información con N(S)=1, pero la estación A solicita una respuesta de B con el bit P=1.

En el time slot 2, la estación B emite un RR con N(R)=2 y F=1 para reconocer la trama número 1 de A. Puede observarse que el bit F fué puesto a 1 en respuesta al bit P de la trama del time slot 1, pero bajo modo ABM, puede continuar transmitiendo.

En el time slot 3, la estación B transmite una trama de información 2.

En el time slot 4, la estación A envía una trama de información 2 y el reconocimiento de las tramas 1 y 2 de B con N(R)=3. La estación B envía una trama de información 3.

En el time slot 5, la estación A no tiene nada que enviar, pero reconoce la trama número 3 de B con un RR y un N(R)=4, además pide una respuesta con P=1. La estación B reconoce la trama número 2 de A con un N(R)=3 en una trama de información con N(S)=4.

En el time slot 6, la estación B responde al bit P anterior con un bit F=1 en un RR.

En el time slot 7, la estación A transmite la trama número 3 y el reconocimiento de la trama número 4 de B con N(R)=5. La estación B transmite la trama número 5.

En el time slot 8, ninguna de las estaciones tiene nada que enviar. La estación A envía un RR con N(R)=6 par indicar recepción de la trama 5 de B. La estación B reconoce la trama 3 de A con un RR y N(R)=4.

Ejemplo de recuperación de error Go-Back-N (punto de chequeo ver figura 2.18).

TIME SLOT	0	1	2	3	4	5	6	7	8
ESTACION A TRANSMITE	B,I N(S)=6 N(R)=4	B,I, N(S)=7 N(R)=4 ERROR	B,I N(S)=0 N(R)=4	B,I,P N(S)=1 N(R)=4		B,I N(S)=7 N(R)=4	B,I N(S)=0 N(R)=4	B,I,P N(S)=1 N(R)=4	
ESTACION B TRANSMITE					B,RR,F N(R)=7				B,RR,P N(R)=2

Figura 2.18
Tramas transmitidas con recuperación de error Go-Back-N.

En los time slots 0, 1, 2, 3, la estación A envía tramas de información 6, 7, 0 y 1. Durante este período la estación B detecta un error en la trama 7. En el time slot 3, la estación A envía un bit P (poll) para actuar como un punto de chequeo, por ejemplo solicitar una respuesta de la estación B.

En el time slot 4, la estación B retorna un RR con un número de secuencia N(R)=7 y F=1. Esto significa que la estación B está esperando recibir la trama 7 de nuevo (y todas las tramas transmitidas después de 7).

En los time slots 5, 6, y 7, la estación A retransmite las tramas 7, 0 y 1 y establece el bit P como un punto de chequeo.

En el time slot 8, la estación B reconoce las tramas 7, 0 y 1 con un RR, N(R)=2 y F=1.

El uso exclusivo del campo de secuencia de recepción N(R) para indicar que no se reconoció una trama no es recomendado para transmisiones full dúplex. Debido a que las tramas están fluyendo en ambas direcciones a través del enlace, los números de secuencia de envío y recepción de las estaciones frecuentemente se traslapan. Por ejemplo si una estación A envía una trama 4 con N(S)=4 y al mismo tiempo una estación B envía una trama con N(R)=4. La estación A podría asumir falsamente que su trama 4 es incorrecta, cuando lo que indica la estación B es que espera la siguiente trama 4.

Ejemplo de recuperación de error Go-Back N (Reject)(Ver figura 2.19).

TIME SLOT	0	1	2	3	4	5	6
ESTACION A TRANSMITE	B,I N(S)=6 N(R)=4	B,I, N(S)=7 N(R)=4 ERROR	B,I N(S)=0 N(R)=4	B,I N(S)=7 N(R)=4	B,I N(S)=0 N(R)=4	B,I,P N(S)=1 N(R)=4	
ESTACION B TRANSMITE			B,REJ,F N(R)=7				B,RR,F N(R)=2

Figura 2.19
Tramas transmitidas con recuperación de error Go-Back-N (Reject).

En los time slot 0, 1 y 2, la estación A envía información de las tramas 6, 7 y 0. La estación B detecta un error en la trama 7, inmediatamente envía una trama de Reject con un N(R)=7. La estación B no espera por un punto de chequeo, pero envía un REJ como una respuesta con F=1. Si la estación B ha enviado el REJ como un comando la estación A tendrá que contestar con RR, RNR o REJ. Sin embargo, debido a que el REJ es una respuesta, la estación A inmediatamente retransmite la trama errónea.

En los time slots 3, 4 y 5, la estación A retransmite las tramas 7 y 0 y envía la trama 1 con P=1.

En el time slot 6, la estación B reconoce las tramas 0, 7 y 1 con RR y N(R)=2.

Ejemplo de recuperación de error (Selective Reject) (Ver figura 2.20).

TIME SLOT	0	1	2	3	4	5
ESTACION A TRANSMITE	B,I N(S)=6 N(R)=4	B,I, N(S)=7 N(R)=4 ERROR	B,I N(S)=0 N(R)=4	B,I N(S)=7 N(R)=4	B,I,P N(S)=1 N(R)=4	
ESTACION B TRANSMITE			B,SREJ,F N(R)=7			B,RR,F N(R)=2

Figura 2.20
Tramas transmitidas con recuperación de error (Selective Reject).

En los time slots 0 1 y 2, la estación A transmite tramas de información 6, 7 y 0. La estación B detecta errores en la trama 7 y transmite un Selective Reject con N(R)=7. La estación B no requiere un RR, RNR o REJ, debido a que la trama en el time slot 2 no es un comando.

En el time slot 3 y 4, la estación A retransmite la trama 7 únicamente y transmite por primera vez la trama 1. Puesto que B envío un Select Reject la trama 0 no se retransmite.

En el time slot 5, la estación B reconoce todas las tramas restantes con un RR Y N(R)=2.

CAPITULO III

INTERCONEXION DE REDES.

3.1 Consideraciones generales.

Uno de los desarrollos tecnológicos con más éxito de los 80's han sido las redes de área local (LAN). Impulsadas por el desarrollo de las estaciones de trabajo (cada vez más poderosas), la popularidad de las redes surge de su capacidad para interconectar sistemas en forma local o sobre distancias extensas, para compartir inteligencia y acceso a recursos de computación y de información.

La importancia de las redes ha conducido a su vez, a una segunda generación de conectividad de estaciones de trabajo-enlace de red a interconexión de "redes a redes".

Existen cuatro tipos de productos de interconexión de redes LAN: Repetidores, Puentes, Enrutadores y Gateways. Cada uno de éstos representa un nivel diferente de conectividad y funcionalidad, definido por el modelo de Interconexión de Sistemas Abiertos (OSI). Este modelo define una base común para el diseño empleado por los desarrolladores que trabajan con cualquier tipo de productos de interconectividad. El modelo se aplica a cualquier clase de productos de interconectividad y cumple favorablemente con los productos de interconectividad LAN, ya que la mayoría de los fabricantes de estos productos utilizan protocolos que se ajustan a alguna capa del modelo.

Algunas definiciones básicas de interconexión de redes son las siguientes:

Conectividad.

Es la habilidad para enlazar diferentes piezas de hardware y software en un ambiente de red donde los recursos (aplicaciones, procesos, etc.) son compartidos.

Interconectividad.

Término que ha surgido para hablar del problema de comunicar redes de computo, del mismo o de diferente tipo, por medio de enlaces de comunicación. El término puede referenciar productos, procedimientos y tecnologías.

Interoperabilidad.

Es la habilidad que presenta el equipo de computación fabricado por diferentes compañías para comunicarse con éxito sobre una red.

3.2 Repetidores.

El equipo más simple de interconexión de redes LAN es el repetidor. Operando en la capa física del modelo de OSI, los repetidores extienden el alcance físico de redes idénticas regenerando señales de un cable y transmitiéndolas a otro. Como conectores de la capa física, los repetidores no efectúan parte alguna del procesamiento de nivel más alto que se requiere en las redes más complejas. Por lo tanto, los repetidores solamente pueden enlazar las redes con formatos de protocolo similares; están severamente limitados por la distancia; y tienen la mala virtud de repetir tanto los datos erróneos como los correctos. Los repetidores apoyan sólo la interconexión de redes locales dentro de un sólo edificio, realizando poco procesamiento de los paquetes de las redes, por lo que obtienen índices altos de producción (ver figura 3.1).

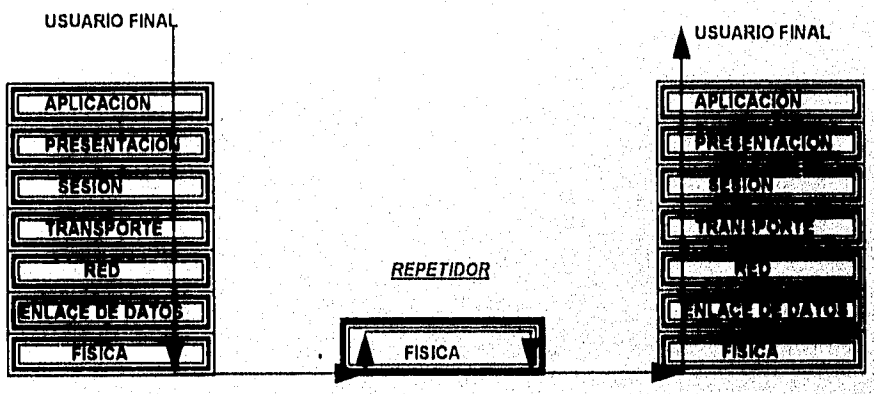


Figura 3.1
Modelo de un Repetidor de acuerdo al modelo OSI.

Como un dispositivo de interconectividad de redes, los repetidores están limitados a distancias cortas.

Teóricamente, un repetidor puede ser usado cuantas veces sea necesario. Prácticamente, muchas redes limitan el número de repetidores entre una estación transmisora y una estación receptora.

Los repetidores se encuentran definidos en la norma IEEE802.3c, IEEE802.3d e IEEE802.3k. Repetidores para 10 BaseT están fuera del alcance de estas normas.

3.3 Puentes (Bridge).

Los puentes interconectan redes en el nivel de enlace de datos, es decir en la capa 2 del modelo de OSI. Como tal, pueden leer la dirección fuente en la trama de datos y la dirección de destino, y si la dirección destino indica un nodo de una red remota, envía los paquetes a esa red (esto es llamado envío). Si la dirección reside en la red localmente conectada, el puente descarta (o filtra) esa trama. Debido a que los puentes pueden filtrar tramas leyendo las direcciones contenidas en éstas, son usualmente usados para dividir redes con demasiado tráfico en 2 segmentos de red.

En efecto los puentes crean redes sencillas, físicamente separadas y lógicamente unificadas.

Como un equipo de interconexión de capas MAC, los puentes ofrecen 2 ventajas claves sobre los repetidores así, como sobre los dispositivos de nivel más alto. Primero, debido a que los puentes no regeneran simplemente la señal eléctrica, sino que más bien regeneran las tramas y sus formatos, pueden extenderse distancias ilimitadas utilizando diferentes tipos de medios de transmisión, tales como líneas telefónicas privadas, conmutadas, enlaces digitales E0, enlaces digitales E1, o inclusive líneas de la Red Digital de Servicios Integrados RDSI (ver figura 3.2).

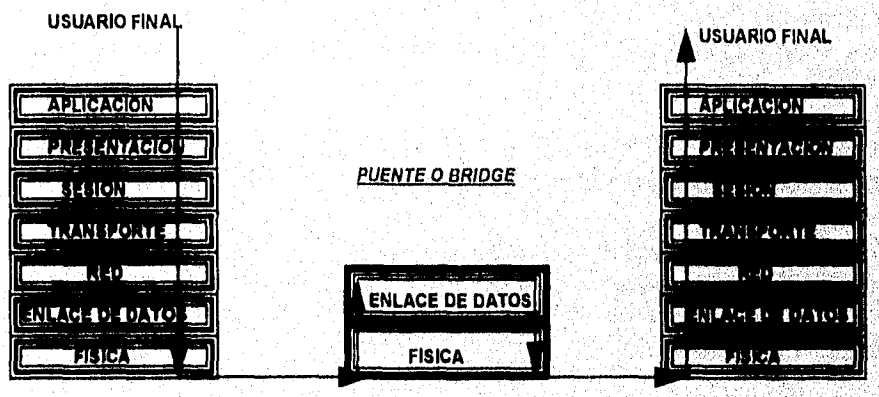


Figura 3.2
Modelo de un puente de acuerdo al modelo OSI.

Los puentes pueden ser usados tanto en medios ambientes locales como remotos. En los medios ambientes locales, un sólo puente con dos interfaces de red es típicamente configurado y el funcionamiento es generalmente similar a la velocidad de la red.

En los medios ambientes remotos, se utilizan dos puentes, teniendo cada uno una conexión para red local y una conexión para una red de área amplia.

Un buen puente tendrá un alto funcionamiento en relación con tres medidas comúnmente utilizadas: envío, filtración y eficiencia de enlace. Un puente debe enviar paquetes a velocidades consistentes con la velocidad del enlace de la red de área amplia.

3.3.1 Características de los puentes.

- Pueden interconectar 2 o más redes de área local, a los cuales se les denomina segmentos de red o subredes.

- Interconectan redes con un protocolo de capa MAC igual o diferente. Por ejemplo una red Ethernet y una red Ethernet o una red Ethernet y una red Token Ring.

- Realizan filtración de tramas. Si la dirección destino en una trama indica una estación en el segmento en donde se recibió la trama, el puente no puede dejar pasar esta trama a los demás segmentos para evitar un tráfico inútil.

- Realizan envío de tramas. Si la dirección destino en una trama indica una estación en otro segmento, entonces el puente envía la trama sólo hacia este segmento, adaptándola previamente al protocolo MAC del segmento destino.

- Realizan broadcast o inundación. Si un puente no conoce en que segmento se encuentra la estación destino envía la trama a todos los segmentos.

- Tienen la capacidad de aprender. Después de realizar broadcasts o inundaciones a segmentos desconocidos, el puente aprende en donde se encuentran los destinos, examinando las direcciones de las tramas que recibe como contestación.

Hay 2 clases de puentes: Transparentes (llamados algunas veces puentes de árbol de expansión o puentes que aprenden) y puentes de enrutamiento fuente.

La capa en la cual el puenteo ocurre, controla el flujo de datos, maneja errores de transmisión, proporciona direccionamiento físico y maneja acceso al medio físico.

Los puentes no son dispositivos complicados. Éstos analizan las tramas entrantes, toman decisiones de envio basados en la información contenida en las tramas, y envían las tramas al destino. En algunos casos (por ejemplo de

enrutamiento fuente) la ruta entera está contenida en la trama. En otros casos las tramas son enviadas a otro puente hacia el destino.

3.3.2 Tipos de puentes.

Los puentes son locales y remotos. Los puentes locales proporcionan una conexión directa entre múltiples segmentos LAN en la misma área. Los puentes remotos conectan múltiples segmentos LAN en diferentes áreas, generalmente con líneas de telecomunicación (ver figuras 3.3 y 3.4).

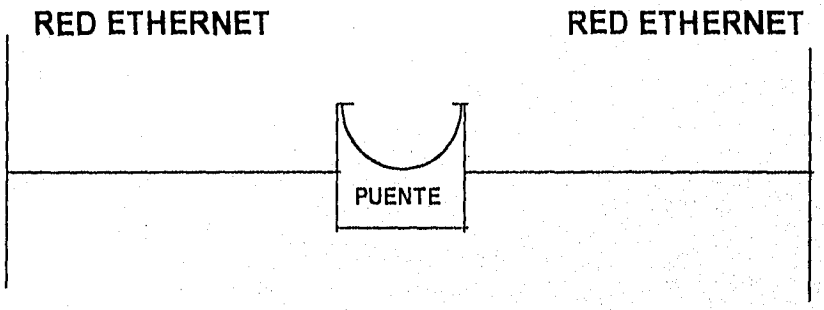


Figura 3.3
Puente Local.

Figura 3.4
Puente Remoto.

3.3.3 Puentes transparentes (Transparent Brindging).

Los puentes transparentes fueron desarrollados por Digital y posteriormente el IEEE incorporo su trabajo en el estándar IEEE 802.1d.

Se llaman puentes transparentes por que su presencia y operación es transparente a las estaciones de la red. Los puentes transparentes aprenden la topología de la red analizando la dirección fuente de las tramas entrantes de todas las redes conectadas. Si por ejemplo un puente ve una trama llegando en la línea 1 proveniente del host A, el puente concluye que el host A puede ser alcanzado a través de la red conectada a la línea 1. Con este proceso los puentes transparentes construyen sus tablas (Ver figura 3.5).

DIRECCION DE ESTACION	NUMERO DE RED
15	1
17	1
12	2
14	3

Figura 3.5
Tabla Típica de un Puente Transparente.

El puente usa su tabla como la base para el envío de tráfico. Cuando una trama es recibida en una de las interfaces del puente, el puente busca la dirección destino de la trama en su tabla interna. Si la tabla contiene alguna asociación entre la dirección destino y alguno de los puertos del puente, la trama es enviada dentro del puerto indicado. Si no se encuentra asociación, la trama es enviada a todos los puertos excepto el puerto entrante. Broadcasts y multicasts son enviados en la misma forma. Los puentes transparentes aíslan exitosamente el tráfico entre segmentos, por lo tanto reducen el tráfico visto en cada segmento individual.

3.3.3.1 Loops de puentes.

Un algoritmo de puentes transparentes falla cuando hay múltiples trayectorias de puentes entre dos LAN, y por lo tanto se requiere un protocolo de puente a puente que ayude a corregir el problema.

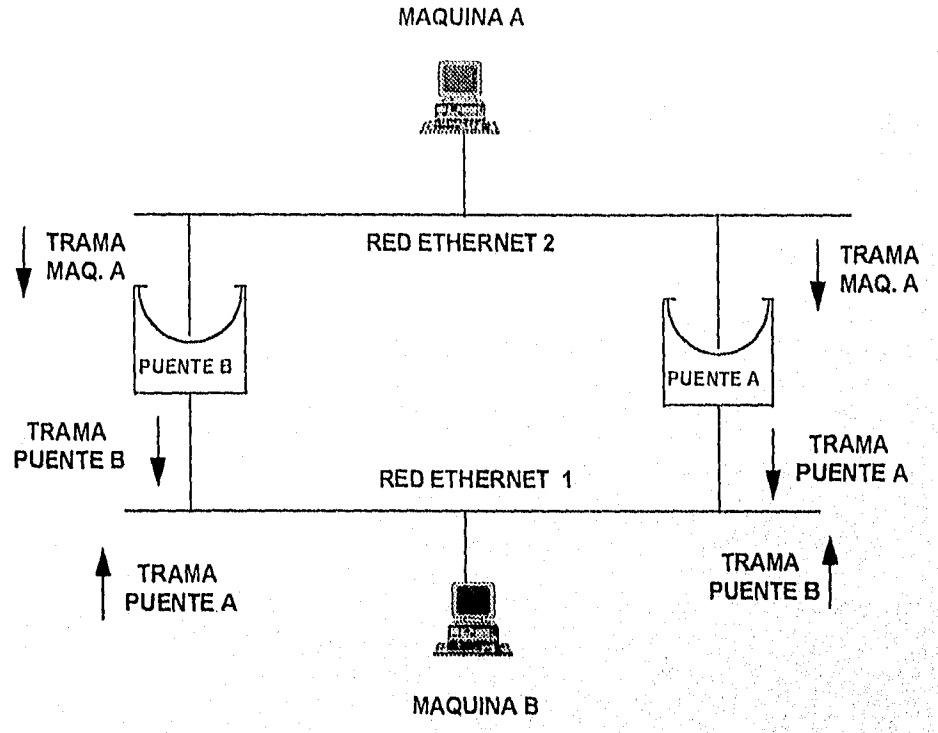


Figura 3.6
Loops de Puentes.

Suponer que se tiene la conexión de la figura 3.6 y la estación A envía una trama a la estación B. Ambos puentes reciben la trama y correctamente concluyen que la estación B está en la red 1. Desafortunadamente, después de que la estación B recibe dos copias de la trama de la estación A, ambos puentes recibirán de nuevo la trama en sus interfaces de red 1, debido a que todos los hosts reciben todos los mensajes en broadcast. En algunos casos los puentes cambiarán sus tablas para indicar que la máquina A está en la red 1 (lo que es falso).

3.3.3.2 Algoritmo de árbol de expansión (SPANNING-TREE STA).

El algoritmo de árbol de expansión (STA) se aplica para solucionar los problemas que se presentan cuando existen trayectorias en loop entre dos o más puentes.

El algoritmo STA utiliza una conclusión de la teoría de grafos como base para la construcción de un subconjunto de la topología de la red libre de loops.

La teoría de grafos expresa lo siguiente :

Para cualquier grafo conectado que consista de nodos y líneas y que conecte pares de nodos, hay un árbol de expansión de líneas que mantiene la conectividad del grafo pero no contiene loops.

En la figura 3.7a se observa como STA elimina los loops. STA llama a cada uno de los puentes para que se les asigne un identificador único. Típicamente, este identificador es su dirección física MAC (Control de Acceso al Medio) más una prioridad. A cada puerto en cada puente también se le asigna un identificador (típicamente su propia dirección MAC). Finalmente, cada puerto del puente es asociado con un costo de trayectoria. El costo de trayectoria representa el costo de transmisión de una trama hasta una LAN a través de ese puerto.

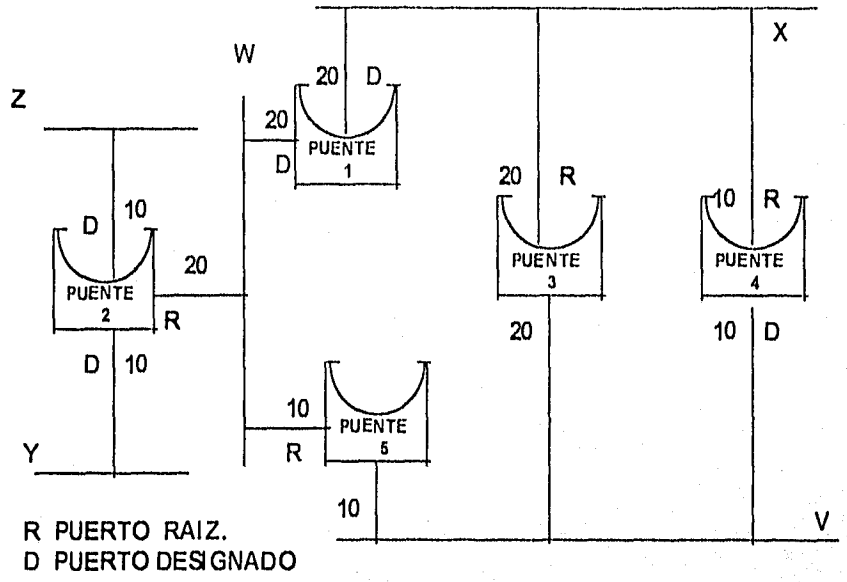
En la figura 3.7a, los costos de trayectoria están anotados en las líneas saliendo de cada puente. Normalmente éstos son valores de default, pero pueden ser cambiados por el administrador de red.

La primera actividad de STA es la selección del puente raíz, el cual es el puente con el más bajo valor de identificador de puente. En la figura 3.7a, el puente raíz es el puente 1. A continuación se asigna el puerto raíz en todos los demás puentes. Un puerto raíz de un puente es el puerto a través del cual el puente raíz puede ser alcanzado con el costo de trayectoria agregado menor. Este valor es llamado el menor costo de la trayectoria a la raíz.

Finalmente, los puentes designados y sus puertos designados son determinados. Un puente designado es el puente en cada LAN que proporciona el mínimo costo de trayectoria raíz. Un puente designado de LAN es el único puente al que se le permite enviar y recibir tramas para la LAN del cual es el designado. Un puerto designado de LAN es el puerto que conecta a esta red con el puente designado.

En algunos casos dos o más puentes pueden tener el mismo costo de trayectoria raíz. Por ejemplo, en la figura 3.7a, los puentes 4 y 5 pueden alcanzar al puente 1 con un costo de trayectoria de 10. En este caso, los identificadores de puente son usados de nuevo, esta vez para determinar los puentes designados. El puerto del puente 4 a la LAN V es seleccionado sobre el puerto del puente 5 a la LAN V.

Usando este proceso, todos excepto uno de los puentes directamente conectados a cada LAN son eliminados, por lo tanto son removidos todos los loops entre 2 LAN's. El STA también elimina todos los loops involucrando más de dos LAN.
La figura 3.7b, muestra el resultado de aplicar el algoritmo de árbol de expansión a la red de la figura



3.7a.

Figura 3.7a
Red Antes de Correr Algoritmo de Árbol de Expansión.

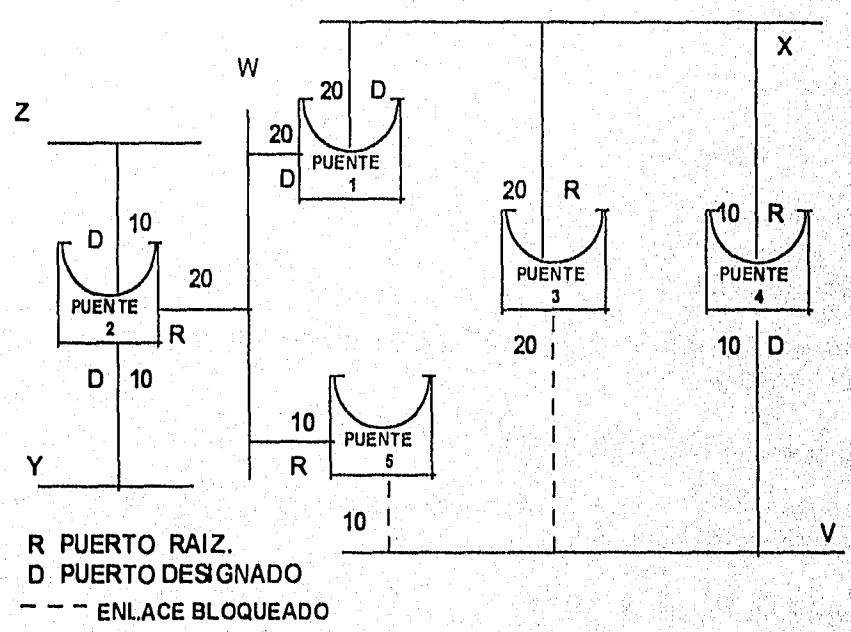


Figura 3.7b
Red Después de Correr Algoritmo de Árbol de Expansión.

3.3.3.3 Formato de trama de puentes transparentes.

Los puentes transparentes intercambian mensajes de configuración y mensajes de cambio en la topología de la red. Los mensajes de configuración son enviados entre puentes para establecer la topología de la red. Los mensajes de cambio de topología son enviados después de que un cambio de topología fue detectado para indicar que el STA debe ser arrancado de nuevo.

2	1	1	1	8	4	8	2	2	2	2	2
IDENTIFI-DOR DE PROTOCOLO	VERSION	TIPO DE MENSAJE	BANDERAS	IDENTIFICA-DOR DE RAIZ.	COSTO DE LA TRAYECTO-RIA RAIZ	IDENTIFI-CADOR DE PUENTE	IDENTIFI-CADOR DE PUERTO	EDAD DEL MENSAJE	EDAD MAXIMA	TIEMPO HELLO	RETAR-DO DE ENVIO.

Figura 3.8
Formato del mensaje de configuración de puentes transparentes.

Formato del mensaje de configuración IEEE802.1d para puenteo transparente TB (ver figura 3.8).

Campo identificador de protocolo.

Es establecido a cero.

Campo de versión.

Es establecido a cero.

Campo de tipo de mensaje.

Es establecido a cero.

Campo de banderas.

Este campo de 8 bytes identifica el puente raíz. Con 2 bytes su prioridad y con 6 bytes su identificación.

Campo de costo de la trayectoria raíz.

Este campo contiene el costo de la trayectoria del puente enviando el mensaje de configuración al puente raíz.

Campo de identificación del puente.

Este campo contiene el número de identificación y la prioridad del puente enviando el mensaje.

Campo de identificación del puerto.

Identifica el puerto del cual el mensaje de configuración fué enviado. Este campo permite que loops creados por múltiples puentes conectados sean detectados y eliminados.

Campo de edad del mensaje.

Especifica la cantidad de tiempo desde que la raiz envío el mensaje de configuración hasta el cual el mensaje de configuración actual está basado.

Campo de edad máxima.

Indica cuando el mensaje de configuración actual debe ser borrado.

Campo de tiempo de hola.

Proporciona el periodo de tiempo entre mensajes de configuración del puente raíz.

Campo de retardo de envío.

Proporciona la cantidad de tiempo que los puentes deben esperar en transición para un nuevo estado, después de un cambio de topología.

Los mensajes de cambio topológico consisten de 4 bytes. Ellos incluyen un campo identificador de protocolo con valor cero, un campo de versión con valor cero y un campo de tipo de mensaje con valor 128.

3.3.4 Puentes de enrutamiento fuente (SRB).

El algoritmo de enrutamiento fuente fue desarrollado por IBM.

Se llaman puentes de enrutamiento fuente, debido a que ellos asumen que la ruta fuente-destino completa es colocada en todas las tramas enviadas por la fuente. Estos puentes almacenan y envían tramas como se indica en los campos de las tramas recibidas.

Por ejemplo refiriéndonos a la figura 3.9, la estación X desea enviar una trama a la estación Y. Inicialmente la estación X no sabe si la estación Y reside en la misma LAN o en otra LAN. Para determinar esto, la estación X envía una trama de prueba. Si la trama retorna a la estación X sin una respuesta positiva asume que la estación Y está en un segmento remoto.

Para determinar la localización exacta de la estación Y, la estación X envía una trama de exploración. Cada puente al recibir la trama de exploración, copia la trama dentro de todos los puertos salientes. La información de la ruta es agregada a las tramas exploradoras conforme ellas viajan a través de las redes. Cuando las tramas de exploración de la estación X alcanzan a la estación Y, la estación Y contesta a cada una individualmente usando la información de la ruta acumulada. Después de recibir las respuestas de todas las tramas, la estación X puede elegir la ruta más conveniente basada en un criterio predeterminado como:

- Primera trama recibida.
- Respuesta con mínimo número de saltos.
- Respuesta con el más grande tamaño de trama permitida.

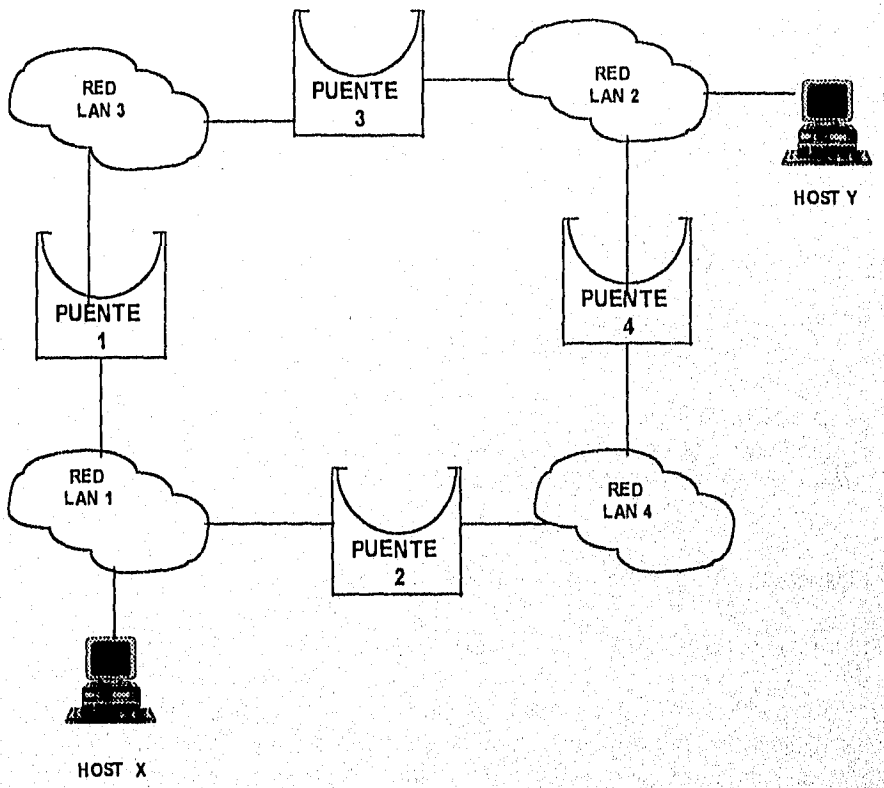


Figura 3.9
Puentes de Enrutamiento Fuente.

Después de que la ruta es seleccionada, ésta es insertada dentro de las tramas destinadas para la estación Y, en forma de un campo de información de enrutamiento (RIF). Un campo de información de enrutamiento únicamente es incluido en aquellas tramas destinadas a otras LAN. La presencia de

información de enrutamiento dentro de la trama se indica por el establecimiento a 1 del bit más significativo del campo de dirección fuente, llamado bit indicador de información de enrutamiento (RII).

El subcampo de tipo en el campo de información de enrutamiento (RIF) indica si la trama debe ser enrutada a un sólo nodo, o grupo de nodos comprendiendo un árbol de expansión de todos los nodos (ver figura 3.10).

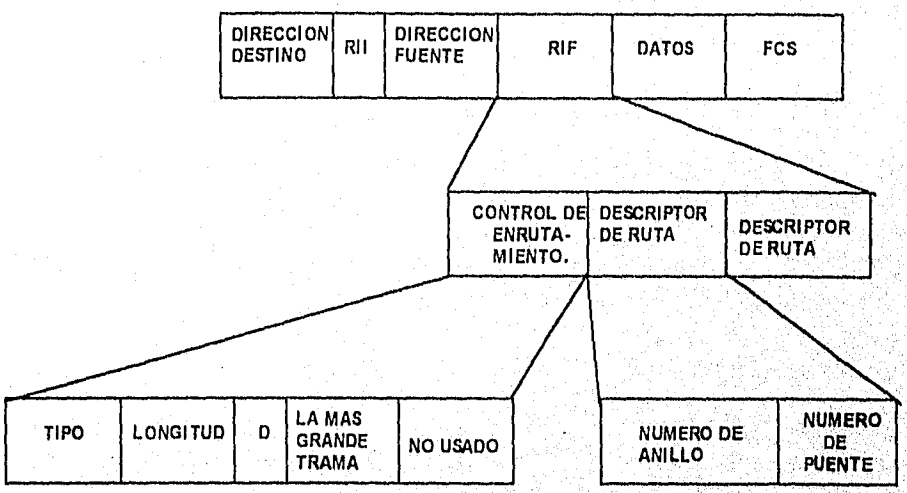


Figura 3.10
Formato de trama IEEE802.5.

3.3.5 Puentes de medio mezclado.

Los puentes transparentes son encontrados predominantemente en redes Ethernet, así como los puentes de enrutamiento fuente son encontrados en redes Token Ring. La pregunta en este punto es ¿Existe alguna forma de comunicar estos puentes?

Últimamente, la meta de interconexión entre puentes transparentes y puentes de enrutamiento fuente es permitir comunicación entre estaciones Ethernet y Token Ring, pero se tienen varios retos de traslado, los cuales se mencionan a continuación:

Incompatible ordenamiento de bits.

Aunque Ethernet y Token Ring soportan direcciones MAC de 48 bits, la representación de hardware interna de estas direcciones difiere. Una cadena serial de bits representando una dirección MAC de Token Ring considera al

primer bit encontrado como el bit de mayor valor significativo. Ethernet, por lo contrario, considera al primer bit encontrado como el bit menos significativo.

Direcciones MAC dentro del campo de porción de datos de la trama.

Como un ejemplo se tiene al protocolo ARP que coloca direcciones en la porción de datos de la trama de capa de enlace. Conversiones de direcciones que pueden o no aparecer en el campo de datos es difícil por que deben manejarse caso por caso.

Incompatibles tamaños de unidad de transferencia máxima.

Token Ring y Ethernet soportan diferentes tamaños de trama máxima. Ethernet soporta aproximadamente 1500 Bytes, mientras que la tramas Token Ring pueden ser mucho más grandes. Como los puentes no son capaces de fragmentación y reensamble de tramas, las tramas que exceden el tamaño máximo de trama son dadas de baja.

Bits de estado de trama.

Las tramas Token Ring incluyen 3 bits de estado de trama A, C y E. El propósito de estos bits es decirle a la fuente de la trama si el destino vió la trama (Bit A establecido a uno), copió la trama (Bit B establecido a uno) y/o encontró errores en la trama (Bit E establecido a uno). Ethernet no soporta estos bits.

Manejo de funciones exclusivas de Token Ring.

Ciertos bits de Token Ring no tienen significado en Ethernet, por ejemplo Ethernet no tiene mecanismo de prioridad.

Los puentes transparentes no saben que hacer con la ruta descubierta en las tramas de puentes de enrutamiento fuente.

El algoritmo de puentes de enrutamiento fuente coloca un campo de información de enrutamiento. El algoritmo de puentes transparentes no tiene un equivalente, y la idea de colocar información de enrutamiento no es válida.

Hay incompatibles algoritmos de árbol de expansión para evitar loops.

Cuando un puente de enrutamiento fuente recibe una trama sin campo de enrutamiento fuente la desecha.

Para resolver los problemas anteriores surgen dos tipos de puentes.

Los puentes traductores y los puentes de enrutamiento fuente transparente. Estos proporcionan una solución relativamente barata para algunos de los muchos problemas involucrados con puenteo entre puentes transparentes y puentes de enrutamiento fuente (ver figura 3.11).

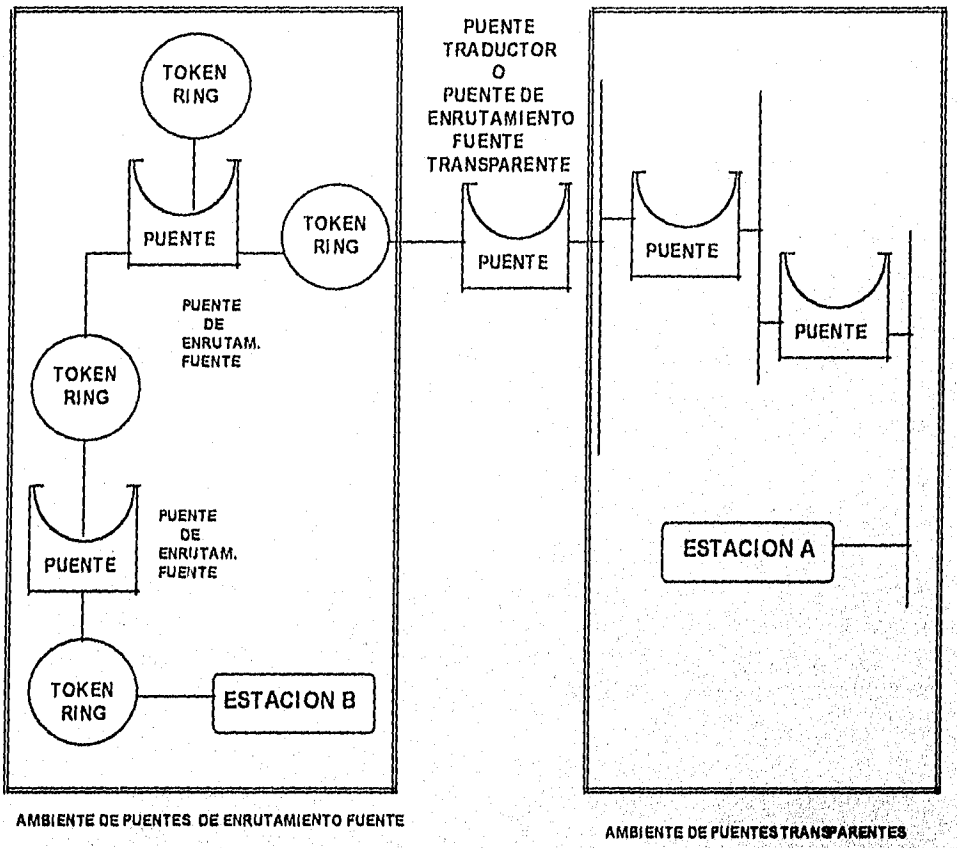


Figura 3.11
PuenteS de Medio Mezclado.

3.3.6 Puentes traductores (SR/TLB).

Los puentes traductores reordenan bits de direcciones fuente y destino cuando convierten tramas de Ethernet a Token Ring. El problema de direcciones contenidas en el campo de datos puede ser resuelto programando el puente para checar varios tipos de direcciones MAC. Algunos puentes traductores checan por las más populares direcciones.

El campo de RIF tiene un subcampo que indica el más grande tamaño de trama que puede ser aceptado por una implementación particular de un puente de

enrutamiento fuente. Los puentes traductores que envían tramas de un puente transparente a un puente de enrutamiento fuente, usualmente establecerán su tamaño máximo de trama a 1500, para limitar el tamaño de tramas Token Ring entrando al dominio de puentes transparentes.
Bits representando funciones de Token Ring que no tienen interpretación Ethernet son desechados por los puentes traductores. Por ejemplo los bits de prioridad, monitoreo y reservación son descartados.

3.3.7 Puentes de enrutamiento fuente transparente (SRTB).

El puente de enrutamiento fuente transparente combina implementaciones de puentes transparentes y puentes de enrutamiento fuente. SRT usa el bit indicador de información de enrutamiento para distinguir entre tramas de puentes de enrutamiento fuente y tramas de puentes transparentes. Si el campo mencionado es establecido a 1, un RIF está presente en la trama, y el puente es de enrutamiento fuente. Si el campo de RIF es puesto a cero, RIF no está presente y el puente es transparente.

3.4 Enrutadores (Routers).

Interconectan redes en la capa de red (capa 3) del modelo de OSI, los enrutadores ofrecen el siguiente nivel de interconectividad con la dirección selectiva de paquetes de datos individuales sobre múltiples trayectorias de comunicaciones (ver figura 3.12).

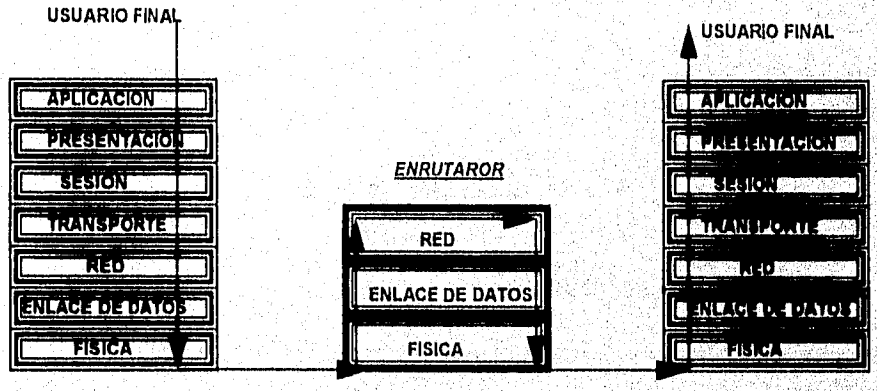


Figura 3.12
Modelo de enrutador de acuerdo al modelo OSI.

La información de la capa 3 normalmente incluye lo que es llamado una dirección de red lógica. A diferencia de la dirección física de los dispositivos

(tarjetas de red, hardware de computadoras, hardware de enrutadores etc.), que no es asignada por el administrador de red, la dirección lógica sí lo es.

Las subdivisiones de la red física en redes lógicas, son frecuentemente llamadas subredes.

Los enrutadores envían información a través de las redes usando la información de dirección de red lógica en lugar de la información de red física.

Está dirección lógica se encontrará en el contenido de los paquetes de datos.

Los enrutadores pueden enviar paquetes sobre diferentes trayectorias en la red, dependiendo de las prioridades del usuario. Con su capacidad de ir más a detalle en los formatos de paquetes, los enrutadores pueden proporcionar segmentación de una red física en varias redes lógicas interconectadas, llamadas subredes. El procesamiento extra requerido para manipular paquetes, afecta negativamente a la producción de paquetes. En la mayoría de los casos los enrutadores introducen retrasos más largos en los paquetes para llegar de un nodo a otro nodo y por consiguiente tiempos de respuesta más lentos.

Existen diversos tipos de enrutadores, pero su clasificación se puede reducir a internos, externos, locales y remotos. De tal forma, que siempre tendremos un enrutador: local interno o externo, remoto interno o externo. La clasificación también dependerá del servicio que ofrezca; si se habla de un enrutador local interno, dará servicio local instalado dentro de un servidor de archivos. Si es local externo, realizará sus tareas instalado en una estación de trabajo.

El enrutador puede ser instalado en una estación dedicada o no al proceso, externo al servidor de archivos; aunque esta configuración existe, lo más recomendable es contar con un enrutador dedicado ya que corren menos riesgos de bloqueo que le impidan desarrollar sus tareas.

Los tipos de enrutadores, se definen por las características con que fueron construidos, y pueden ser de hardware o de software, simples y múltiples.

Un enrutador simple, brinda servicios de enrutamiento para un protocolo específico, mientras que un enrutador multiprotocolo lo hace para diferentes protocolos como: IPX, IP, Apple Talk, OSI, etc.

- Enrutadores multiprotocolo.

Estos enrutadores son capaces de manejar un número importante de puertos para redes de área local y puertos síncronos para redes de área amplia. Cada puerto puede ser configurado para manejar un protocolo diferente, lo que

implica un esquema de direccionamiento diferente. Estos enrutadores son capaces de encapsular un protocolo en otro, es decir, enviar en la porción de datos del mensaje de un protocolo, mensajes de otro protocolo.
Los enrutadores utilizan algoritmos específicos de enrutamiento para calcular la mejor trayectoria a través de la red. Ejemplos de estos algoritmos son: RIP, IGRP y OSPF.

Enrutamiento involucra dos actividades básicas: Determinación de las trayectorias de enrutamiento óptimas y el transporte de grupos de información (paquetes) a través de las redes.

La determinación de la trayectoria puede estar basada en una variedad de métricas o combinación de métricas. Implementaciones de software de algoritmos de enrutamiento calculan las métricas de cada ruta para determinar la ruta óptima al destino.

Para ayudar en el proceso de determinación de la trayectoria, los algoritmos de enrutamiento inicializan y mantienen tablas de enrutamiento, las cuales contienen información de las rutas.

Los enrutadores se comunican entre sí y mantienen sus tablas de enrutamiento a través del intercambio de mensajes.

3.4.1 Conmutación.

Los algoritmos de conmutación son relativamente simples y básicamente son los mismos en la mayoría de los protocolos de enrutamiento. En muchos casos una estación A determina que debe de enviar un paquete a una estación B. Habiendo adquirido la dirección física del enrutador por algún medio, la estación fuente A envía un paquete con la dirección física del enrutador, pero con la dirección de protocolo de la estación destino B. Examinando la dirección de protocolo del paquete, el enrutador determina que no conoce la estación destino B y envía el paquete al siguiente enrutador cambiando la dirección física destino anterior del paquete con la dirección física del siguiente enrutador y dejando la dirección de protocolo del destino igual. El proceso de conmutación continua entre enrutadores, cambiándose la dirección física destino del paquete y dejándose constante la dirección de protocolo destino, hasta que se entrega el paquete a la estación destino B.

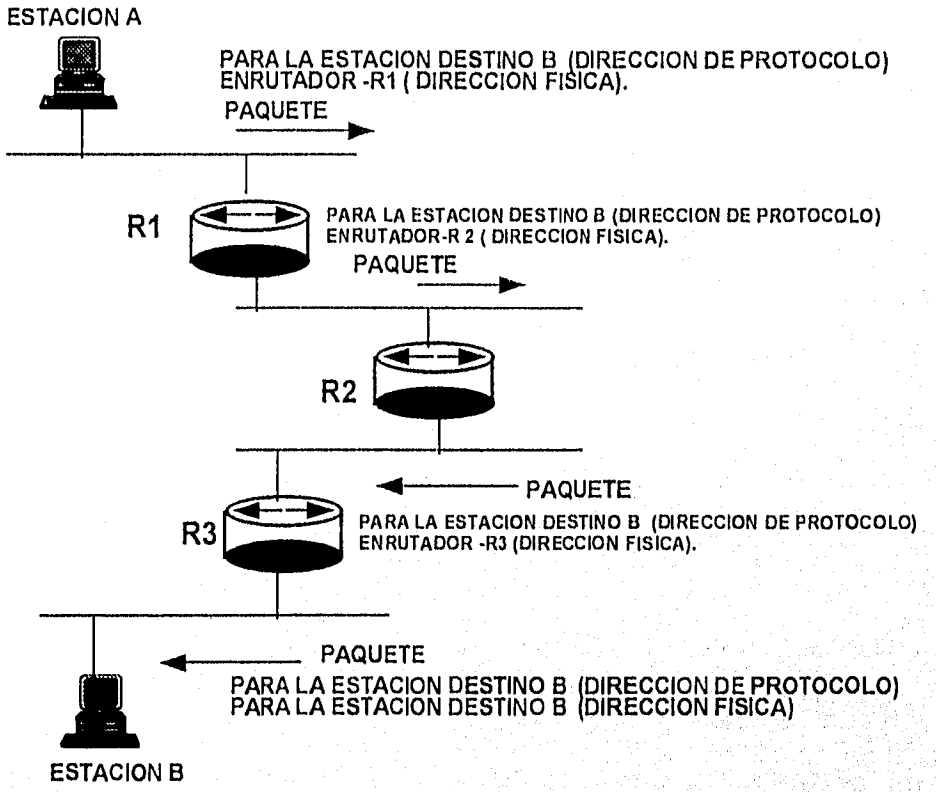


Figura 3.13
Ejemplo de conmutación de enrutadores.

3.4.2 Métricas de enrutamiento.

Longitud de la trayectoria.

La longitud de la trayectoria es la más frecuente métrica de enrutamiento. Algunos protocolos de enrutamiento definen el conteo de nodos (enrutadores) por donde los paquetes deben viajar en la ruta de la fuente al destino, otros asignan costos.

Confiabilidad.

La confiabilidad generalmente es asignada por el administrador de red, y es generalmente un factor numérico que especifica que tan seguro es un enlace con respecto de otro, tomando en cuenta el comportamiento de éstos dentro de la red.

Retardo.

El retardo se refiere a la cantidad de tiempo requerido para llevar un paquete de la fuente al destino a través de las redes. El retardo depende de muchos factores, incluyendo el ancho de banda de enlaces de red intermedios, las colas de información en cada enrutador a lo largo del camino, la congestión de la red y la distancia física a ser recorrida.

Ancho de banda.

El ancho de banda se refiere a la capacidad de tráfico disponible en el enlace.

Carga.

Carga se refiere al grado en el cual un recurso de la red está ocupado. La carga puede ser calculada en por ciento de utilización de CPU y paquetes procesados por segundo.

3.4.3 Clasificación de los algoritmos de enrutamiento.

Estáticos o dinámicos.

En los algoritmos estáticos la tablas de enrutamiento son establecidas por el administrador de red antes del inicio del enrutamiento. Debido a que los sistemas de enrutamiento estático no pueden reaccionar a cambios de la red, son considerados hoy en día inconvenientes.

Los algoritmos dinámicos ajustan en tiempo real los cambios ocurridos en la red, mediante mensajes de actualización de enrutamiento.

Trayectoria simple o multitrayectoria.

Algunos protocolos de enrutamiento soportan múltiples trayectorias al mismo destino. Estos algoritmos permiten tráfico multiplexado sobre múltiples líneas a diferencia de los algoritmos de trayectoria simple.

Horizontales o jerárquicos.

En un sistema de enrutamiento horizontal todos los enrutadores son iguales a los otros. En un sistema de enrutamiento jerárquico algunos enrutadores forman lo que equivale al backbone de enrutamiento. Los paquetes de los enrutadores que no pertenecen al backbone viajan a través de los enrutadores del backbone, hasta que ellos alcanzan el área general del destino. En este punto

ellos viajan del último enrutador de backbone a través de uno o más enrutadores que no pertenecen al backbone hasta el destino final.

Estación inteligente o enrutador inteligente.

Algunos protocolos asumen que el extremo del nodo fuente determinará la ruta completa. Esto es comúnmente llamado enrutamiento fuente.
Otros algoritmos asumen que las estaciones no saben nada acerca de las rutas. En estos algoritmos los enrutadores determinan la trayectoria a través de las redes con sus propios cálculos.

Estado del enlace o vector a distancia.

Los algoritmos de estado del enlace o algoritmos de primera trayectoria más corta, inundan de información de enrutamiento a todos los nodos entre las redes. Sin embargo, cada enrutador envía solamente la porción de la tabla de enrutamiento que describe el estado de sus propios enlaces. Los algoritmos de vector a distancia piden que cada enrutador envíe toda o porción de sus tablas de enrutamiento pero únicamente a sus vecinos. En resumen, los algoritmos del estado del enlace envían pequeñas actualizaciones a todos los enrutadores, mientras que los algoritmos de vector a distancia envían grandes actualizaciones únicamente a los enrutadores vecinos.

3.4.4 Enrutamiento directo IP.

Si los dos hosts están en la misma subred (segmento LAN), no es necesario un enrutador IP. Los protocolos ARP y RARP pueden proporcionar la información necesaria para entregar la información a la correcta dirección física de interface de red.

3.4.5 Enrutamiento indirecto IP.

El término enrutamiento indirecto se refiere al hecho de que el host fuente no alcanzará al host destino sin un enrutador IP. Por lo tanto la entrega de los datos no será manejada por el host directamente usando las direcciones físicas de la interface de red, sino indirectamente usando las direcciones IP y uno o más enrutadores IP.

Existen 3 métodos o formas básicas para que un enrutador pueda encontrar una ruta al host solicitado.

- Método de enrutamiento de manejo de tabla.
- Método de enrutamiento por default.
- Método de enrutamiento de host específico.

Los protocolos de enrutamiento IP son dinámicos. Enrutamiento dinámico significa que las rutas son calculadas por intervalos con el software de los dispositivos de enrutamiento.

El enrutamiento IP especifica como el datagrama viaja a través de las redes de un enrutador a otro. La ruta entera no es conocida. En lugar de tener la ruta completa conocida en cada enrutador se calcula el siguiente destino, comparando la dirección destino dentro del datagrama con la tabla de enrutamiento del enrutador.

3.5 Gateways.

Ninguno de los dispositivos discutidos hasta aquí muestra la necesidad de interconectar dos o más subredes que usen diferentes protocolos por encima de la capa de red. Cuando pequeñas redes son integradas físicamente con grandes redes, incompatibles protocolos de capa alta deben interoperar. El dispositivo que interconecte estas redes debe de alguna forma trasformar entre las implementaciones de los protocolos que son incompatibles. Ésta es la función del Gateway (ver figura 3.14).

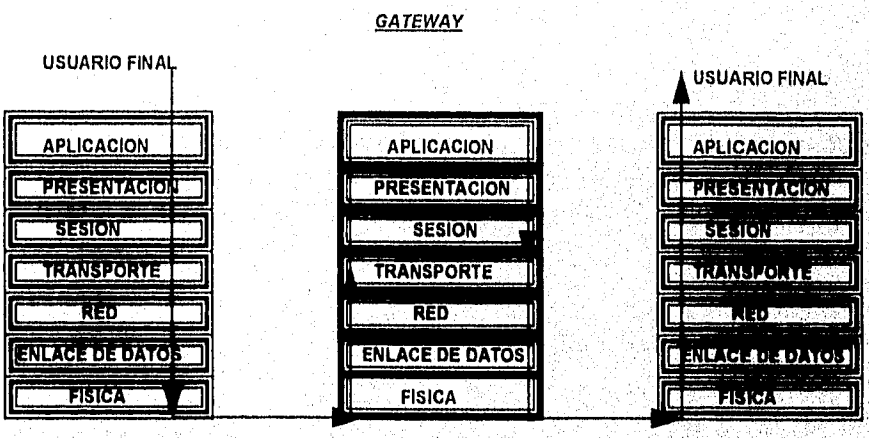


Figura 3.14
Modelo de un Gateway de acuerdo al modelo OSI.

Algunos ejemplos de Gateways son los siguientes:

Gateway IEEE802.3 a SNA
Gateway de IPX (Novell) a SNA
Gateway IEEE802.3 a X.25
Gateway Decnet-SNA

3.6 Escenarios de Interconexión.

a) Computadora personal PC remota a red de área local LAN.

b) Computadora personal PC remota a red de área amplia WAN.

c) Terminal asíncrona a red de área local LAN.

d) Red de área local a Red de área local.

e) Red de área local a Red de área amplia.

f) Red de área amplia a Red de área amplia.

a) El primer caso se presenta cuando se desea consultar información en una red LAN aislada desde un computadora personal en un sitio remoto. Un ejemplo de la situación anterior se tiene cuando un viajero desea consultar alguna información en la red de área local a la que pertenece su oficina.

Una solución para el ejemplo, es contar con un servidor de comunicaciones conectado a la red de área local al que se pueda accesar por la línea telefónica, y contar con un paquete de emulación de terminal y un módem en la PC remota (Ver figura 3.15).

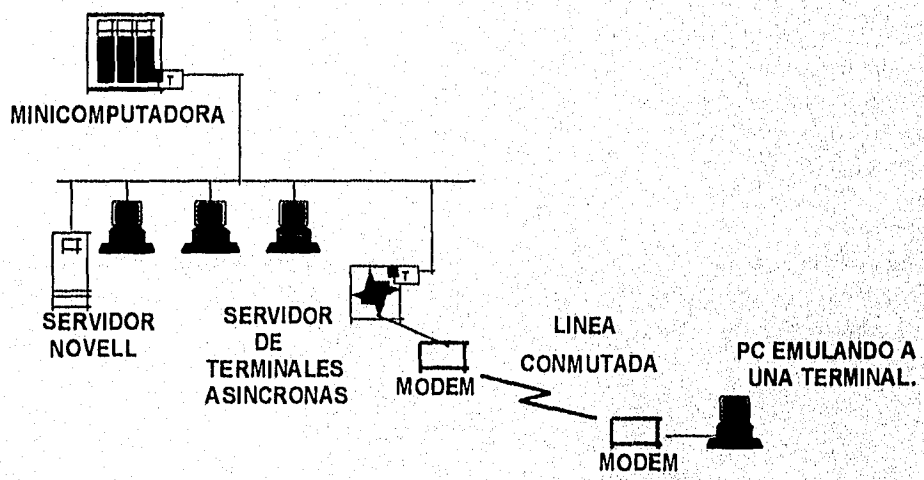


Figura 3.15
PC -remota accesando a una red de área local.

En un esquema de interconexión de redes UNIX-DOS con protocolo TCP/IP, esta opción permite manejar una sesión de terminal tonta a minicomputadora con sistema operativo UNIX.

Otra solución podría ser un servidor RLN dedicado conectado a la red de área local y un módem, así como software de cliente RLN y un módem en la PC remota (Ver figura 3.16).

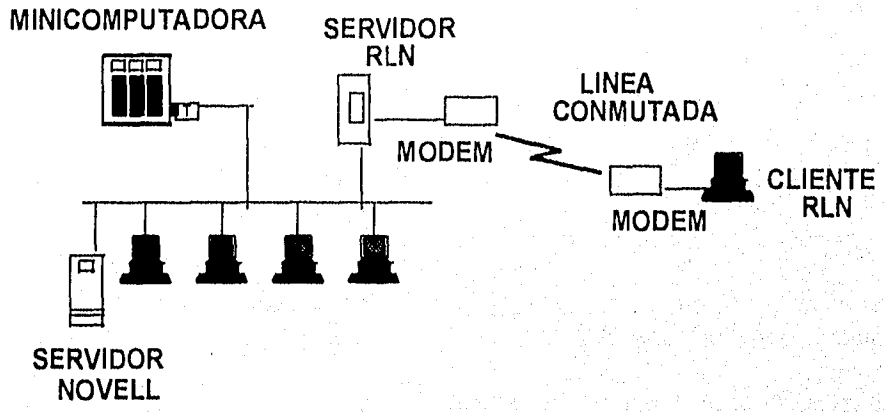


Figura 3.16
PC-Remota con software RLN accesando a una red de área local.

En un esquema de interconexión de redes UNIX-DOS con protocolos TCP/IP y SPX/IPX, esta opción permite que la PC se comporte como una estación de trabajo de una red Novell con sistema operativo DOS, o como un Host TCP/IP capaz de manejar una sesión de terminal virtual tonta a minicomputadora, con sistema operativo UNIX en la red local que se llama o cualquier otra red local interconectada.

b) Para realizar la comunicación de una PC a una red WAN se necesita algún producto de emulación de terminal asíncrona que controle la conexión PC-WAN con el propósito de transferencia de archivos (Ver figura 3.17).

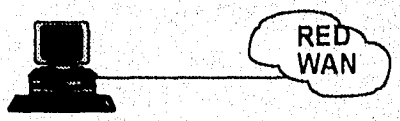


Figura 3.17
PC emulando una terminal para conectarse a una red WAN.

Para una red WAN TCP/IP, la forma de acceso de una PC sería similar a la mostrada en la opción a).

c) Cuando se requiere aprovechar las terminales asincronas de los sistemas multiusuarios o simplemente tener más estaciones que accesen a un servidor de UNIX a través de una red de área local, se pueden usar servidores de comunicaciones conectados a la red local, los cuales tienen puertos asíncronos para conectar terminales (Ver figura 3.18).

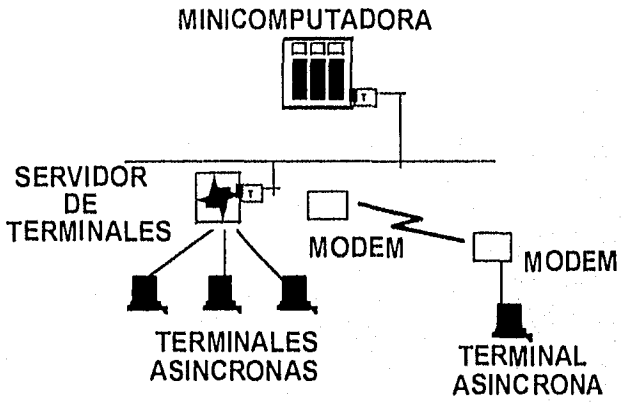


Figura 3.18
Acceso por servidor de terminales a una red de área local.

En un esquema de interconexión de redes UNIX-DOS con protocolo TCP/IP, esta opción permite manejar sesiones de terminales virtuales tontas a minicomputadora, con sistema operativo UNIX a través de red Ethernet y no a través del sistema multiusuario de la minicomputadora.

d) Interconectar redes de área local representa una conexión directa entre dos o más LAN's del mismo tipo, o de distintos tipos. La interconectividad se puede realizar con diferentes equipos tales como: Repetidores, Puentes, Enrutadores y Gateways. La configuración resultante es económica, limitada geográficamente, de alta o mediana velocidad y óptima para configuraciones pequeñas.

- Dos redes de área local de la misma topologia, mismo protocolo de comunicación y mismo sistema operativo se pueden conectar con un repetidor. Como el caso de dos redes Ethernet para DOS o UNIX.

Como ejemplos de repetidores tenemos el Repetidor Multipuerto Thick-Thin Ethernet y el Repetidor Multipuerto Ethernet 10BaseT-10Base2.

Repetidor Multipuerto Thick-Thin Ethernet.

Este equipo proporciona una manera simple, económica y flexible de conectar de 4 a 8 redes Ethernet IEEE802.3 10Base2 (Thin-Ethernet) a 1 ó 2 segmentos de redes Ethernet IEEE802.3 10Base5 (Ver figura 3.19).

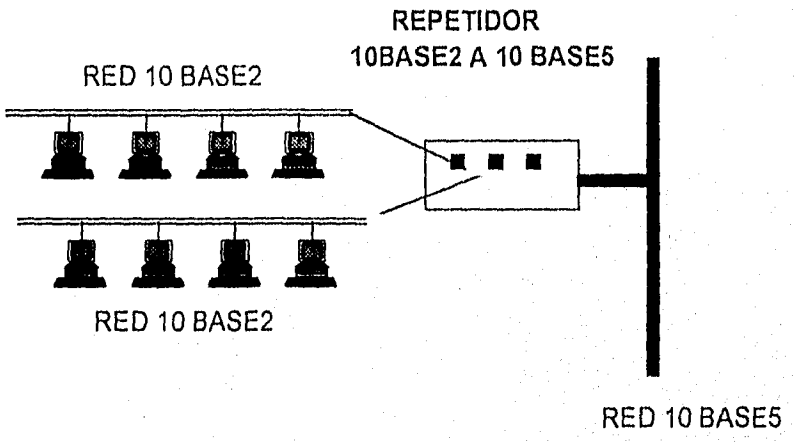


Figura 3.19
Redes de área local conectadas con un repetidor 10base2-10 base5.

Repetidor Multipuerto Ethenet 10BaseT-10Base2.

Este equipo permite conectar una red de área local IEEE802.3 10BaseT a una red IEEE802.3 10Base2 (Ver figura 3.20).

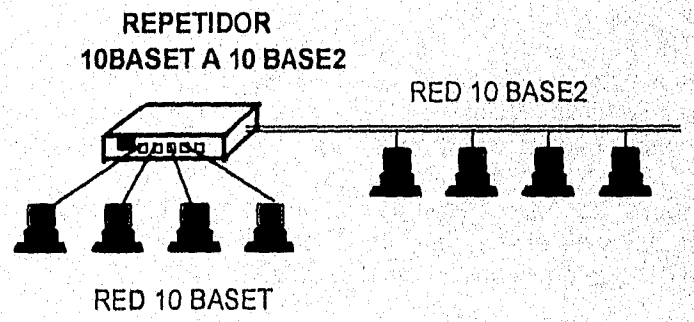


Figura 3.20
Repetidor 10BaseT-10Base2.

- Dos redes de área local de igual o diferente topología (IEEE802.3, IEEE802.5) pero mismo sistema operativo de red se pueden interconectar con un puente (Ver figura 3.21).

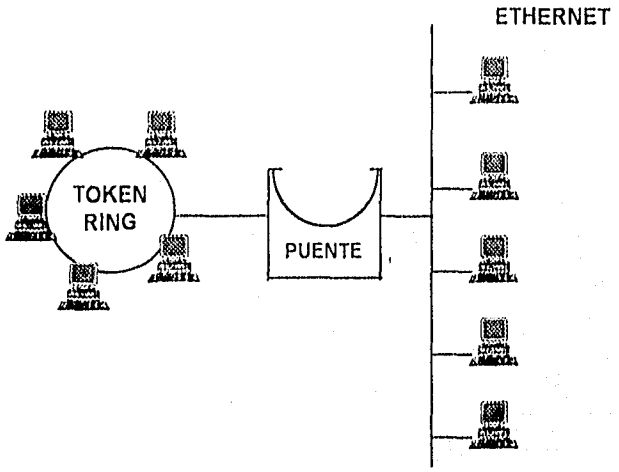


Figura 3.21
Uso de un puente entre una red Ethernet y una red Token Ring.

- Para interconectar redes de área local dispersas se utilizan normalmente enrutadores multiprotocolo, conectados entre sí, vía enlaces digitales E1 punto a punto o enlaces digitales E1-E0 punto a multipunto, formando una red WAN TCP/IP. También pueden usarse para interconectar las redes de área local otras redes de área amplia como X.25, Frame Relay o una Red Digital de Servicios Integrados ISDN (Ver figura 3.22).

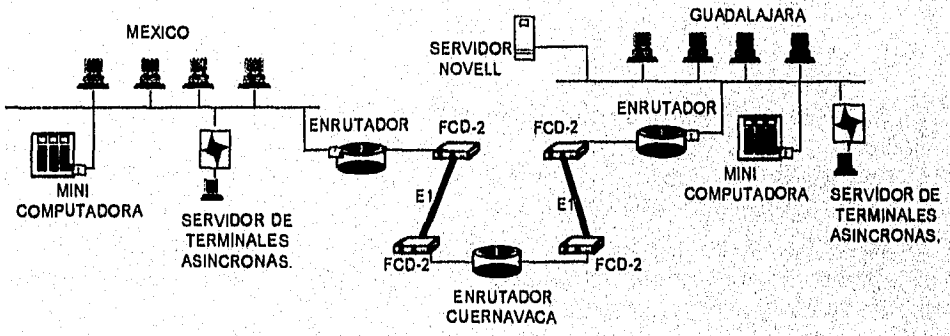


Figura 3.22
Uso de enrutadores para interconectar dos redes de área local con enlaces digitales.

e) Para interconectar redes de área local a redes de área amplia existen 2 posibilidades, los enrutadores multiprotocolo o los Gateway's. Estos últimos son comunes en la interconexión de redes de área local Ethernet y redes SNA (Ver figura 3.23).

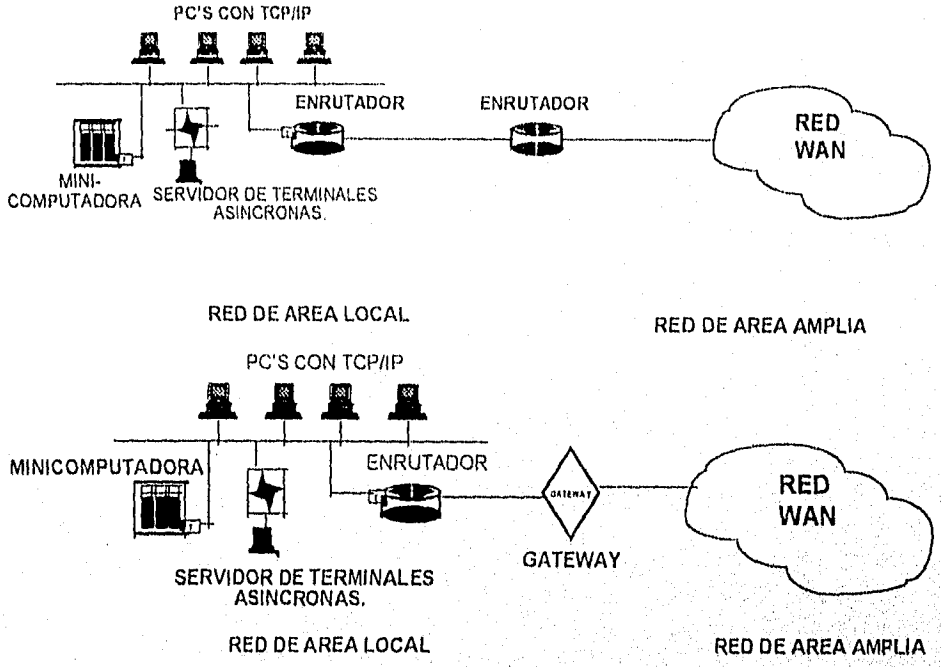


Figura 3.23.
Equipos que permiten la interconexión de redes de área local a redes WAN.

f) Las WAN de mayor uso actualmente son completamente incompatibles: SNA de IBM y TCP/IP de las máquinas UNIX. Parece que la única solución para interconexión es encapsular el tráfico de SNA en los paquetes TCP/IP. El problema radica en el hecho de que las redes SNA están orientadas a conexión, mientras que la arquitectura TCP/IP se basa en el concepto de datagramas, orientados a no conexión. Actualmente la forma más utilizada de interconectar redes WAN es por medio de Gateways.

A continuación se presentan diversas explicaciones y diagramas de inteconexión de redes Ethernet TCP/IP con diversas redes como SNA, X.25 y APPLE TALK.

Interconexión SNA-TCP/IP.

En la figura 3.24, se tienen 4 formas de interconexión de un mainframe SNA con una red TCP/IP.

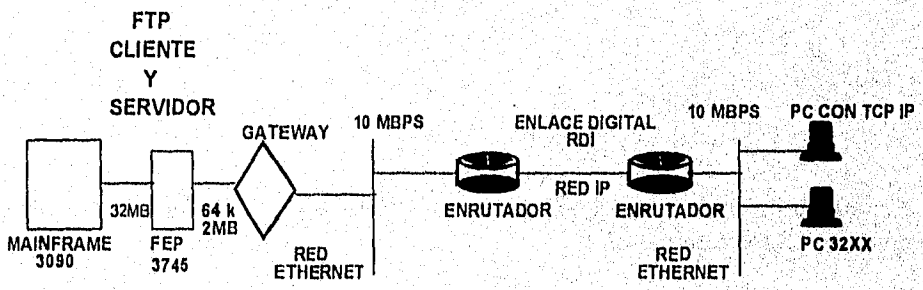
En el primer caso, mostrado en la figura 3.24a, se tiene un Gateway que realiza la conversión de protocolos SNA a TCP/IP. El Gateway tiene un puerto AUI para acceso a una red Ethernet con TCP/IP, y un puerto serial síncrono hasta de 2 Mbps para su conexión a un procesador frontal perteneciente a la arquitectura del mainframe SNA.

En este esquema de interconexión, un host (PC con software TCP/IP o minicomputadora con TCP/IP) puede tener acceso a un mainframe vía las aplicaciones TELNET o FTP.

En el segundo caso, mostrado en la figura 3.24b, el mainframe ya cuenta con software TCP/IP integrado, y la comunicación a una red TCP/IP se realiza por medio de un enrutador, sin necesidad de convertir ninguna información.

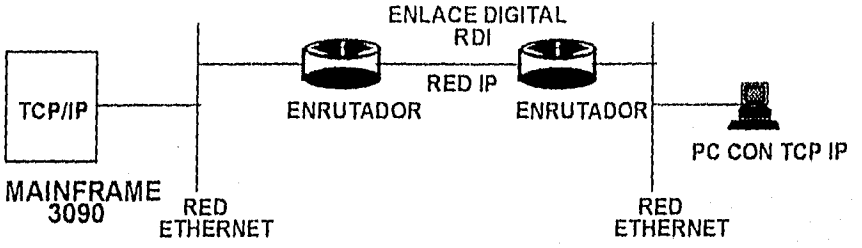
En el tercer caso, mostrado en la figura 3.24c, se tiene un Gateway que convierte de protocolo SNA a TCP/IP y de topología Ethernet (bus) a Token Ring (anillo).

En el cuarto caso, mostrado en la figura 3.24d, se tiene un mainframe y un procesador frontal comunicándose con otro procesador frontal usando la red TCP/IP sólo como transporte de mensajes SNA. En este esquema se usan enrutadores para encapsular el tráfico SNA sobre TCP/IP y dar servicio a terminales que accesan al mainframe.



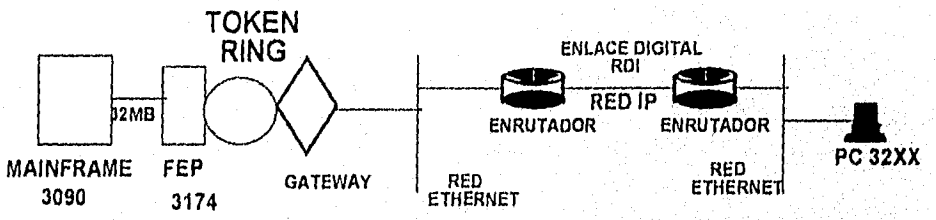
a)

Figura 3.24
Interconexión de una red SNA con una red TCP/IP usando un Gateway.



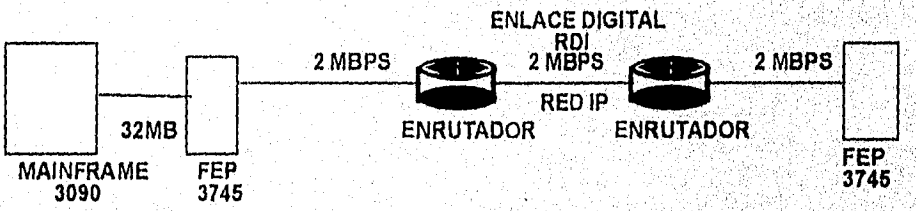
b)

Comunicación de un Mainframe a una red de área local Ethernet usando TCP/IP.



c)

Comunicación de un Mainframe y una pc emulando terminal 32XX a través del uso de un Gateway y una red Token Ring.



d)

Comunicación de un Mainframe a un controlador 3745 con enrutadores usando el protocolo TCP/IP.

Figura 3.24

Formas de interconectar dispositivos de una red de área local a una red SNA.

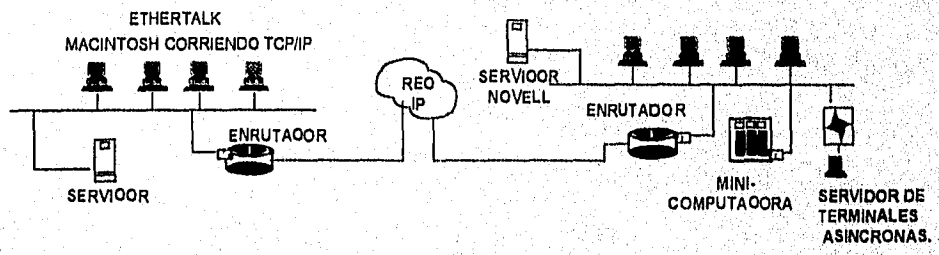
Interconexión TCP/IP-Macintosh.

La mayoría de los productos TCP/IP para Macintosh, permiten hablar TCP/IP y AppleTalk sobre el mismo cable físico cuando se utilizan redes Ethernet.

La forma más popular de correr protocolos TCP/IP en una computadora MAC es con el software MacTCP. MacTCP conforma varios estándares Internet y proporciona los protocolos IP relacionados (TCP, UDP, IP). MacTCP permite correr procesos TCP/IP y AppleTalk simultáneamente. Por ejemplo una sesión de TELNET y una impresión en LaserWriter (Ver figura 3.25 a).

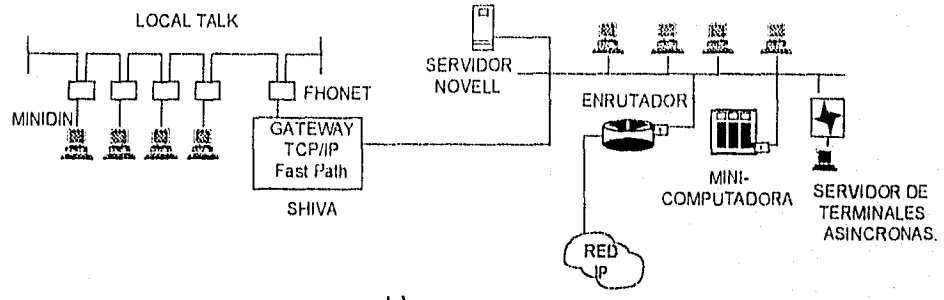
A diferencia de Ethernet, el cableado LocalTalk no puede transportar TCP/IP. Por lo tanto para transportar un paquete TCP/IP sobre LocalTalk, éste debe estar encapsulado dentro de un paquete LocalTalk. El paquete LocalTalk viaja a un Gateway de LocalTalk, el cual extrae el paquete TCP/IP y lo envía sobre Ethernet o cualquier otro cableado apropiado. Un proceso similar ocurre cuando el tráfico fluye en dirección contraria. Cuando un paquete TCP/IP que se destina a la Macintosh llega al lado Ethernet del Gateway, se le encapsula en un paquete de LocalTalk y se le envía a la Macintosh (ver figura 3.25b).

En algunos casos, no se desea una conexión directa entre máquinas Apple y otra, sino utilizar una red TCP/IP para conectar dos redes Macintosh. En este caso lo mejor es emplear tunneling, una característica encontrada en el FastPath. Los paquetes AppleTalk se encapsulan dentro de paquetes TCP/IP y después se les envía, a través de la red TCP/IP, a la red AppleTalk destino, en donde se les extrae (Ver figura 3.25c).



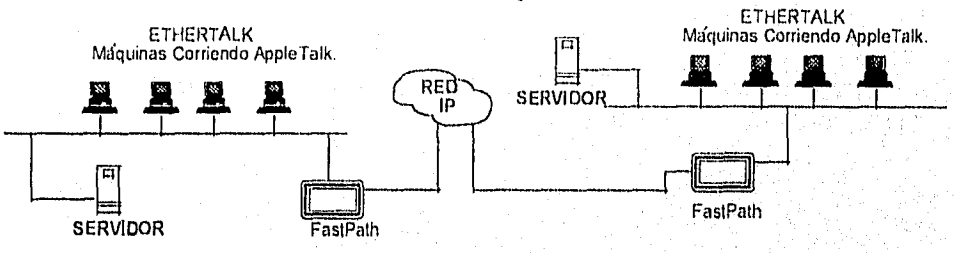
a)

Figura 3.25
Comunicación de redes AppleTalk con software TCP/IP.



b)

Comunicación de una red localTalk y una red Ethernet TCP/IP.



c)

Interconexión de redes AppleTalk a través de una red TCP/IP.

Figura 3.25

Formas de interconectar dispositivos de una red TCP/IP con una red Macintosh.

Interconexión TCP/IP-X.25.

Una forma de comunicar dispositivos que utilizan protocolo de comunicación X.25 es encapsular en la porción de datos del datagrama IP los mensajes X.25 y transportarlos a través de la red TCP/IP hasta su destino, donde son desencapsulados y entregados al equipo destino, como muestra la figura 3.26. Este esquema de interconexión necesita enrutadores multiprotocolo capaces de manejar protocolos X.25 y TCP/IP.

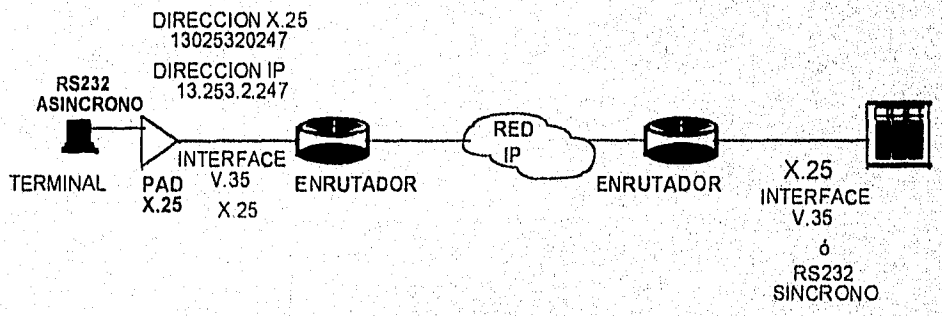


Figura 3.26

Utilizando una red IP para comunicar dispositivos X.25.

CAPITULO IV

EL CONJUNTO DE PROTOCOLOS TCP/IP

4.1 Consideraciones generales.

En los 70's diversos grupos alrededor del mundo comenzaron a preocuparse por las redes y la compatibilidad de aplicaciones de las mismas. El término internetworking que significa la interconexión de redes fué adoptado. Los pioneros en conceptos de interconexión de redes fueron el CCITT, la ISO y los diseñadores originales de ARPANET.

El CCITT (Comité Consultivo para la Telefonía y la Telegrafía Internacional) es auspiciado por el ITU-TSS (Unión de Telecomunicaciones Internacional de la ONU) y realiza recomendaciones técnicas en telegrafía, telefonía e interfaces de comunicación de datos. Entre los estándares más populares de esta organización se encuentran la V24 y la X.25.

ISO (Organización de Estándares Internacional) define y desarrolla estándares en una gran variedad de tópicos. Casi 100 países están representados en ISO. En los Estados Unidos el representante es la ANSI (Instituto Nacional de Estándares Americano). Entre los estándares más populares de esta organización se encuentran el modelo OSI (Interconexión de Sistemas Abiertos), el protocolo HDLC (Control de Enlace de Datos de Nivel Alto) y estándares de redes de área local adoptados del IEEE 802.

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) es una de las más grandes organizaciones profesionales en el mundo. Es responsable del desarrollo de los estándares IEEE 802 para redes de área local y además desarrolla estándares de ingeniería eléctrica y de computación.

Otras instituciones responsables de la generación de estándares son:

La EIA (Asociación de Industrias de Electrónica) ha generado normas como la EIA-RS232C y la EIA-RS449.

La ECMA (Asociación de Fabricantes de Computadoras Europea).

El ITI (Instituto de Tecnología Industrial).

Las instituciones mencionadas anteriormente generan y siguen investigado para el desarrollo de estándares, pero además existen otros estándares llamados estándares de facto.

Los estándares de facto (se vuelven estándares por el uso y aceptación de los usuarios) son utilizados por fabricantes líderes de la industria para producir dispositivos electrónicos o sistemas informáticos, donde las normas y especificaciones de estos estándares a tenido éxito y son tomados con gran aceptación por los usuarios. Muchas agrupaciones donde intervienen centros universitarios o de investigación y firmas prestigiosas, son los responsables de desarrollar, promover y regular tales estándares.

Un ejemplo notable de este tipo de estándares, es la serie de protocolos que pertenecen a la familia TCP/IP. A mediados de los 60's, hubo un proyecto conocido como el proyecto de ARPANET (Advanced Research Proyect Agency NETwork; Agencia de Proyectos de Investigación Avanzada de Redes), que fué uno de los primeros esfuerzos por lograr que computadoras de diferentes fabricantes pudiesen intercambiar información. ARPANET tuvo éxito al iniciar sus operaciones conectando computadoras, nodos que incluían la Universidad de California en San Bernardino, el Instituto de Investigaciones de Estanford y la Universidad de Utah. ARPANET mantuvo sus funciones hasta fines de los 70's cuando fué segregada en varias redes, de las que surgieron por ejemplo NSFNET (National Science Foundation NETwork; Red de la fundación nacional de la ciencia) y MILNET (Military Network; Red Militar) que actualmente sirven a las principales universidades y centros de investigación más importantes del mundo y a la OTAN respectivamente.

La experiencia que brindó la creación de la red ARPANET, que empleo en sus inicios protocolos de comunicación rudimentarios, sirvió de base en el desarrollo de protocolos más complejos. ARPANET fué uno de los primeros intentos en la comunicación de datos con técnicas de conmutación de paquetes de información. Así mismo ARPANET fué una aventura en la que participaron organismos no oficiales en cuestión de estándares internacionales.

En la segunda mitad de los 70's, el departamento de la defensa de los Estados Unidos de Norteamérica (DoD), que entonces controlaba en gran parte la red ARPANET (de hecho por aquel entonces ARPANET era conocido como DARPANET), a través de la agencia de proyectos de investigación avanzada del mismo departamento de la defensa (DARPA por DoD Advanced Research Proyect Agency), propuso un proyecto el cual debía generar el desarrollo de un protocolo para comunicaciones entre nodos de computadoras, de una extensa red. Tal protocolo debía cumplir con ciertos requisitos para ser instalado. Así, que en 1979, se publicó el documento que contenía todo el marco teórico del protocolo **TCP/IP** (Protocolo de control de Transmisión/Protocolo Internet). En 1983, prácticamente las redes que surgieron de ARPANET, habían abandonado los viejos protocolos, para implantar el nuevo conjunto de protocolos TCP/IP.

El principal acierto del protocolo fué haber desarrollado una arquitectura de comunicaciones sólida en caso de que la red o sus componentes sufrieran fallas, además de que puede acomodar múltiples servicios de comunicación

sobre una gran gama de redes de área local y de área amplia. La figura 4.1 muestra el conjunto de protocolos TCP/IP que serán analizados en este capítulo, así como las aplicaciones existentes para el usuario.

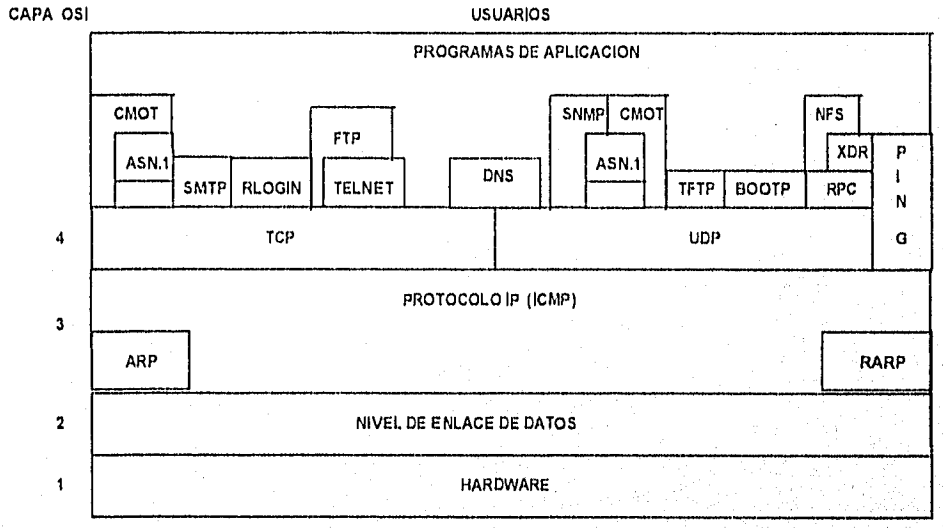


Figura 4.1
Protocolos y aplicaciones TCP/IP.

4.2 Esquema de direccionamiento TCP/IP.

El conjunto de protocolos TCP/IP basa la comunicación en un protocolo de capa 3 OSI, llamado IP.

Para realizar la comunicación de los hosts en una red, es necesario establecer un método de identificación de cada host en la red. Este método consiste en asignar una dirección lógica a cada host en la red, además los hosts con varios puertos de comunicación recibirán direcciones diferentes para cada uno de éstos.

En este momento cabe aclarar que como host se entiende cualquier computadora personal, minicomputadora, mainframe, enrutador, servidor de comunicaciones, concentrador o cualquier máquina o equipo de cómputo con CPU.

En una red TCP/IP una dirección lógica única de 32 bits es asignada a cada host y es usada en todas las comunicaciones con ese host (Ver figura 4.2). Esta dirección es conocida como dirección IP.

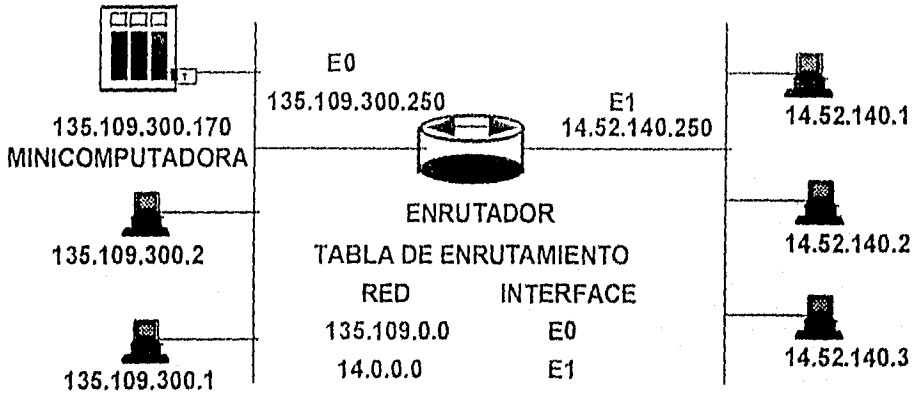


Figura 4.2
Direcciones IP en los hosts.

Cada Dirección IP es un par (identificador de red, identificador de host). En la práctica, cada dirección IP debe tener uno de los primeros tres formatos mostrados en la figura 4.3.

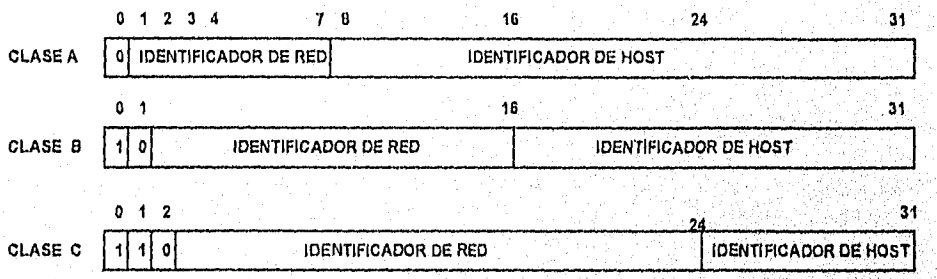


Figura 4.3
Direcciones IP de 32 bits.

Se debe notar que las direcciones IP no especifican únicamente la dirección de una máquina individual, sino una conexión a una red, al codificar red y host en el mismo formato

Las direcciones de clase A son usadas para manejar redes que tienen más de 65,536 hosts y un máximo de 128 redes, es decir, se utilizan 7 bits para el identificador de red y 24 bits para el identificador de host. Las redes clase B se han implementado para redes de tamaño mediano, donde el identificador de red usa 14 bits y el identificador de host 16 bits. Finalmente la redes clase C asignan 21 bits para el identificador de red y 8 bits para el identificador de host (Ver Tabla 4.4).

CLASES DE REDES IP (EL PRIMER OCTETO DETERMINA EL TIPO DE RED)		
RED PRIMER OCTETO	NUMERO DE HOSTS DISPONIBLES	NUMERO DE REDES DISPONIBLES
CLASE A 00 000001 1 011111110 126	2^{24}- 2 = 16,777,214	2^{7}.2 = 126 DE LA RED 1.0.0.0 A LA RED 126.0.0.0
CLASE B 10 000000 128 10 111111 191	2^{16}- 2 = 65,532	2^{14}.2 = 16382 DE LA RED 128.1.0.0 A LA RED 191.254.0.0
CLASE C 110 00000 192 110 11111 223	2^{8} - 2 = 254	2^{21}.2 = 2,097,150 DE LA RED 192.0.1.0 A LA RED 223.255.254.0
CLASE D 11100000 224 11101111 239	MULTICAST	MULTICAST
CLASE E 11110	USU FUTURO	USO FUTURO

Tabla 4.4.

Además de las clases de direcciones mencionadas existen direcciones IP que indican un broadcast restringido con un valor de 1 en los 32 bits de la dirección IP (255.255.255.255) y broadcast dirigido con valor de 1 en los bits pertenecientes al host en la dirección IP (por ejemplo 131.108.3.255 en una red clase B).

4.2.1 Subdireccionamiento.

Es la técnica de asignar una sola dirección de red IP a varias redes físicas. Lo anterior se logra tomando parte de los bits del identificador de host para el direccionamiento de dichas redes a las cuales se les llama subredes (Ver figuras 4.5a y 4.5b). Por ejemplo en la figura 4.5a se muestra una red Ethernet con direccionamiento IP clase B 135.109.0.0 y con hosts 135.109.1.1, 135.109.1.2, etcétera. Se puede notar que por el número de hosts existentes, el único octeto utilizado para su direccionamiento es el cuarto y por lo tanto el tercer octeto de esta red permanece fijo. Lo anterior se puede aprovechar para numerar diversas redes físicas con el sólo incremento de valor del tercer octeto como lo muestra la figura 4.5b.

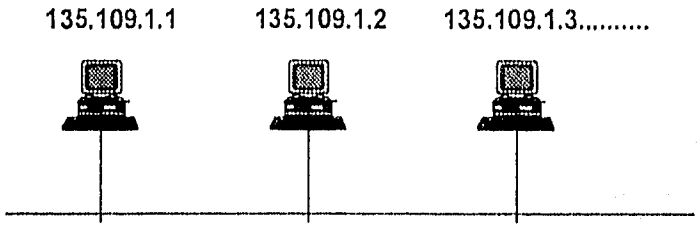


Figura 4.5a
Red clase B 136.109.0.0 sin subdireccionamiento.

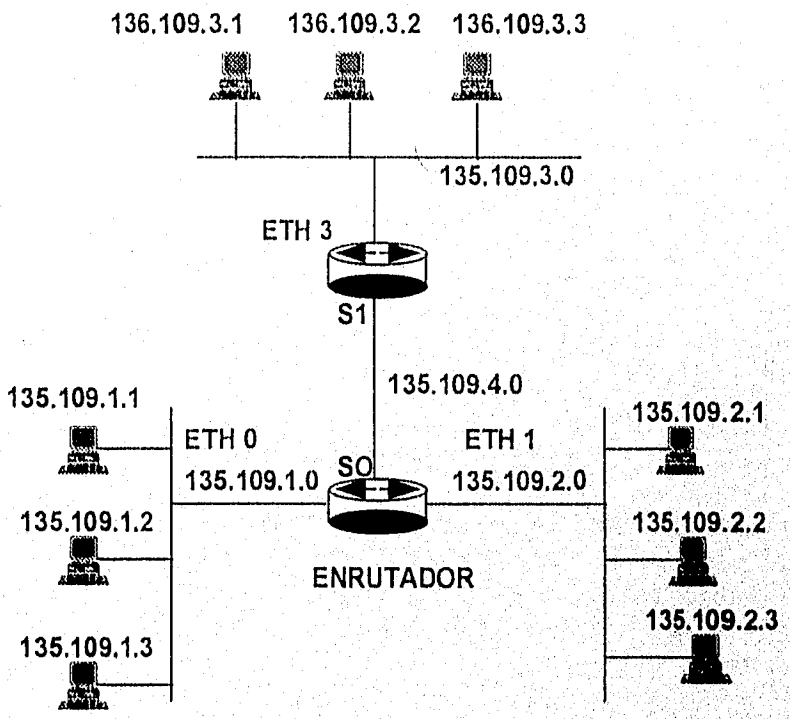


Figura 4.5b
Red clase B 135.109.0.0 con subdireccionamiento según el tercer octeto.

Cuando se agregan subredes únicamente cambia la interpretación de las direcciones IP. En lugar de dividir los 32 bits de la dirección IP en un prefijo de red y un sufijo de host, el subdireccionamiento divide la dirección en una porción de red y una porción local. La interpretación de la porción de red es la misma que la del identificador de red que no usa subdireccionamiento. La porción local es dividida en dos partes que identifican una red física y un host en esa red (Ver figura 4.6).

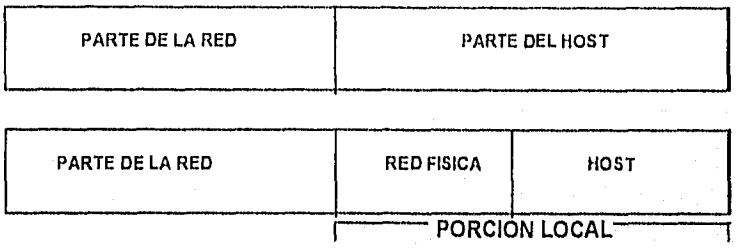


Figura 4.6
Dirección IP de 32 bits con subdireccionamiento.

4.2.2 Máscaras de subdireccionamiento.

Cuando se usa subdireccionamiento la interpretación de la dirección IP cambia, por lo que es necesario implementar una forma de decirle a los hosts y enrutadores como interpretar las direcciones IP que manejan. Lo anterior se logra con el concepto de máscara de subred de 32 bits para cada red. Los bits en la máscara de subred son establecidos a 1, si la red debe tratar los correspondientes bits en la dirección IP como parte de la direcclón de red, y 0 si ésta, debe tratar los bits como parte del identificador de host.

Por Ejemplo, la máscara de subred de 32 bits:

255.255.255.0 en decimal

11111111 11111111 11111111 00000000 en binario

especifica que los primeros 3 octetos en la dirección 135.109.2.250, identifican la red 135.109.2.0 y el cuarto octeto identifica un host 250 en la red (Ver Tabla 4.7).

MASCARA DE SUBRED PARA IDENTIFICAR SUBREDES DE UNA RED CLASE B.

	RED		SUBRED	HOST	
135.109.2.250	10000111	01101101	00000010	11111010	AND
255.255.255.0	11111111	11111111	11111111	00000000	
	10000111	01101101	00000010	00000000	
	135	109	2	0	

Tabla 4.7
La red 135.109.0.0 cuenta con la subred 135.109.2.0.

4.2.3 Algoritmo de enrutamiento de subredes.

El algoritmo de enrutamiento estándar sabe que una dirección IP es particionada en identificador de red e identificador de host y además sabe de que tipo de red se trata por el valor de los bits más significativos de la dirección IP. Con subredes, no es posible determinar que bits corresponden a la red física y cuales al host de una sola dirección IP. El algoritmo usado con subredes mantiene información adicional en la tabla de enrutamiento. Cada entrada en la tabla contiene un campo adicional que especifica la máscara de subred usada con la red.
Cuando un enrutador elige rutas, el algoritmo modificado usa la máscara de subred para extraer bits de la dirección destino y compararlos con la tabla. La extracción anterior se logra mediante la aplicación de una función lógica AND entre la dirección IP y la máscara de subred (Ver tabla 4.7).

4.3 El Protocolo de resolución de dirección (ARP).

Dos máquinas en una misma red física (mismo segmento de red o subred) pueden comunicarse únicamente, si cada una de ellas conoce la dirección física de la otra.
¿ Cómo una máquina o host mapea una dirección IP a la dirección física correcta cuando necesita enviar un paquete a través de la misma red física?.

El protocolo ARP es usado por un host en la red que conoce la dirección IP de la estación destino con la que quiere hablar, pero no conoce su dirección física. Este protocolo sólo es aplicable cuando las 2 máquinas se encuentran en el mismo segmento de red.

4.3.1 Encapsulación ARP.

Cuando un mensaje ARP viaja de una máquina a otra, debe ser transportado dentro de la porción de datos de una trama (Ver figura 4.8). Para identificar que una trama transporta datos ARP, el emisor asigna un valor especial al campo de tipo dentro del encabezado de la trama. En las tramas de redes Ethernet conduciendo mensajes ARP, el campo de tipo tiene un valor de 0806 en hexadecimal.

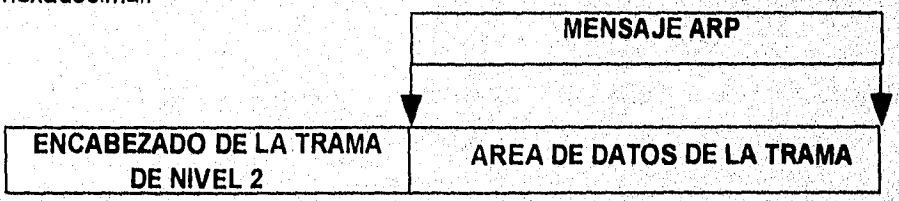


Figura 4.8
Mensaje ARP encapsulado en la trama de nivel de enlace de datos.

4.3.2 Funcionamiento del protocolo ARP.

En la figura 4.9, se muestra una máquina A que quiere comunicarse con la máquina B, pero no conoce su dirección física, sólo conoce su dirección IP. Ésta envía una trama con la dirección física destino en Broadcast (FFFFFFFFFFFF) y la dirección IP de la máquina B. Todas las máquinas, incluyendo B reciben el paquete, pero únicamente la máquina B reconoce su dirección IP y envía una respuesta que contiene su dirección física.

Cuando A recibe la respuesta de B, ésta usa la dirección física de B para enviar paquetes IP directamente a B.

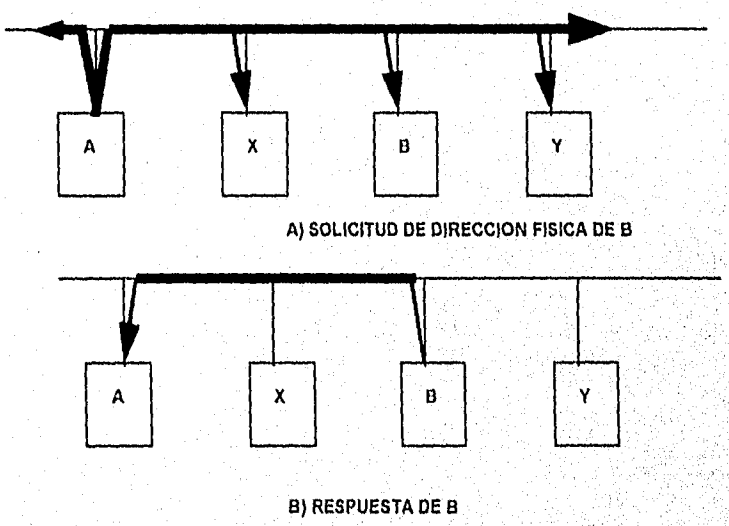


Figura 4.9
Funcionamiento del protocolo ARP.

4.3.3 Formato del mensaje ARP.

El formato del mensaje para el protocolo ARP se muestra en la figura 4.10 y es descrito a continuación:

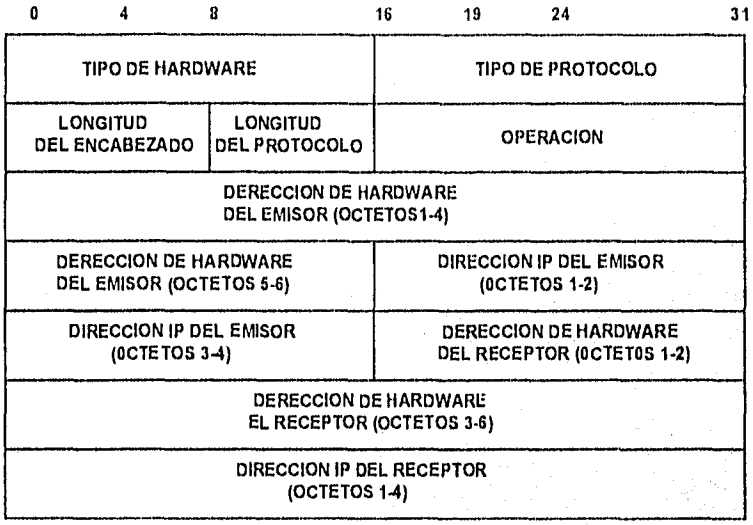


Figura 4.10
Formato del mensaje ARP.

Tipo de Hardware ARP.

Este campo indica el tipo de hardware utilizado en la capa física de la red. Tal como 0001 para redes Ethernet.

Tipo de protocolo ARP.

Este campo contiene un código utilizado para mostrar el tipo de dirección de protocolo de nivel-alto que es usada en la red. Por ejemplo 0800 para IP.

Longitud del hardware ARP.

Este campo muestra el número de bytes usados para la dirección de hardware. Este campo es establecido a 6 para redes Ethernet. La longitud mencionada es la longitud de la dirección Ethernet de las tarjetas de red de las estaciones de trabajo y/o dirección de hardware de los puertos de un host.

Longitud del protocolo ARP.

Este campo contiene la longitud en bytes de la dirección del protocolo de capa 3. En el caso de IP es establecido a 4.

Operación ARP.

Indica que operación el protocolo está realizando.
0001 ARP Solicitud (request)
0002 ARP Respuesta (reply)

Dirección de hardware fuente ARP.

Dirección de Capa física del equipo que envía el mensaje.

Dirección de protocolo fuente ARP.

Es la dirección de Capa 3 (dirección IP) de la estación que envía el mensaje.

Dirección de hardware destino ARP.

Dirección de Capa ísica del dispositivo que recibe el mensaje.

Dirección de protocolo destino ARP.

Es la dirección de Capa 3 (dirección IP) de la estación que recibe el mensaje.

La forma de observar la aplicación del protocolo ARP es usar una de las aplicaciones de TCP/IP, el comando PING.

Cuando se usa la aplicación PING se puede observar en los resultados obtenidos con un analizador de protocolos que se generan dos mensajes ARP uno de solicitud y uno de respuesta. En el mensaje de solicitud se observa como se usa una dirección de broadcast para asegurarse que la estación destino escuchará el mensaje de solicitud y lo contestará poniendo en la respuesta su dirección física.

Un caso especial del protocolo ARP es el conocido como Proxy ARP.

Proxy ARP se aplica cuando una máquina que quiere comunicarse se encuentra en una red física y el destino en otra y además, estas redes están interconectadas por un enrutador.

Proxy ARP consiste en responder con la dirección física del enrutador la solicitud ARP de una máquina en una red física a otra máquina en una red física diferente (Ver figura 4.11).

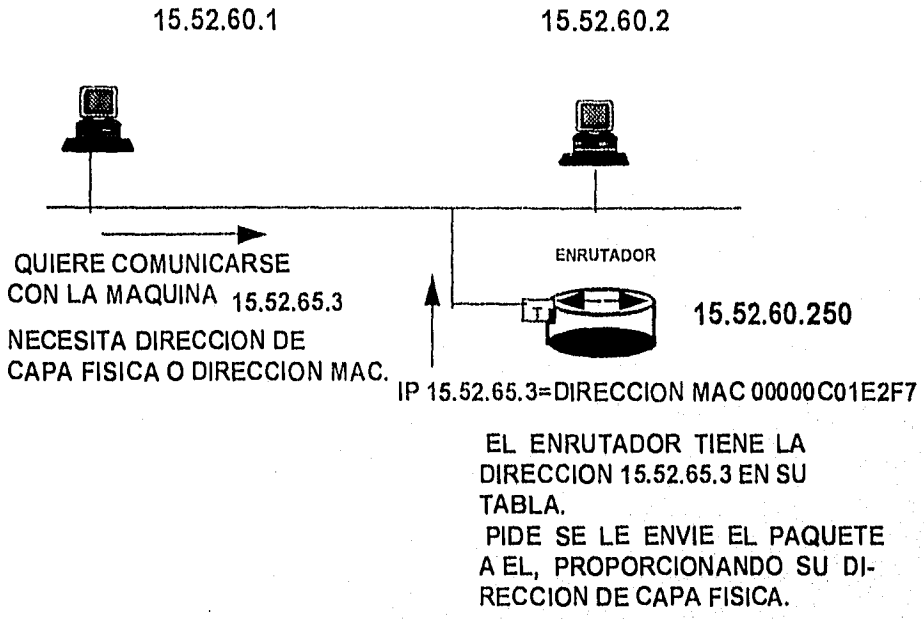


Figura 4.11
Aplicación del protocolo proxy ARP.

Un caso que funciona al revés del protocolo ARP es el protocolo RARP.

El protocolo RARP trabaja en forma inversa al protocolo ARP. En este caso lo que se busca es la dirección IP de la máquina origen. Un ejemplo en donde no se conoce la dirección IP de la máquina origen es cuando se tiene una estación de trabajo sin disco duro (Diskless). En este caso la estación envía una solicitud RARP en broadcast como dirección destino y la dirección física de la máquina enviante. Todas las máquinas en la red física reciben la solicitud, sin embargo, únicamente un servidor RARP responderá la solicitud.

El protocolo RARP utiliza la misma estructura de mensaje de ARP y un servidor que responde a una petición, llena el campo de dirección de protocolo destino y cambia el código de operación del mensaje RARP de solicitud a respuesta (3=solicitud, 4=a respuesta). El campo de tipo Ethernet en la trama se codifica como 8035 en hexadecimal cuando los datos en la trama corresponden al protocolo RARP.

Una alternativa del protocolo RARP mencionado anteriormente es el protocolo BOOTP.

Las máquinas sin disco duro deben aprender su dirección IP de otra fuente, pero no sólo necesitan su dirección IP, usualmente estas máquinas tienen una

ROM interna que contiene un pequeño grupo de programas de arranque, entonces requieren obtener una imagen de software a ejecutar. Cada máquina de este tipo debe conocer la dirección IP del servidor de archivos para obtener y guardar datos y requiere la dirección del enrutador más cercano

A diferencia de RARP el protocolo BOOTP utiliza UDP para transportar mensajes y los mensajes UDP son encapsulados en datagramas IP. En este punto parece que no es lógico utilizar IP, si lo que buscamos es la dirección IP local, pero BOOTP utiliza una dirección IP destino de broadcast limitado (225.255.255.255). El software IP puede aceptar datagramas en broadcast aún antes de que sepa que dirección IP local le corresponde.

Suponer que una máquina A quiere usar BOOTP para encontrar su información de arranque (incluyendo su dirección IP) y suponer que la máquina B es el servidor en la misma red física que responderá la solicitud. Debido a que A no conoce la dirección IP de B, envía una solicitud usando un broadcast limitado. La respuesta del servidor de BOOTP también es un brodcast limitado aunque éste si conoce la dirección de A. Lo anterior se hace de esa manera, por que A no sabe su dirección IP todavía y no puede procesar la respuesta directamente.

4.4 El protocolo de capa 3 IP.

El protocolo Internet IP es un mecanismo de entrega de datagramas sin conexión no confiable. IP proporciona tres importantes definiciones. Primera, el protocolo define la unidad básica de transferencia de datos usada para las redes TCP/IP. Segunda, el software IP realiza la función de enrutamiento, eligiendo una trayectoria sobre la cual los datos pueden ser enviados. Tercera, IP incluye un conjunto de reglas acerca de como los enrutadores y los hosts deben procesar los datagramas, como y cuando los mensajes de error deben ser generados, y las condiciones bajo las cuales los datagramas deben ser descartados.

4.4.1 Formato del datagrama IP.

La unidad de transferencia del protocolo IP es un datagrama, éste se divide en dos partes: el encabezado y el área de datos (Ver figura 4.12).

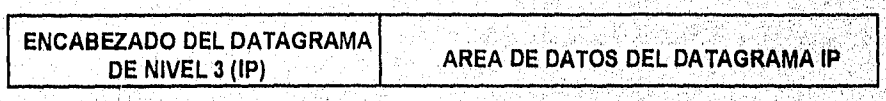


Figura 4.12
Datagrama IP.

El encabezado IP está formado por campos de diversa longitud que se muestran en la figura 4.13

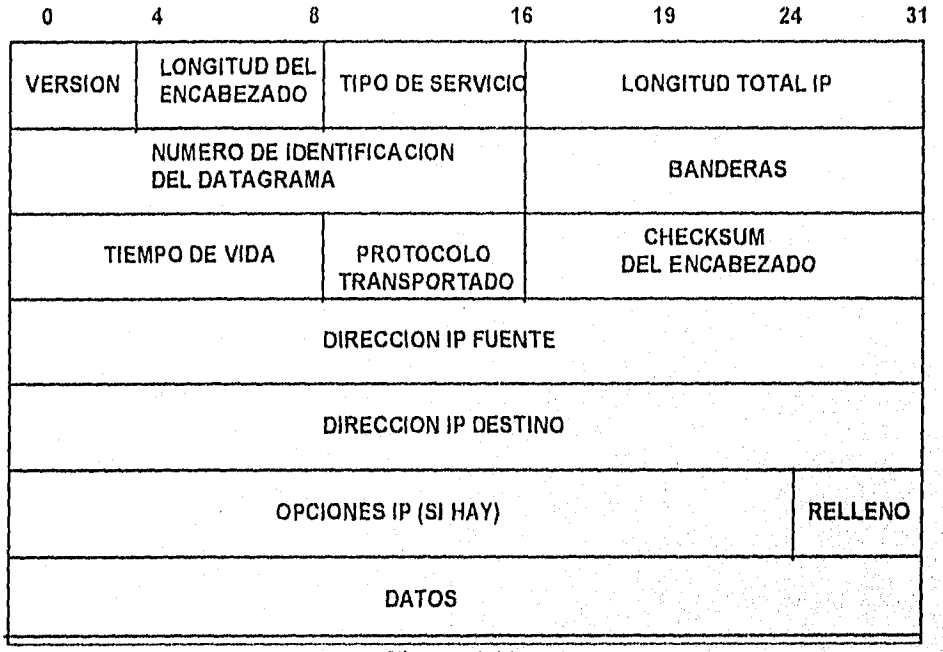


Figura 4.13
Campos que forman el datagrama IP.

Versión IP.

Es un campo de 4 bits que indica el número de revisión de IP que creo el encabezado. Este campo es importante debido a que dos redes con diferente versión de IP no podrán conectarse. La versión actual es 4.

Longitud del encabezado IP (HLEN).

Este campo de 4 bits es la longitud del encabezado IP expresado en palabras de 32 bits. Un encabezado IP normal sin opciones es de 5 palabras (20 octetos) y con opciones puede llegar a tener F palabras (60 octetos).

Campos de tipo de servicio (SERVICE TYPE).

Los bits de la precedencia de los datos, el retardo, el rendimiento, y la confiabilidad son llamados colectivamente campos del octeto de tipo de servicio o TOS (tipo de servicio). Estos campos indican el servicio de enrutamiento solicitado a cada enrutador por el cual pasan (Ver figura 4.14).

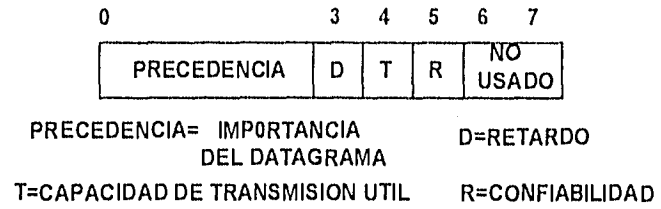


Figura 4.14
Subcampos del byte de tipo de servicio.

Precedencia de los datos (Precedence).

Este campo de 3 bits le dice al enrutador IP receptor, a lo largo del camino de comunicación, que tan importantes son los datos. La mayoría de los valores posibles de este campo son establecidos por DARPA, pero existen diversos valores de uso potencial para resolver problemas de congestión de la red y para el uso de herramientas de administración de red.

Precedencia	Valor
Control de red.	111
Control de interconexión entre redes	110
Critico	101
Predominantemente Urgente	100
Urgente	011
Inmediato	010
Prioridad	001
Rutinarios	000

Bit de retardado (Delay).

Este bit permite que algunas aplicaciones soliciten rutas con la menor cantidad de retardo de propagación. Para solicitar el mínimo retardo este bit es establecido a 1.

Bit de capacidad de transmisión útil (Througput).

Si este bit es establecido a 1, los enrutadores soportando los datos utilizarán las trayectorias de comunicación con más alta capacidad de transmisión de datos útil.

Bit de confiabilidad (Reliability).

Este campo de un bit permite que las aplicaciones soliciten que los datos viajen a través de la ruta con menor oportunidad de pérdida de datos. De la

misma manera que los bits de retardo y capacidad de transmisión, éste trabaja cuando es establecido a 1 y los enrutadores en la red lo soportan.

Los bits de retardo, capacidad de transmisión y confiabilidad son mutuamente excluyentes. Por lo tanto se puede poner a uno únicamente uno de los tres bits.

Longitud total IP (Total Length).

Este campo de 2 octetos le dice al destino IP, la longitud total del datagrama incluyendo el encabezado IP. Con 16 bits el tamaño de datagrama máximo es de 65535 octetos.

Número de identificación del datagrama (Identification).

Este campo de 2 octetos conduce el número de identificación del datagrama que es enviado por el host. Éste es usado principalmente para corregir errores lógicos y para ayudar en el reensamble de fragmentos de datagramas. Cuando la fragmentación ocurre cada datagrama, que es parte de el mensaje original, tendrá el mismo número de identificación.

Campo de banderas (Flags).

Está formado por 4 subcampos en 2 octetos como se muestra en la figura 4.15 y se describen a continuación.

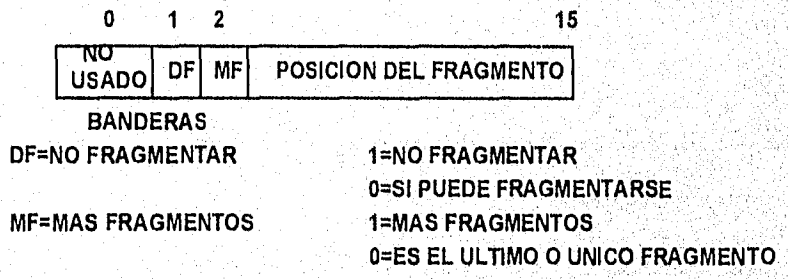


Figura 4.15
Subcampos de los dos bytes del campo de banderas.

No Fragmentar (Don't Fragment DF).

Es un campo de un bit que si es establecido a uno por una aplicación, se estará solicitando que el segmento de información TCP no sea fragmentado por IP.

Más fragmentos (More Fragments MF).

Si este bit es establecido a cero entonces el host final a recibido el fragmento final. Si el bit es establecido a 1 entonces el host final debe esperar más

fragmentos. El uso de este bit y del bit de posición del fragmento permite al host destino saber si ha recibido todos los datos para un mensaje particular.

Posición del fragmento (Fragment offset).

Este campo de 13 bits conduce el número de palabras de 64 bits que indica la posición de este fragmento en el datagrama original. Hay un máximo de 8192 fragmentos por datagrama.

Tiempo de vida (Time to live).

Este campo de un octeto indica el número de segundos que el datagrama puede existir en la red antes de que sea descartado o entregado.

Campo de protocolo transportado (Protocol).

Este campo de 8 bits contiene el número de identificación del protocolo de capa alta (capa de transporte), que el datagrama contiene en su campo de información. El valor más común es el número 06 que corresponde al protocolo TCP.

Checksum del encabezado IP (Header Checksum).

Este campo de 2 octetos proporciona chequeo de error en el encabezado IP y no cubre los datos que está conduciendo. Si el destino IP recibe un datagrama con el checksum erróneo el datagrama es descartado.

El cálculo del valor de este campo se realiza tratando al encabezado como una secuencia de enteros de 16 bits, los cuales se suman usando aritmética de complemento a uno y entonces tomando el complemento a uno del resultado. El campo del checksum para el cálculo se pone en ceros.

Dirección IP fuente (Source IP Address).

Es una dirección de 32 bits (4 octetos) del emisor.

Dirección IP destino (Destination Address).

Es una dirección de 32 bits(4 octetos) del receptor.

Relleno (Padding).

Este campo representa bits con valor de cero que pueden necesitarse para asegurar que el encabezado del datagrama se extiende a un múltiplo exacto de 32 bits.

4.4.2 Opciones del datagrama IP (IP Options).

Las opciones en el datagrama IP son principalmente incluidas para fines de pruebas de enrutamiento, sello de tiempo y depuración de red.

La longitud del campo de opciones varía de acuerdo a que opciones son seleccionadas. Algunas opciones son de un octeto de longitud. Cuando las opciones están presentes en el datagrama IP, ellas aparecen contiguas, sin separadores especiales entre ellas. Cada opción consiste de un sólo octeto de código de opción, el cual puede ser seguido de un sólo octeto de longitud y un conjunto de octetos de datos para esa opción. El octeto de código de opción está dividido en 3 campos. Los campos consisten de 1 bit de bandera para copia, dos bits que indican la clase de opción, y 5 bits designando el número de opción. El bit de bandera de copia controla como los enrutadores tratan las opciones durante fragmentación. Cuando el bit de bandera de copia es establecido a 1, éste especifica que la opción debe ser copiada dentro de todos los fragmentos. Cuando es establecido a cero, significa que la opción únicamente debe ser copiada dentro del primer fragmento (Ver figura 4.16 y tablas 4.17a y 4.17b).

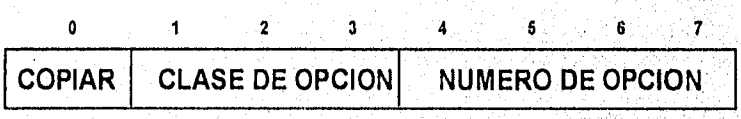


Figura 4.16
Octeto de código de opción IP.

Clase de Opción	Significado
0	Datagrama o control de Red
1	Reservado para uso futuro.
2	Depuración y Medición.
3	Reservado para uso futuro.

Tabla 4.17a

Clase de opción	Número de Opción	Longitud 40 oct. max.	Descripción
0	3	var	Enrutamiento fuente Aproximado (83H)
0	7	var	Registro de ruta (07H)
0	9	var	Enrutamiento fuente estricto (89H)
2	4	var	Sello de tiempo (44H)

Tabla 4.17b
Valores codificados en el octeto de código de opción.

4.4.2.1 Opción de registro de ruta.

Esta opción permite que la fuente cree una lista vacía de direcciones IP y pide que cada enrutador que maneje el datagrama agregue su dirección a la lista.

Si un enrutador maneja un datagrama que tiene la opción de registro de ruta establecida, éste agrega su dirección IP a la lista del registro de ruta. Para agregarse por sí mismo un enrutador a la lista, compara el apuntador y el campo de longitud. Si el apuntador es más grande que la longitud, la lista está llena, entonces el enrutador envía el datagrama sin insertar su dirección. Si la lista no está llena, el enrutador inserta su dirección IP en la posición indicada por el apuntador e incrementa el apuntador en 4 (Ver figura 4.18a y 4.18b).

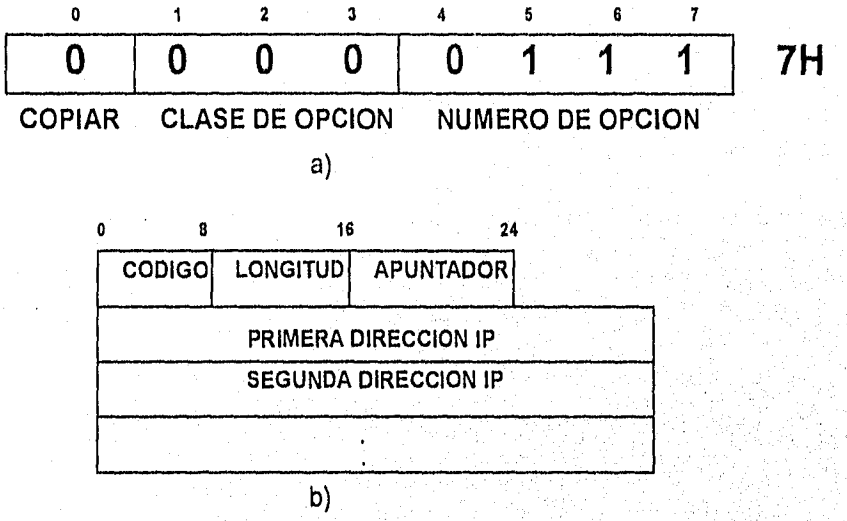


Figura 4.18
Formato de la opción de registro de ruta IP.

4.4.2.2 Opciones de enrutamiento fuente.

La opción de enrutamiento fuente proporciona una forma para que el emisor seleccione un ruta a través de los enrutadores entre las diversas redes. Para probar el rendimiento sobre una trayectoria, los administradores de red pueden usar el enrutamiento fuente para forzar a los datagramas IP a atravesar una determinada red. IP soporta dos formas de enrutamiento fuente. Una forma llamada enrutamiento fuente estricto que especifica una trayectoria de enrutamiento incluyendo una secuencia de direcciones IP. Enrutamiento estricto significa que las direcciones especifican la trayectoria exacta que el datagrama debe seguir para alcanzar su destino. La otra forma llamada enrutamiento

fuente aproximado, también incluye una secuencia de direcciones IP, pero permite múltiples saltos de red entre las direcciones en la lista (Ver figura 4.19).

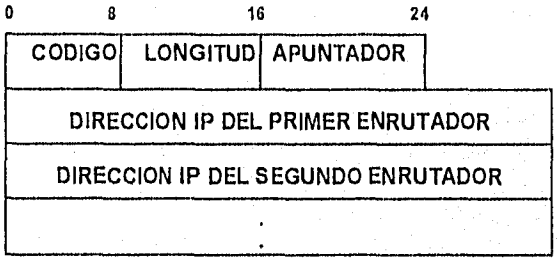


Figura 4.19
Formato de la opción de enrutamiento fuente estricto IP.

4.4.2.3 Opción del sello de tiempo.

La opción de sello de tiempo trabaja como la opción de registro de ruta. La opción de sello de tiempo contiene una lista vacía inicialmente, y cada enrutador perteneciente a la trayectoria de la fuente al destino pone su dirección IP y un entero de 32 bits con su sello de tiempo (Ver figura 4.20).

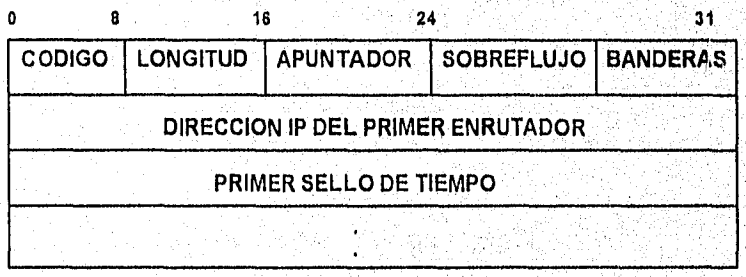


Figura 4.20
Formato de la opción de sello de tiempo IP.

4.4.2.4 Procesando opciones durante fragmentación.

Cuando un datagrama es fragmentado, un enrutador duplica algunas opciones IP en todos los fragmentos o en algunos casos sólo en un fragmento. Por ejemplo considerar la opción de registro de ruta. Si un datagrama de este tipo se fragmenta y a los fragmentos se les incluye esta opción, el destino podría recibir una lista de diferentes rutas de cada fragmento y por lo tanto la lista final no ser útil. Por lo tanto el estándar IP especifica que la opción de registro de ruta debe ser copiada únicamente en uno de los fragmentos de un datagrama.

4.4.2.5 Campos de las Opciones IP.

Copiar (Copy Thru Gate).

Si este bit es establecido a 1 y el mensaje IP es fragmentado, todos los fragmentos deben conducir el campo de opciones. Si éste es establecido a cero, únicamente el primer fragmento contendrá el campo de opciones.

Clase de opción (Option Class).

Este campo de dos bits tiene únicamente dos clases de opciones activas 00 datagrama o control de red y 10 para depuración y mediciones del sistema.

Número de opción.

Es un campo de 5 bits usado para seleccionar la opción IP que será invocada.

Longitud.

Usado para determinar la longitud total de el campo de opciones IP. Éste también indicará el tamaño máximo que los datos de las opciones pueden llegar a tener.

Apuntador (Pointer).

Usado para determinar la siguiente localidad donde los datos deben ser insertados dentro de los datos de opciones. Si la longitud es igual al pointer los datos de opciones están completos.

Sobreflujo (Overflow).

El número de enrutadores IP a través de los cuales el datagrama ha pasado podrían no agregar sus sellos de tiempo debido a que la opción estuviera llena.

Banderas de Sello de tiempo.

Usadas por la aplicación para dar instrucciones adicionales a los enrutadores acerca de la opción.

0000 únicamente sello de tiempo
0001 sello de tiempo + dirección IP
0010 no asignada
0011 sello de tiempo + leer IP
0100-1111 no asignadas

4.4.3 Encapsulación del datagrama IP.

Todos los datagramas deben ser transportados por una trama de la capa de enlace de datos. El datagrama es vaciado en el campo de datos de la trama y esto se conoce como encapsulación del datagrama IP (Ver figura 4.21).

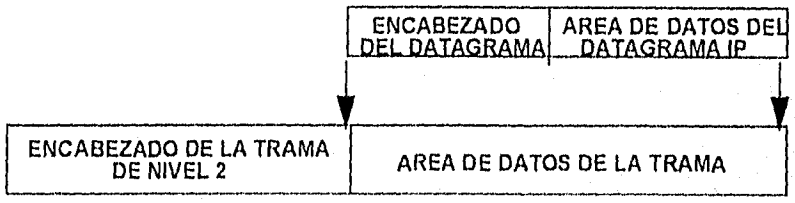


Figura 4.21
Datagrama IP encapsulado en la trama de nivel de enlace de datos.

4.4.4 Tamaño del datagrama, unidad de transferencia máxima de red y fragmentación.

- En el caso ideal, un datagrama IP siempre podría ser alojado en el campo de datos de una trama, haciendo la transmisión a través de la red muy eficiente. Sin embargo el datagrama debe viajar por redes muy diversas con diferentes tamaños de trama o diferentes unidades de transferencia máxima. El protocolo IP se diseño de tal manera que en lugar de tratar de cumplir un tamaño estándar de unidad de transferencia máxima para las diferentes redes, se elige un tamaño inicial de datagrama y se arregla una forma de dividir grandes datagramas dentro de pequeñas piezas cuando el datagrama necesita atravesar una red que tiene una trama pequeña. Las pequeñas piezas en las cuales el datagrama es dividido son llamadas fragmentos y el proceso de dividir el datagrama es conocido como fragmentación.

- La fragmentación usualmente ocurre en un enrutador. El enrutador usualmente recibe un datagrama de una red con una unidad de transferencia y debe enrutar ésta sobre una red en la cual la unidad de transferencia es más pequeña que el tamaño del datagrama.

En la figura 4.22, dos hosts se conectan directamente a redes Ethernet las cuales tienen una unidad de transferencia de 1500 octetos. Los dos hosts pueden enviar datagramas hasta de 1500 octetos. La trayectoria entre ellos incluye, sin embargo, una red con una unidad de transferencia máxima de 620 octetos. Si el host A envía un datagrama al host B más grande que 620 octetos, el enrutador R1 fragmentará el datagrama. Similarmente R2 fragmentará un datagrama grande del host B que se envíe al host A.

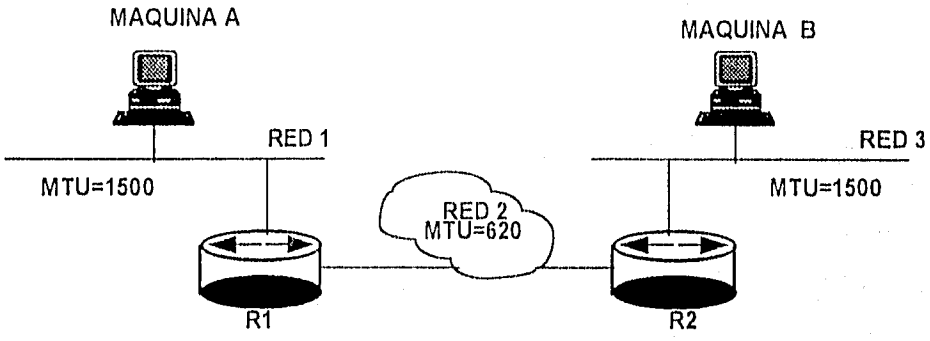


Figura 4.22
Fragmentación de una trama Ethernet.

El tamaño del fragmento es elegido de modo que cada fragmento pueda ser alojado en una sola trama. Adicionalmente IP representa la posición de los datos en múltiplos de 8 octetos.

El protocolo IP no limita el tamaño de los datagramas, ni garantiza que los datagramas sean entregados sin fragmentación. La fuente puede elegir cualquier tamaño de datagrama que piense sea apropiada; la fragmentación y reensamble ocurren automáticamente. La especificación IP señala que los enrutadores deben aceptar datagramas de hasta la unidad de transferencia máxima de las redes donde están conectados. Además los enrutadores deben siempre manejar datagramas de hasta 576 octetos. Los hosts también deben ser capaces de aceptar y reensamblar datagramas de al menos 576 octetos.

La fragmentación de un datagrama significa dividirlo en diversas piezas, como se puede ver en la figura 4.23. Cada pieza tiene el mismo formato que el datagrama original. Cada fragmento contiene un encabezado de datagrama que duplica muchos de los datos del encabezado del datagrama original (excepto un bit en el campo de banderas), seguido por datos hasta un límite del tamaño de la trama.

ENCABEZADO DEL DATAGRAMA (E)	600 OCTETOS DE DATOS (D1)	600 OCTETOS DE DATOS (D2)	200 OCTETOS DE DATOS (D3)

ENCABEZADO DEL FRAGMENTO 1 (E)	600 OCTETOS DE DATOS (D1)	FRAGMENTO 1 (OFFSET 0)
ENCABEZADO DEL FRAGMENTO 2 (E)	600 OCTETOS DE DATOS (D2)	FRAGMENTO 2 (OFFSET 600)
ENCABEZADO DEL FRAGMENTO 3 (E)	200 OCTETOS DE DATOS (D3)	FRAGMENTO 3 (OFFSET 1200)

Figura 4.23
Fragmentación de una trama en 3 fragmentos.

-Reensamble de Fragmentos.

Una vez que un datagrama es fragmentado, todos los fragmentos viajan a través de los enrutadores hasta alcanzar su destino final donde son reensamblados.

4.4.5 Control de Fragmentación.

Tres campos en el encabezado del datagrama, número de identificación de datagrama, banderas, y la posición de fragmento controlan la fragmentación y el reensamble de datagramas. El campo de identificación contiene un entero único que identifica el datagrama. Se debe tomar en cuenta también que cuando un enrutador fragmenta un datagrama, éste copia muchos de los campos en el encabezado del datagrama de cada uno de los fragmentos. El campo de identificación debe ser copiado.

Cada uno de los fragmentos tiene exactamente el mismo formato que el datagrama completo, el campo de posición de fragmento especifica la posición en el datagrama original de los datos siendo conducidos en el fragmento, medido en unidades de 8 octetos, comenzando en la posición cero. Para reensamblar el datagrama, el destino debe obtener todos los fragmentos comenzando con el fragmento que tiene la posición cero hasta el fragmento con la más alta posición. Los fragmentos no necesariamente llegan en orden, y no hay comunicación entre el enrutador que fragmenta el datagrama y el destino tratando de reensamblar éste.

Los 2 bits de más bajo orden de los 3 bits del campo de banderas controlan la fragmentación. El primer bit de control indica si el datagrama puede ser fragmentado o no. El fragmento de más bajo orden especifica si el fragmento contiene datos de la mitad del datagrama original o del final. Éste es llamado el bit de más fragmentos. Para darse cuenta por que tal bit es necesario, considerar que el destino intenta reensamblar el datagrama. El destino necesita saber cuando ha recibido todos los fragmentos de un datagrama. Cuando un fragmento llega, el campo de longitud total en el encabezado se refiere al tamaño del fragmento y no al tamaño del datagrama original, entonces el destino no puede usar el campo de longitud total para saber si todos los fragmentos han sido colectados. El bit de más fragmentos resuelve el problema; una vez que el destino recibe un fragmento con el bit de más fragmentos en cero, éste sabe que este fragmento contiene datos de el final del datagrama original. De los campos de posición del fragmento y longitud total, el destino puede calcular la longitud del datagrama original.

4.4.6 Tiempo de Vida.

El campo de tiempo de vida especifica cuanto tiempo, en segundos, al datagrama le es permitido viajar entre las redes hasta llegar a su destino. La idea es que si una máquina inyecta un datagrama dentro de la red, ésta establece el máximo tiempo que el datagrama debe vivir. Enrutadores y hosts que procesen los datagramas deben decrementar el campo de tiempo de vida y remover el datagrama cuando este tiempo expira. Cada enrutador debe decrementar en 1 el tiempo de vida de un datagrama, cuando éste procesa el encabezado. Además, para manejar casos de sobrecarga de enrutadores que introducen grandes demoras, cada enrutador registra el tiempo local cuando el datagrama llega, y decrementa el tiempo de vida por el número de segundos que el datagrama permanece dentro del enrutador esperando por servicio.

4.4.7 Enrutamiento IP.

El algoritmo de enrutamiento IP emplea una tabla de enrutamiento (algunas veces llamada tabla de enrutamiento IP). Si el software de enrutamiento IP necesita transmitir un datagrama, éste consulta la tabla de enrutamiento para decidir a donde enviar el datagrama. Como las direcciones IP indican la red y el host en esa red, las tablas de enrutamiento únicamente contienen prefijos de red y no las direcciones IP de cada máquina.

Típicamente una tabla de enrutamiento contiene pares (N,G), donde N es la dirección IP de la red destino, y G es la dirección IP de el "siguiente" enrutador en la trayectoria a la red N. De este modo, la tabla de enrutamiento de un enrutador G únicamente especifica un paso de G a la red destino. El enrutador no conoce la trayectoria completa al destino.

Es importante comprender que la tabla de enrutamiento siempre señala el enrutador que puede ser alcanzado a través de una sola red. Esto es, todos los enrutadores listados en una tabla de enrutamiento M deben de ser los que están conectados en redes a donde M se conecta directamente. Cuando un datagrama está listo para salir de M, el software IP localiza la dirección destino y extrae la porción de red. M entonces utiliza el identificador de red para tomar decisiones de enrutamiento, seleccionando un enrutador que pueda ser alcanzado directamente.

La figura 4.24 muestra un ejemplo concreto que ayuda a explicar las tablas de enrutamiento. El ejemplo consiste de 4 redes conectadas por 3 enrutadores. En la figura 4.24 se muestra la tabla de enrutamiento de el enrutador G. Debido a que G se conecta directamente a las redes 20.0.0.0 y 30.0.0.0, éste puede alcanzar cualquier host en esas redes directamente. Si se tiene un datagrama

destinado para un host en la red 40.0.0.0, G enruta éste a la dirección 30.0.0.7, la dirección del enrutador H. H entonces entregará el datagrama directamente. G puede alcanzar la dirección 30.0.0.7 debido a que G y H están conectados directamente a la red 30.0.0.0.

La figura 4.24 demuestra que el tamaño de la tabla de enrutamiento depende de el número de redes y no de los hosts en esas redes; ésta únicamente crece cuando nuevas redes son agregadas.

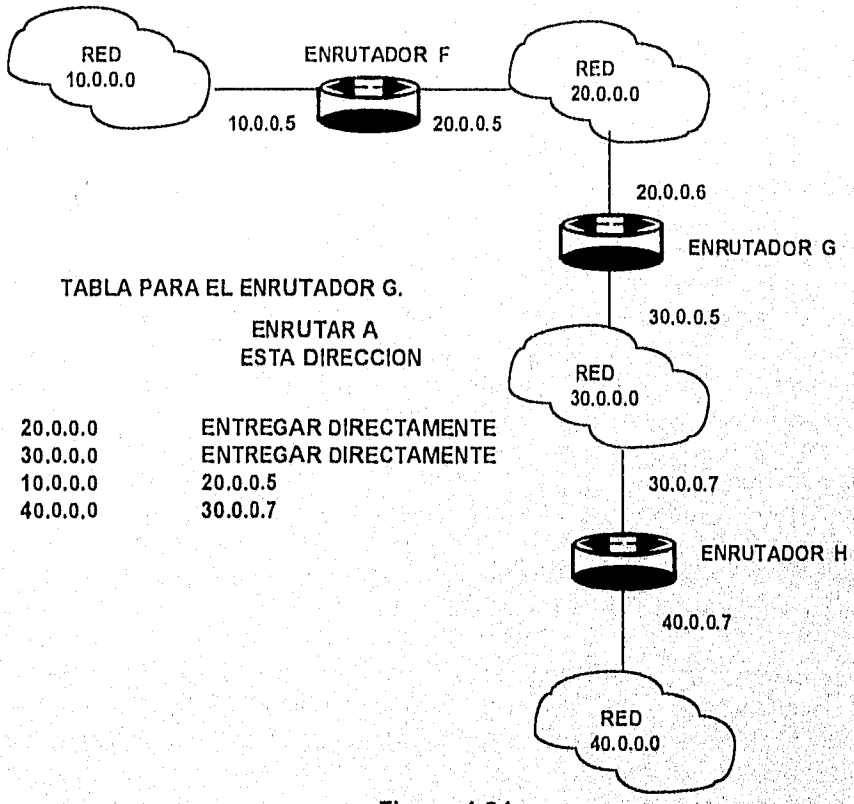


Figura 4.24
Tablas de enrutamiento para un enrutador en una red IP.

4.4.7.1 Enrutando con direcciones IP.

Es importante comprender que el enrutamiento IP no altera el datagrama original. En particular las direcciones fuente y destino del datagrama permanecen inalteradas. Cuando IP ejecuta el algoritmo de enrutamiento, éste calcula una nueva dirección. La dirección IP calculada por el algoritmo de enrutamiento es conocida como dirección del "siguiente punto", debido a que ésta dice a donde el datagrama debe ser enviado. ¿Dónde almacena IP esta

dirección? no se almacena en el datagrama. Después de ejecutar el algoritmo de enrutamiento, IP pasa el datagrama y la dirección de el "siguiente punto" al software de interface de red responsable de la red física sobre la cual el datagrama debe ser enviado. El software de interface de red física relaciona la dirección de el "siguiente punto" a una dirección física, forma una trama usando esa dirección física, y envía el resultado. Después de usar la dirección del "siguiente punto" el software de interface de red descarta esta dirección.

Se puede ver estraño que las tablas de enrutamiento almacenan la dirección IP del "siguiente punto" para cada red destino cuando esas direcciones deben ser trasladadas a sus correspondientes direcciones físicas antes de que el datagrama pueda ser enviado. Si nosotros imaginamos un host enviando datagramas a la misma dirección destino, el uso de la dirección IP parecerá totalmente ineficiente. IP extrae la dirección destino en cada datagrama y usa la tabla de enrutamiento, para producir la dirección del siguiente punto. Éste entonces pasa el datagrama al siguiente punto a la interface de red, la cual calcula la dirección física

¿Por qué IP evita usar direcciones físicas cuando almacena y calcula rutas?

Primero, usar únicamente direcciones IP en la tabla de enrutamiento facilita a los administradores el chequeo de la actualización de las rutas. Segundo todo el software puede ser escrito para comunicarse usando direcciones IP y el conocimiento de direcciones físicas es relegado a un par de rutinas de bajo nivel.

4.4.7.2 Manejando datagramas entrantes.

Cuando un datagrama IP llega a un enrutador se tienen dos casos: el datagrama pudo haber alcanzado su destino final, o puede viajar más.

Determinar si el datagrama ha alcanzado su destino final no es cosa trivial. Cuando un datagrama IP llega, el enrutador debe comparar la dirección IP destino con la dirección IP de sus conexiones de red. Si alguna interface cumple la comparación, éste mantiene el datagrama y lo procesa. En el caso de que la comparación no sea exitosa, IP decrementa el campo de tiempo de vida en el encabezado del datagrama, descartando el datagrama si el contador alcanza cero.

Enrutamiento IP consiste en decidir donde enviar un datagrama basado en el contenido de la tabla de enrutamiento. La ruta es directa si la máquina destino cae en la red en la cual la máquina enviante está conectada. La ruta es indirecta si el datagrama debe ser enviado a un enrutador para su entrega.

Enrutamiento IP produce la dirección IP de la siguiente máquina a la cual el datagrama debe ser enviado; IP pasa el datagrama y la dirección del siguiente punto al software de interface de red. La transmisión de un datagrama de una

máquina a la siguiente involucra siempre encapsular el datagrama en una trama física, mapeando la siguiente dirección IP a una dirección física.

El algoritmo de enrutamiento IP es de manejo de tabla y usa únicamente direcciones IP. Este basa sus decisiones de enrutamiento en la dirección de la red destino en lugar del host destino, manteniendo tablas de enrutamiento pequeñas.

Hasta aquí se mostró como IP enruta los datagramas basado en el contenido de tablas de enrutamiento, sin decir como el sistema inicializa sus tablas de enrutamiento o actualiza éstas con los cambios de red.

4.4.7.3 Algoritmos de enrutamiento.

Para inicializar y actualizar las tablas de enrutamiento los enrutadores hacen uso de algoritmos de enrutamiento que pueden ser clasificados en dos tipos: los algoritmos de vector a distancia y los algoritmos de estado del enlace.

Algoritmos de vector a distancia.

El término vector-distancia se refiere a la clase de algoritmos que los enrutadores usan para propagar información de enrutamiento. Se asume que cada enrutador comienza con un conjunto de rutas de aquellas redes a las cuales está conectado. Éste mantiene una lista de las rutas en una tabla, donde cada entrada identifica una red destino y da la distancia a esa red medida en saltos.

Periódicamente cada enrutador envía una copia de su tabla de enrutamiento a cualquier otro enrutador que pueda alcanzar directamente.

El término vector-distancia viene de la información enviada en mensajes periódicos. Un mensaje contiene una lista de pares (V, D), donde V identifica un destino (llamado el vector), y D es la distancia al destino.

A continuación se muestra un ejemplo de la tabla de un enrutador, "A" y un mensaje de actualización de un enrutador, "B".

TABLA DE ENRUTADOR A			MENSAJE DE ACTUALIZACION DEL ENRUTADOR B.	
DESTINO	DISTANCIA	RUTA	DESTINO	DISTANCIA
RED 1	0	DIRECTA	RED 1	2
RED 2	0	DIIRECTA	→ RED 4	3
RED 4	8	ENRUTADOR L	RED 20	6
RED 20	5	ENRUTADOR M	→ RED 25	4
RED 30	6	ENRUTADOR B	RED 30	5
RED 40	2	ENRUTADOR Q	RED 40	10
RED 45	2	ENRUTADOR B	→ RED 45	3

Se debe notar que si B reporta distancia N, la entrada actualizada en A reportará distancia N+1 (se incluye ahora la distancia a B). Las tablas de enrutamiento también contienen un tercer campo que indica el siguiente punto en la ruta (que enrutador sigue).

Ejemplos de protocolos de vector a distancia son el RIP y el IGRP.

Algoritmos de estado del enlace.

Los algoritmos de estado del enlace requieren que cada enrutador participante tenga información completa de la topología de la red. En lugar de enviar mensajes que contienen listas de destinos, un enrutador participante en un algoritmo de estado del enlace realiza dos tareas. Primero, éste activa pruebas del estado de todos los enrutadores vecinos. Segundo, éste periódicamente propaga información de estado del enlace a todos los otros enrutadores.

Para informar a todos los enrutadores, cada enrutador periódicamente envía un mensaje en broadcast que lista el estado de cada uno de sus enlaces. El mensaje de estado no reporta rutas, simplemente indica si la comunicación es posible entre pares de enrutadores.

Siempre que un mensaje de estado del enlace llega, un enrutador usa la información para actualizar su mapa de la red, marcando los enlaces arriba y abajo. Siempre que el estado de un enlace cambia, el enrutador recalcula sus rutas aplicando el algoritmo de Dijkstra. El algoritmo de Dijkstra calcula las trayectorias más cortas a todos los destinos desde una fuente.

Ejemplos de protocolos de estado del enlace son el OSPF.

4.5 El protocolo de mensajes de control Internet ICMP.

Como se vió el protocolo de red IP proporciona un servicio de entrega de datagramas sin conexión no confiable, y un datagrama viaja de un enrutador a otro hasta alcanzar uno que pueda entregar el datagrama a su destino final.

Si un enrutador no puede entregar el datagrama, o si un enrutador detecta una condición no usual, como congestión de red, que afecta su habilidad para enviar el datagrama, éste necesita avisarle a la fuente original que tome acción para evitar o corregir el problema.

En este punto se describe un mecanismo que los enrutadores y máquinas en las redes usan para comunicar tal información de control de error.

Además de las fallas de las líneas de comunicación y procesadores, el protocolo IP falla en la entrega de datagramas cuando la máquina destino está temporalmente o permanentemente desconectada de la red, cuando el contador de tiempo de vida expira, o cuando enrutadores intermedios están tan congestionados que no pueden procesar el tráfico entrante. Para permitir que los enrutadores en la red reporten errores o proporcionen información acerca de las circunstancias no esperadas, los diseñadores agregaron un mecanismo de mensajes de propósito especial para los protocolos TCP/IP. El mecanismo es conocido como protocolo de mensajes de control internet ICMP.

Técnicamente ICMP es un mecanismo de reporte de errores. ICMP únicamente reporta condiciones de error a la fuente original; la fuente debe relacionar errores con programas de aplicación individual y tomar acción para corregir el problema.

¿Por qué se restringe ICMP con la fuente original?. La respuesta es que el datagrama únicamente contiene campos que especifican la fuente original y el destino final. Éste no contiene un registro de su viaje a través de la red.

4.5.1 Encapsulamiento del mensaje ICMP.

Los mensajes ICMP requieren ser encapsulados en la porción de datos de un datagrama IP (Ver figura 4.25). Los datagramas conduciendo mensajes ICMP son enrutados exactamente como los datagramas conduciendo información para usuarios.

Los mensajes ICMP pueden ser extraviados o descartados, pero no se generan mensajes de reporte de error que resulten de datagramas conduciendo mensajes de error ICMP.

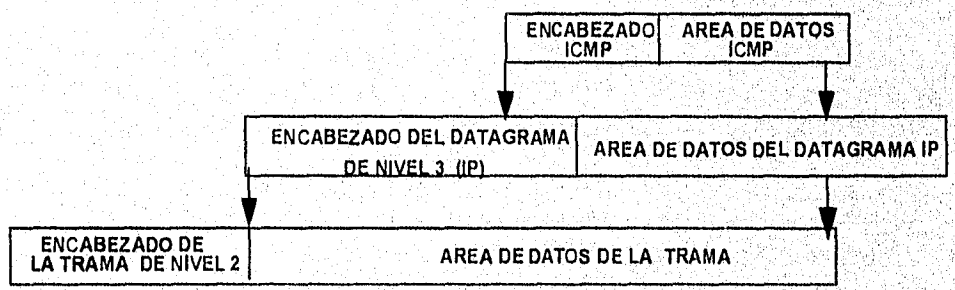


Figura 4.25
Encapsulamiento del mensaje ICMP.

4.5.2 Formato del mensaje ICMP.

Aunque cada mensaje ICMP tiene su propio formato, todos ellos comienzan con los mismos tres campos: Un campo de tipo de mensaje que contiene un entero de 8 bits, un campo de código de 8 bits que proporciona información adicional acerca del tipo de mensaje y un campo de CHECKSUM de 16 bits para el encabezado ICMP. Adicionalmente, mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama con problemas.

La razón de regresar más información que sólo el encabezado del datagrama es permitir al receptor determinar más precisamente que protocolos y cuales programas de aplicación fueron responsables del datagrama.

El campo de tipo ICMP define el formato del mensaje, así como su significado y se muestran a continuación:

Campo de Tipo	Tipo de Mensaje ICMP.
0	Respuesta de eco.
3	Destino no alcanzable.
4	Apaciguar fuente (Source Quench).
5	Redirector(Cambiar de ruta).
8	Solicitud de Eco.
11	Tiempo excedido para un datagrama.
12	Problema de parámetros en un datagrama.
13	Solicitud de sello de tiempo.
14	Respuesta de sello de tiempo.
17	Solicitud de dirección de máscara.
18	Respuesta de dirección de máscara.

4.5.3 Probando si un destino puede ser alcanzado y su estado.

Los protocolos TCP/IP proporcionan facilidades para ayudar a los administradores de red o usuarios a identificar problemas de red. Una de las más frecuentes herramientas de depuración invoca los mensajes de solicitud y respuesta de eco ICMP. Un host o enrutador envía un mensaje de solicitud de eco ICMP para un destino específico. Cualquier máquina que reciba una solicitud de eco genera una respuesta de eco y retorna ésta al emisor original. La solicitud contiene un área de datos opcional; la respuesta contiene una copia del área de datos enviada en la solicitud. La solicitud de eco y la respuesta asociada pueden ser usadas para probar si un destino es alcanzable y si responde. Debido a que ambos solicitud y respuesta viajan en un datagrama, la recepción exitosa de una respuesta verifica la mayoría de las piezas del

sistema de transporte. Primero el software en la máquina fuente debe enrutar el datagrama. Segundo, los enrutadores intermedios entre la fuente y el destino deben estar operando y deben enrutar los datagramas correctamente. Tercero, la máquina destino debe estar encendida y ambos IP e ICMP trabajando. Finalmente las rutas de regreso entre los enrutadores deben estar trabajando. En muchos sistemas el comando de usuario invocado para enviar solicitudes de eco ICMP es llamado ping.

4.5.3.1 Formato del mensaje de solicitud y respuesta de eco.

El campo mostrado en la figura 4.26 como datos opcionales es un campo de longitud variable que contiene datos a ser devueltos al emisor y generalmente tiene un valor de 256 octetos. Una respuesta de eco siempre regresa exactamente los mismos datos que fueron puestos en una solicitud de eco. Los campos identificador y número de secuencia son usados por el emisor para comparar parejas de solicitudes y respuestas. El valor del campo de tipo especifica si el mensaje es una solicitud (8) o una respuesta (0).

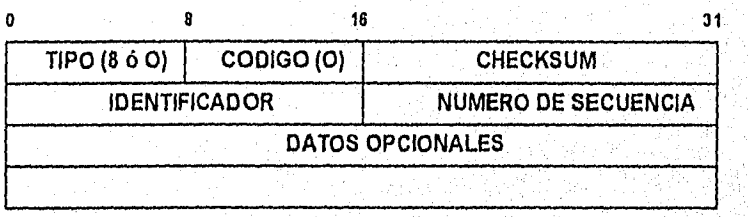


Figura 4.26
Mensaje de solicitud y respuesta de eco ICMP.

4.5.3.2 Reporte de destinos no alcanzables.

Cuando un enrutador no puede entregar un datagrama IP, éste envía un mensaje de destino no alcanzable ICMP de regreso a la fuente original, usando el formato mostrado en la figura 4.27.

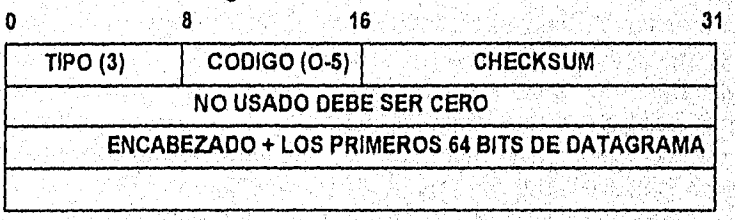


Figura 4.27
Mensaje de reporte de destinos no alcanzables ICMP.

El campo de código contiene un entero que describe el problema.

Los posibles valores son:

Valor del Código	Significado.
0	Red no alcanzable.
1	Host no alcanzable.
2	Protocolo no alcanzable.
3	Puerto no alcanzable.
4	Fragmentación necesaria.
5	Falla de ruta fuente.
6	Red destino desconocida.
7	Host destino desconocido.
8	Host fuente aislado.
9	Comunicación con red destino prohibida por administración.
10	Comunicación con host prohibida por administración.
11	Red no alcanzable por tipo de servicio.
12	Host no alcanzable por tipo de servicio.

Aunque IP es un mecanismo de entrega con el mejor esfuerzo, los datagramas descartados no deben ser tomados a la ligera. Cuando un datagrama tiene errores un enrutador lo descarta y envía un mensaje de destino no alcanzable a la fuente. Errores de redes no alcanzables usualmente implican errores de enrutamiento; errores de hosts no alcanzables implican fallas de entregas. Debido a que el mensaje contiene un prefijo corto del datagrama que tuvó el problema, la fuente sabrá exactamente que dirección causo el problema.
Los destinos pueden ser no alcanzables porque el hardware está fuera de servicio, o porque el emisor especifico una dirección de destino no existente. Debe notarse que aunque los enrutadores reportan fallas que ellos encuentran, ellos no pueden saber sobre algunas fallas de entrega. Por ejemplo si la máquina destino está conectada a una red Ethernet, el hardware de red no proporciona reconocimientos. Por lo tanto un enrutador puede continuar enviando paquetes a un destino, después de que el destino es apagado sin recibir ninguna indicación de que los datagramas no han sido entregados.

4.5.4 Congestión y datagrama de control de flujo.

Es importante comprender que la congestión puede ocurrir por dos diferentes razones. Primero una computadora de alta velocidad puede ser capaz de generar tráfico más rápido de lo que la red puede transferirlo. Segundo si

muchas computadoras simultáneamente necesitan enviar datagramas a través de un solo enrutador, el enrutador puede experimentar congestión.

Cuando los datagramas llegan demasiado rápido, se hacen colas en memorias temporales. Si los datagramas son parte de una pequeña ráfaga, los buffers resuelven el problema. Si el tráfico continua, el host o el enrutador no es capaz de almacenar en memoria los datagramas y empieza a descartar datagramas. Una máquina utiliza un mensaje apaciguar fuente ICMP para tratar de aliviar la congestión. Un mensaje apaciguar fuente es una solicitud para la fuente, donde se le indica que reduzca la velocidad de transmisión de datagramas. Usualmente los enrutadores congestionados envían un mensaje apaciguar fuente por cada datagrama descartado.

Un host que recibe un mensaje apaciguar fuente de alguna máquina, baja la velocidad a la cual envía los datagramas hasta detenerse si es necesario; éste gradualmente incrementa la velocidad de envío de los datagramas en la medida que deja de recibir los mensajes de apaciguar fuente.

4.5.4.1 Formato del mensaje apaciguar fuente (Source Quench).

Este mensaje contiene los tres campos generales de tipo, código y checksum, un campo de 32 bits que no tiene uso y un prefijo con información del datagrama descartado (Ver figura 4.28).

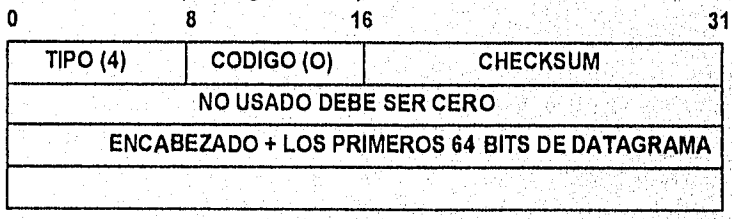


Figura 4.28
Mensaje de apaciguar fuente ICMP.

4.5.5 Solicitud de cambio de ruta por enrutadores.

Las tablas de enrutamiento usualmente permanecen estáticas durante largos periodos de tiempo. Los enrutadores inicializan ellas de un archivo de configuración durante el arranque, y los administradores raramente hacen cambios de enrutamiento durante operación normal. Si la topología de la red cambia, las tablas de enrutamiento de un enrutador o host pueden ser incorrectas. Un cambio puede ser temporal o permanente. Como se vió anteriormente los enrutadores intercambian información de enrutamiento periódicamente para adaptarse a cambios de la red y actualizar sus rutas. Como regla general se asume que los enrutadores conocen las rutas y los hosts

comezando con mínima información de enrutamiento y aprendiendo nuevas rutas de los enrutadores. En un caso especial, cuando un enrutador detecta un host usando una ruta no óptima, éste envía al host un mensaje ICMP, llamado redirector, solicitando que el host cambie sus rutas.

Los mensajes de redirección no resuelven el problema de propagación de rutas en forma general, sin embargo, ellos son limitados a interacciones entre un enrutador y un host en una red local.

4.5.5.1 Formato del Mensaje de Redirección ICMP.

Este mensaje se muestra en la figura 4.29. Contiene los tres campos generales, donde el campo de código especifica como interpretar la dirección destino, basado en los valores asignados como sigue:

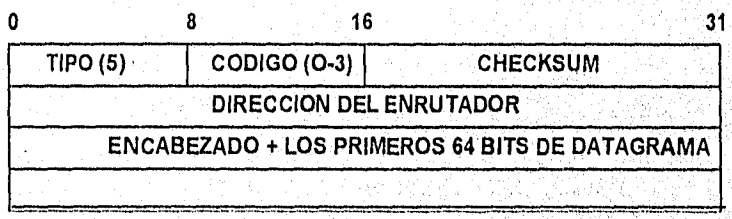


Figura 4.29
Mensaje de redirección ICMP.

Valor del Código	Significado.
1	Redireccionar datagramas para el Host.
2	Redireccionar datagramas para el tipo de servicio y red.
3	Redireccionar datagramas para el tipo de servicio y Host.

Además cada mensaje contiene un campo de 32 bits con la dirección del enrutador que el host usa para alcanzar el destino mencionado en el encabezado del datagrama.

4.5.6 Detectando rutas de longitud excesiva o circulares.

Debido a que los enrutadores calculan el "siguiente punto" en la ruta de transmisión usando sus tablas locales, errores en las tablas producirán errores

en el enrutamiento como ciclos cerrados o rutas demasiado largas. Si un datagrama ingresa en un ciclo de enrutamiento, permanecerá ahí indefinidamente. Para evitar lo anterior el datagrama contiene un tiempo de vida algunas veces llamado hop count. Cuando el tiempo de vida del datagrama se vence, éste es descartado.

Si un enrutador descarta un datagrama debido a que su tiempo de vida se ha excedido o debido a que ha expirado el temporizador de fragmentos del datagrama, éste envía un mensaje ICMP de tiempo excedido de regreso a la fuente del datagrama.

4.5.6.1 Formato del Mensaje tiempo Excedido.

Este datagrama contiene los tres campos generales donde el campo de código indica la naturaleza del tiempo vencido (Ver figura 4.30).

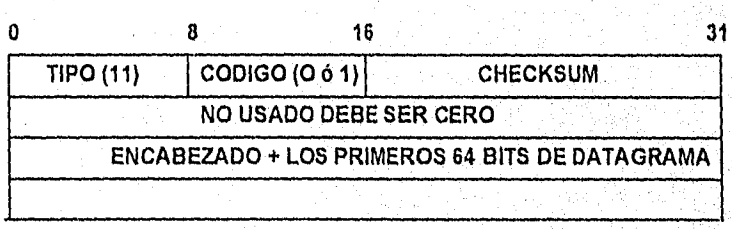


Figura 4.30
Mensaje de tiempo excedido ICMP.

Valor del código	Significado.
0	Contador del tiempo de vida excedido.
1	Tiempo de reensamble de fragmentos excedido.

4.5.7 Reportando otros problemas.

Cuando un enrutador o host encuentra problemas con un datagrama no cubiertos por los mensajes ICMP mencionados, éste envía un mensaje de problema de parámetros a la fuente original (ver figura 4.31).

Para hacer el mensaje menos ambiguo, el emisor usa el apuntador en el encabezado del mensaje para identificar cual octeto en el datagrama causo el problema.

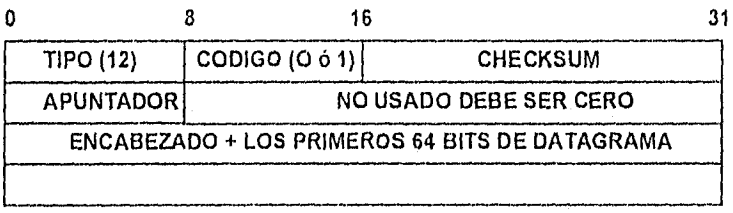


Figura 4.31.
Mensaje de problema de parámetros ICMP.

4.5.8 Sincronización de reloj y estimación de tiempo de tránsito.

Aunque las máquinas en una red pueden comunicarse, usualmente ellas operan independientemente, con cada máquina siguiendo su propia noción del tiempo. Relojes que difieren ampliamente pueden confundir a los usuarios. El protocolo TCP/IP incluye diversos mensajes que pueden ser usados para sincronizar relojes. Una de las más simples técnicas usa un mensaje ICMP para obtener el tiempo de otra máquina. Una máquina solicitante envía un mensaje de solicitud de sello de tiempo ICMP a otra máquina, pidiendo que la segunda máquina retorne su valor actual del tiempo del día. La máquina receptora retorna una contestación de sello de tiempo a la máquina que le hizo la solicitud.

En la práctica la estimación exacta del viaje de ida y vuelta puede ser difícil y substancialmente restringe la utilidad de los mensajes de sello de tiempo.

4.5.8.1 Formato del mensaje de solicitud y respuesta de sello de tiempo.

El campo de tipo identifica el mensaje como una solicitud (13) o como respuesta (14); el identificador y número de secuencia son usados por la fuente para asociar solicitudes con respuestas. El campo de sello de tiempo contiene la hora en la que el paquete es transmitido, el campo de sello de tiempo de recepción es llenado con la hora de recepción de una solicitud de sello de tiempo, el campo de sello de tiempo de transmisión es llenado inmediatamente antes de que la respuesta es transmitida.
Los hosts usan los tres campos de sello de tiempo para calcular el tiempo de retardo entre ellos y para sincronizar sus relojes. Debido a que la respuesta incluye el campo de sello de tiempo origen, un host puede calcular el tiempo total requerido por una solicitud para viajar al destino, ser transformada en una respuesta y regresar. Debido a que la respuesta conduce el tiempo en que la solicitud ingreso a la máquina destino, así como el tiempo en el cual la respuesta salió, el host puede calcular el tiempo de tránsito de red, y de éste estimar las diferencias entre los relojes local y remoto (Ver figura 4.32).

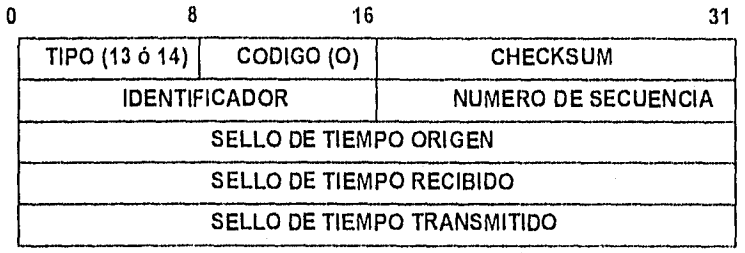


Figura 4.32
Mensaje de solicitud y respuesta de sello de tiempo ICMP.

4.5.9 Obteniendo una máscara de subred.

Para aprender la máscara de subred usada por la red local, una máquina puede enviar un mensaje de solicitud de dirección de máscara a un enrutador y recibir una respuesta de dirección de máscara. La máquina haciendo la solicitud puede enviar la solicitud directamente si conoce la dirección del enrutador o puede enviar un mensaje broadcast en caso contrario.

4.5.9.1 Formato del mensaje de solicitud o respuesta de dirección de máscara de subred.

El campo de tipo en el mensaje especifica si el mensaje es una solicitud (17) o una respuesta (18). Una respuesta contiene una máscara de direccionamiento de subredes. El identificador y número de secuencia asocian solicitudes con respuestas. El campo de máscara de direccionamiento contiene el número de máscara de direccionamiento de subredes (Ver figura 4.33).

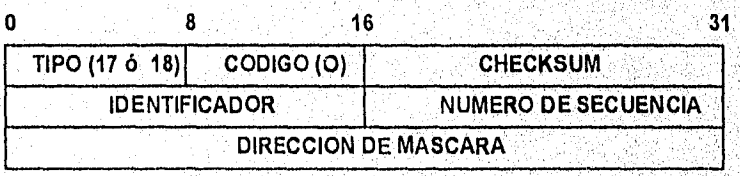


Figura 4.33
Mensaje de solicitud o respuesta de dirección de máscara de subred ICMP.

4.6 El protocolo de datagrama de usuario UDP.

Muchos sistemas operativos en muchas computadoras soportan multiprogramación, lo que significa que permiten a múltiples programas de aplicación ejecutarse simultáneamente. Es muy natural decir que un proceso es el destino final para un mensaje. Sin embargo, decir que un proceso particular es el destino final para un datagrama es de alguna manera erróneo. Primero, porque los procesos son creados y destruidos dinámicamente. Segundo, es necesario poder reemplazar procesos en las máquinas sin tener que avisar a todos los emisores. Tercero, se necesita identificar los destinos basados en las funciones que ellos implementan sin conocer el proceso que implementa la función.

En lugar de pensar en un proceso como último destino, nosotros imaginaremos que cada máquina contiene un conjunto de puntos de destino abstractos, llamados puertos del protocolo. Cada puerto de protocolo es identificado por un número entero. El sistema operativo local proporciona un mecanismo de interface que usa procesos para especificar un puerto o acceso a éste.

Muchos sistemas operativos proporcionan acceso síncrono a los puertos. Desde un punto de vista de un proceso particular, acceso síncrono significa que la computación se detiene durante la operación de acceso a un puerto. Por ejemplo, si un proceso intenta extraer datos de un puerto antes de que los datos lleguen, el sistema operativo detiene el proceso hasta que los datos llegan. Una vez que los datos llegan, el sistema operativo pasa los datos al proceso y reinicia éste. En general a los puertos le son asignados buffers, así que los datos que llegan antes de que un proceso esté listo para aceptarlos, no se perderán. Para comunicarse una máquina con otra, el emisor necesita la dirección IP de la máquina destino y el número de puerto de protocolo del destino dentro de la máquina. Cada mensaje lleva el número de puerto destino y el número de puerto fuente.

El protocolo de datagrama de usuario UDP proporciona el mecanismo primario que los programas de aplicación usan para enviar datagramas a otros programas de aplicación. UDP proporciona puertos de protocolo para distinguir entre múltiples programas ejecuntandose en una máquina. Esto es, en adición a los datos enviados, cada mensaje UDP contiene número de puerto destino y número de puerto fuente, haciendo posible que el software UDP en el destino entregue el mensaje al recipiente correcto.

UDP utiliza el protocolo IP para transportar mensajes de una máquina a otra, y proporciona la misma entrega de datagramas sin conexión no confiable que IP.

No usa reconocimientos para asegurar que los mensajes lleguen, no ordena mensajes y no proporciona control de flujo.

Un programa de aplicación que usa UDP acepta la responsabilidad completa de manejar el problema de la confiabilidad, incluyendo pérdida de mensajes, duplicación, retardo, entrega fuera de orden, y pérdida de conectividad.

4.6.1 Multiplexaje, demultiplexaje y puertos UDP.

UDP acepta datagramas de muchas aplicaciones y los entrega para transmisión al protocolo IP, además acepta datagramas UDP provenientes de IP y los pasa a la aplicación apropiada.

Conceptualmente, todo el multiplexaje y demultiplexaje entre software UDP y programas de aplicación ocurre a través del mecanismo de puertos. En la práctica, cada programa de aplicación debe negociar con el sistema operativo para obtener un puerto del protocolo antes de enviar un datagrama UDP. Una vez que el puerto ha sido asignado, cualquier datagrama del programa de aplicación enviado a través del puerto tendrá ese número de puerto en su campo correspondiente.

Mientras se procesa una entrada, UDP acepta datagramas entrantes del software IP y los demultiplexa de acuerdo al puerto destino UDP (Ver figura 4.34).

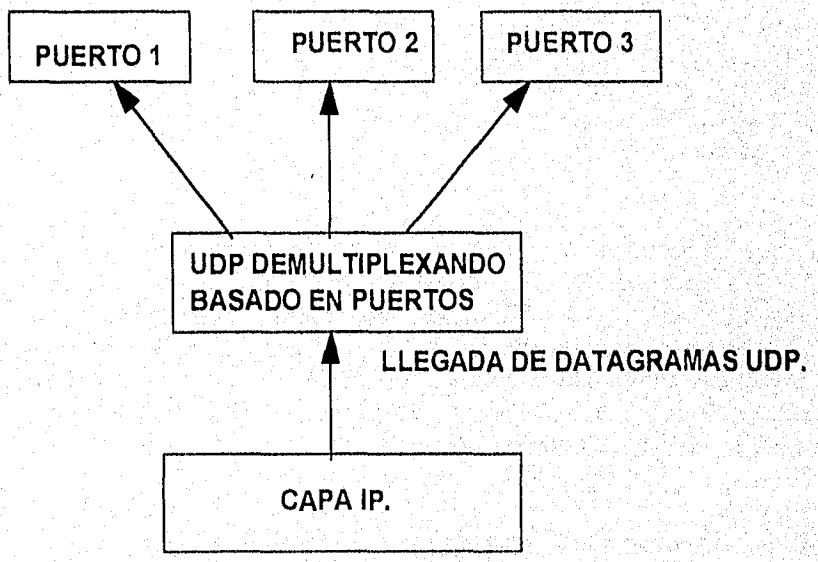


Figura 4.34
Diagrama de utilización de puertos UDP.

La más fácil forma de pensar en un puerto UDP es una cola. En muchas implementaciones, cuando un programa de aplicación negocia con el sistema operativo que puerto usar, el sistema operativo crea una cola interna que puede alojar a los mensajes entrantes. Frecuentemente la aplicación puede especificar o cambiar el tamaño de la cola. Cuando UDP recibe un datagrama, checa el número de su campo de puerto destino y lo compara con sus puertos en uso. Si el puerto no está en uso, éste envía un mensaje de error de puerto no alcanzable ICMP y descarta el datagrama. Si el puerto está en uso, UDP pone en la cola el nuevo datagrama en el puerto donde la aplicación va a accesar a éste.

4.6.2 Números de puerto UDP disponibles y reservados.

Hay dos formas fundamentales de asignar los puertos. La primera usa una autoridad central que asigna los números de puertos con diversos servicios y publica una lista. A estos puertos se les da el nombre de puertos bien conocidos (Ver figura 4.35).

La segunda forma para asignación de puertos usa asignación dinámica del software de red y los puertos no son conocidos de antemano, sino que se asignan aleatoriamente.

Los valores de los puertos bien conocidos toman valores bajos (0-1024), dejando valores enteros grandes para asignación dinámica (1025 a 65535).

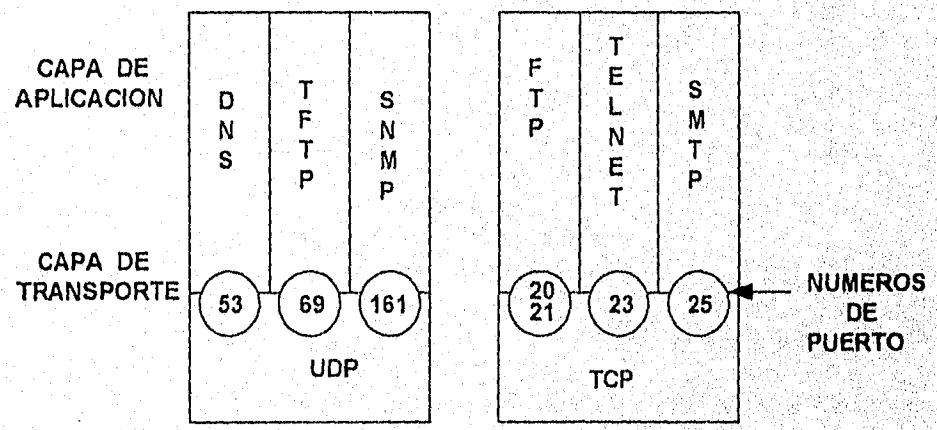


Figura 4.35
Puertos utilizados por las aplicaciones para accesar a la capa de transporte UDP y TCP.

4.6.3 Encapsulamiento UDP.

El mensaje UDP compuesto por un encabezado y datos es encapsulado en un datagrama IP como se muestra en la figura 4.36.

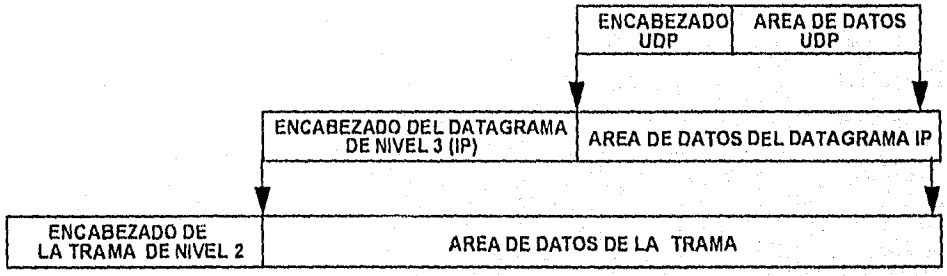


Figura 4.36
Encapsulamiento del mensaje UDP en un datagrama IP.

4.6.4 Formato del datagrama UDP.

Cada mensaje UDP es llamado un datagrama de usuario. La figura 4.37 muestra que el encabezado está dividido en 4 campos de 16 bits que se describen a continuación:

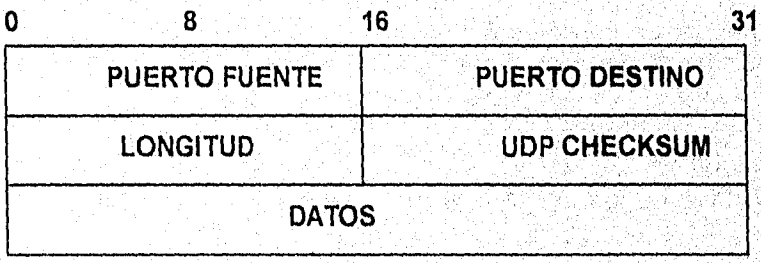


Figura 4.37
Formato del datagrama UDP.

Puerto fuente y destino UDP.

Estos campos contienen números de protocolo UDP de 16 bits.

El puerto destino es un puerto bien conocido y se asocia con una aplicación, por ejemplo el puerto 69 UDP para la aplicación TFTP.

El puerto fuente es un puerto aleatorio mayor a 1024.

Longitud del mensaje UDP.

Este campo indica la longitud del mensaje total incluyendo el encabezado y los datos UDP en octetos.

Checksum UDP.

Este es un campo de chequeo de errores opcional en el encabezado UDP y los datos que éste conduce. Para calcular el valor de este campo, el software primero almacena ceros en el campo de checksum del mensaje, entonces realiza una suma de enteros de 16 bits con aritmética de complemento a uno incluyendo una estructura denominada pseudo-encabezado UDP y el mensaje UDP. Se toma el complemento a uno de la suma realizada y el resultado se ingresa en el campo de checksum UDP.

4.6.5 El seudo-encabezado UDP.

El checksum UDP cubre más información que sólo la del datagrama UDP. El propósito de usar un seudo-encabezado es verificar que el datagrama UDP ha alcanzado su destino correcto. UDP en la máquina emisora calcula un checksum que cubre la dirección IP destino, la dirección IP fuente, así como el datagrama UDP. En el destino final, el software UDP verifica el checksum usando la dirección IP destino obtenida del encabezado del datagrama IP que transportó el mensaje UDP.

El seudo-encabezado utilizado en el cálculo del checksum UDP consiste en 12 octetos de datos como se muestran en la figura 4.38.

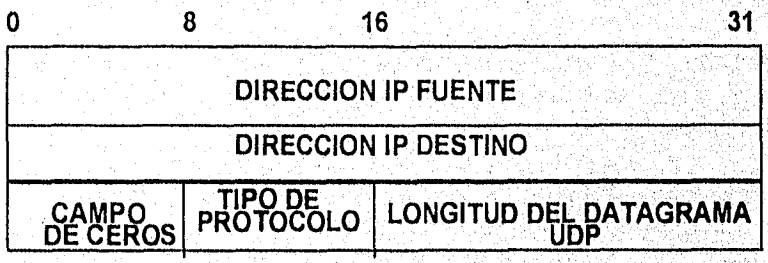


Figura 4.38
Pseudo-encabezado UDP.

Los campos son la dirección IP fuente y destino que se utilizarán en el datagrama IP para enviar el mensaje UDP.

Un campo de tipo de protocolo con un valor de 11 hex. (17dec.) para UDP y la longitud del datagrama UDP.

4.7 El protocolo de control de transmisión TCP.

El protocolo TCP especifica el formato de los datos y reconocimientos que dos computadoras intercambian para lograr una transferencia de datos confiable, así como los procedimientos que las computadoras usan para asegurar que los datos llegan correctamente. El protocolo también permite especificar como el software distingue entre múltiples destinos en una máquina dada, y como las máquinas en comunicación se recuperan de errores como pérdida o duplicación de paquetes.

4.7.1 Puertos, conexiones y puntos finales.

TCP usa números de puerto de protocolo para identificar el destino final dentro de una máquina. A cada puerto le es asignado un pequeño entero para identificarlo.

Los puertos TCP son más complejos que los puertos UDP, ya que un puerto TCP no corresponde a un solo objeto. TCP usa una conexión, no el puerto del protocolo, las conexiones son identificadas por un par de puntos finales.

Una conexión consiste de un acuerdo de transmisión de datos entre dos programas de aplicación. TCP define un punto final como un par de enteros (host y puerto), donde el host es la dirección TCP para un host y puerto es el puerto TCP en el host. Por ejemplo el punto final (128.10.2.3.25).

Debido a que TCP identifica una conexión con un par de puntos finales, un número de puerto TCP dado puede ser compartido por múltiples conexiones en la misma máquina.

Las aplicaciones accesan a la red vía puertos TCP. La razón de tener puertos es que los procesos pueden ser solicitados por su bien conocida identidad y el cliente que está solicitando el servicio puede usar un puerto aleatorio, permitiendo que más de una sesión corra con ese servicio desde la misma dirección IP.

Los puertos de los servicios bien conocidos tienen un valor menor a 1024.

Los puertos aleatorios tienen valores de 1025 a 65535.

4.7.2 Aperturas pasivas y activas.

TCP es un protocolo orientado a conexión que requiere que ambos puntos finales estén de acuerdo en el establecimiento de la conexión. Para hacer esto, el programa de aplicación en un extremo realiza una apertura pasiva indicando que acepta una llamada entrante. Al mismo tiempo el sistema operativo asigna un número de puerto TCP para su extremo de la conexión.
El programa de aplicación en el otro extremo debe entonces contactar a su sistema operativo usando una solicitud de apertura activa para establecer una conexión. Una vez que la conexión ha sido creada, los programas de aplicación pueden comenzar a pasar datos.

4.7.3 Segmentos, cadenas y números de secuencia.

TCP ve la cadena de datos como una secuencia de octetos o bytes que son divididos dentro de segmentos para transmisión. Usualmente cada segmento viaja a través de la red en un sólo datagrama IP.

TCP utiliza un mecanismo de ventana deslizante especial para resolver dos importantes problemas: transmisión eficiente y control de flujo. El mecanismo de ventana deslizante opera a nivel de octeto, no a nivel de paquete. Octetos de la cadena de datos son numerados secuencialmente y el emisor mantiene 3 apuntadores asociados con cada conexión. El primer apuntador marca el extremo izquierdo de la ventana deslizante, separando octetos que han sido enviados y reconocidos de los octetos enviados y no reconocidos. Un segundo apuntador marca el extremo derecho de la ventana deslizante y define el octeto más alto en la secuencia que puede ser enviado antes de que más reconocimientos sean recibidos. El tercer apuntador marca el límite dentro de la ventana que separa aquellos octetos que ya han sido enviados y no reconocidos de aquellos octetos que no han sido enviados, pero que serán enviados sin demora (Ver figura 4.39).

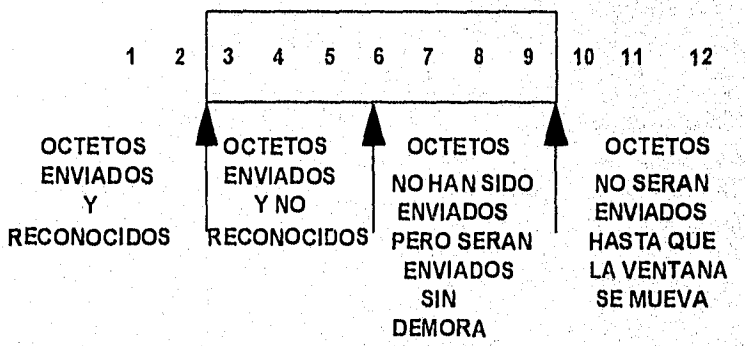


Figura 4.39
Ventana deslizante TCP.

La descripción anterior es como la ventana deslizante del emisor se comporta, pero el receptor debe mantener una ventana similar para el manejo de la conexión. Es importante comprender, sin embargo, que debido a que las conexiones TCP son full dúplex, es decir dos procedimientos de transferencia sobre cada conexión, se necesitan en total 4 ventanas.

4.7.4 Tamaño de ventana variable.

Una diferencia entre el protocolo de ventana deslizante TCP y el protocolo de ventana deslizante normal es que TCP permite que el tamaño de la ventana deslizante varíe con el tiempo. Cada reconocimiento, el cual especifica cuantos octetos han sido recibidos, contiene un aviso de ventana que especifica cuantos octetos adicionales el receptor está preparado para aceptar. Lo anterior permite control de flujo extremo a extremo, pero no control de congestión.

4.7.5 Formato del segmento TCP.

La unidad de transferencia entre el software TCP en dos máquinas es llamada segmento. Los segmentos son intercambiados para establecer conexiones, transferencia de datos, envío de reconocimientos, avisos de tamaño de ventana y cierre de conexiones. El segmento TCP se muestra en la figura 4.40.

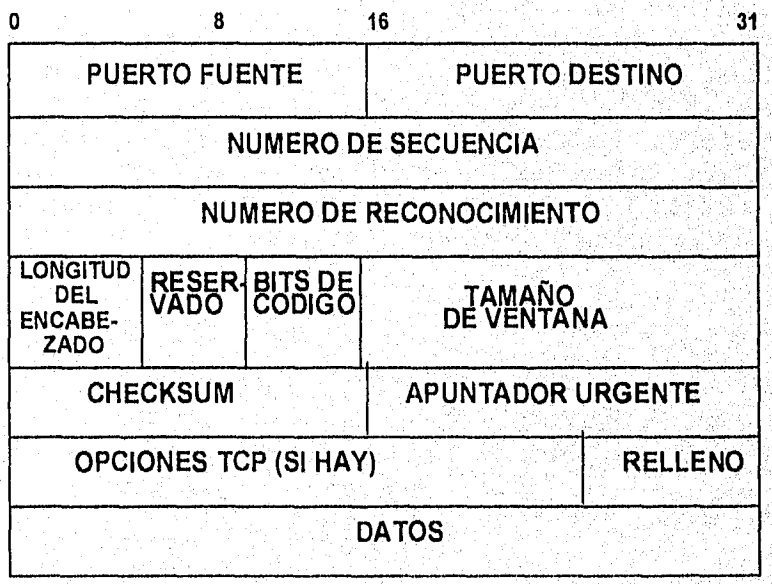


Figura 4.40
Formato del segmento TCP.

Puerto fuente (Source Port).

Es un número de 16 bits que identifica un programa de aplicación de capa superior que usa la conexión TCP. Éste es el puerto TCP de la sesión fuente.

Puerto destino (Destination Port).

Es un campo de 16 bits con el número de puerto TCP de la sesión destino. Por ejemplo: 13.61.73.185.21 es un puerto para FTP.

Número de secuencia fuente (Sequence Number).

Campo de 4 octetos que identifica la posición del primer octeto de los datos en el segmento.

Número de secuencia de reconocimiento (Acknowledgement).

Este número de 4 octetos muestra el número del siguiente octeto que es esperado por el destino en la siguiente transmisión para esta sesión. Proporciona reconocimiento inclusivo, reconociendo todos los octetos anteriores al número indicado menos uno.

Longitud del encabezado TCP (HLEN).

Este campo de 4 bits es usado para decirle al destino la longitud del encabezado del segmento en múltiplos de 32 bits.

Reservado.

Es un campo de 6 bits puesto en ceros que se deja para uso futuro.

Bits de Código (Code Bits).

TCP usa estos bits para determinar el propósito del contenido del segmento.

Algunos segmentos pueden conducir únicamente un reconocimiento, mientras que otros pueden conducir datos. Otros pueden conducir solicitudes para establecer o cerrar una conexión.

Estos bits se encuentran representados en la figura 4.41 y se describen a continuación:

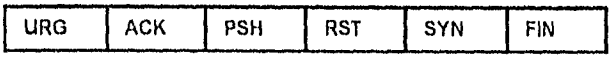


Figura 4.41
Bits de código.

Bit Urgente (URG).

Si este bit es establecido a 1 los datos en este paquete son urgentes y deben ser procesados antes de los demás datos. Los datos más frecuentes de esta naturaleza son comandos para cancelar la sesión o hacer cambios en el estado de la sesión. Si una estación no está aceptando datos, debido a problemas con el buffer o a otros problemas es obligada a procesar los paquetes de datos urgentes.

Reconocimiento Válido (ACK).

Este bit es puesto a 1, si los datos encontrados en el campo de reconocimiento son un número válido. Durante el inicio de una sesión TCP el número de este campo será establecido a 0 mostrando que datos no han sido todavía intercambiados y el número de secuencia enviado del destino es desconocido.

Solicitud de Empuje (PSH).

Este bit es usado para solicitar que los datos de un usuario normal sean procesados inmediatamente. Esto es frecuentemente hecho cuando un usuario está frente al teclado y el tiempo de respuesta rápido es altamente deseado, como en sesiones TELNET o FTP.

Reseteo de Conexión (RST).

Cuando este bit es establecido a 1, el emisor está solicitando que la sesión nombrada sea terminada y las aplicaciones apropiadas sean notificadas que la conexión ha terminado.

Números de secuencia de Sincronización (SYN).

Este bit es establecido en 1 cuando una sesión inicia para indicarle al host destino que un número de secuencia válido de inicio, del emisor, está contenido

en el paquete. Estos no son iniciados en cero o en algún otro número común. Estos números son establecidos aleatoriamente en el inicio de la sesión.

Envío de datos final (FIN).

Cuando este bit es establecido a 1 el proceso destino sabe que el final de datos para esta sesión ha sido enviado por el emisor.

Tamaño de la Ventana (Window).

Este número de 2 octetos indica cuantos octetos adicionales de datos el receptor está preparado para aceptar.

Checksum.

El campo de checksum contiene un entero de 16 bits usado para checar el encabezado TCP y los datos. El cálculo de este valor se realiza en la misma forma que el valor del checksum de UDP.

Apuntador Urgente (Urgent Pointer).

Es un campo de 2 octetos que se utiliza para indicar un desplazamiento en octetos a partir del número de secuencia actual, en el que se encuentran datos urgentes. Los datos urgentes se llaman también datos fuera de banda.

Campo de Opciones (Options).

Actualmente la única ocasión en que este campo es usado es durante el inicio de una sesión TCP. El número de la opción es 02 y su longitud es siempre 04. La porción del mensaje de esta opción es usada para indicar el más grande tamaño de segmento que el emisor es capaz de recibir para esta sesión. Los valores comunes son 64 a 4096 bytes.

Relleno (Padding).

Campo con bits en cero para completar un múltiplo de palabras de 32 bits.

4.7.6 Encapsulamiento del segmento TCP.

El contenido del segmento TCP se encapsula en el área de datos de un datagrama de IP como se muestra en la figura 4.42.

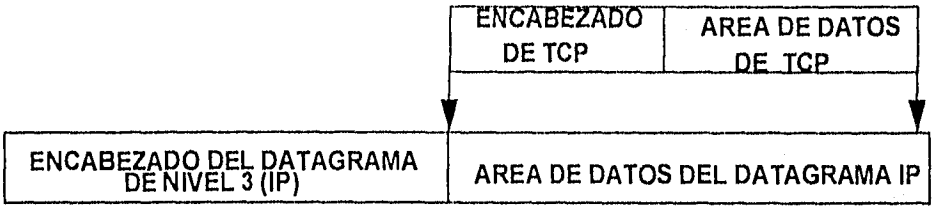


Figura 4.42
Mensaje TCP encapsulado en el datagrama IP.

4.7.7 Datos Fuera de Banda.

Aunque TCP es un protocolo orientado a cadena, es importante algunas veces para el programa en un extremo de la conexión enviar datos fuera de banda, sin esperar a que el programa en el otro extremo de la conexión lea octetos ya en la cadena.

Para acomodar datos fuera de banda, TCP permite que el emisor especifique datos como urgentes, significando que el programa receptor debe ser notificado a su llegada, inmediatamente, sin importar su posición en la cadena. Por ejemplo cuando TCP es usado para una sesión de login remoto, el usuario puede decidir enviar una secuencia del teclado que interrumpa o aborte el programa en el otro extremo. Las señales deben ser enviadas sin esperar a que el programa lea octetos ya en la cadena TCP.

4.7.8 Opción del tamaño de segmento máximo

No todos los segmentos enviados a través de una conexión serán del mismo tamaño. Sin embargo, ambos extremos de la conexión necesitan estar de acuerdo en el tamaño máximo del segmento que ellos transferirán. El segmento TCP usa el campo de opciones para negociar con el software TCP del otro extremo de la conexión.

Una de las opciones permite que el software TCP especifique el tamaño máximo de segmento que puede recibir. Por ejemplo, cuando una computadora personal pequeña que únicamente tiene un par de cientos de bytes de buffer de espacio se conecta a un gran supercomputadora, ésta puede negociar una unidad de transferencia máxima de acuerdo al tamaño de su buffer. Es especialmente importante con computadoras que están conectadas a redes de área local de alta velocidad elegir un tamaño de segmento que llene los paquetes o ellos no harán un buen uso del ancho de banda. Por lo tanto si los dos puntos de comunicación caen en la misma red física, TCP usualmente calcula un número de segmento máximo de modo que los datagramas IP serán

del tamaño máximo al soportado por la red. Si los puntos en comunicación no caen en la misma red física, la especificación actual sugiere usar un tamaño de segmento máximo de 536 (el tamaño default del datagrama IP, 576, menos el tamaño estándar de los encabezados TCP e IP).

4.7.9 Reconocimientos.

Debido a que TCP envía datos en segmentos de longitud variable, y debido a que segmentos retransmitidos pueden incluir más datos que el original, los reconocimientos no pueden referenciarse fácilmente a datagramas o segmentos. En lugar de esto, ellos se referencian a posiciones en la cadena usando los números de secuencia de la cadena. El receptor colecta octetos de datos de segmentos que llegan y reconstruye una copia exacta de la cadena. Debido a que los segmentos viajan en datagramas IP, ellos pueden perderse o entregarse en forma desordenada. El receptor usa los números de secuencia para reordenar segmentos.

El esquema de reconocimiento TCP es llamado acumulativo debido a que éste reporta cuanto de la cadena ha sido acumulado.

4.7.10 Establecimiento de una conexión TCP.

Para el establecimiento de una conexión TCP se usan tres mensajes de handshake.
El primer segmento de handshake puede ser identificado por que éste tiene el bit **SYN=1** en el campo de bits de código. El segundo mensaje tiene el bit **SYN=1** y el bit **ACK=1**, indicando que éste reconoce al primer segmento **SYN** y continua el handshake. El mensaje de handshake final es únicamente un reconocimiento final **ACK=1** y es usado para informar al destino que ambos lados están de acuerdo en que la conexión sea establecida (Ver figura 4.43).

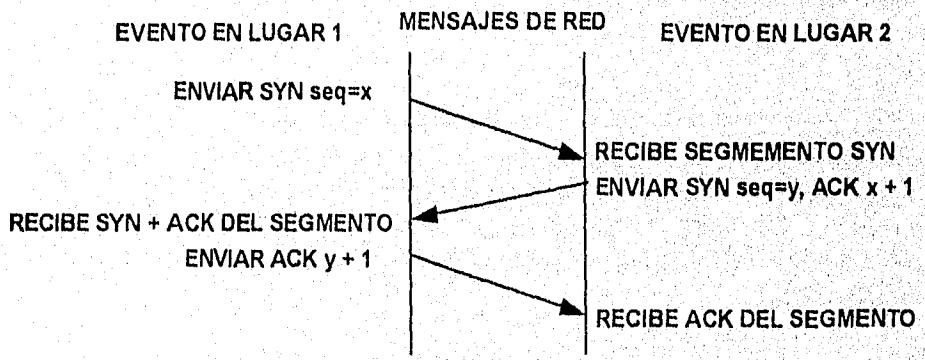


Figura 4.43
Apertura de una conexión TCP.

Números de secuencia inicial.

Los números de secuencia son enviados y reconocidos durante el handshake. Cada máquina debe elegir un número de secuencia inicial aleatorio que usará para identificar bytes en la cadena que está enviando.

Para ver como las máquinas se ponen de acuerdo en los números de secuencia, se puede recordar que cada segmento contiene un campo de número de secuencia y un campo de reconocimiento. La máquina que inicia el handshake, llamada A, pasa su número de secuencia inicial, "x" en el campo de secuencia del primer segmento SYN. La segunda máquina B, recibe el SYN, graba el número de secuencia y contesta enviando su número de secuencia inicial "y" en el campo de secuencia, así como un reconocimiento que especifica que B espera el octeto "x+1". El mensaje final de A "reconoce" haber recibido todos los octetos de B hasta "y".

4.7.11 Cierre de una conexión TCP.

Cuando un programa de aplicación le dice a TCP que no tiene más datos que enviar, TCP cierra la conexión en una dirección. Para cerrar la conexión TCP envía los datos restantes de la máquina transmisora, espera que el receptor reconozca éstos, y entonces envía un segmento con el campo del bit FIN=1. El TCP en la máquina receptora reconoce el segmento de FIN e informa al programa de aplicación que no hay más datos disponibles.

Una vez que la conexión se cierra en una dirección, TCP rehusa aceptar más datos para esa dirección. Mientras tanto, los datos pueden continuar fluyendo en la dirección opuesta hasta que el emisor cierra la conexión. Se puede notar que los reconocimientos siguen fluyendo hacia el emisor aún después de que la conexión ha sido cerrada.

El cierre de una conexión ocurre después de que una máquina recibe el segmento de **FIN** inicial. En lugar de generar un segundo segmento de FIN inmediatamente, TCP envía un reconocimiento **ACK** y entonces informa a la aplicación de la solicitud de cierre de conexión. Finalmente cuando el programa instruye a TCP para cerrar la conexión completamente, TCP envía el segundo segmento de **FIN** y el lugar original contesta con un reconocimiento **ACK** (Ver figura 4.44).

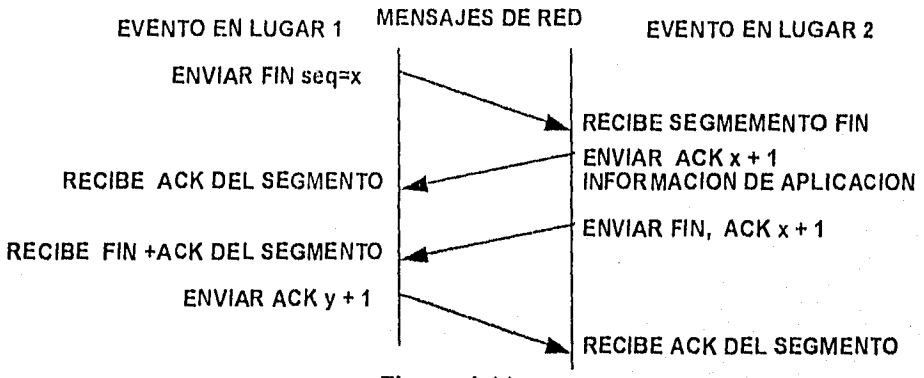


Figura 4.44
Cierre de una conexión TCP.

4.8 Aplicaciones TCP/IP.

Desde el punto de vista de los usuarios la relación entre los protocolos TCP/IP, las estaciones de trabajo y máquinas de computo en general, así como los equipos de interconexión de redes, deben ser invisibles. Para hacer uso de una red con estas características se deben proporcionar servicios que puedan ser utilizados con la invocación de comandos.

La mayoría de las redes que se comunican mediante el protocolo TCP/IP, utilizan servicios de correo electrónico, transferencia de archivos FTP (File Transfer Protocol; Protocolo de Transferencia de Archivos) y TELNET (Protocolo que en sí mismo opera como aplicación de emulación de terminal), proceso a través del cual se pueden tener sesiones interactivas a una computadora remota.

Transferencia de Archivos.

La transferencia de archivos permite mover el archivo de una computadora remota a una local, aunque cada computadora tenga un sistema operativo y formato de almacenamiento diferente. Los archivos pueden ser de cualquier tamaño y pueden contener datos, programas, reportes, etc.

Correo Electrónico.

Este servicio permite al usuario mandar mensajes electrónicamente a individuos o grupos de individuos.
Los programas del sistema operativo que manejan el correo aceptan y almacenan mensajes que llegan de usuarios de otros nodos. Estos programas reciben el correo del nodo y los distribuyen al usuario al cual va dirigido. La

mayoría de los usuarios tienen un buzón personal de correo donde todos los mensajes recibidos se almacenan.

Acceso Remoto con Terminal Virtual.

Con esta herramienta el usuario puede conectarse a una computadora que se encuentre en otra red remota desde una red local. Una vez conectada y establecida la sesión con el nodo remoto, el usuario puede correr programas, capturar datos o hacer cualquier otra operación como si el nodo remoto fuera uno local.

La figura 4.45 muestra las aplicaciones existentes para TCP/IP y se describirán las más usuales en una red privada.

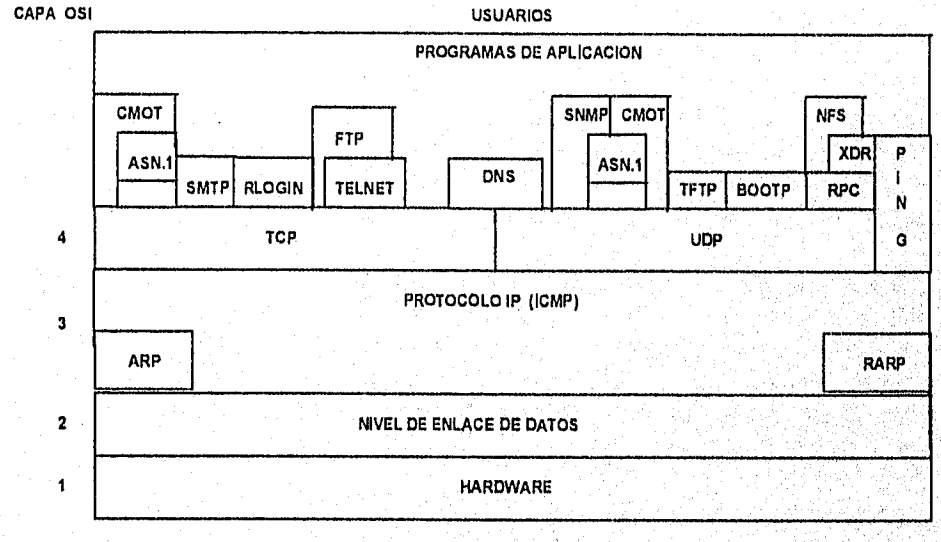


Figura 4.45
Aplicaciones TCP/IP.

Los organismos que actualmente controlan nuevas mejoras, modificaciones y desarrollos para TCP/IP son el Internet Activities Board (IAB) y el Network Information Center (Centro de Información de Redes; NIC).

El Network Information Center, conserva una serie de documentos que describen en forma cronológica el desarrollo de la familia de protocolos de TCP/IP. Estos textos se conocen como RFC's (Request For Comments; Solicitud de comentarios) y están disponibles para cualquier persona u organización que desee desarrollar tecnología de informática sobre TCP/IP.

4.8.1 La aplicación PING.

Se usa ping para ver si un host está activo (prendido y funcionando) o para aislar un problema en un ambiente de redes interconectadas. El comando ping envía una solicitud de eco a otro host y espera por una respuesta, usando el protocolo ICMP/IP (Ver figura 4.46).

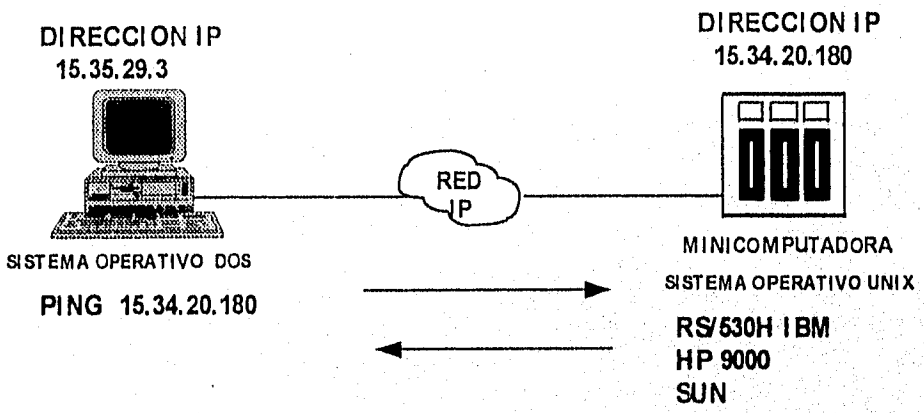


Figura 4.46
Prueba de conectividad entre una PC y una minicomputadora con la aplicación PING.

El comando ping reporta si tuvo éxito con un mensaje Host Responding (host responde), y con un arreglo de estadísticas. En caso de falla, éste también reporta resultados con un mensaje Ping Failed seguido por la razón de falla.

El comando para esta aplicación tiene la siguiente sintaxis en el sistema operativo DOS y con el software de red PC/TCP versión 2.3 :

ping [-opciones]host

Las opciones pueden ser:

-d[bytes]. Despliega información del encabezado y la parte de bytes que se indique del paquete entrante en números hexadecimales. Con la opción -t se despliega la información del primer paquete.

-d#[bytes]. Despliega información del encabezado y la parte de bytes que se indique del paquete saliente en números hexadecimales. Con la opción -t se despliega la información del primer paquete.

-e. Cancela cualquier opción de seguridad extendida IP.

host. Especifica el nombre o dirección IP del host remoto.

-i segundos. Establece el tiempo de vida (TTL) para el paquete saliente, y despliega el tiempo de vida del paquete entrante. El rango es de 1 a 255 y el default es 64.

-j destino1....destinoN. Establece la opción IP de enrutamiento fuente no estricto. Cada destino es la dirección IP del enrutador a través del cual el paquete debe pasar aunque pase por otros enrutadores.

-k destino1....destinoN. Establece la opción de enrutamiento fuente estricto IP. Cada destino es la dirección IP del enrutador a través del cual el paquete debe pasar hasta llegar a su destino y no se permite que pase por otros enrutadores.

-l longitud. Establece la longitud en bytes de los datos en el paquete. La longitud default de los datos es 256 bytes. La longitud está limitada por el tamaño máximo de paquete de la red a donde la PC está conectada. Por ejemplo para Ethernet es 1472 bytes.

-n veces. Envía un número especifico de solicitudes de eco y entonces se detiene.

-p precedencia. Establece el nivel de precedencia IP. El nivel de precedencia es un número de 0 a 7.

-q. Establece la opción de trazo de ruta, la cual incrementa el tiempo de vida del paquete para identificar todos los enrutadores en la ruta y desplegar sus direcciones IP.

-r. Establece la opción de registro de ruta.

-s. nivel[autoridad]. Establece un nivel de seguridad IP y, si es especificado, el tipo de autoridad. El nivel es un número de 0-4 y la autoridad es un número de 1-5.

-t. Esta opción permite entrar en un loop de envío continuo de solicitudes de eco, esperando por respuesta antes de enviar la siguiente solicitud.

-v tipo. Solicita opción de tipo de servicio. La variable tipo es un número de 0 a 15.

-w segundos. Especifica el número de segundos para esperar una respuesta antes de renunciar. El rango es de 1 a 32767.

-x. Establece la opción de sello de tiempo IP. La opción de sello de tiempo será llenada por todos los enrutadores encontrados en la trayectoria.

-x l. Especifica que cada sello de tiempo es precedido por la dirección IP del enrutador llenando la opción.

-x 3 destino1... destinoN. Especifica que los sellos de tiempo serán llenados únicamente por los enrutadores designados (incluyendo el host final en la ruta).

-z. Establece el modo abreviado, donde no se dan estadísticas, sino solamente exitoso o fallado.

-?. Explica la utilidad del comando.

-version. Despliega la versión del comando.

4.8.2 La aplicación TELNET.

El comando telnet permite que un host establezca una sesión de terminal virtual con un host remoto en la red.

El comando telnet negocia con el host remoto para determinar la terminal apropiada a emular. Telnet ofrece como default la terminal DEC VT220.

Una vez que se está conectado al host remoto, se pueden usar comandos de escape para cambiar características de la conexión, crear conexiones a otros

hosts, desplegar información acerca de la conexión y transferir datos entre el host remoto y el host local (Ver figura 4.47)

Para finalizar una conexión telnet se puede usar Ctrl-D o exit. En caso de no poder salir del host remoto utilizar la tecla de escape y "c" o "q".

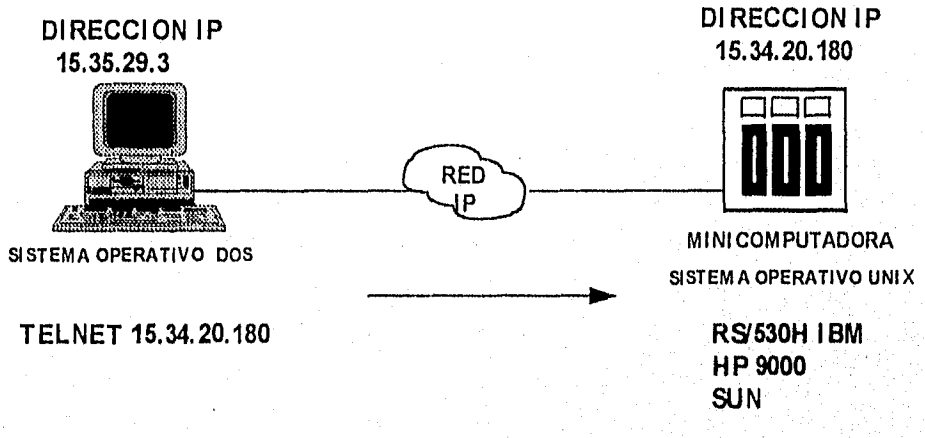


Figura 4.47
Establecimiento de una sesión de terminal entre un PC con DOS y una minicomputadora con UNIX.

Sintaxis del comando.

telnet[-h][-w][-n][-D][-ttipo][-k realm]host[puerto].

-h. Incrementa el número de líneas de pantalla desplegado. La altura de la pantalla varia dependiendo de la terminal emulada y la capacidad de la tarjeta de vídeo y el monitor, de la PC.

Terminales DEC VT. La pantalla se incrementa de 23 a 40 ó 50 líneas.

Terminales IBM 3278. La pantalla se incrementa de 24 a 32 ó 43 líneas.

Terminales IBM 3279. La pantalla se incrementa a 32 líneas.

host. Especifica la dirección IP del host remoto.

-n. Solicita que telnet negocie únicamente para tipos de terminal sin atributos extendidos.

port. Especifica el número de puerto en el host remoto para realizar la conexión telnet a un puerto diferente que el 23.

-t ttipo. Solicita que telnet ofrezca un rango de tipos de terminales, comenzando con el tipo especificado, durante negociación con el host remoto.

El orden de default en el cual telnet negocia los tipos de terminales es:

DEC VT220
DEC VT100
DEC VT52
IBM 3278 Modelo 2.

Se puede cambiar el orden con la opción presente usando la variable ttipo con valores de la lista siguiente:

vt,vt220,vt100 y vt52 3277 3278 3279.

-w. Permite despliegue de pantalla amplia, si telnet negocia emulación 3270 y si la tarjeta de vídeo y monitor lo soportan. Esta opción está disponible únicamente con tipo de terminal 3278 (el terminal de default de IBM). Esta opción causa que la pantalla tenga 132 columnas y 43 líneas.

-x ttipo. Solicita negociación de un tipo de terminal específico.

Los valores de ttipo pueden ser:

vt vt220 vt100 vt52 3277 3278 3279.

-?. Despliega y explica la utilidad del comando.

-version. Despliega la versión del comando.

Comandos de escape.

Para invocar un comando de escape en una sesión telnet, presionar la tecla escape; entonces ingresar el comando escape en el prompt Command:. La tecla escape es Alt-F10 (para emuladores de terminal DEC VT, F10 también trabaja).

?. Despliega un mensaje de ayuda listando los comandos de escape.

!. Invoca a un interprete de comandos para DOS, pero no cierra la conexión telnet. Para retornar al host remoto, teclear exit.

0-9. Crea una nueva conexión, o conmuta a una conexión existente identificada por el número suministrado. Para crear una nueva conexión, presionar la tecla escape (Alt-F10) e ingresar un número de 0 a 9 (ingresar Ctrl-s para ver lista de conexiones existentes). El siguiente prompt aparece:

No connection. Host to connect to?

Ingresar el nombre del host al cual tu quieres conectarte, o presionar la tecla enter para regresar a la conexión actual.
Las opciones que se deseen, se tienen que teclear antes del nombre del host a conectarse.

a. Envía un comando "estas ahí" del protocolo telnet al host remoto para determinar si la conexión esta activa. Muchos hosts reponden YES.

b. Envía un comando de interrupción de proceso al host remoto. En algunos hosts remotos, éste detiene un proceso corriendo en el host remoto, pero no termina la conexión telnet.

c. Cierra la conexión telnet.

tecla Enter. Conmuta la sesión actual a la siguiente conexión abierta en la lista. Máximo 10 conexiones pueden ser abiertas a la vez.

F. Comienza o detiene un servidor FTP en la PC.

l. Despliega la dirección IP del host local en la línea de estado.

i. Envía el contenido de un archivo como entrada a la línea de comandos del host remoto.

l. Habilita el modo de eco local. El host remoto recibe tus instrucciones ingresadas por teclado, pero no las envía de regreso a tu PC sobre la conexión TELNET.

o. Graba las instrucciones introducidas por teclado y el resultado de la salida del sistema remoto en un archivo en la PC. El programa de login remoto te pregunta por el nombre del archivo. Presionar el comando de escape "o" de nuevo para cerrar un archivo de salida abierto.

p. Especifica la página de códigos DOS usada para sesiones de login remoto.

Q. Finaliza todas las conexiones existentes reseteandolas en lugar de cerrarlas. Usar esta opción únicamente cuando no se pueda salir normalmente.

q. Finaliza la sesión actual de login remoto reseteando la sesión en lugar de cerrarla.

r. Habilita modo de eco remoto. El host remoto hace eco de las instrucciones suministradas por teclado de regreso a el host local sobre la conexión telnet. Usar el comando de escape Ctrl-t para ver si el modo de eco local o remoto está habilitado.

S. Este comando se usa para prevenir inapropiada activación de un programa residente para protección de pantalla, mientras se tiene una sesión remota.

t. Envía una señal de rompimiento al host remoto.

z. Envía un comando Abort al host remoto. Este comando permite que el proceso actual finalice, pero no envíe su salida.

Ctrl-b. Habilita o deshabilita el modo binario (8 bits) de un emulador de terminal DEC VT.

Ctrl-h. Despliega un mensaje de ayuda listando los comandos de escape de caracteres de control.

Ctrl-l. Redibuja la pantalla de la conexión actual.

Ctrl-n. Despliega información de estado de la red, incluyendo estadísticas del Kernel TCP, IP, UDP e ICMP.

Ctrl-s. Lista las conexiones actuales, y muestra el estado de la conexión activa y el servidor FTP.

Ctrl-t. Despliega información acerca de la sesión telnet y la conexión actual, y muestra el estado del servidor FTP. También indica si un emulador está pasando instrucciones por teclado para DOS y si un procesamiento de archivo de entrada o salida está activo.

4.8.3 Aplicación FTP.

El comando ftp permite establecer sesiones de transferencia de archivos entre hosts en una red. Con este comando se pueden establecer sesiones entre hosts como:

PC-PC.
PC-Minicomputadora.
PC-Mainframe.
PC-VAX.
PC-Gateway.
Minicomputadora-Minicomputadora.
Minicomputadora-Mainframe.
Minicomputqdora-VAX.
Minicomputadora-Gateway
Etc.

El modo de transferencia de default es texto ASCII. Para enviar o recibir archivos binarios, se establece una sesión FTP con el servidor FTP remoto y se usa el comando binary, tenex o image (Ver figura 4.48). Como se menciono el destino de una sesión FTP debe ser un servidor y en el caso de una PC se debe ejecutar el comando ftpsrv.

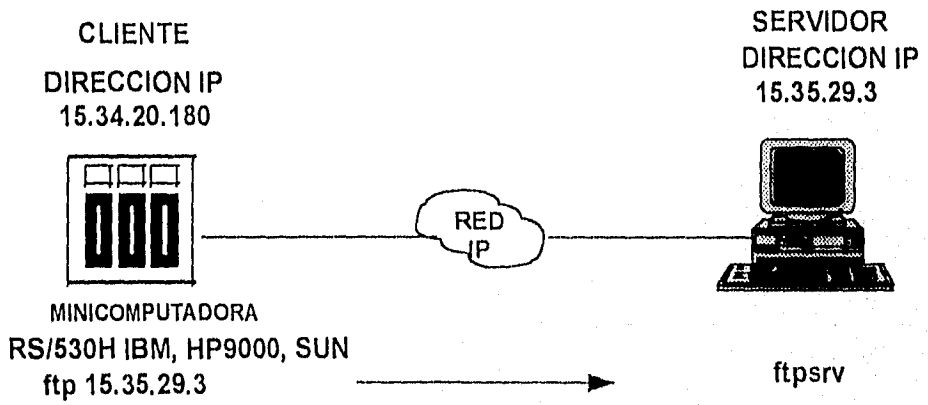


Figura 4.48
Ejemplo de una sesión de transmisión de archivos FTP, usando como servidor a una PC.

Sintaxis del comando.

ftp[-d][-uuseridpassword][-p num_puerto][host][command].

Opciones del comando.

-d. Despliega todos los comandos y respuestas de red FTP que son enviados sobre la conexión de control FTP.

host. Especifica el nombre del host con el que se establecerá una sesión FTP.

-p num_puerto. Especifica el número de puerto remoto para el servidor FTP.

-u userid password. Cuando se establece una sesión con un host remoto es posible dar nombre de usuario en la variable userid y password.

-?. Despliega y explica el comando.

-version. Despliega la versión del comando ftp usado.

Comandos ftp interactivos.

Durante una sesión FTP, tu puedes usar un gran número de comandos interactivos como:

![comando]. Ejecuta un comando de DOS y retorna al prompt FTP.

?[comando]. Despliega una lista de comandos y si se indica un comando muestra la utilidad de éste.

append[archivo_local archivo_remoto]. Agrega un archivo local a un archivo remolo en el host remoto.

ascii. Habilita la transferencia de archivos de texto ASCII.

cd. Hace lo mismo que fcd.

delete nombre_archivo. Borra el archivo especificado en la máquina remota.

dir,[argumento[nombre_archivo]],fdir. Lista el directorio actual en la máquina remota. La opción de argumento, se puede usar para especificar la trayectoria de directorios. Si se especifica el nombre de un archivo, la información normalmente desplegada es salvada en ese archivo.

drive letra_drive. Cambia el drive actual en la PC.

exit,bye,quit. Termina la sesión FTP.

fcd[path],cd. Cambia el directorio de trabajo actual en la máquina remota.

Fpwd, pwd. Muestra el nombre del directorio de trabajo actual en la máquina remota.

get[archivo_remoto archivo_local], retrieve. Copia un archivo de la máquina remota a la PC.

help. Lista los comandos soportados por ftp.

iget[archivo_remoto archivo_local]. Como get, pero transfiere un archivo remoto al directorio local usando modo image.

image,binary. Habilita la transferencia de archivos binarios entre máquinas similares.

iput[archivo_local archivo_remoto]. Como put, pero copia un archivo local a un archivo remoto usando modo image.

lcd[directorio_local]. Cambia el directorio de trabajo actual en la PC al directorio especificado.

ldir [path\nombre_archivo]. Despliega el directorio local.

lmkdir. Crea un nuevo directorio en la PC con el nombre especificado.

local n. Habilita la transferencia de archivos binarios para y de un host que utiliza diferente tamaño de byte con respecto a la PC. donde n es el tamaño del byte de la máquina local.

login usuario. Establece tu nombre de usuario como usuario de la máquina remota.

lpwd. Muestra el nombre del directorio actual en la PC.

ls[argumento[nombre_archivo]. Hace lo mismo que dir.

mdelete nombre con comodines. Borra múltiples archivos en la máquina remota.

mget nombre con comodines. Transfiere múltiples archivos a la máquina local usando sintaxis con comodines.

mkdir directorio_remoto. Crea un directorio en la máquina remota.

mput nombre con comodines. Transfiere múltiples archivos a la máquina remota usando sintaxis con comodines.

passive. Ejecuta la siguiente transferencia en modo pasivo (en lugar de que el servidor abra la conexión de datos, la PC abre la conexión de datos).

put[archivo_local archivo_remoto],send,store. Copia un archivo local en un archivo remoto.

rename [nombre_actual nombre nuevo]. Renombra un archivo existente en el host remoto.

rmdir directorio_remoto. Borra un directorio especificado en la máquina remota.

show nombre_archivo. Despliega el texto de un archivo especificado de la máquina .

stat. Pregunta al servidor remoto por su estado actual.

take archivo_local. Lee comandos para ftp de un archivo local

tenex. Habilita la transferencia de archivos binaria para o de una máquina TOPS-20 y de muchas máquinas LISP. El modo tenex es equivalente a local 8.

tget[archivo_remoto archivo_local]. Como get, pero transfiere un archivo remoto a un directorio local usando modo tenex.

tput[archivo_local archivo_remoto]. Como put, pero transfiere un archivo local a un directorio remoto usando modo tenex.

type tipo. Despliega el modo de transferencia de archivos. Si se especifica el tipo, éste establece el modo de transferencia de archivos.

version. Despliega la versión del comando.

4.8.4 Otras aplicaciones

Rlogin/rsh.

El sistema UNIX incluye un servicio de establecimiento de sesión remota, rlogin, que soporta hosts de confianza. Éste permite a los administradores del sistema elegir un conjunto de máquinas sobre las cuales los nombres de login y protecciones de acceso de archivo son compartidas para establecer equivalencias entre login's de usuario. Los usuarios pueden controlar sus cuentas autorizando login remoto basados en el host remoto y el nombre del usuario remoto. De modo que es posible para un usuario tener nombre de login "X" en una máquina y "Y" en otra, y ser capaz de remotamente hacer login de una de las máquinas a la otra sin teclear un password en cada máquina.

Una variante del rlogin es el comando rsh, que invoca a un interprete de comandos en la máquina UNIX remota y pasa los argumentos de la línea de comandos al interprete de comandos, saltándose el paso de login completamente.

Por ejemplo:

rsh merlin ps

CMOT (CMIP/CMIS) Protocolos ISO de administración de red para enrutadores TCP/IP.

DNS sistema de base de datos distribuida en línea, usada para mapear nombres de máquina (nombres utilizados por humanos) con direcciones IP. DNS soporta mapeos entre destinos de correo y direcciones IP.

XDR Estándar de representación de una estructura de datos independiente de una máquina y que desarrollo Sun Microsystems. Para usar XDR el emisor

convierte de una representación local de la máquina a un estándar de representación externo y el receptor convierte de la representación externa a la local.

NFS Protocolo desarrollado por Sun Microsystems que usa IP para permitir a un conjunto de computadoras accesar una a otra a sus sistemas de archivos como si ellos fueran locales a cada máquina.

El Protocolo de Manejo de Red simple SNMP.

Es un protocolo de la capa de aplicación diseñado para facilitar el intercambio de información manejado entre dispositivos de red usando datos SNMP (tales como paquetes/seg, tazas de error de red, estado del dispositivo, acceso a reconfiguración, etc.). Con esta aplicación los administradores de red pueden monitorear fácilmente el funcionamiento de la red y encontrar y resolver problemas de red.
Entre los dispositivos de red que pueden monitorearse se encuentran los enrutadores, concentradores, estaciones de trabajo etc.

La comunicación se logra por medio de agentes SNMP (módulos de software) que corren en los dispositivos de red y estaciones de manejo de red NMS (computadoras que tienen rápidos CPU. display gráfico y color, memoria extendida y mucho espacio en disco).

Cada dispositivo de red es un agente capaz de reportar y/o recibir comandos de un administrador. El administrador es un dispositivo corriendo el protocolo de manejo de red simple SNMP y aplicaciones de control de red.

Cada característica de un agente manejado está definida como un objeto en una base de datos llamada base de información de administración MIB.

Entre los productos existentes para la administración de redes TCP/IP se encuentran Sunnet Manager, Cisco Works y HP Open View que corren sobre el sistema operativo UNIX.

Los protocolos y aplicaciones se encuentran documentados en RFC's de acuerdo con la siguiente tabla:

Protocolo	Descripción	RFC
IP	Protocolo Internet	791
ICMP	Protocolo de mensajes de control Internet	792
IGMP	Protocolo de grupo multicast Internet	1112
UDP	Protocolo de datagrama de usuario	768
TCP	Protocolo de control de transmisión	793
SNMP	Protocolo de administración de red simple	1157
TELNET	Protocolo TELNET	854
FTP	Protocolo de transferencia de archivos	959
SMTP	Protocolo de transferencia de correo simple	821
ARP	Protocolo de resolución de dirección	826
RARP	Protocolo de resolución de dirección inverso	903
BOOTTP	Protocolo bootstrap	951,1048,1084
TFTP	Protocolo de transferencia de archivos trivial	783

Ejemplo de una red TCP/IP con enrutadores y enlaces digitales.

El diagrama de la figura 4.49 muestra la interconexión de una red TCP/IP que incluye redes de área local Ethernet con servidores UNIX y computadoras personales con DOS que se conectan a un puerto Ethernet de un enrutador con ayuda de un concentrador actuando como bus. Esta red también puede manejar comunicaciones con el protocolo IPX de Novell con ayuda de los enrutadores y los servidores Novell conectados a las redes Ethernet.

Se muestra también en la figura 4.49 la conexión, de los enrutadores a través de un puerto serial V.35 y un FCD-2, a un nodo de la red digital integrada que proporciona servicios de E1 (2.048 Mbps) y E0 (64 Kbps).

Los FCD's son equipos convertidores de interface que cuentan con puertos V.35 y puertos G.703 (BNC). Los puertos G.703 se conectan hacia la red digital integrada y el puerto V.35 hacia el enrutador.

Los enrutadores de todas las redes se comunican vía enlaces punto a punto (Enlaces E1) o punto a multipunto (Enlace E1 a E0's) con ayuda de un multiplexor TDM.

Existe también un servicio de 64 Kbps llamado DSO proporcionado con un equipo ISDN y una línea privada a 2 hilos que permite comunicación del enrutador a la red digital integrada y por lo tanto a toda la red de enrutadores.

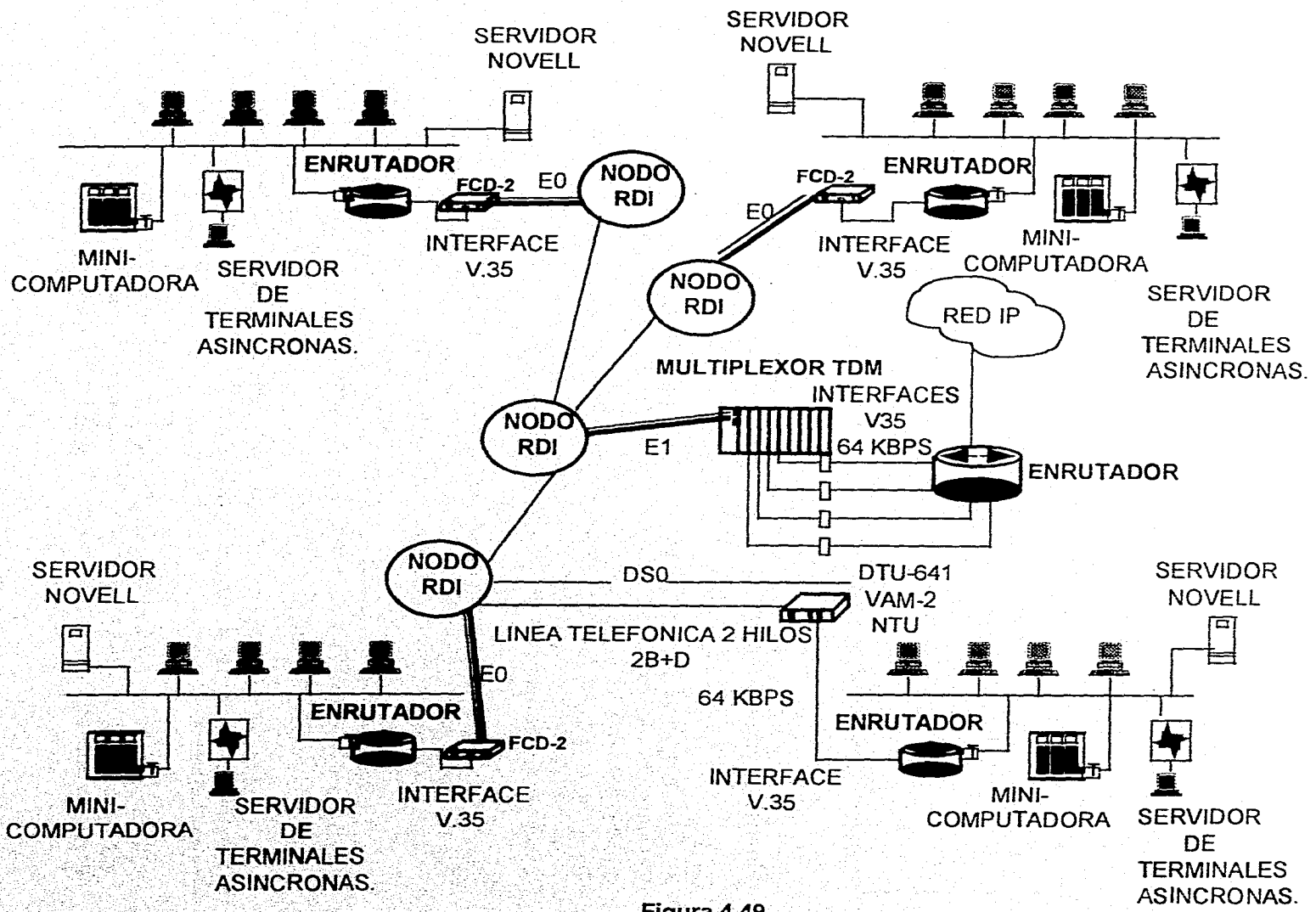


Figura 4.49

Esquemas de interconexión TCP/IP sobre RDI.

CAPITULO V

DEMOSTRACION DE LA INTERPRETACION DE LOS PROTOCOLOS TCP/IP

5.1 Consideraciones básicas.

En este capítulo se presenta una demostración de los protocolos TCP/IP que se realizó tomando como datos a un conjunto de tramas obtenidas en un analizador de protocolos Wandell & Goltermann DA-30 y almacenadas en archivos ASCII. Las tramas conteniendo la información de capas OSI 2 3 y 4, se obtuvieron realizando pruebas con las aplicaciones PING, TELNET y FTP en una red de área local Ethernet 10 BaseT, en donde se conectó el analizador de protocolos.

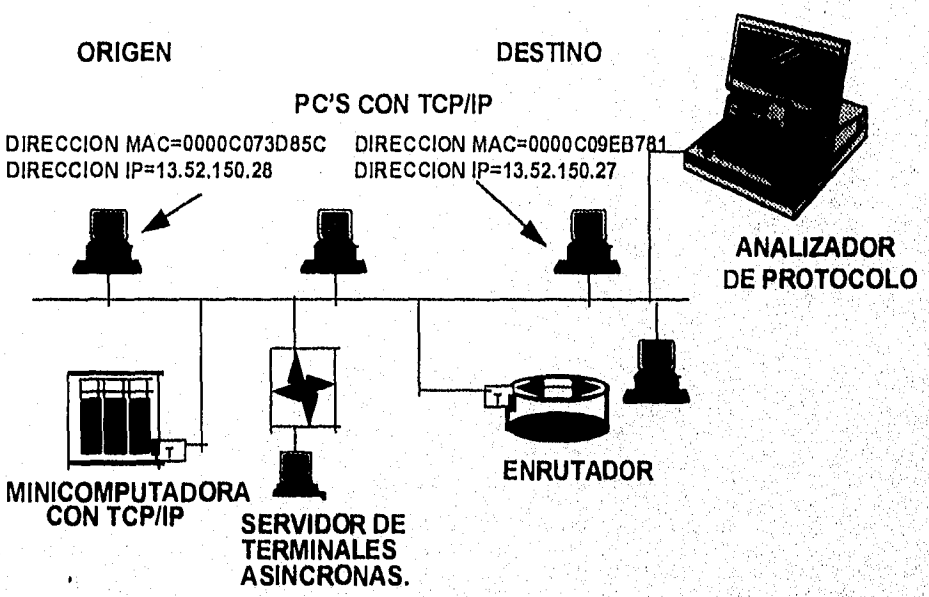


Figura 5.1
Diagrama que muestra la conexión a una red Ethernet, utilizada para la prueba de la aplicación PING de TCP/IP.

La primera prueba se realizó con la aplicación PING, y se uso la configuración mostrada en la figura 5.1. En la PC con dirección IP 13.52.150.28 se utilizó el comando PING 13.52.150.27, para probar si se tenía conectividad a la PC con dirección IP 13.52.150.27, obteniéndose en el analizador de protocolos 4 tramas que se muestran a continuación:

Tramas generadas por la aplicación PING.

```
 Frame # 1          Time =  19:09:45.77974  Size: 64
0000- FF FF FF FF FF FF 00 00 C0 73 D8 5C 08 06 00 01
0010- 08 00 06 04 00 01 00 00 C0 73 D8 5C 0D 34 96 1C
0020- 5C FA E8 44 45 87 0D 34 96 1B 00 00 00 00 00 00
0030- 00 00 00 00 00 00 00 00 00 00 00 00 F2 87 CC D5

 Frame # 2          Time =  19:09:45.81932  Size: 64
0000- 00 00 C0 73 D8 5C 00 00 C0 7D 21 73 08 06 00 01
0010- 08 00 06 04 00 02 00 00 C0 7D 21 73 0D 34 96 1B
0020- 00 00 C0 73 D8 5C 0D 34 96 1C 00 00 00 00 00 00
0030- 00 00 00 00 00 00 00 00 00 00 00 00 2C AD 0E BE

 Frame # 3          Time =  19:09:45.82032  Size: 302
0000- 00 00 C0 7D 21 73 00 00 C0 73 D8 5C 08 00 45 00
0010- 01 1C 00 02 00 00 40 01 33 40 0D 34 96 1C 0D 34
0020- 96 1B 08 00 8B BD EB 03 00 01 29 23 BE 84 E1 6C
0030- D6 AE 52 90 49 F1 F1 BB E9 EB B3 A6 DB 3C 87 0C
0040- 3E 99 24 5E 0D 1C 06 B7 47 DE B3 12 4D C8 43 BB
0050- 8B A6 1F 03 5A 7D 09 38 25 1F 5D D4 CB FC 96 F5
0060- 45 3B 13 0D 89 0A 1C DB AE 32 20 9A 50 EE 40 78
0070- 36 FD 12 49 32 F6 9E 7D 49 DC AD 4F 14 F2 44 40
0080- 66 D0 6B C4 30 B7 32 3B A1 22 F6 22 91 9D E1 8B
0090- 1F DA B0 CA 99 02 B9 72 9D 49 2C 80 7E C5 99 D5
00A0- E9 80 B2 EA C9 CC 53 BF 67 D6 BF 14 D6 7E 2D DC
00B0- 8E 66 83 EF 57 49 61 FF 69 8F 61 CD D1 1E 9D 9C
00C0- 16 72 72 E6 1D F0 84 4F 4A 77 02 D7 E8 39 2C 53
00D0- CB C9 12 1E 33 74 9E 0C F4 D5 D4 9F D4 A4 59 7E
00E0- 35 CF 32 22 F4 CC CF D3 90 2D 48 D3 8F 75 E6 D9
00F0- 1D 2A E5 C0 F7 2B 78 81 87 44 0E 5F 50 00 D4 61
0100- 8D BE 7B 05 15 07 3B 33 82 1F 18 70 92 DA 64 54
0110- CE B1 85 3E 69 15 F8 46 6A 04 96 73 0E D9 16 2F
0120- 67 68 D4 F7 4A 4A D0 57 68 76 21 93 40 9D

 Frame # 4          Time =  19:09:45.87456  Size: 302
0000- 00 00 C0 73 D8 5C 00 00 C0 7D 21 73 08 00 45 00
0010- 01 1C 00 01 00 00 40 01 33 41 0D 34 96 1B 0D 34
0020- 96 1C 00 00 93 BD EB 03 00 01 29 23 BE 84 E1 6C
0030- D6 AE 52 90 49 F1 F1 BB E9 EB B3 A6 DB 3C 87 0C
0040- 3E 99 24 5E 0D 1C 06 B7 47 DE B3 12 4D C8 43 BB
0050- 8B A6 1F 03 5A 7D 09 38 25 1F 5D D4 CB FC 96 F5
0060- 45 3B 13 0D 89 0A 1C DB AE 32 20 9A 50 EE 40 78
0070- 36 FD 12 49 32 F6 9E 7D 49 DC AD 4F 14 F2 44 40
0080- 66 D0 6B C4 30 B7 32 3B A1 22 F6 22 91 9D E1 8B
0090- 1F DA B0 CA 99 02 B9 72 9D 49 2C 80 7E C5 99 D5
00A0- E9 80 B2 EA C9 CC 53 BF 67 D6 BF 14 D6 7E 2D DC
00B0- 8E 66 83 EF 57 49 61 FF 69 8F 61 CD D1 1E 9D 9C
00C0- 16 72 72 E6 1D F0 84 4F 4A 77 02 D7 E8 39 2C 53
00D0- CB C9 12 1E 33 74 9E 0C F4 D5 D4 9F D4 A4 59 7E
00E0- 35 CF 32 22 F4 CC CF D3 90 2D 48 D3 8F 75 E6 D9
00F0- 1D 2A E5 C0 F7 2B 78 81 87 44 0E 5F 50 00 D4 61
0100- 8D BE 7B 05 15 07 3B 33 82 1F 18 70 92 DA 64 54
0110- CE B1 85 3E 69 15 F8 46 6A 04 96 73 0E D9 16 2F
0120- 67 68 D4 F7 4A 4A D0 57 68 76 64 61 CD 01
```

La segunda prueba, se llevó a cabo con la aplicación de Terminal Virtual Remota TELNET. En la prueba se uso una PC que estableció una sesión TELNET a un enrutador, para supervisión del mismo (Ver Figura 5.2).

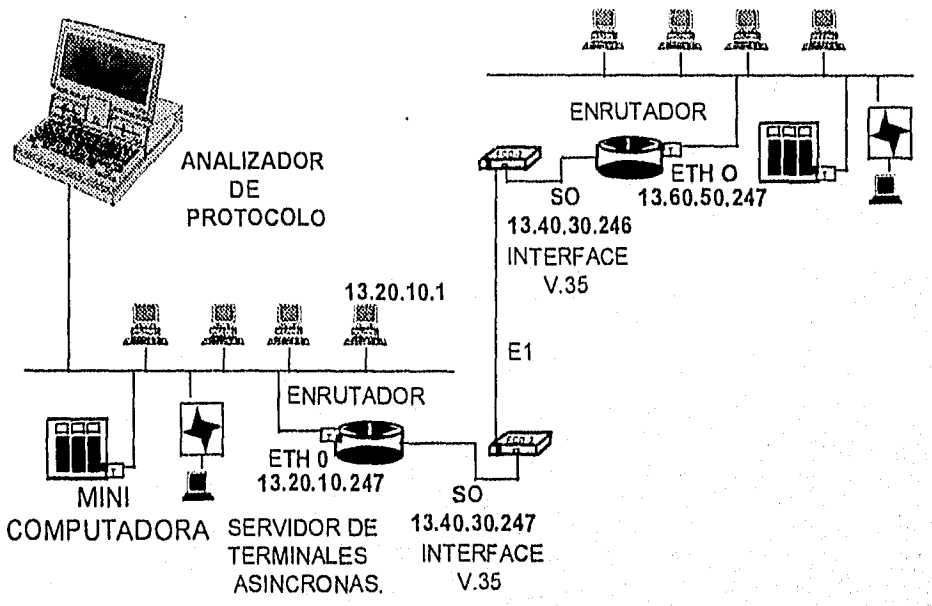


Figura 5.2
Diagrama de conexión para la prueba de la aplicación TELNET de TCP/IP.

En la PC con dirección IP 13.20.10.1 se utilizó el comando telnet 13.20.10.247 (dirección del enrutador). Las tramas que se obtuvieron con esta aplicación varían de acuerdo a lo que se realice en la sesión, pero a continuación se muestran las tramas más importantes para el establecimiento y liberación de la conexión, así como para la transferencia de datos.

Tramas generadas por la aplicación TELNET.

```
Ethernet Trace
 Frame # 1          Time =  19:10:10.46720  Size: 122
0000- 00 00 0C 09 9C 95 00 00 0C 09 9C 95 90 00 00 00
0010- 01 00 00 00 01 7D 00 00 01 7C FF FF 00 3A 56 5C
0020- 0A 01 00 17 12 12 00 1B E2 5E 0D 9E 12 1E 50 10
0030- 08 44 64 12 00 00 02 04 05 B4 73 77 6F 72 64 20
0040- 33 36 0D 00 00 00 00 00 00 00 00 00 00 00 00 00
0050- 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060- 00 00 00 00 00 00 6E FD 19 8C

Frame # 2          Time =  19:10:13.90512  Size: 64
0000- FF FF FF FF FF FF 00 00 C0 73 D8 5C 08 06 00 01
0010- 08 00 06 04 00 01 00 00 C0 73 D8 5C 0D 14 0A 01
0020- 5C FA E8 44 45 87 0D 14 0A F7 00 00 00 01 60 02
0030- 08 00 38 C8 00 00 02 04 05 B4 00 00 9C DE B6 FE

Frame # 3          Time =  19:10:13.90611  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-0C-09-9C-95
0000- 00 00 C0 73 D8 5C 00 00 0C 09 9C 95 08 06 00 01
0010- 08 00 06 04 00 02 00 00 0C 09 9C 95 0D 14 0A F7
0020- 00 00 C0 73 D8 5C 0D 14 0A 01 00 00 00 01 60 02
0030- 08 00 38 C8 00 00 02 04 05 B4 00 00 50 99 06 E9
```

```
 Frame # 4        Time =  19:10:13.90681  Size: 64
Dest: 00-00-0C-09-9C-95  Src: 00-00-C0-73-D8-5C
0000- 00 00 0C 09 9C 95 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 2C 08 CD 00 00 40 06 42 D0 0D 14 0A 01 0D 14
0020- 0A F7 12 14 00 17 00 52 31 00 00 00 00 01 60 02
0030- 08 00 1D 89 00 00 02 04 05 B4 00 00 1A D5 C3 C5

 Frame # 5        Time =  19:10:13.90854  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-0C-09-9C-95
0000- 00 00 C0 73 D8 5C 00 00 0C 09 9C 95 08 00 45 00
0010- 00 2C 00 00 00 00 FF 06 8C AC 0D 14 0A F7 0D 14
0020- 0A 01 00 17 12 14 00 3A 8A DC 00 52 31 01 60 12
0030- 00 32 9A 30 00 00 02 04 05 B4 73 77 B5 81 66 0F

 Frame # 6        Time =  19:10:13.90985  Size: 64
Dest: 00-00-0C-09-9C-95  Src: 00-00-C0-73-D8-5C
0000- 00 00 0C 09 9C 95 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 08 CE 00 00 40 06 42 D3 0D 14 0A 01 0D 14
0020- 0A F7 12 14 00 17 00 52 31 01 00 3A 8A DD 50 10
0030- 08 00 AA 1F 00 00 00 00 00 00 00 00 DB C2 17 7C

 Frame # 71       Time =  19:10:27.60828  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-0C-09-9C-95
0000- 00 00 C0 73 D8 5C 00 00 0C 09 9C 95 08 00 45 00
0010- 00 28 00 1D 00 00 FF 06 8C 93 0D 14 0A F7 0D 14
0020- 0A 01 00 17 12 14 00 3A 8B 39 00 52 31 23 50 19
0030- 08 3E A9 5A 00 00 02 04 05 B4 73 77 78 70 CB D8

 Frame # 72       Time =  19:10:27.66236  Size: 64
Dest: 00-00-0C-09-9C-95  Src: 00-00-C0-73-D8-5C
0000- 00 00 0C 09 9C 95 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 08 F2 00 00 40 06 42 AF 0D 14 0A 01 0D 14
0020- 0A F7 12 14 00 17 00 52 31 23 00 3A 8B 3A 50 10
0030- 07 A4 A9 FC 00 00 00 00 00 00 00 00 4E 7A D5 6E

 Frame # 73       Time =  19:10:27.67264  Size: 64
Dest: 00-00-0C-09-9C-95  Src: 00-00-C0-73-D8-5C
0000- 00 00 0C 09 9C 95 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 08 F3 00 00 40 06 42 AE 0D 14 0A 01 0D 14
0020- 0A F7 12 14 00 17 00 52 31 23 00 3A 8B 3A 50 11
0030- 07 A4 A9 FB 00 00 00 00 00 00 00 00 6B 49 AB F0

 Frame # 74       Time =  19:10:27.67382  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-0C-09-9C-95
0000- 00 00 C0 73 D8 5C 00 00 0C 09 9C 95 08 00 45 00
0010- 00 28 00 1E 00 00 FF 06 8C 92 0D 14 0A F7 0D 14
0020- 0A 01 00 17 12 14 00 3A 8B 3A 00 52 31 24 50 10
0030- 08 3E A9 61 00 00 02 04 05 B4 73 77 46 0D BA E7
 Frame # 75       Time =  19:10:28.00275  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-0C-09-9C-95
0000- 00 00 C0 73 D8 5C 00 00 0C 09 9C 95 08 00 45 00
0010- 00 28 00 1F 00 00 FF 06 8C 91 0D 14 0A F7 0D 14
0020- 0A 01 00 17 12 14 00 3A 8B 3A 00 52 31 24 50 10
0030- 08 3E A9 61 00 00 02 04 05 B4 73 77 FE A3 7E 84

 Frame # 76       Time =  19:10:28.04592  Size: 64
Dest: 00-00-0C-09-9C-95  Src: 00-00-C0-73-D8-5C
0000- 00 00 0C 09 9C 95 00 00 C0 73 D8 5C 08 00 45 00
0010- 00 28 08 F4 00 00 40 06 42 BD 0D 14 0A 01 0D 14
0020- 0A F7 12 14 00 17 00 52 31 24 00 3A 8B 3A 50 1C
0030- 00 00 B1 93 00 00 02 04 05 B4 73 77 9C 2F E5 94
```

La tercera y última prueba se realizó con la aplicación de transferencia de archivos FTP entre 2 PC's como lo muestra la figura 5.3. La PC con dirección 13.52.150.37 actúa como servidor de FTP y es necesario utilizar el comando ftpsrv. La PC con dirección IP 13.52.150.28 actúa como cliente FTP.

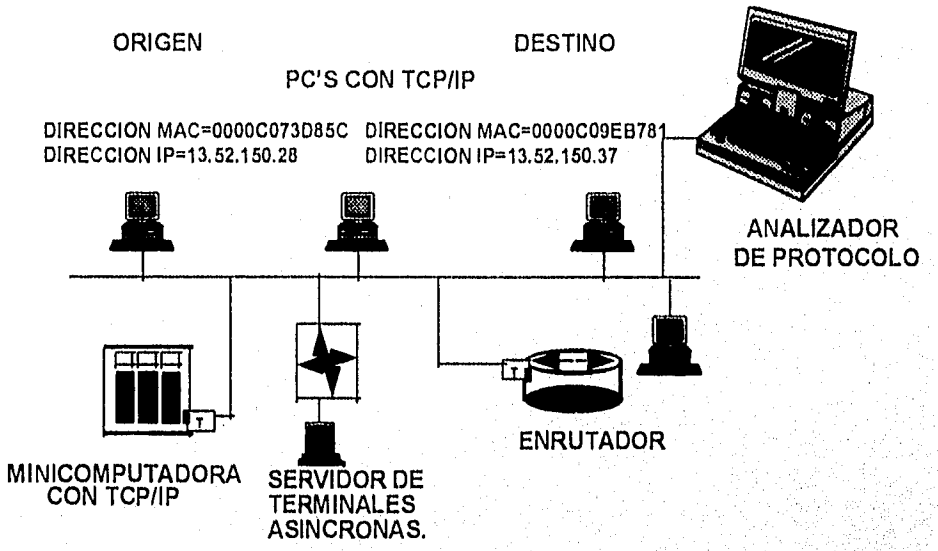


Figura 5.3

Diagrama de conexión de una red Ethernet para la prueba de la aplicación FTP de TCP/IP.

El comando utilizado para la prueba en la PC cliente con dirección 13.52.150.28 fue:

C:\tesis**ftp 13.52.150.37**
La respuesta al comando es:

Userid for logging in on 13.52.150.37(gosorno)
230 user OK, no password, directory is c:\tesis

ftp:13.52.150.37> Prompt de la aplicación esperando por comando.

Un comando que puede utilizarse para ver el directorio de archivos es:

ftp:13.52.150.37>**dir** Un comando similar al del sistema operativo DOS.

La respuesta al comando es:

p_ftp.txt Un archivo en el directorio c:\tesis
226 transfer successful. Closing data connection

El comando y archivo utilizados para la prueba de transmisión de archivos fué:

ftp:13.52.150.37>**get p_ftp.txt** Este comando pide la transferencia del archivo mostrado de la máquina origen 13.52.150.37 a la máquina destino 13.52.150.38.

La respuesta al comando es:

Transferred 393 bytes en 1 segundo (3144 bits/seg)
226 Transfer successful. Closing data connection

El mensaje anterior indica que la transmisión del archivo tuvó éxito.

El contenido del archivo utilizado en la transferencia p_ftp.TXT es:
ARCHIVO DE PRUEBA DE TRANSFERENCIA DE ARCHIVOS CON EL PROTOCOLO FTP.
EL PROTOCOLO FTP ES UNA APLICACION QUE UTILIZA LOS SERVICIOS DE LOS PROTOCOLOS TCP/IP.
LA PRUEBA SE REALIZA ENTRE DOS PC'S CON DOS Y EL SOFTWARE PCTCP.
UNA PC CORRE UNA UTILERIA PARA ACTUAR COMO SERVIDOR. LA OTRA MAQUINA ACTUA COMO CLIENTE INVOCANDO LA APLICACION CON EL COMANDO FTP Y LA DIRECCION IP DEL SERVIDOR.

Los mensajes generados en el servidor durante la prueba fueron:

Connection from 13.52.150.28, port 4656
User gosorno logged in at c:\tesis

Las tramas más importantes para el establecimiento de conexión, transmisión de datos y liberación de conexión se muestran a continuación:

Tramas generadas por la aplicación FTP.

```
Ethernet Trace
 Frame # 1        Time =  18:59:04.94454  Size: 64
Dest: 00-00-C0-9E-B7-81  Src: 00-00-C0-73-D8-5C
0000- 00 00 C0 9E B7 81 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 2C 00 2B 00 00 40 06 33 E8 0D 34 96 1C 0D 34
0020- 96 25 12 30 00 15 09 99 0B 00 00 00 00 01 60 02
0030- 08 00 22 9E 00 00 02 04 05 B4 00 00 86 09 9F 77
```

```
 Frame # 2        Time =  18:59:04.94537  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-C0-9E-B7-81
0000- 00 00 C0 73 D8 5C 00 00 C0 9E B7 81 08 00 45 10
0010- 00 2C 00 34 00 00 40 06 33 DF 0D 34 96 25 0D 34
0020- 96 1C 00 15 12 30 08 3C 1A 00 09 99 0B 01 60 12
0030- 08 00 00 52 00 00 02 04 05 B4 00 00 C7 57 E6 52


Frame # 3        Time =  18:59:04.94662  Size: 64
Dest: 00-00-C0-9E-B7-81  Src: 00-00-C0-73-D8-5C
0000- 00 00 C0 9E B7 81 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 00 2C 00 00 40 06 33 EB 0D 34 96 1C 0D 34
0020- 96 25 12 30 00 15 09 99 0B 01 08 3C 1A 01 50 10
0030- 08 00 18 0F 00 00 02 04 05 B4 00 00 0F 69 F8 6D


Frame # 4        Time =  18:59:04.95388  Size: 186
Dest: 00-00-C0-73-D8-5C  Src: 00-00-C0-9E-B7-81
0000- 00 00 C0 73 D8 5C 00 00 C0 9E B7 81 08 00 45 10
0010- 00 A8 00 35 00 00 40 06 33 62 0D 34 96 25 0D 34
0020- 96 1C 00 15 12 30 08 3C 1A 01 09 99 0B 01 50 18
0030- 08 00 A4 32 00 00 32 32 30 2D 4D 52 41 4D 49 52
0040- 45 5A 20 50 43 2F 54 43 50 20 46 54 50 20 53 65
0050- 72 76 65 72 20 56 65 72 73 69 6F 6E 20 32 2E 32
0060- 20 62 79 20 46 54 50 20 53 6F 66 74 77 61 72 65
0070- 20 72 65 61 64 79 0D 0A 32 32 30 20 43 6F 6E 6E
0080- 65 63 74 69 6F 6E 20 69 73 20 61 75 74 6F 6D 61
0090- 74 69 63 61 6C 6C 79 20 63 6C 6F 73 65 64 20 69
00A0- 66 20 69 64 6C 65 20 66 6F 72 20 35 20 6D 69 6E
00B0- 75 74 65 73 0D 0A 6A 64 09 D2


 Frame # 5        Time =  18:59:05.16972  Size: 64
Dest: 00-00-C0-9E-B7-81  Src: 00-00-C0-73-D8-5C
0000- 00 00 C0 9E B7 81 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 00 2D 00 00 40 06 33 EA 0D 34 96 1C 0D 34
0020- 96 25 12 30 00 15 09 99 0B 01 08 3C 1A 81 50 10
0030- 07 80 18 0F 00 00 02 04 05 B4 00 00 33 B4 83 01


 Frame # 46       Time =  19:04:16.99667  Size: 88
Dest: 00-00-C0-73-D8-5C  Src: 00-00-C0-9E-B7-81
0000- 00 00 C0 73 D8 5C 00 00 C0 9E B7 81 08 00 45 10
0010- 00 46 00 4B 00 00 40 06 33 AE 0D 34 96 25 0D 34
0020- 96 1C 00 15 12 30 08 3C 1B 6A 09 99 0B 5D 50 18
0030- 07 A4 33 E1 00 00 32 32 31 20 43 6C 6F 73 69 6E
0040- 67 20 63 6F 6E 6E 65 63 74 69 6F 6E 2C 20 42 79
0050- 65 21 0D 0A 4D BF 82 10


Frame # 47       Time =  19:04:16.99753  Size: 88
Dest: 00-00-C0-73-D8-5C  Src: 00-00-C0-9E-B7-81
0000- 00 00 C0 73 D8 5C 00 00 C0 9E B7 81 08 00 45 10
0010- 00 46 00 4C 00 00 40 06 33 AD 0D 34 96 25 0D 34
0020- 96 1C 00 15 12 30 08 3C 1B 6A 09 99 0B 5D 50 19
0030- 07 A4 33 E0 00 00 32 32 31 20 43 6C 6F 73 69 6E
0040- 67 20 63 6F 6E 6E 65 63 74 69 6F 6E 2C 20 42 79
0050- 65 21 0D 0A 82 86 21 29
```

```
 Frame # 48       Time =  19:04:16.99884  Size: 64
Dest: 00-00-C0-9E-B7-81  Src: 00-00-C0-73-D8-5C
0000- 00 00 C0 9E B7 81 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 00 3F 00 00 40 06 33 D8 0D 34 96 1C 0D 34
0020- 96 25 12 30 00 15 09 99 0B 5D 08 3C 1B 89 50 10
0030- 06 79 17 B2 00 00 02 04 05 B4 00 00 B6 BD 06 3A


 Frame # 49       Time =  19:04:17.02518  Size: 64
Dest: 00-00-C0-9E-B7-81  Src: 00-00-C0-73-D8-5C
0000- 00 00 C0 9E B7 81 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 28 00 40 00 00 40 06 33 D7 0D 34 96 1C 0D 34
0020- 96 25 12 30 00 15 09 99 0B 5D 08 3C 1B 89 50 11
0030- 06 79 17 B1 00 00 02 04 05 B4 00 00 E9 5F 3A 90


 Frame # 50       Time =  19:04:17.02592  Size: 64
Dest: 00-00-C0-73-D8-5C  Src: 00-00-C0-9E-B7-81
0000- 00 00 C0 73 D8 5C 00 00 C0 9E B7 81 08 00 45 10
0010- 00 28 00 4D 00 00 40 06 33 CA 0D 34 96 25 0D 34
0020- 96 1C 00 15 12 30 08 3C 1B 89 09 99 0B 5E 50 10
0030- 07 A4 16 86 00 00 02 04 05 B4 00 00 55 37 2A 67
```

5.2 Diagrama de flujo para elaboración del programa de análisis de protocolos TCP/IP.

El diagrama de flujo se elaboró de acuerdo con la información analizada en el capítulo 4, en donde se estudió la forma de presentación e interpretación de los diferentes protocolos TCP/IP en una red de área local Ethernet (Ver figura 5.4).

El diagrama tiene como inicio la lectura del archivo en donde se encuentran almacenadas las tramas de la aplicación. Limpia el archivo de los datos que nos son necesarios y lee el total de tramas almacenadas para posicionarse en la primera. Una vez que se encuentra en la trama número 1 se hace el análisis de esta trama, comenzando con la capa 2 (Ethernet) y checandose en el campo de tipo de datos el siguiente protocolo existente, ARP o IP. Si el siguiente protocolo es ARP se analiza y se despliega el análisis total. Si el siguiente protocolo es IP(capa 3) se analiza y se checa el protocolo contenido en campo de datos, ICMP o TCP. Cuando el protocolo almacenado en IP es ICMP o TCP se analiza y despliega el análisis total. Una vez que se analizó completamente la primera trama y el análisis de ésta ha sido desplegado, es necesario elegir una opción para continuar con el análisis de la siguiente trama o para salir.

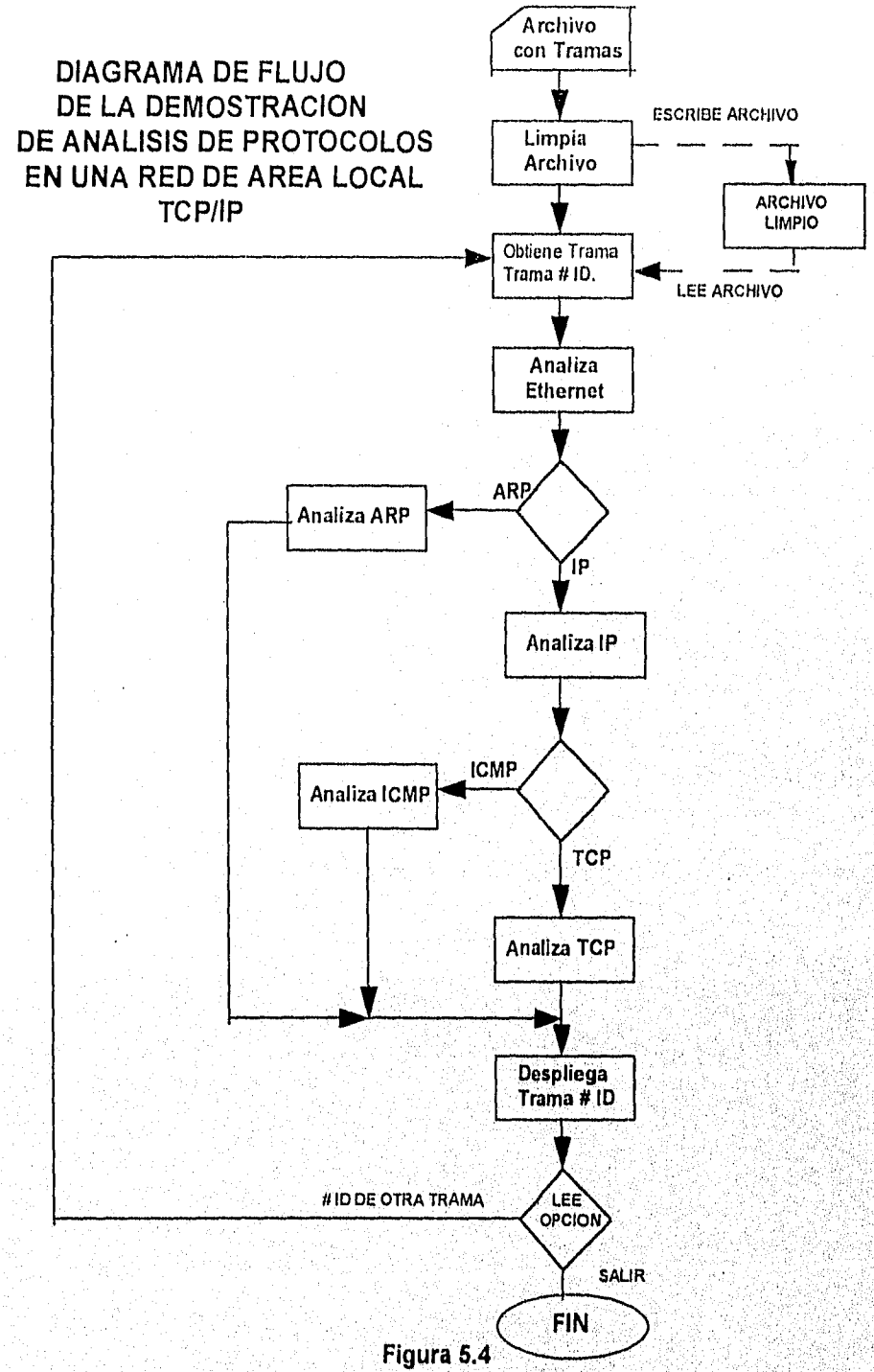


Figura 5.4

Diagrama de flujo del programa de demostrastración de protocolos TCP/IP.

5.3 Módulos de análisis del programa de demostración y despliegue en pantallas.

Módulo de presentación.
Módulo de lectura de archivos.
Módulo de análisis de protocolos Ethernet, ARP,IP,ICMP,TCP.
Módulo de conversión de hexadecimal a decimal.
Módulo de conversión de hexadecimal a binario.

El programa en principio contiene un módulo de presentación que consiste de una pantalla de datos generales y una pantalla de inicio para el despliegue de los protocolos analizados.

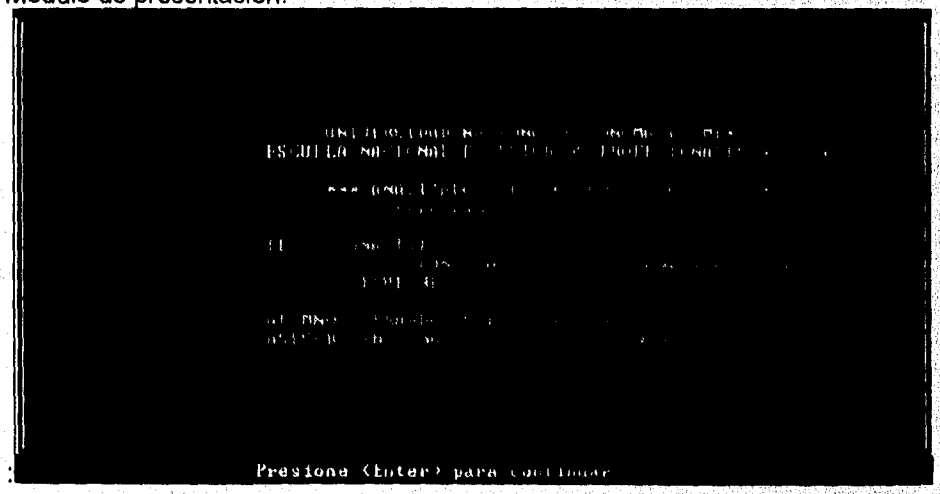
El programa contiene un módulo de lectura de archivos. Este módulo permite leer el contenido de un archivo en donde se encuentran guardadas las tramas de las pruebas realizadas para la demostración.

El programa analiza los diferentes protocolos contenidos en una trama de acuerdo con la lógica mostrada en el diagrama de flujo y con los diferentes módulos de análisis de protocolos mencionados anteriormente. Al mismo tiempo que va determinando los protocolos contenidos en la trama, es capaz de analizar cada uno de los campos de los mismos.

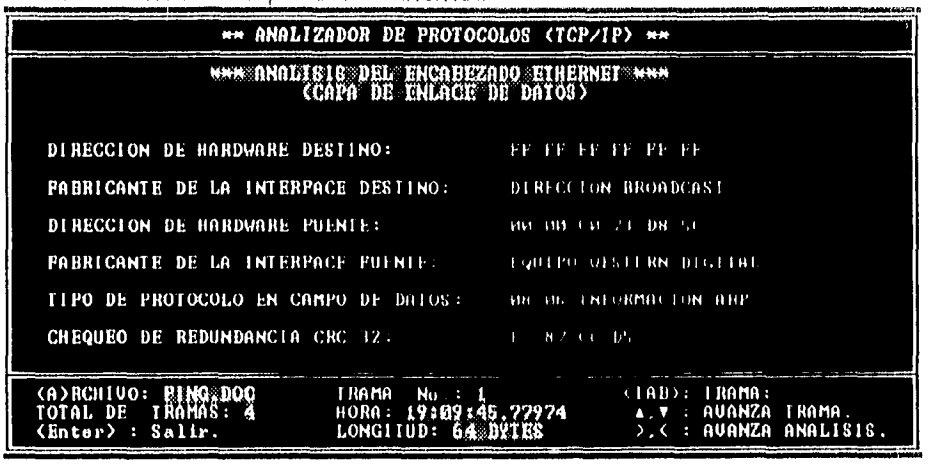
Durante el análisis de campos de protocolo es necesario realizar algunas conversiones de hexadecimal a decimal y de hexadecimal a binario, lo cual es implementado en dos módulos de conversión en el programa.

A continuación se despliegan los módulos del programa de análisis de protocolos TCP/IP:

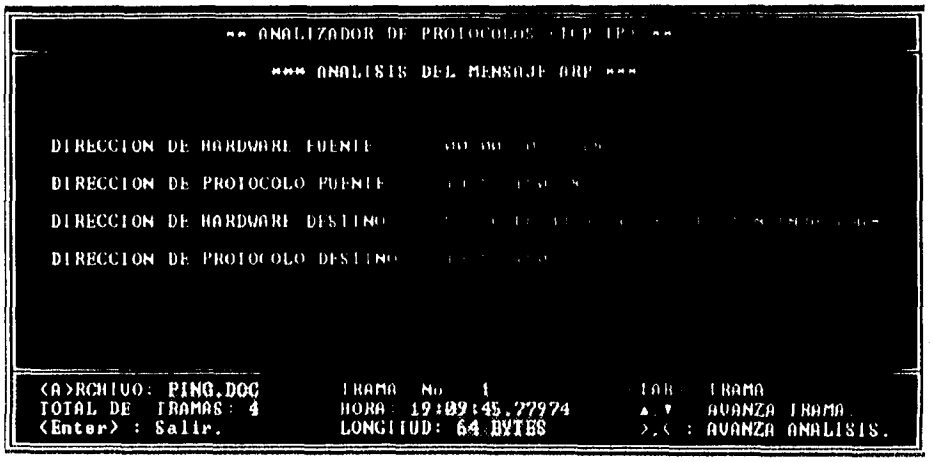
Módulo de presentación.



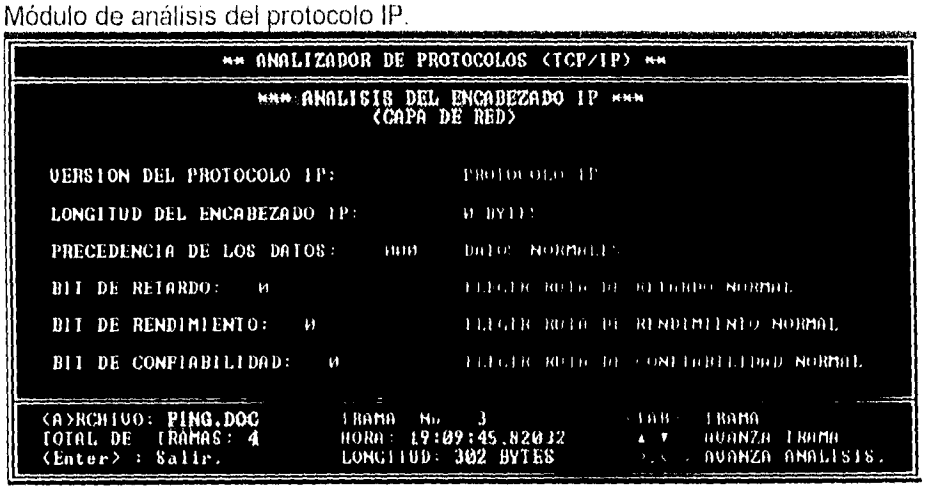
Módulo de análisis del protocolo Ethernet.

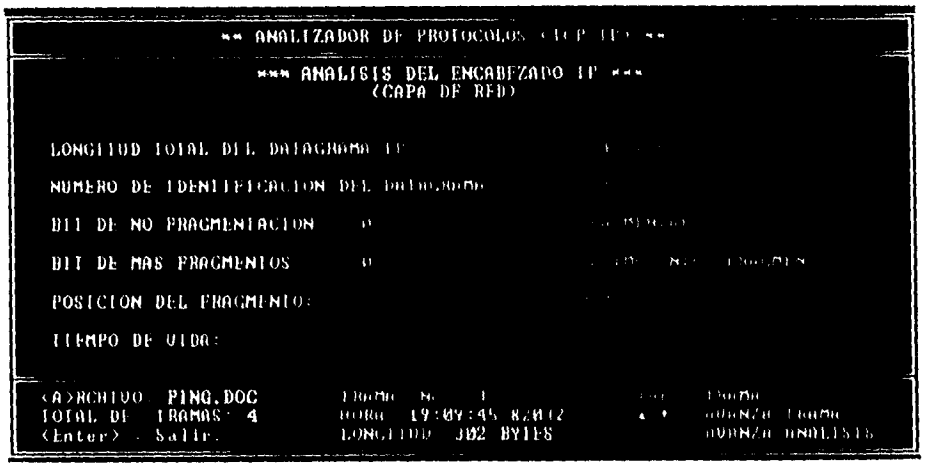


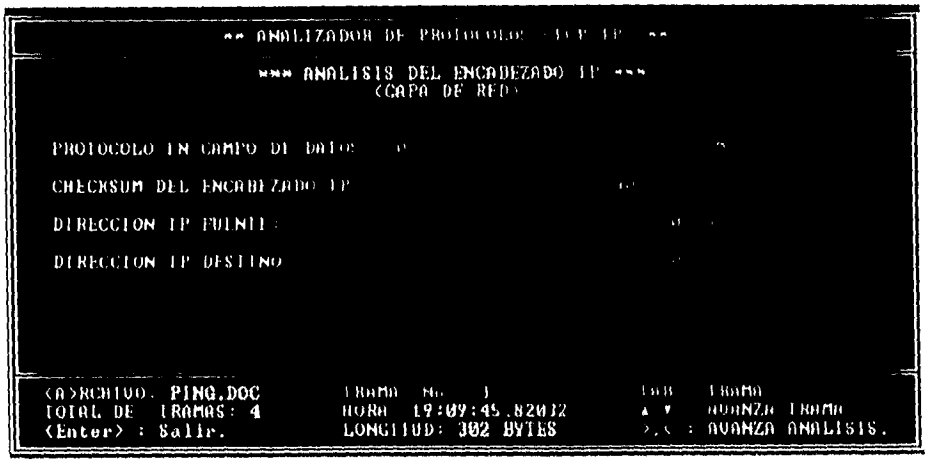
Módulo de análisis del protocolo ARP.



Módulo de análisis del protocolo IP.

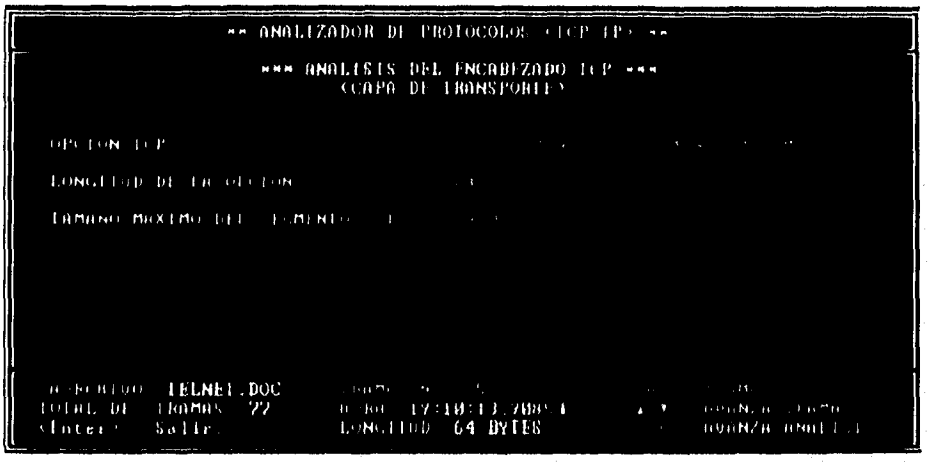






Módulo de análisis del protocolo ICMP.

Módulo de análisis del protocolo TCP.



5.4 Código del programa de demostración de análisis de protocolos TCP/IP en redes Ethernet.

El programa se realizó en lenguaje C utilizando el compilador de Turbo C ++ versión 3.1 y el código del mismo se encuentra contenido en un archivo de código fuente y un archivo de cabecera con código fuente también que se entrega en un disco para PC de 31/2. Los tipos y nombres de archivo son:

Archivos fuente para Borland C++ 3.1.
analiza.cpp
analizad.h

El archivo ejecutable de la demostración.

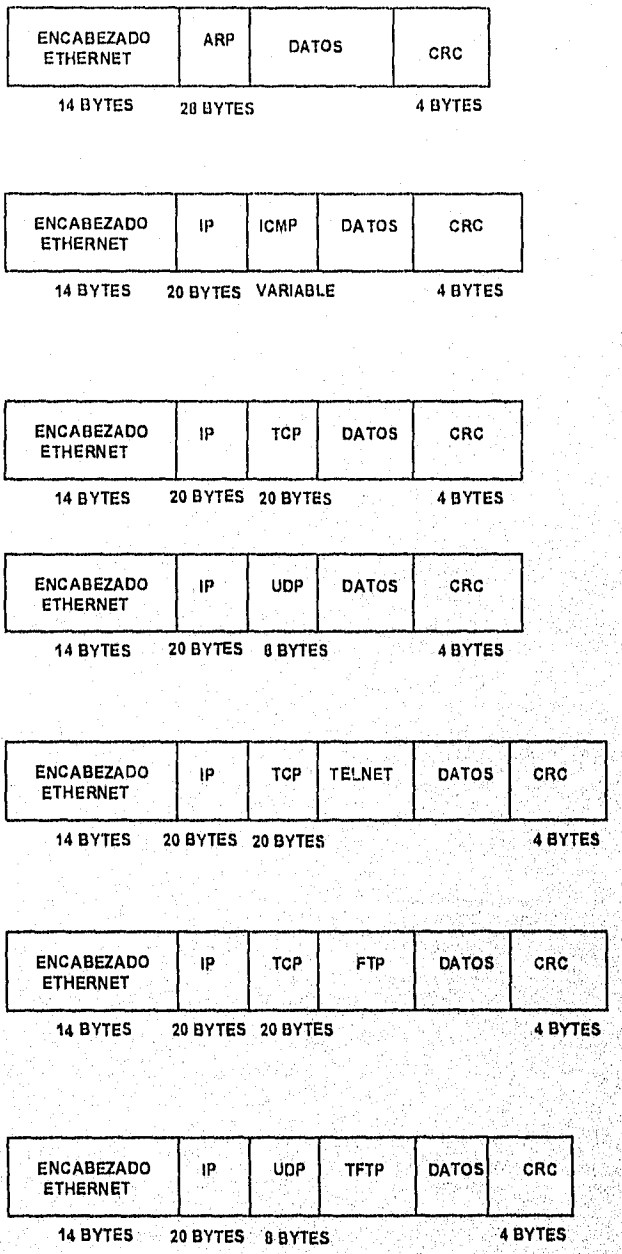
analiza.exe.

Los archivos con las tramas de las aplicaciones analizadas.

ping.doc
telnet.doc
ftp.doc

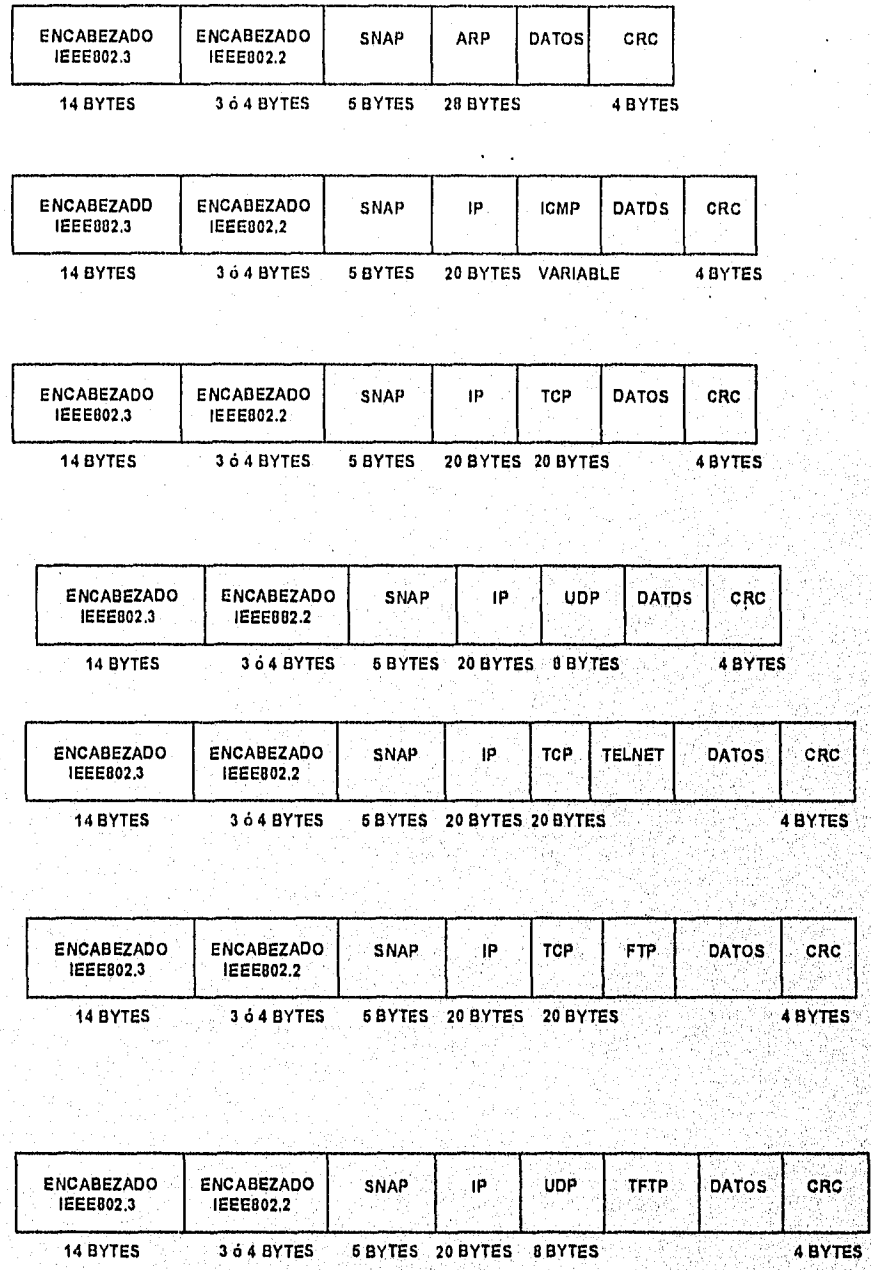
Para elaborar el programa se utilizaron los diagramas de encapsulamiento Etehernet, las tablas de protocolos y las tablas de valores de los diferentes campos mostradas a continuación:

ENCAPSULAMIENTO DE LOS PROTOCOLOS TCP/IP EN ETHERNETII.



* VALORES DE ENCABEZADOS SIN OPCIONES

ENCAPSULAMIENTO DE LOS PROTOCOLOS TCP/IP EN IEEE802.



* VALORES DE ENCABEZADOS SIN OPCIONES

PROTOCOLO ETHERNET

CAMPOS DE LA TRAMA	LONGITUD
DIRECCION DEL DESTINO ETHERNET	6 BYTES
DIRECCION FUENTE ETHERNET	6 BYTES
TIPO DE PROTOCOLO CONTENIDO EN ETHERNET	2 BYTES
CAMPO DE DATOS ETHERNET	VARIABLE
CRC 32 EN ETHERNET	4 BYTES

Tabla de protocolo Ethernet.

PROTOCOLO ARP

CAMPOS DEL MENSAJE	LONGITUD
TIPO DE HARDWARE	2 BYTES
TIPO DE PROTOCOLO	2 BYTES
LONGITUD DE HARDWARE	1 BYTE
LONGITUD DE PROTOCOLO	1 BYTE
OPERACION	2 BYTES
DIRECCION DE HARDWARE FUENTE	6 BYTES
DIRECCION DE PROTOCOLO FUENTE	4 BYTES
DIRECCION DE HARDWARE DESTINO	6 BYTES
DIRECCION DE PROTOCOLO DESTINO	4 BYTES

Tabla protocolo ARP.

PROTOCOLO IP

CAMPOS DEL DATAGRAMA	LONGITUD	
VERSION IP	4 BITS	
LONGITUD DEL ENCABEZADO IP	4 BITS	
PRECEDENCIA DE LOS DATOS	3 BITS	
BIT DE RETARDO	1 BIT	2 BYTES
BIT DE CAPACIDAD DE TRANSMISION UTIL	1 BIT	
BIT DE CONFIABILIDAD	1 BIT	
BITS RESERVADOS	2 BITS	
LONGITUD TOTAL DEL DATAGRAMA IP	2 BYTES	
NUM. IDENTIFICACION DE DATAGRAMA	2 BYTES	
BIT RESERVADO	1 BIT	
BIT DE NO FRAGMENTAR	1 BIT	
BIT DE MAS FRAGMENTOS	1 BIT	2 BYTES
POSICION DEL FRAGMENTO	13 BITS	

TIEMPO DE VIDA	1 BYTE	
PROTOCOLO TRANSPORTADO	1 BYTE	
CHECKSUM DEL ENCABEZADO IP	2 BYTES	
DIRECCION FUENTE IP	4 BYTES	
DIRECCION DESTINO IP	4 BYTES	20BYTES
BIT DE COPIA	1 BIT	
CLASE DE OPCION	2 BITS	1 BYTE
NUMERO DE OPCION	5 BITS	
LONGITUD VAR DE LOS DATOS DE OPCIONES		

Tabla protocolo IP.

PROTOCOLO UDP

CAMPOS DEL DATAGRAMA	*LONGITUD*
PUERTO FUENTE UDP	2 BYTES
PUERTO DESTINO UDP	2 BYTES
LONGITUD DEL MENSAJE	2 BYTES
CHECKSUM UDP	2 BYTES

Tabla de protocolo UDP.

PROTOCOLO TCP

CAMPOS DEL SEGMENTO	*LONGITUD*	
PUERTO FUENTE TCP	2 BYTES	
PUERTO DESTINO TCP	2 BYTES	
NUM. DE SECUENCIA FUENTE	4 BYTES	
NUM. DE SECUENCIA DE RECONOCIMIENTO	4 BYTES	
LONGITUD DEL ENCABEZADO TCP	4 BITS	
BITS RESERVADOS	6 BITS	
BIT URGENTE	1 BIT	
BIT DE RECONOCIMIENTO VALIDO	1 BIT	2 BYTES
BIT DE PUSH REQUEST	1 BIT	
BIT DE RESET DE SESION	1 BIT	
BIT DE SINCRONIZACION	1 BIT	
FIN DE DATOS ENVIADOS	1 BIT	
TAMAÑO DE LA VENTANA DEL EMISOR	2 BYTES	
CHECKSUM DEL ENCABEZADO TCP	2 BYTES	
APUNTADOR DE DATOS URGENTES	2 BYTES	20 BYTES
TIPO DE OPCIONES	1 BYTE	
LONGITUD DE OPCIONES	1 BYTE	
TAMAÑO MAXIMO DEL SEGMENTO TCP	2 BYTES	24 BYTES

Tabla de protocolo TCP.

Tablas utilizadas para el análisis de los campos de los protocolos TCP/IP.

```
TABLA 1

DIRECCIONES DE HARDWARE ETHERNET PARA CADA FABRICANTE.

00000C DIRECCION DE HARDWARE 00000C, EQUIPO CISCO
00001B DIRECCION DE HARDWARE 00001B, EQUIPO NOVELL
00001D DIRECCION DE HARDWARE 0000ID, EQUIPO CABLETRON
000093 DIRECCION DE HARDWARE 000093, EQUIPO PROTEON
0000A2 DIRECCION DE HARDWARE 0000A2, EQUIPO WELLFLEET
0000AA DIRECCION DE HARDWARE 0000AA, EQUIPO XEROX
0000C0 DIRECCION DE HARDWARE 0000C0, EQUIPO WESTERN DIGITAL
0000D8 DIRECCION DE HARDWARE 0000D8, EQUIPO 3COM
080002 DIRECCION DE HARDWARE 080002, EQUIPO 3COM
080009 DIRECCION DE HARDWARE 080009, EQUIPO HP
00008A DIRECCION DE HARDWARE 08000A, EQUIPO NESTAR
08000B DIRECCION DE HARDWARE 08000B, EQUIPO UNISYS
080010 DIRECCION DE HARDWARE 080010, EQUIPO AT&T
08001E DIRECCION DE HARDWARE 08001E, EQUIPO APOLO
080020 DIRECCION DE HARDWARE 080020, EQUIPO SUN
08002B DIRECCION DE HARDWARE 08002B, EQUIPO DEC
080038 DIRECCION DE HARDWARE 080038, EQUIPO BULL
08005A DIRECCION DE HARDWARE 08005A, EQUIPO IBM
08006E DIRECCION DE HARDWARE 08006E, EQUIPO EXCELAN
```

```
TABLA 2

CAMPO DE TIPO DE REDES ETHERNET

0800 CAMPO DE TIPO 0800 INFORMACION IP
0805 CAMPO DE TIPO 0805 INFORMACION X.25 CAPA 3
0806 CAMPO DE TIPO 0806 INFORMACION ARP
0A00 CAMPO DE TIPO 0A00 INFORMACION IEEE802.3 XEROX
6003 CAMPO DE TIPO 6003 INFORMACION DECNET FASE 4
8019 CAMPO DE TIPO 8019 INFORMACION COMPUTADORAS APOLO
809D CAMPO DE TIPO 809D INFORMACION APPLETALK
814C CAMPO DE TIPO 814C INFORMACION SNMP
```

```
TABLA 3

TIPO DE HARDWARE EN PROTOCOLO ARP

0001 TIPO DE HARDWARE 1, ETHERNET
0006 TIPO DE HARDWARE 6, IEEE802
0007 TIPO DE HARDWARE 7, ARCNET
0009 TIPO DE HARDWARE 9, LANSTAR
000B TIPO DE HARDWARE 11, LOCALTALK
```

```
TABLA 4

CAMPO DE TIPO DE PROTOCOLO ARP

0800 CAMPO DE TIPO 0800 INFORMACION IP
0805 CAMPO DE TIPO 0805 INFORMACION X.25 CAPA 3
0806 CAMPO DE TIPO 0806 INFORMACION ARP
6003 CAMPO DE TIPO 6003 INFORMACION DECNET FASE 4
8019 CAMPO DE TIPO 8019 INFORMACION COMPUTADORAS APOLO
809D CAMPO DE TIPO 809D INFORMACION APPLETALK
814C CAMPO DE TIPO 814C INFORMACION SNMP
```

```
TABLA 5

OPERACION ARP.

0001 CODIGO DE OPERACION 1, SOLICITUD DE DIRECCION DE HARDWARE DESTINO.
0002 CODIGO DE OPERACION 2, RESPUESTA DE DIRECCION DE HARDWARE DESTINO.
```

```
TABLA 6

NUMEROS DE VERSION IP (4 BITS).

0 RESERVADO
1 NO ASIGNADO
4 VERSION 4 PROTOCOLO IP.
5 VERSION 5 MODO DE DATAGRAMA ST.
```

```
TABLA 7

BITS DE PRECEDENCIA

000 PRECEDENCIA 000 DATOS NORMALES
001 PRECEDENCIA 001 DATOS DE PRIORIDAD
010 PRECEDENCIA 010 DATOS INMEDIATOS
011 PRECEDENCIA 011 DATOS FLASH
100 PRECEDENCIA 100 DATOS FLASH OVERRIDE
101 PRECEDENCIA 101 DATOS CRITICOS
111 PRECEDENCIA 111 DATOS DE CONTROL DE RED
```

```
TABLA 8

NUMEROS DE PROTOCOLO EN CAMPO DE DATOS IP

00 RESERVARDO
01 NUMERO DE PROTOCOLO 1, PROTOCOLO ICMP
02 NUMERO DE PROTOCOLO 2, PROTOCOLO IGMP
03 NUMERO DE PROTOCOLO 3, ENRUTADOR A ENRUTADOR
06 NUMERO DE PROTOCOLO 6, PROTOCOLO TCP
08 NUMERO DE PROTOCOLO 8, PROTOCOLO EGP
09 NUMERO DE PROTOCOLO 9, PROTOCOLO IGP
11 NUMERO DE PROTOCOLO 17, PROTOCOLO UDP
58 NUMERO DE PROTOCOLO 88, PROTOCOLO IGRP
```

TABLA 9

TIPOS DE MENSAJES ICMP.

00 MENSAJE ICMP 00 RESPUESTA DE ECO ICMP
03 MENSAJE ICMP 03 DESTINO NO ALCANZABLE
04 MENSAJE ICMP 04 FUENTE AHOGADA (SOURCE QUENCH)
05 MENSAJE ICMP 05 REDIRECCION ICMP
08 MENSAJE ICMP 08 SOLICITUD DE ECO ICMP
0B MENSAJE ICMP 11 TIEMPO EXCEDIDO PARA UN DATAGRAMA
0C MENSAJE ICMP 12 PROBLEMA DE PARAMETROS
0D MENSAJE ICMP 13 SOLICITUD DE SELLO DE TIEMPO
0E MENSAJE ICMP 14 RESPUESTA DE SELLO DE TIEMPO
11 MENSAJE ICMP 17 SOLICITUD DE DIRECCION DE MASCARA
12 MENSAJE ICMP 18 RESPUESTA DE DIRECCION DE MASCARA

TABLA 10

NUMEROS DE PUERTO TCP

0000 RESERVADO
0014 PUERTO 20, PUERTO PARA TRANSFERENCIA DE ARCHIVOS FTP-DATOS
0015 PUERTO 21, PUERTO PARA TRANSFERENCIA DE ARCHIVOS FTP-CONTROL
0017 PUERTO 23, PUERTO PARA TERMINAL REMOTA TELNET.
0019 PUERTO 25, PUERTO PARA TRANSFERENCIA DE CORREO SIMPLE.
0043 PUERTO 67, PUERTO PARA PROTOCOLO BOOTSTRAP DEL SERVIDOR BOOTPS
0044 PUERTO 68, PUERTO PARA PROTOCOLO BOOTSTRAP DEL CLIENTE BOOTPC
0045 PUERTO 69, PUERTO PARA TRANSFERENCIA DE ARCHIVOS TRIVIAL TFTP
00A1 PUERTO 161, PUERTO PARA SNMP SNMP
00A2 PUERTO 162, PUERTO PARA SNMPTRAP SNMPTRAP
00B3 PUERTO 179, PUERTO PARA PROTOCOLO BGP

Nota: 401 A FFFF PUERTO 1025 A 65535 PUERTO ALEATORIO.

TABLA 11

INTERPRETACION DEL CAMPO DE BITS DE CODIGO.

002 SEGMENTO DE SINCRONIZACION Y RECONOCIMIENTO NO VALIDO
012 SEGMENTO DE SINCRONIZACION Y RECONOCIMIENTO VALIDO
010 SEGMENTO DE RECONOCIMIENTO VALIDO
018 SEGMENTO DE RECONOCIMIENTO VALIDO Y PUSH REQUEST
019 SEGMENTO DE RECONOCIMIENTO VALIDO, PUSH REQUEST Y FIN DE DATOS ENVIADOS
011 SEGMENTO DE RECONOCIMIENTO VALIDO Y FIN DE DATOS ENVIADOS.
01C SEGMENTO DE RECONOCIMIENTO VALIDO, PUSH REQUEST Y RESET DE SESION.

5.5 Análisis de resultados sobre redes Ethernet.

Análisis para la aplicación PING trama 1.

```
Ethernet Trace
 Frame # 1        Time =  19:09:45.77974  Size: 64

   Dest: FF-FF-FF-FF-FF-FF  Src: 00-00-C0-73-D8-5C
0000- FF FF FF FF FF FF 00 00 C0 73 D8 5C 08 06 00 01
0010- 08 00 06 04 00 01 00 00 C0 73 D8 5C 0D 34 96 1C
0020- 5C FA E8 44 45 87 0D 34 96 1B 00 00 00 00 00 00
0030- 00 00 00 00 00 00 00 00 00 00 00 00 F2 87 CC D5
```

Análisis Ethernet

6 bytes dirección de hardware Ethernet destino. FF FF FF FF FF FF (broadcast)

6 bytes dirección de hardware Ethernet fuente. 00 00 C0 73 D8 5C

2 bytes Campo de tipo de información transportada en datos (prot. 0806) Información ARP.

Análisis ARP.

2 bytes Tipo de hardware	00 01 (Ethernet)
2 bytes Tipo de protocolo	08 00 (Información IP)
1 byte Longitud de la dirección de Hardware	06
1 byte Longitud de la dirección de Protocolo	04
2 bytes Operación	00 01 Solicitud de dirección
6 bytes Dirección de Hardware Fuente	00 00 C0 73 D8 5C
4 bytes Dirección de Protocolo Fuente	0D 34 96 1C (13.52.150.28)
6 bytes Dirección de Hardware Destino	5C FA E8 44 45 87
4 bytes Dirección de Protocolo Destino	0D 34 96 1B (13.52.150.27)
4 bytes CRC-32 Ethernet	F2 87 CC D5

Análisis para la aplicación TELNET trama 4.

```
Frame # 4        Time =  19:10:13.90681  Size: 64

  Dest: 00-00-0C-09-9C-95  Src: 00-00-C0-73-D8-5C
0000- 00 00 0C 09 9C 95 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 2C 08 CD 00 00 40 06 42 D0 0D 14 0A 01 0D 14
0020- 0A F7 12 14 00 17 00 52 31 00 00 00 00 01 60 02
0030- 08 00 1D 89 00 00 02 04 05 B4 00 00 1A D5 C3 C5
```

Análisis Ethernet

6 bytes dirección de hardware Ethernet destino	00 00 0C 09 9C 95
6 bytes dirección de hardware Ethernet fuente	00 00 C0 73 D8 5C
2 bytes Campo de tipo de información transportada en datos	(prot. 0800) Información IP

Análisis IP

4 bits Versión IP.	4
4 bits Longitud del encabezado IP	5 (20 bytes)
3 bits precedencia de los datos	000 Datos normales
1 bit Bit de retardo	1 Elegir ruta de menor retardo.
1 bit Bit de capacidad de transmisión	0 Elegir ruta de rendimiento normal.
1 bit Bit de confiabilidad	0 Elegir ruta de confiabilidad normal.
2 bits Reservados no utilizados	
2 bytes Longitud Total IP	00 2C (44 bytes)
2 bytes Número de Identificación de datagrama	08 CD (2253 dec.)
1 bit Bit reservado sin uso	
1 bit No fragmentación	0 Fragmentar
1 bit Más fragmentos	0 Ultimo/único fragmento.
13 bits Posición del fragmento	0 0000 0000 0000 0 dec.
1 byte Tiempo de vida	40 (64 seg).
1 byte Protocolo en campo de datos	06 protocolo TCP.
2 bytes Checksum del encabezado IP	42 D0.
4 bytes Dirección Fuente IP	0D 14 0A 01 (13.20.10.1)
4 bytes Dirección Destino IP	0D 14 0A F7 (13.20.10.247)

Análisis TCP dentro de IP

2 bytes	Puerto Fuente TCP	1214 (4628 Puerto aleatorio)
2 bytes	Puerto Destino TCP	00 17 (23 Puerto Telnet).
4 bytes	Número de Secuencia Fuente	00 52 31 00
4 bytes	Número de Secuencia de Reconocimiento	00 00 00 01
4 bits	Longitud del encabezado TCP	6 (palabras de 32 bits) 24 bytes TCP con opciones

6 bits Bits reservados sin uso
6 bits Bits de código. 002
Segmento de sincronización y reconocimiento no válido.

2 bytes	Tamaño de la ventana del emisor	08 00 (2048 bytes)
2 bytes	Checksum del encabezado TCP	1D 89
2 bytes	Apuntador de datos urgentes	00 00
1 byte	Tipo de Opciones	02
1 byte	Longitud de Opciones	04
2 bytes	Tamaño máximo del Segmento TCP	05 B4 (1460 Bytes)

4 bytes	CRC-32 Ethernet	1A D5 C3 C5

Análisis para la aplicación FTP trama 1.

```
Ethernet Trace
 Frame # 1        Time =  18:59:04.94454  Size: 64

   Dest: 00-00-C0-9E-B7-81  Src: 00-00-C0-73-D8-5C
0000- 00 00 C0 9E B7 81 00 00 C0 73 D8 5C 08 00 45 10
0010- 00 2C 00 2B 00 00 40 06 33 E8 0D 34 96 1C 0D 34
0020- 96 25 12 30 00 15 09 99 0B 00 00 00 00 01 60 02
0030- 08 00 22 9E 00 00 02 04 05 B4 00 00 86 09 9F 77
```

Análisis Ethernet

6 bytes dirección de hardware Ethernet destino 00 00 C0 9E B7 81

6 bytes dirección de hardware Ethernet fuente. 00 00 C0 73 D8 5C

2 bytes Campo de tipo de información transportada en datos (prot. 0800) Información IP

Análisis IP

4 bits Versión IP. 4
4 bits Longitud del encabezado IP 5 (20 bytes)

3 bits precedencia de los datos. 000 Datos normales
1 bit Bit de retardo. 1 Elegir ruta de menor retardo.
1 bit Bit de capacidad de transmisión. 0 Elegir ruta de rendimiento normal.
1 bit Bit de confiabilidad. 0 Elegir ruta de confiabilidad normal.
2 bits Reservados no utilizados.
2 bytes Longitud Total IP. 00 2C (44 bytes)
2 bytes Número de Identificación de datagrama. 00 2b (43 dec.)

1 bit Bit reservado sin uso
1 bit No fragmentación. 0 Fragmentar
1 bit Más fragmentos 0 Ultimo/único fragmento.
13 bits Posición del fragmento 0 0000 0000 0000 0 dec.
1 byte Tiempo de vida 40 (64 seg).
1 byte Protocolo en campo de datos 06 protocolo TCP.
2 bytes Checksum del encabezado IP 33 E8.
4 bytes Dirección Fuente IP. 0D 34 96 1C (13.52.150.28)
4 bytes Dirección Destino IP. 0D 34 96 25 (13.52.150.37)

Análisis TCP dentro de IP

2 bytes	Puerto Fuente TCP	1230 (4656 Puerto aleatorio)
2 bytes	Puerto Destino TCP	00 15 (21 Puerto FTP)
4 bytes	Número de Secuencia Fuente	09 99 0B 00
4 bytes	Número de Secuencia de Reconocimiento	00 00 00 01
4 bits	Longitud del encabezado TCP	6 (palabras de 32 bits) 24 bytes TCP con opciones

6 bits Bits reservados sin uso.
6 bits Bits de código. 002.
Segmento de sincronización y reconocimiento no válido.

2 bytes	Tamaño de la ventana del emisor	08 00 (2048 bytes)
2 bytes	Checksum del encabezado TCP	22 9E
2 bytes	Apuntador de datos urgentes	00 00
1 byte	Tipo de Opciones	02
1 byte	Longitud de Opciones	04
2 bytes	Tamaño máximo del Segmento TCP	05 B4 (1460 bytes)

4 bytes	CRC-32 Ethernet	86 09 9F 77

CONCLUSIONES

Como se mostró durante el análisis de los protocolos TCP/IP, éstos son muy convenientes por que permiten utilizar el mismo formato de direccionamiento para redes de área local y de área amplia, además existen una amplia variedad de equipos de interconexión de redes para protocolos TCP/IP que cuentan con puertos para las redes mencionadas en el mismo bastidor y por lo tanto procesan con efectividad las tramas, datagramas y unidades de información de las diferentes redes que conectan.

Otra ventaja de TCP/IP es que existe en una ancha variedad de estándares de aplicaciones y productos en venta. Muchas implementaciones están basadas en la característica propuesta por el modelo OSI de protocolos por capas, en la cual TCP/IP es encapsulado dentro de unidades de datos de otros protocolos u otros protocolos son encapsulados dentro de segmentos TCP y datagramas IP.

Se debe mencionar que aunque TCP/IP cumple con las funciones propuestas por el modelo OSI, los protocolos TCP/IP son incompatibles con algunas de sus recomendaciones. Lo anterior sugiere dos tendencias diferentes como solución para la interconexión de redes, sin embargo, las mejores razones para confiar en TCP/IP son: primero, que está aquí y trabaja; segundo, una gran cantidad de productos que utilizan los protocolos TCP/IP. Tercero, éste tiene una bien fundada estructura de administración de red con los protocolos SNMP. Cuarto, proporciona fácil acceso a la administración. Quinto, es usado en muchos productos UNIX y computadoras personales.

Sumado a lo anterior, tecnologías de Frame Relay, ATM y el equipo fabricado para interconexión de redes soportando éstas, contempla el soporte de los protocolos TCP/IP.

APENDICE A

A.I Líneas Telefónicas.

Son circuitos conmutados y representan la forma más simple de comunicación entre computadoras a larga distancia. Para poder utilizar las líneas telefónicas se necesita conectar un módem a la computadora y a una línea telefónica, después marcar un número donde se encuentra la computadora remota que contestará la llamada con ayuda de otro módem.

Este método es simple y directo para la comunicación, pero hay un número de problemas con estos circuitos de marcación directa. El costo de la llamada es alto, la calidad de la línea es insignificante para transmitir sin errores y además no se puede lograr alta velocidad de transmisión de datos.

A.2 Líneas Privadas.

Cuando la utilización de una línea conmutada es muy grande es preferible usar un circuito privado. Un circuito privado establece una trayectoria fija de extremo a extremo, sin necesidad de marcarse un número telefónico. Las líneas privadas pueden ser de 2 o 4 hilos.

A.3 Enlaces digitales E1 de 2.048 Mbps.

¿Qué es un E1?

Es una especificación para la transmisión de datos, que define la interconexión física entre redes, a través de la cual viajaran los datos, sobre un esquema de transmisión digital remota.
El E1 es un canal compuesto de 32 canales lógicos, de los cuales 31 se utilizan para la transmisión de datos y uno para la sincronización. Cada canal cuenta con un ancho de banda de 64 Kbps, haciendo un total de 2048 Kbps, es decir la capacidad que cubre un E1.

Los fundamentos en los que se basa un E1 son los sistemas PCM y las recomendaciones G.703, G.704 y G.711 del CCITT que definen las características físicas, eléctricas y funcionales de las interfaces digitales.

Sistemas PCM y enlaces digitales.

Expresado en simples palabras, la función de un sistema PCM es convertir una señal analógica dentro de una señal digital que pueda ser transmitida.

Los sistemas PCM pueden tener variadas capacidades de canal. La capacidad más frecuente es de 32 canales, al cual se le llama sistema de primer orden (2.048 Mbit/seg). Este sistema sirve como un módulo básico para la creación de sistemas PCM de más alto orden. Un PCM de segundo orden contiene 4 sistemas PCM de primer orden multiplexados, dando como resultado una capacidad de 128 canales. Un PCM de tercer orden contiene 512 canales y así sucesivamente.

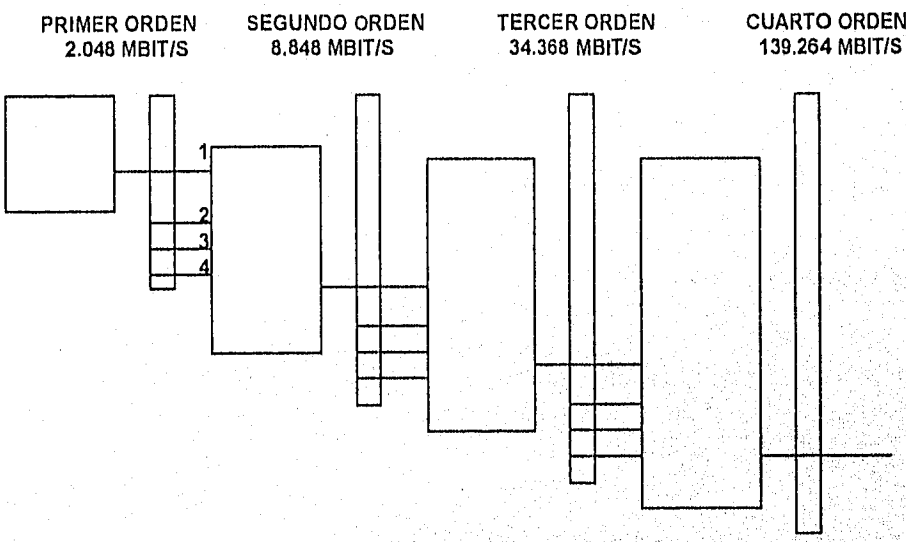


Figura A.1
Jerarquías de los sistemas PCM.

Las etapas que comprende un sistema de comunicación PCM son las que se muestran en la figura A.2 y se describen a continuación:

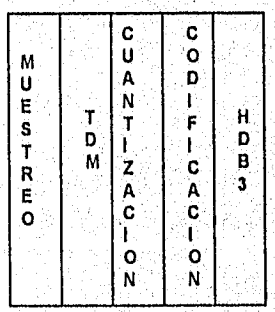


Figura A.2.
Etapas de un sistema de comunicación PCM para telefonía y datos.

Muestreo.

El principio básico de la transmisión de señales analógicas en un sistema PCM es que la señal analógica no es transmitida continuamente. En lugar de esto, 8000 valores instantáneos son transmitidos cada segundo y estos valores son tomados de la señal analógica que está presente en cada canal.

La señal analógica es entonces reconstruida en el extremo receptor por medio de los valores instantáneos recibidos.

La figura A.3 indica el procedimiento de muestreo. Conmutadores electrónicos son controlados por pulsos de reloj lo cual causa que los contactos cierren en orden consecutivo en los 32 canales. Esta secuencia es repetida 8000 veces por segundo. Cada canal genera 8000 valores de voltaje instantáneo llamadas muestras.

PAM (Modulación por amplitud de pulso).

Una vez que se tienen todas las muestras de la señal analógica se obtienen diversos valores de amplitud que se conocen como modulación por amplitud de pulso. La secuencia anterior puede considerarse alternativamente como una secuencia periódica de pulsos (la portadora) cuya amplitud se modula (o varía) de acuerdo con la información que se transmite. Esto es evidente en la expresión para los datos muestreados $Fs(t)=F(t)S(t)$. La función de conmutación $S(t)$ representa la portadora de pulsos sin modulación y $F(t)$ la información que modula la portadora.

Multiplexaje por División de Tiempo (TDM).

Cuando se llevan las muestras de los 32 diferentes canales a un tren de pulsos común, cada canal es enviado en predeterminados intervalos de tiempo y esto es lo que se conoce como multiplexaje por división de tiempo.

Cuantización.

En un sistema PCM, la señal PAM, obtenida por el muestreo es cuantizada. Esto se logra dividiendo la variación de amplitud total de la señal en intervalos de amplitud discretos igualmente espaciados. En el centro de cada uno de estos intervalos se ubican los niveles de cuantización. La señal cuantizada se obtiene ajustando cada una de las muestras de la señal PAM al nivel de cuantización correspondiente al intervalo de amplitud discreto, donde la señal está ubicada.

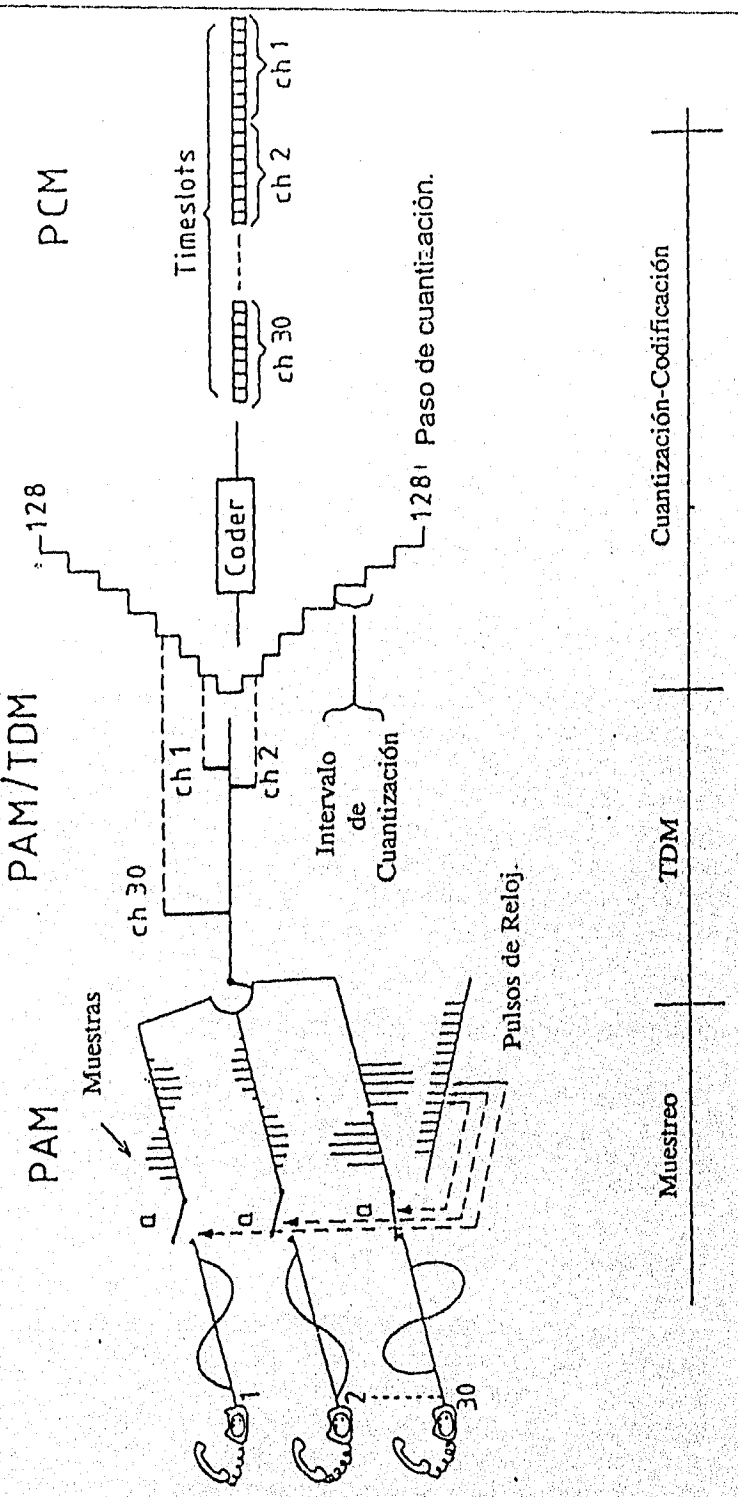


Figura A.3
Procedimiento de muestreo.

Aunque la división en intervalos discretos uniformes de la señal es una forma fácil de explicar, con frecuencia en la práctica esta separación no es uniforme con objeto de mejorar el comportamiento del sistema al ruido.

La opción mencionada consiste en comprimir la señal en forma no lineal y después aplicar el espaciamiento uniforme a los niveles de la señal ya comprimida. En el receptor la señal es expandida con una característica no lineal inversa y, a este proceso se le conoce como compansión.

Cuantización para un sistema PCM de primer orden.

El número de valores de amplitud disponible está limitado a 256 y éstos son divididos dentro 128 valores positivos y 128 negativos llamados pasos de cuantización. Como se muestra en la figura A.4, un chequeo es hecho para establecer el intervalo de cuantización de cada amplitud de la muestra y entonces se codifica.

Note que los diferentes intervalos de cuantización no son constantes. Entre más alto es el nivel, más grande es el intervalo de cuantización. Esta función ha sido especificada por el CCITT y es conocida como la ley A.

La razón para intervalos de cuantización más cortos para señales pequeñas es que se asegura una mayor exactitud en la reproducción de las señales pequeñas, ya que de otro modo se tendría una distorsión de cuantización alta.

Distorsión de Cuantización.

Debido a que únicamente 256 niveles de cuantización están disponibles, no es posible evitar introducir un cierto grado de errores cuando se cuantiza la señal real.

La diferencia entre la señal real y el nivel de cuantización representa la distorsión de cuantización ver figura A.4.

Codificación.

Un tren de pulsos PCM debe consistir de unos y ceros únicamente, no de pulsos de amplitud variable. Se debe encontrar una forma de convertir los valores de amplitud variable (resultado de la cuantización) en unos y ceros, y para este propósito se introduce el concepto de time-slot. El CCITT ha descrito que cada time-slot debe tener 8 bits, y los diferentes valores dentro de este time-slot son usados para indicar los diferentes valores de amplitud de la muestra.

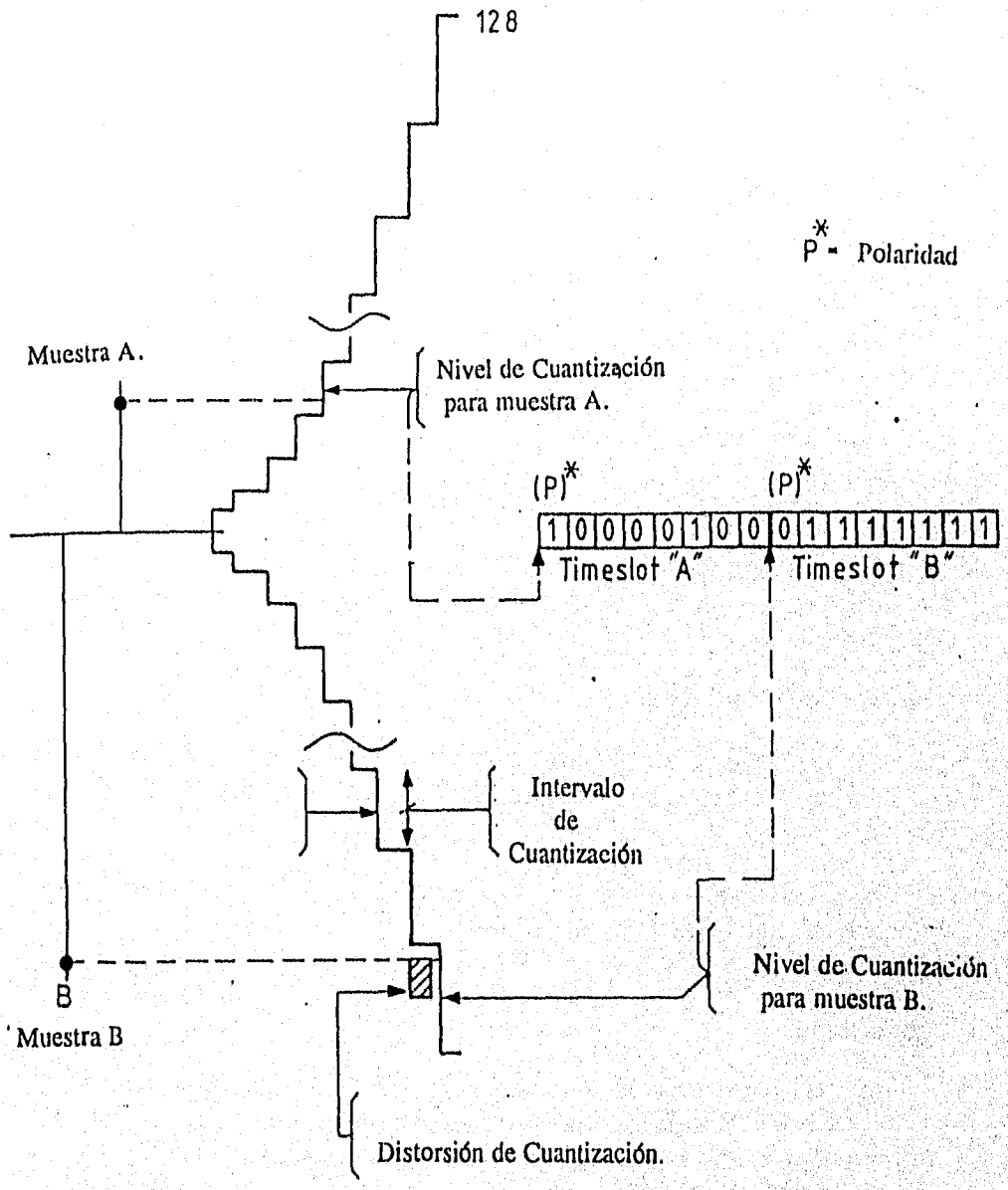


Figura A.4
Nivel de cuantización y Distorsión de cuantización de una señal.

El total de diferentes valores que pueden ser codificados con 8 bits es 256.

Cuando la señal ha sido cuantizada, el valor de los pasos que ésta ocupa en los tiempos de muestreo es trasmitido en forma de códigos binarios. La ley de codificación A usa 13 segmentos, de los cuales 12 tienen cada uno 16 rangos y el primer segmento 64 rangos (dando un total de 256 rangos). Los rangos ocupados son codificados en palabras binarias de 8 bits como se muestra en la figura A.5.

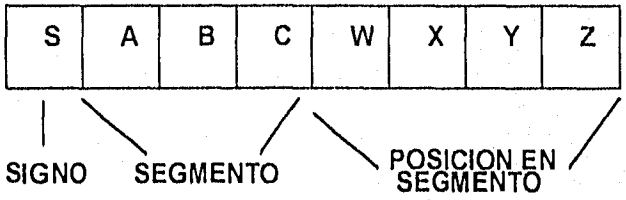


Figura A.5
Forma de codificación de 8 bits de una señal cuantizada.

El primer bit representa el signo del voltaje de entrada, los siguientes 3 bits el número de segmento, y los últimos 4 bits el rango (1 a 16) en el segmento.

Nota: El Segmento 0 y 1, tanto en la parte positiva y negativa forman el segmento 1 (4 segmentos con 16 rangos dando 64 rangos).

Recomendación G.704 del CCITT.

Como se dijo antes, cada canal PCM debe ser muestreado 8000 veces por segundo. En la figura A.6 se muestra donde los 30 canales telefónicos están localizados en los diferentes time slots de 1-15 y de 17 a 31. Puede observarse que existen dos canales extra que son los time-slots 0 y 16.

El time-slot 16 es el canal de señalización y el time-slot 0 es de sincronización. Los canales telefónicos y el canal de señalización (canal 16) pueden usarse para transmisión de datos.

Figura A.6
Localización de los 30 canales telefónicos en una trama de 32 time-slots.

Time-slot 0 (recomendación G.704 del CCITT).

Vamos a asumir que nosotros tenemos un sistema PCM de 4 canales. Los time-slots en la línea serán enviados como se muestran en la figura A.7.

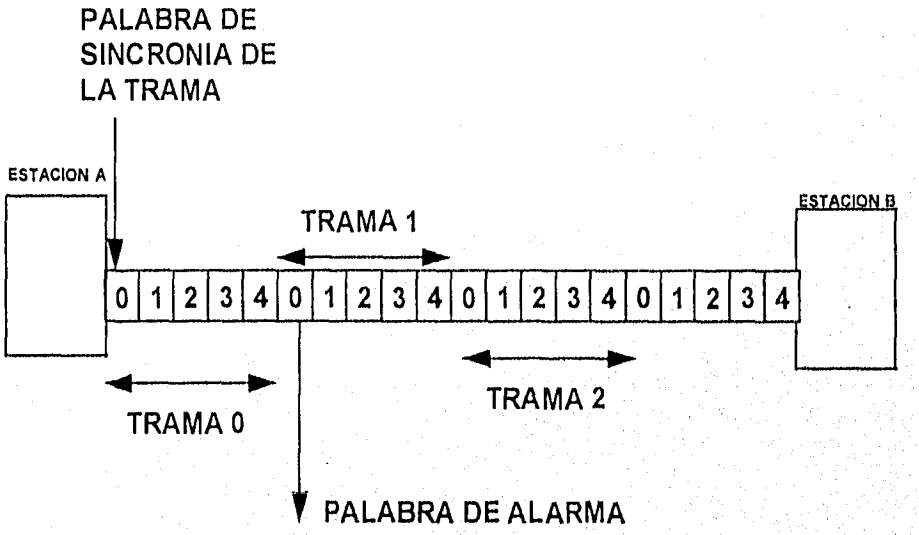


Figura A.7
Sistema PCM de 4 canales que muestra la necesidad de sincronía.

En el lado receptor, la terminal A debe de ser capaz de identificar los time-slots 1,2,3 y 4. La pregunta es: ¿La terminal A puede identificar los time-slots mencionados? La respuesta es No.

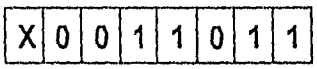
Nosotros podemos ayudar a la terminal A para identificar a los time-slots enviando un time-slot (llamado time slot 0) con un especial patrón de identificación llamado palabra de alineación de trama (palabra de sincronización de trama). La terminal A sabrá que la palabra de alineación de trama es seguida por los diferentes time-slots en orden consecutivo.

La secuencia que comienza con el time-slot 0 y finaliza con el time-slot 31 en un sistema PCM de 32 canales, es llamado una trama.

Considerando que cada canal es muestreado 8000 veces en un segundo, el tiempo para un trama será 1/8000 seg. o 125 microsegundos.

El patrón de bits de la palabra de alineación de trama es siempre como se muestra en la figura A.8.

CANAL 0



X=1 Si no es usado para CRC o internacionalmente.

10011011 Palabra de alineación de trama.
(Tramas pares)

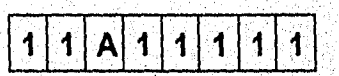
Figura A.8
Patrón de bits de la palabra de alineación de trama en time slot 0.

Sin embargo, la terminal A únicamente necesita recibir la palabra de alineación de trama en cada segunda trama, y por lo tanto la palabra es únicamente enviada en números de trama pares (tramas 0,2,4,6 etc.).

Palabra de Alarma.

El time-slot 0 de los números de trama impares (tramas 1,3,5,etc) se usa para enviar la palabra de alarma. En algunos casos información acerca de situaciones de falla es enviada entre dos terminales por medio de los bits en la palabra de alarma (Ver figura A.9).

CANAL 0



A=ALARMA DE TRAMA DISTANTE

11111111 SIN SEÑAL DE ALINEACIÓN DE TRAMA.
(TRAMAS IMPARES)

Figura A.9
Patrón de bits de la palabra de alarma en el time slot 0 de tramas impares.

Multitrama (recomendación G.704 del CCITT).

Una multitrama consiste de 16 tramas numeradas de 0 a 15 (Ver figura A.10).

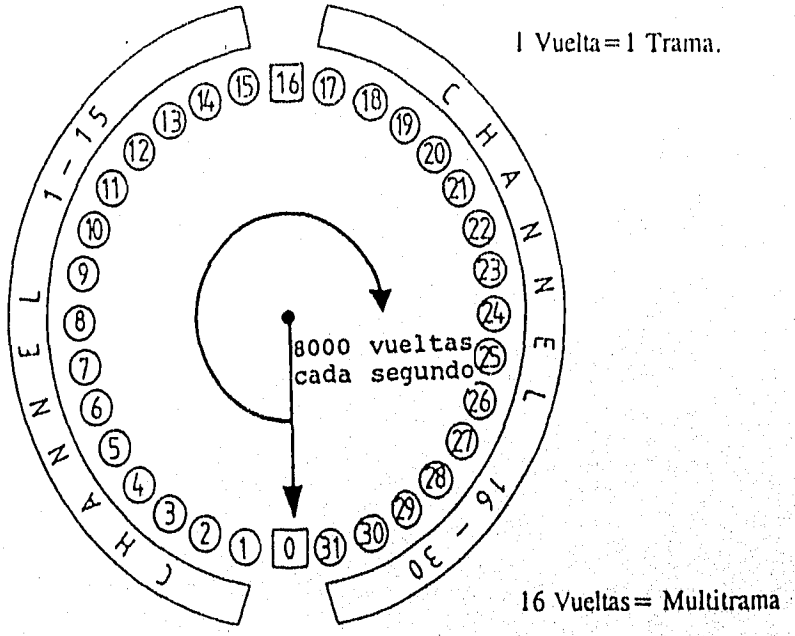


Figura A.10
Diagrama que muestra 16 vueltas de 32 canales formando una multitrama.

La multitrama es necesaria para la señalización por canal asociado en el time slot 16. El CCITT ha precisado que cada vez que se envía el time slot 16 (en cada trama), debe contener información de señalización para 2 canales telefónicos (Ver figura A.11).

CANAL 16

0	0	0	0	1	1	1	1

Figura A.11
Información de señalización para canales telefónicos en el canal 16 de cada trama.

Una secuencia de 15 tramas será requerida para transmitir información de señalización para 30 canales telefónicos por medio del procedimiento anterior.

Esta secuencia en realidad comienza por el envío de la palabra de alineación multitrama en el time-slot 16 de la primera trama. La primera trama es seguida por 15 tramas conduciendo señalización para los 30 canales. La secuencia de 16 tramas es llamada una multitrama. Las tramas en la multitrama son numeradas de 0 a 15 (Ver figura A.12).

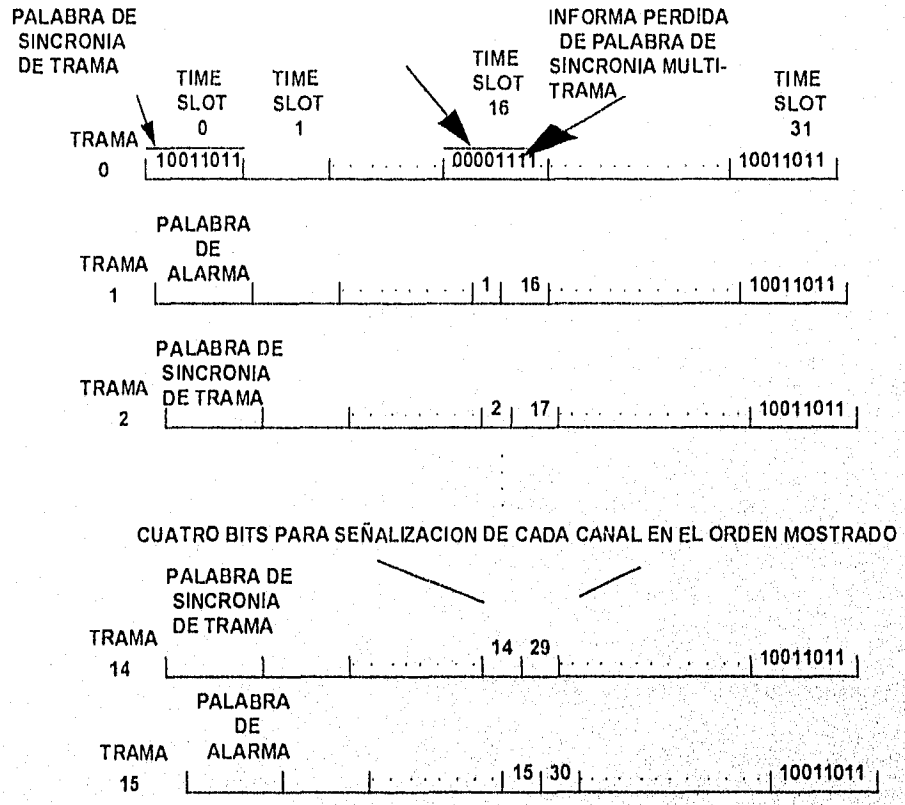


Figura A.12.
Tramas 0 a 15 formando una multitrama).

El propósito de la palabra de alineación multitrama es ayudar al receptor a identificar las diferentes tramas en la multitrama.

En el time-slot 16 de la trama 0 se tienen 8 bits disponibles de los cuales 4 son suficientes para el patrón de alineación multitrama. Este patrón consiste de 4 ceros.
Los 4 bits restantes pueden ser usados para indicar la causa de la falla indicada por la palabra de alarma en el time-slot 0 (Ver figura A.13).

CANAL 16

0	0	0	0	X	A	X	X

X=Bit de servicio no usado y establecido a 1.

A=Alarma multitrama (Pérdida de alineación multitrama)
00001011 Operación normal.
00001111 Alarma
(Trama 0 de una multitrama)

Figura A.13
Palabra de alineación multitrama en el time slot 16 de la trama 0

Adaptación de PCM a la línea.

Después de la codificación en el proceso de conversión de una señal analógica a digital se obtiene un tren de pulsos llamado tren de bits unipolares, lo cual indica que un uno es representado por una amplitud positiva de 488 nanosegundos. Este tren de pulsos no es conveniente para transmisión. La razón de la inconveniencia es que los regeneradores no distinguen los bits en un tren de pulsos unipolar, parte por que dos pulsos consecutivos son combinados para formar un pulso más ancho y parte por que un tren de pulsos de este tipo contiene una componente de corriente directa que impide el trabajo de los regeneradores.

El tren de pulsos unipolar debe entonces ser convertido a un tren de pulsos bipolar, además cada "pulso" uno debe ser convertido a un código de retorno a cero.
Un tren de pulsos bipolar significa que los "unos" son enviados en forma de pulsos positivos y negativos alternativamente. El código de retorno a cero significa que los unos son convertidos a pulsos con amplitud durante 244 nanosegundos y permanencia en cero otros 244 nanosegundos.

Los regeneradores no aceptan muchos ceros consecutivos en un tren de pulsos debido a que ellos toman el reloj de la señal entrante. El CCITT por lo tanto reglamenta que si un PCM envía más de tres ceros consecutivos, falsos "unos" deben ser insertados en el tren de pulsos, y esto se logra con la utilización de un código llamado HDB3 (Ver figura A.14).

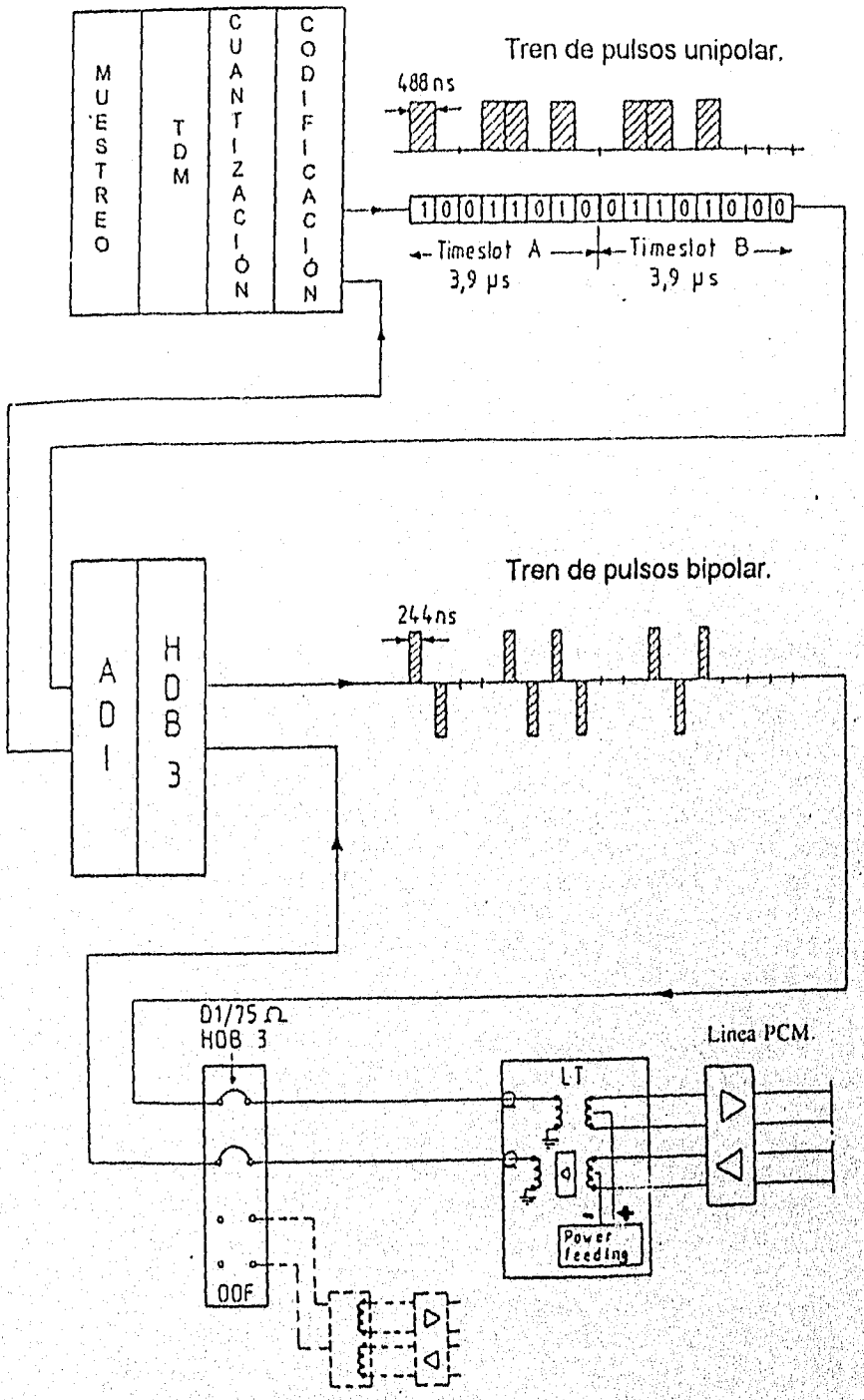


Figura A.14.
Adaptación de PCM a la línea.

Código HDB3 (Recomendación G.703 del CCITT).

Código bipolar que elimina secuencias de 4 ceros consecutivos.

Este código debe cumplir con las siguientes reglas :

- Regla de bipolaridad: Los bits 1's se codifican alternativamente como +1 y -1, con RZ a la mitad del periodo de cada bit. Cuando 2 sucesivos 1's tienen la misma polaridad, esto corresponde a una violación de la regla de polaridad.

- No debe de haber más de tres 0's consecutivos. Para lograr esto, el cuarto "0" es reemplazado por un "1". Para detectar esta sustitución y borrar los falsos 1's en la recepción, éstos son enviados como violaciones de la regla de bipolaridad.

- Violaciones sucesivas deben de ser de polaridad opuesta. Cuando el número de 1's entre dos violaciones no es impar un bit packing en "1" es agregado en lugar del primer bit "0" (Ver figura A.15).

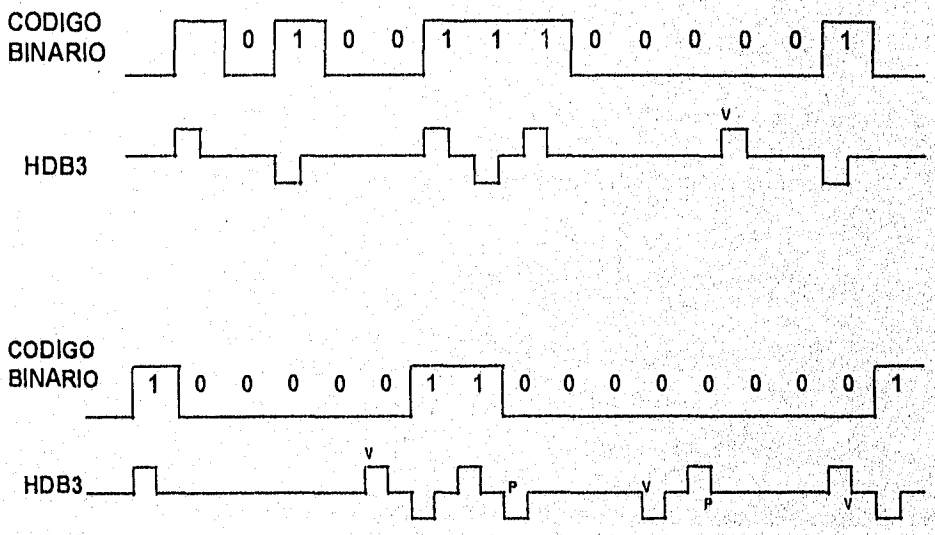


Figura A.15.
Código HDB3.

Especificación G.821 del CCITT.

Análisis de la calidad de un sistema digital por medio de la evaluación de la tasa de error.

Es importante contar con los elementos necesarios para garantizar la calidad que debe tener la red de comunicaciones que permita la transmisión de información en forma rápida y confiable.

Un criterio que define si un sistema digital será o no confiable está establecido por el CCITT por medio de la evaluación de la tasa de errores de estos sistemas.

La Recomendación G.821 establece las condiciones de tasa de error (BER) que deben cumplir los sistemas digitales para garantizar la calidad necesaria en las señales transmitidas.

Para establecer los criterios de evaluación, la recomendación G.821 establece tres términos en cuanto a la cantidad de errores que se generan durante la operación del sistema de comunicaciones: Segundos con error (ES), Segundos severamente errados (SES) y Minutos degradados (DM) que se definen a continuación:

Segundo con Error (ES).

Intervalo de tiempo de un segundo en el que se presenta cuando menos un error.

Segundo Severamente Errado (SES).

Intervalo de tiempo de un segundo que presenta una tasa de error mayor a diez a la menos tres.

Minuto Degradado (DM).

Intervalo de tiempo de un minuto que presenta una tasa de errores mayor a diez a la menos seis.

La condición que establece si el sistema está acorde con la recomendación es el número de veces durante el intervalo de medición que cada una de las condiciones anteriores se presentan, éstas condiciones son:

Segundos con Error: Menos del 8% de los intervalos de un segundo.

Segundos Severamente Errados: Menos del 0.2% de los intervalos de un segundo.

Minutos Degradados: Menos del 10% de los intervalos de un minuto.

Tiempo Disponible e Indisponible.

Durante la medición es posible que se presenten condiciones extremas que provoquen una degradación demasiado alta del enlace, sin que necesariamente los componentes del mismo no tengan la calidad suficiente. A estos intervalos de tiempo se les conoce como periodos de tiempo indisponible y están definidos por la recomendación G.821 como aquellos intervalos que durante 10 segundos consecutivos presentan una tasa de error peor que diez a la menos tres en cada segundo.
El tiempo indisponible deberá restarse del tiempo disponible para hacer la evaluación de los ES, SES y DM.

Determinación de los ES, SES y DM.

El CCITT recomienda que las mediciones de los tres parámetros se lleve a cabo durante un periodo de un mes, cualquier falla en el cumplimiento de los objetivos de calidad para cada uno de los tres objetivos implica que el sistema no está acorde con la recomendación.

Para determinar los segundos errados, el criterio que se aplica es el siguiente: dado que la prueba se está aplicando sobre canales digitales a 64 kbit/s, entonces una tasa de error de 10 a la menos tres quiere decir que durante un segundo ocurrieron 64 errores 64/64000=10 a la menos tres).
En el caso de los minutos degradados, el CCITT establece el límite de tasa de error de 10 a la menos seis. Dado que el intervalo de tiempo es un minuto y la velocidad de transmisión de 64 kbit/s, entonces esa tasa de error equivale a un total de 3.84 errores. Como los resultados deben redondearse al entero superior, esto nos da un total de 4 errores durante un minuto para que se le considere un minuto degradado.

Metodología para determinar la calidad de un sistema digital:

1) Monitorear el enlace durante el intervalo de tiempo especificado en un intervalo de medición de cuando menos un minuto, repetitivamente, Stot.

2) Contar los intervalos de tiempo indisponibles, es decir los segundos en que ocurrieron más de 64 errores durante 10 segundos consecutivos. Restar éstos de Stot para obtener Sdisp.

Sdisp=Stot-Sindis, y Mdisp=Sdisp/60

3) Dentro de Sdisp, contar el número de segundos que presentaron un error o más, éstos nos dan los segundos con error.
4) Dentro de Sdisp contar el número de intervalos de un segundo que presentaron más de 64 errores, éstos son los segundos severamente errados.

5) Restar SES de Sdisp y agrupar los intervalos restantes en grupos de 60, contando el número de grupos que tienen más de 4 errores, éstos son los minutos degradados. Se concluye la prueba determinando si se cumple con los objetivos de calidad expresados anteriormente.

Segundos disponibles=Segundos totales menos Segundos indisponibles.

$S_{disp} = S_{tot} - S_{indisp}$

S_{indisp}=periodos con más de 64 errores en un segundo para 10 segundos consecutivos.

Segundos disponibles=Segundos con error más Segundos severamente errados.

$S_{disp} = S_{error} + S_{severra}$

S_{error}=segundos con 1 hasta 64 errores.

$S_{severra}$=segundos con más de 64 errores 64/64000= tasa de error 10^{-3}

$S_{error/60}$=Minutos degradados.

Si Minutos degradados $\geq$ 4 La tasa de error es de 10^{-6}

ENLACES DS0

Un enlace DS0 es un enlace a 64 Kbps que se utiliza para dar servicio a los lugares remotos que no cuentan con la infraestructura de nodos digitales RDI.

Un enlace DS0 se encuentra compuesto por un enlace digital E0 del un nodo RDI-1 (donde se encuentra la punta A) a otro nodo RDI-2 y por un enlace con una línea privada a 2 hilos de un multiplexor digital en el nodo RDI-2 al lugar a conectar denominado punta B como lo muestra la figura 5.5.

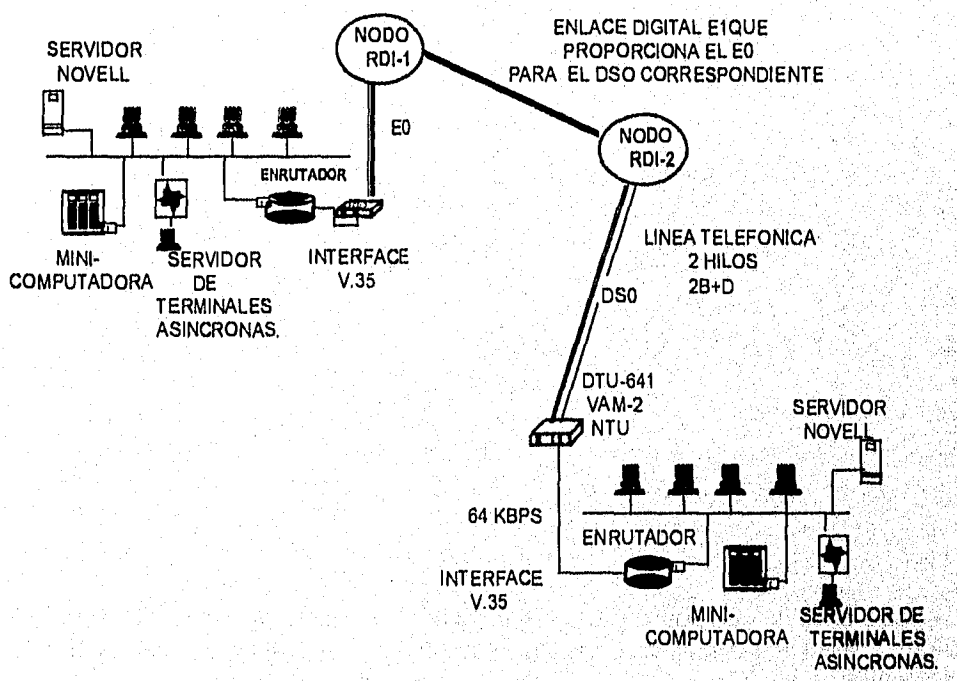


Figura 5.5
El servicio DS0 de 64 kbps.

En el lugar denominado punta B, se remata la línea privada a un equipo de comunicaciones DSU que puede ser un equipo DTU-641 de AT&T, un equipo VAM-2 de Alcatel, o un equipo de cualquier otra marca como Tellabs.

La interface en el equipo DSU puede ser V-35, X.21 o RS232 DCE.

En el caso de la VAM-2 de Alcatel se tienen señales de V.35 alambradas en un conector DB-25 y es necesario por lo tanto hacer un cable convertidor con conector Winchester de 34 pines hembra en un extremo y un conector DB25 macho en el otro (Ver tabla 1 de relación de pines).

Conector Winchester	Conector DB-25	Señal
A	1	FGND
B	13	SGND
C	4	RTS
D	16	CTS
E	5	DSR
F	6	DCD
H	10	DTR
P	2	TxD+
R	3	RxD+
S	14	TxD-
T	15	RxD-
U	7	SCTE+
V	9	SCR+
W	19	SCTE-
X	21	SCR-
Y	8	SCT+
AA	20	SCT-

Tabla 1.

La línea privada utilizada para estos enlaces a 64 Kbps debe cumplir con las características siguientes para garantizarse su funcionamiento del nodo RDI-2 a la punta B.

1) Longitud de la línea debe ser menor o igual a 3 KM.

2) El calibre de la línea deberá de ser de 0.4 mm.

Se puede incrementar la longitud de la línea a 3.5 Km aprox. con un calibre de 0.5 mm pero cumpliendose el punto 3.

Se puede incrementar la longitud de la línea a 4.0 Km aprox. con un calibre de 0.64 mm pero cumpliéndose el punto 3.

3) La atenuación permisible debe ser de 0 a 30 DB a 120 KHZ o un equivalente haciendo una prueba con patrones digitales de un equipo de medición y obtener un BER < 1 x 10 a la menos 7.

Para probar este tipo de enlace se tienen dos variantes:

1) Es necesario conectar un equipo de medición de tasa de error al DSU que se tenga y hacer un loop en el extremo remoto con un barrilito BNC o con ayuda de RDI en el DACS.

2) Para el caso del DTU-641 se tiene un botón que permite hacer un loop en el equipo y el enlace se puede probar conectando el PFA-30 en los cables coaxiales del E0 en la parte digital.

Una variante del enlace a 64 Kbps es el que se puede hacer con dos DTU-641 conectados espalda con espalda mediante una línea privada de 2 hilos. En este esquema ya no se tienen los nodos RDI y el enlace no puede ser supervisado.

APENDICE B

INTERFACES.

En el nivel físico de cualquier sistema de comunicaciones la interface entre el DTE y el DCE debe estar definida en términos de atributos físicos y lógicos.

Estos atributos son:

- Dimensiones y Construcción del conector.
- Número de pines en el conector.
- Señales eléctricas en los pines.
- Significado de las señales eléctricas en cada pin.
- Interrelación entre señales.
- Procedimientos de intercambio de información entre el DTE y el DCE.

El CCITT ha introducido un número de estándares cubriendo el área de interfaces DTE-DCE, con recomendaciones separadas para las diferentes características de una interface. Así cualquier interface puede ser definida por la combinación de un número de estándares. En la parte central del sistema de estándares de interface CCITT está la recomendación V.24 la cual define todos los circuitos de interface y sus funciones.

La recomendación V.24 define 55 circuitos. Sin embargo, ninguna conexión usará todos los posibles circuitos y cualquier implementación de interface incluirá únicamente aquellos circuitos que requiera.

Cada circuito es identificado por un número de tres dígitos. Un conjunto de circuitos con números en el rango de 100 a 199 contiene circuitos asociados con control, temporización y datos mientras que otro conjunto con números en el rango de 200 a 299 contiene circuitos usados para llamada automática.

Interface V.24.

Circuitos de la interface V.24.

Circuitos de temporización.

Los circuitos de temporización conducen señales que son usadas para mantener un velocidad de transmisión. Un circuito de temporización es encendido y apagado en periodos iguales de tiempo y éste proporciona una referencia para las señales siendo conducidas en los circuitos de datos. La transición de alto a bajo del circuito de temporización debe coincidir con el

centro de cada bit de la señal de datos y la transición de bajo a alto con el límite entre los bits de datos.

El reloj que proporciona la señal de temporización de transmisión puede estar en el DTE o en el DCE. La temporización de recepción es siempre tomada del módem.

Circuitos de canal Backward.

Los circuitos de canal Backward (118-123) son equivalentes a algunos de los circuitos de canal Forward (103-106,109 y 110), pero se usan cuando los enlaces proporcionan canales secundarios de baja velocidad en la misma línea, Circuitos de temporización no son necesarios debido a que la transmisión es asíncrona.

Circuitos de llamada automática.

Donde se implementa llamada automática (recomendación CCITT V.25 y EIA RS366), circuitos de intercambio separados se implementan para el establecimiento de la llamada.

La unidad de llamada automática convierte los dígitos del número a ser marcado a tonos o pulsos y los envía por la línea, una vez que se obtiene comunicación, el módem envía una señal llamante y espera por un tono de contestación antes de conectar el DTE a la línea.

Aparte de los circuitos de control hay 4 circuitos, operando en paralelo, que se usan para pasar los dígitos a través del DTE a la unidad llamante.

Circuitos de prueba.

Los circuitos de prueba son usados en la operación de procedimientos de loopback como se define en la recomendación V.54.

Cuatro loops son definidos y sus funciones son como sigue:

Loop 1 se usa como una prueba básica en el DTE regresando las señales transmitidas al DTE.

Loop 2 permite un chequeo de la línea hasta el DCE remoto.

Loop 3 Es usado para checar el trabajo del DCE local.

Loop 4 está diseñado para checar la operación de líneas de 4 hilos.

El control de loops puede ser manual o automático. En ambos casos el circuito es establecido a alto para indicar que el loop 2,3, o 4 ha sido establecido.

La tabla siguiente muestra los diferentes circuitos **V.24**, su nombre, la dirección de la señal en el circuito y su tipo.

101		Protective Ground	
102		Signal Ground	
102a		DTE Common Return	
102b		DCE Common Return	
102c	Common Return.		
103	Transmitted Data.	DTE A DCE	DATOS
104	Received Data.	DCE A DTE	DATOS
105	Request to Send.	DTE A DCE	CONTROL
106	Ready for Sending.	DCE A DTE	CONTROL
107	Data Set Ready.	DCE A DTE	CONTROL
108/1	Connect Data Set to Line.	DTE A DCE	CONTROL
108/2	Data Terminal Ready.	DTE A DCE	CONTROL
109	Data Channel Received Line Signal Detector.	DCE A DTE	CONTROL
110	Data Signal Quality Detector.	DCE A DTE	CONTROL
111	Data Signal Rate Selector (DTE).	DTE A DCE	CONTROL
112	Data Signal Rate Selector (DCE).	DCE A DTE	CONTROL
113	Transmitter Signal Element Timing (DTE).	DTE A DCE	TEMPORIZACION
114	Transmitter Signal Element Timing (DCE).	DCE A DTE	TEMPORIZACION
115	Receiver Signal Element Timing (DCE).	DCE A DTE	TEMPORIZACION
116	Select Standby.	DTE A DCE	CONTROL
117	Stanby Indicator.	DCE A DTE	CONTROL
118	Transmitted Backward Channel Data.	DTE A DCE	DATOS
119	Received Backward Channel Data.	DCE A DTE	DATOS
120	Transmitted Backward Channel line Signal.	DTE A DCE	CONTROL
121	Backward Channel Ready.	DCE A DTE	CONTROL
122	Backward Channel Received line Signal Detector.	DCE A DTE	CONTROL
123	Backward Channel Signal Quality Detector.	DCE A DTE	CONTROL

124	Select Frecuency Groups.	DTE A DCE	CONTROL
125	Calling Indicator.	DCE A DTE	CONTROL
126	Select Transmit Frecuency.	DTE A DCE	CONTROL
127	Select Receive Frecuency.	DTE A DCE	CONTROL
128	Receiver Signal Element Timing (DTE).	DTE A DCE	TEMPORIZACION
129	Request to Receive.	DTE A DCE	CONTROL
130	Transmit Backward Tone.	DTE A DCE	CONTROL
131	Received Character Timing.	DCE A DTE	TEMPORIZACION
132	Return to non Data Mode.	DTE A DCE	CONTROL
133	Ready for Receiving.	DTE A DCE	CONTROL
134	Received Data Present.	DCE A DTE	CONTROL
136	New Signal.	DTE A DCE	CONTROL
140	LoopBack/Maitenance Test.	DTE A DCE	CONTROL
141	Local Loopback.	DTE A DCE	CONTROL
142	Test Indicator.	DCE A DTE	CONTROL
191	Transmitted Voice Answer.	DTE A DCE	CONTROL
192	Received Voice Answer	DCE A DTE	CONTROL
201	Signal Ground.		AUTOLLAMADA
202	Call Request.	DTE A DCE	AUTOLLAMADA
203	Data Line Occupied.	DCE A DTE	AUTOLLAMADA
204	Distant Station Connected.	DCE A DTE	AUTOLLAMADA
205	Abandon Call.	DCE A DTE	AUTOLLAMADA
206	Digit Signal.	DTE A DCE	AUTOLLAMADA
207	Digit Signal.	DTE A DCE	AUTOLLAMADA
208	Digit Signal.	DTE A DCE	AUTOLLAMADA
209	Digit Signal.	DTE A DCE	AUTOLLAMADA
210	Present Next Digit.	DCE A DTE	AUTOLLAMADA
211	Digit Present.	DTE A DCE	AUTOLLAMADA
213	Power Indication.	DCE A DTE	AUTOLLAMADA

V.28 (RS232).

La recomendación V.28 cubre circuitos desbalanceados y se aplica a velocidades de datos de hasta 20 Kbps. Típicamente los voltajes utilizados para indicar las condiciones de encendido y apagado son +/- 12 Volts aunque cualquier valor entre +\-3 y +\- 15 Volts puede usarse.

El estándar EIA RS232 incluye características eléctricas idénticas.

V.35 (ISO 2593)

La recomendación V.35 se aplica a transmisión de datos de 48 Kbps a 4 Mbps e incluye características eléctricas para circuitos balanceados. La diferencia entre los voltajes en los hilos A y B se especifica como +/- 0.55 Volts.

V.10 (X.26, RS423).

La recomendación V.10 especifica características eléctricas para circuitos desbalanceados operando a velocidades hasta de 100 Kbps. Esta usa voltajes entre +/-3 y +/-6 Volts para indicar las condiciones de encendido y apagado.
El EIA RS423 es el equivalente de la V.10 y la recomendación X.26 del CCITT especifica las mismas características eléctricas para interfaces de redes de datos públicas.

V.11 (X.27, RS422).

La recomendación V.11 especifica características eléctricas para circuitos balanceados operando a velocidades hasta de 10 Mbps. La diferencia entre los voltajes en los hilos A y B se especifica como +/- 0.3 con un voltaje máximo en los hilos de 6 volts.

El estándar EIA RS422 es el equivalente de **V.11** y la recomendación del CCITT X.27 especifica las mismas características eléctricas para interfaces de redes de datos públicas.

Una variedad de conectores son usados para las interfaces **V.24**, dependiendo del particular tipo de interface y de sus características eléctricas.

Asignación circuitos en conector de 25 pines para interfaces **V.28** (RS232).

Circuito V.24	**Numero de Pin**
Cable screen/101	1
102	7
103	2
104	3
105	4
106	5
107	6
108	20
109	8
110	21 **Para RS232C**
111/112	23 **Para RS232C y EIA232 D**
113	24
114	15
115	17
118	14
119	16
120	19
121	13

122	12 Para RS232C
122/112	12 Para EIA232D
125	22
126	11 No usado fuera de V.24.
140/110	21 Para EIA232 D
141	18 Para EIA232 D
142	25 Para EIA 232D

La interface V.35 requiere un conector cuadrado (Winchester de 34 pines).

Nombre del circuito	Identificador de Pin
Cable Screen	A
102	B
103	P CON S
104	R CON T
105	C
106	D
107	E
108	H
109	F
113	U CON W
114	Y CON AA
115	V CON X
125	J
-	HH(CONTROL DE RELOJ Tx)

	A		B
C		D	
	E		F
H		J	
	K		L
M		N	
	P		R
S		T	
	U		V
W		X	
	Y		Z
AA		BB	
	CC		DD
EE		FF	
	HH		JJ
KK		LL	
	MM		NN

Conector de 34 pines Cuadrado (Winchester)

La interface RS449 y sus estándares asociados RS422 (V.11) y RS423 (V.10) requiere de dos conectores tipo D uno de 37 pines y otro de 9 pines.

Conector de 37 pines.

Número y nombre del circuito		Identificador de pin
102	Signal Ground or common return.	19
102a	DTE common return.	37
102b	DCE common return.	20
103	Transmitted Data.	4 y 22
104	Received Data.	6 y 24
105	Request to Send.	7 y 25
106	Ready for sending.	9 y 27
107	Data Set Ready.	11 y 29
108	Connect Data Set to Line/Data Terminal Ready.	12 y 30
109	Data Channel Received Line Signal Detector.	13 y 31
110	Data Signal Quality Detector.	33
111	Data Signal Rate Selector (DTE).	16
112	Data Signal Rate Selector (DCE).	2
113	Transmitter Signal Element Timing (DTE).	17 y 35
114	Transmitter Signal Element Timing (DCE).	5 y 23
115	Receiver Signal Element Timing (DCE).	8 y 26
116	Select Standby.	32
117	Stanby Indicator.	36
125	Calling Indicator.	15
126	Select Transmit Frecuency.	16
135	Terminal Available for Service.	28
136	New Signal.	34
140	LoopBack/Maitenance Test.	14
141	Local Loopback.	10
142	Test Indicator.	18

Conector de 9 pines.

Número y nombre del circuito		Identificador de pin
102	Signal Ground or common return.	5
102a	DTE common return.	9
102b	DCE common return.	6
118	Transmitted Backward Channel Data.	3
119	Received Backward Channel Data	4
120	Transmitted Backward Channel line Signal	7

121	Backward Channel Ready.	8
122	Backward Channel Received.	
	line signal Detector	2
	Cable screen.	1

EIA-530

Es una especificación eléctricamente compatible con RS449 sobre un conector tipo D de 25 pines como el de la interface RS232.

Número de pin y descripción.

1 SHIELD	
2 Tx (A)	DTE
3 Rx(A)	DCE
4 RTS (A)	DTE
5 CTS (A)	DCE
6 DCE READY (A)	DCE
7 SIGNAL GROUND	
8 RECEIVED LINE SIGNAL DETECTOR (A)	DCE
9 RECEIVER SIGNAL ELEMENT TIMING (B)	
10 RECEIVED LINE SIGNAL DETECTOR (B)	
11 EXT. TRANSMIT SIGNAL ELEMENT TIMING (B)	
12 TRANSMIT SIGNAL ELEMENT TIMING (B)	
13 CTS (B)	
14 Tx (B)	
15 TRANSMIT SIGNAL ELEMENT TIMING (A)	DCE
16 Rx(B)	
17 RECEIVER SIGNAL ELEMENT TIMING (A)	DCE
18 LOCAL LOOPBACK	DTE
19 RTS (B)	
20 DTE READY (A)	DTE
21 REMOTE LOOPBACK	DTE
22 DCE READY (B)	
23 DTE READY (B)	
24 EXT. TRANSMIT SIGNAL ELEMENT TIMING (A)	DTE
25 TEST MODE	DCE

GLOSARIO

10BASE5 Especificación de capa física (physical layer) de banda base (baseband) IEEE 802.3 similar a Ethernet, que emplea cable coaxial grueso y que funciona a 10 Mbps.

10BROAD36 Especificación de banda amplia (broadband) IEEE 802.3 que emplea cable coaxial grueso y que funciona a 10 Mbps.

10BASET Especificación IEEE 802.3 que emplea cable de par torcido (twisted pair) simple y que funciona a 10 Mbps.

ABM Modo balanceado asíncrono (Asynchronous Balanced Mode). Modo de comunicación HDLC (y su protocolo derivado) que maneja comunicaciones de punto a punto entre nodos equivalentes (peer) para dos estaciones, en donde cualquiera de ellas puede iniciar la transmisión.

ACK respuesta enviada por el receptor al transmisor para indicar recepción de datos con éxito y significa reconocimiento.

AIS Señal de alarma (Alarm Indication Signal). En un E1 es una señal de bits en uno que se transmite en lugar de la señal normal para mantener continuidad en la transmisión e indicar al equipo de recepción que hubo una falla de transmisión localizada en, o antes de, el equipo de transmisión.

A-Law Ley A. Estándar de compresión y expansión (companding) empleado por CCITT para la conversión entre señales analógicas y digitales en sistemas PCM. Se usa más bien en redes telefónicas europeas y es similar al estándar norteamericano (ley μ). En México se usa la ley A.

ARM Modo de respuesta asíncrono (Asynchronous Response Mode). Modo de comunicación HDLC con una estación primaria y al menos un estación secundaria.

ARP Protocolo de resolución dirección (Address Resolution Protocol). Protocolo Internet usado para ligar una dirección IP a direcciones Ethernet/802.3. Está definido en el documento RFC 826.

ARPANET Red pionera de conmutación de paquetes (packet switching desarrollado a inicio de los años 70 por la empresa BBN y financiada por la agencia ARPA (luego DARPA). ARPANET se convirtió luego en 'Internet'. El término ARPANET desapareció oficialmente en 1990.

ARQ Solicitud automática de repetición (Automatic Repeat Request). Técnica de comunicaciones en la cual el receptor detecta errores y solicita retransmisiones.

ATM Modo de transferencia asíncrono (Asynchronous Transfer Mode). Estándar CCITT para transmisión de celdas (Cell relay) en la cual la información para diferentes tipos de servicios (voz, vídeo, datos) se transmite en pequeñas celdas de tamaño fijo. También, modo de transmisión B-ISDN en el cual una versión acelerada del multiplexaje por división de tiempo asíncrono (ATDM) para transferir flujos múltiples de información en un canal de comunicación.

AUI Interface de unidad de conexión (Attachment Unit Interface). Cable IEEE 802.3 que conecta la unidad de acceso al medio (MAU: Media Access Unit) al dispositivo en red. El término AUI también puede usarse para referirse al conector de 15 pines de cualquier equipo de redes.

BERT Dispositivo para prueba de tasa de errores de bits (Bit Error Rate Tester Device). Determina la tasa de error de bits en un canal de comunicaciones.

BNC connector Conector estándar empleado para ligar el cable coaxial IEEE802.3 10BASE2 a un receptor o transmisor.

Bridge Puente. Dispositivo que conecta dos segmentos de una red y pasa tramas con información entre ellos. Los puentes operan en el nivel 2 del modelo de referencia OSI (capa de enlace de datos: link layer) y no son sensibles a los protocolos de niveles superiores.

Buffer. Zona temporal de almacenamiento empleada para el manejo de datos transitorios. Los buffers suelen emplearse para compensar las diferencias de velocidad de procesamiento entre dispositivos de una red. Las emisiones rápidas de datos se almacenan en un buffer hasta que los pueda procesar el dispositivo receptor que funciona más lentamente.

Circuit switching Circuitos conmutados. Sistema de conmutación en el que debe existir un circuito físico dedicado entre el emisor y el receptor durante la llamada. De amplio uso en la red telefónica, los circuitos conmutados se contrastan con los métodos de competencia (contention) y token passing para acceso al canal, y con la conmutación de paquetes (packet switching) como técnica de conmutación.

Communication controller Controlador de comunicaciones. En SNA, nodo de subárea que contiene un programa NCP. Normalmente es un dispositivo IBM 3745.

CRC Cyclic Redundancy Check: Chequeo de redundancia cíclica. Técnica de verificación de errores en la cual el receptor de la trama (frame) calcula el residuo de dividir el contenido de la trama entre un divisor binario primo (a lo cual a veces también se llama CRC) y lo compara con el valor previamente calculado que el nodo emisor almacenó en la misma trama.

CSMA/CD Acceso múltiple con detección de portadora y detección de colisiones (Carrier Sense Multiple Access With Collision Detection) . Mecanismo de acceso al canal en el cual los dispositivos que desean transmitir primero verifican la existencia de portadora en el canal. Si no se detecta portadora en un cierto lapso de tiempo, los dispositivos pueden transmitir. Si dos de ellos transmiten a la vez, ocurre una colisión, que es detectada por dispositivos especiales, que entonces retardan la transmisión durante un periodo aleatorio. El acceso CSMA/CD es empleado por Ethernet y por IEEE 802.3.

Datagram Datagrama. Agrupamiento lógico de información enviada como unidad de datos de la capa de red (network layer) en medio de una transmisión, sin establecimiento previo de un circuito virtual. Los términos paquete, trama, segmento y mensaje también se emplean para describir agrupaciones lógicas de información en varios niveles del modelo de referencia OSI y en otras áreas de la tecnología.

Los datagramas IP son las unidades primarias de información en Internet.

Differential Manchester encoding Codificación Diferencial Manchester. Esquema de codificación digital en el que se emplea una transición durante el bit para señal de reloj, y donde una transición al inicio del tiempo de cada bit denota un cero. Es el esquema de codificación empleado por las redes IEEE 802.5/Token Ring.

Dijkstra's algorithm algoritmo de Dijkstra. Algoritmo de enrutamiento de trayectoria mínima que itera sobre la longitud del camino para determinar el árbol de expansión (spanning tree) de trayectoria mínima. Es de uso común en los algoritmos de enrutamiento de estado de enlace.

EBCDIC Código extendido de intercambio decimal codificado en binario. (Extended Binary Coded decimal Interchange Code): Código de caracteres de 8 bits desarrollado por IBM para representación de datos en sus grandes sistemas de computo.

Encapsular Técnica usada por protocolos de capas, donde un protocolo de capal baja acepta un mensaje de información de un protocolo de capa alta y coloca éste en la porción de datos de la unidad de información manejada.

Ethernet Especificación de red LAN de banda base inventada por la corporación Xerox y desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet operan a 10 Megabits por segundo utilizando CSMA/CD sobre cable coaxial. Es similar a una serie de estándares producidos por IEEE y conocidos como IEEE 802.3.

EtherTalk Red con protocolos Apple Talk que funciona en Ethernet.

FCS Secuencia de verificación de trama (Frame Check Sequence). Término HDLC adoptado por los protocolos de enlace de datos y que se refiere a los caracteres extra que se añaden a la trama para propósitos de control de errores.

FDM Multiplexaje por división de frecuencia (Frecuency Division Multiplexing). Técnica en la que en un sólo cable se le puede asignar a la información de múltiples canales un ancho de banda basado en la frecuencia.

FOIRL Enlace Inter-Repetidor de fibra óptica (Fiber-Optic Inter-Repeater Link): Metodología de señalización de fibra óptica basada en la especificación de fibra óptica IEEE 802.3.

Frame Trama. Agrupamiento lógico de información enviado a un medio de transmisión como una unidad de la capa de enlace (link layer). Los términos paquete, datagrama, segmento y mensaje también se emplean para describir agrupamientos lógicos de información en varias capas del modelo de referencia OSI y en círculos técnicos.

G.703 Especificación eléctrica y mecánica CCITT para conexiones entre equipo de telecomunicaciones y DTE´s, usando sistemas de transmisión digital.

Hardware address. Dirección de hardware. También conocida como dirección física o MAC- address.

HDLC Control de enlace de datos de alto nivel (High-level Data Link Control). Protocolo de capa de enlace de datos y emitido como estándar ISO. Especifica un método de encapsulamiento de datos en enlaces seriales síncronos.

Hub Concentrador. Dispositivo que sirve como centro de una red con topología tipo estrella. También se refiere a un dispositivo que contiene múltiples módulos de equipos de redes.

ICMP Protocolo de mensajes de control Internet. Parte integral de IP que maneja mensajes de control y error. Enrutadores y hosts usan ICMP para enviar reportes de problemas acerca de datagramas enviados por una máquina. Está documentado en RFC 792.

IEEE Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronic Engineers). Organización profesional que define estándares de redes. Los estándares LAN de IEEE son los predominantes en la actualidad e incluyen protocolos similares o virtualmente equivalentes a Ethernet y Token Ring.

Internet Término empleado para referirse al sistema de interconexión de redes más grande del mundo, que conecta miles de redes en todo el planeta y que desarrolla una cultura basada en simplicidad, investigación y estandarización fundamentada en el uso real. Buena parte de la tecnología de punta en redes vino de esta comunidad. Internet evoluciono a partir de ARPANET.

Internetwork Redes interconectadas. Conjunto de redes interconectadas por enrutadores y que en forma genérica funciona como una sola. A veces se le llama internet, lo cual no debe confundirse con la palabra Internet.

Internetworking Interconexión de redes. Término genérico usado para referirse a la industria que surgió alrededor del problema de conectar redes. El término se puede referir tanto a productos como a procedimientos y tecnologías.

IP Protocolo Internet (Internet Protocol). Protocolo de capa 3 (capa de red) que contiene información de direccionamiento y de control para permitir el enrutamiento de datagramas. Este Protocolo define el datagrama IP como la unidad de información utilizada a través de internet y proporciona un servicio de entrega de datagramas con el mejor esfuerzo y sin conexión. Esta documentado en RFC 791.

IPRouter Enrutador IP. Dispositivo que enruta datagramas usando las direcciones IP de destino. Es un equipo responsable de tomar las desiciones de las trayectorias de tráfico a seguir.

IPX Intercambio de paquetes de interconexión de redes (Internetworking Packet Exchange). Protocolo Novell de capa 3, similar a XNS e IP que se emplea en redes NetWare.

LAN Red de área local (Local Area Network). Red que cubre un área geográfica relativamente pequeña (usualmente no mayor que un grupo local de edificios). Comparadas con las redes WAN las redes LAN suelen caracterizarse por velocidades de transferencia de datos relativamente altas y una relativamente baja incidencia de errores.

Leased line Línea arrendada o privada. Línea de transmisión reservada por un portador de comunicaciones para uso privado de un cliente.

Link Enlace. Canal de comunicaciones de la red consistente en un circuito o una trayectoria de transmisión, incluido el equipo existente entre el transmisor y el receptor. Suele usarse para referirse a una conexión en una red WAN.

MAC sublayer Subcapa de control de acceso al medio (Media Access Control Sublayer). Como está definida por la IEEE, se trata de la porción baja de la capa de enlace de datos del modelo OSI. La subcapa MAC se encarga de los asuntos de acceso al medio de comunicaciones, como por ejemplo determinar si se usara token passing (paso de estafeta) o contención.

MAN Red de área metropolitana (Metropolitan Area Network). En términos generales se refiere a una red que ocupa una área metropolitana, geográficamente mayor que la ocupada por una red local (LAN), pero menor que la de una red amplia (WAN).

Manchester encoding Codificación Manchester. Esquema de codificación digital en el que se emplea una transición durante el bit para señal de reloj, donde una transición a alto durante la primera mitad del tiempo del bit denota un uno. Es el esquema de codificación empleado por IEEE 802.3/Ethernet.

MAU Unidad de conexión al medio (Medium Attachment Unit IEEE 802.3):. Es un dispositivo que realiza las funciones de la capa 1 de IEEE 802.3, que incluyen la detección de colisiones y la inyección de bits a la red. Una unidad MAU se conoce como transceiver (transmisor/receptor) en la especificación Ethernet. Otro significado es Unidad de acceso a estaciones múltiples a veces llamada también MSAU para que no se confunda con la primera (Multistation Access Unit IEEE 802.5). Se trata de concentradores de cables a los cuales se conectan los nodos de Token Ring.

MTU Unidad de transferencia de datos máxima (Maximum Transfer Unit). Se refiere al paquete de tamaño máximo, en bytes, que una interface en particular puede manejar.

Name server Servidor de nombres. Servidor que la red ofrece para resolver nombres de la red y asociarlos con localidades (direcciones) de la red.

NFS Network File System: Sistema de archivos en red. Como se emplea normalmente, es un conjunto de protocolos de sistemas de archivos distribuidos desarrollados por la empresa Sun Microsystems, que permite el acceso remoto a archivos en una red. En realidad, NFS es uno de los protocolos del conjunto, que incluye NFS, XDR (External Data Representation:Representacion externa de datos), RPC (Remote Procedure Call: Llamada remota a procedimientos), y otros. Estos protocolos son parte de una arquitectura mayor que la empresa Sun nombra como ONC (Open Network Computing).

Packet Paquete. Agrupamiento lógico de información que incluye un encabezado (header) y (normalmente) datos del usuario.

Packet switching Conmutación de paquetes. Red en la cual los nodos de los paquetes comparten el ancho de banda porque mandan unidades lógicas de información (packets) en forma intermitente. En contraste, una red de conmutación de circuitos (circuit switching) dedica un circuito a la vez para la transmisión de datos.

PCM Modulación por código de pulsos (Pulse Code Modulation). Transmisión de información analógica en forma digital mediante muestreo y codificación con un número fijo de bits.

Protocol Protocolo. Una descripción formal de los formatos de los mensajes y las reglas que 2 o más máquinas deben seguir.

Puente Equipo que conecta 2 o más redes y envía tramas entre ellos operando en el nivel de enlace de datos.

RFC Solicitud de comentarios (Request For Comments). Documentos empleados como el medio primario de comunicaciones de información sobre Internet. Algunos RFC son designados por IAB como "Estándares Internet". La mayoría documentan especificaciones de protocolos, como Telnet y FTP.

RIF Campo de información de enrutamiento utilizado en la trama de redes IEEE 802.5.

RJ-11 Conectores estándar de 4 hilos para líneas telefónicas.

RJ-45 Conectores estándar de 8 hilos para redes IBASE5 o 10BASET de IEEE 802.3. También se usa para conexión de líneas de teléfono en algunos casos.

Router Enrutador. Equipo de interconexión de redes a nivel de capa de red.

Routing table Tabla de enrutamiento. Tabla almacenada en un enrutador o en algún otro dispositivo de las redes, que lleva cuenta de las rutas (y, en algunos casos, de su métrica) hacia destinos particulares en la red.

RS-232C Interface de capa física de baja velocidad. Es virtualmente idéntica a la especificación V.24.

RS-422 Realización eléctrica balanceada de RS-449 para transmisión de datos a alta velocidad.

RS-423 Realización eléctrica no balanceada de RS-449 para compatibilidad con RS-232C, pero que soporta mayor velocidad.

RS-449 Interface de capa fisica bastante popular. Se trata esencialmente de una versión más rápida (hasta 2 Mbps) de RS-232C con capacidad de manejar cables más largos.

SAP Punto de acceso al servicio (Service Access Point). Interface entre capas OSI adyacentes. También se refiere al Protocolo de anuncio de servicios (Service Advertisement Protocol). Un protocolo Novell mediante el cual se hacen conocidos a los clientes recursos de la red tales como servidores.

Segment Segmento. Término usado en la especificación de TCP para describir una unidad de información de la capa de transporte.

Single mode fiber Fibra de modo único. Fibra de diámetro relativamente angosto, a través de la cual solo se propaga un nodo. Tiene un ancho de banda mayor que la fibra multimodo, pero requiere una fuente de luz de espectro reducido (por ejemplo, un láser).

Sliding window Control de flujo de ventana deslizante. Método de control de flujo en el que el receptor da al transmisor permiso de transmitir datos hasta que la ventana se llene. Cuando esto sucede, el transmisor debe detenerse hasta que el receptor anuncie una ventana mayor. TCP, otros protocolos de transporte y varios protocolos de la capa de enlace usan este método de control de flujo.

SLIP IP en línea serial (Serial Line IP). Protocolo Internet usado para conexiones seriales punto a punto usando TCP/IP.

SNMP Protocolo simple de administración de redes (Simple Network Management Protocol). El protocolo de administración de redes ofrece medios para seguir y determinar la configuración de la red, permitiendo el monitoreo de eventos o fallas.

Socket Estructura de software que opera como punto final de comunicaciones en un dispositivo de la red.

Source-route bridging Puenteo de enrutamiento fuente. Método de puenteo originado por IBM en la cual la ruta completa a un destino se predetermina en tiempo real antes del envío de datos al destino. Esto contrasta con transparent bridging: puenteo transparente, en donde el puenteo ocurre trayecto (hop) por trayecto. También conocido por las siglas SRB, es mas popular en las redes Token Ring.

Source-route transparent bridging Puente de enrutamiento fuente transparente. Esquema de puenteo propuesto por IBM, que intenta reunir las dos estrategias prevalecientes de puenteo (transparente, y de rutas fuente). SRTB, como a veces se le conoce, emplea ambas tecnologías en un mismo dispositivo para satisfacer las necesidades de todos los nodos finales. No se hace traducción entre los protocolos de puenteo, a diferencia de lo que sucede con source -route translational bridging (SR/TLB).

Spanning tree Árbol de Expansión. Subconjunto sin lazos cerrados de la topología de una red.

SQE Signal Quality Error: Error de calidad en la señal. Transmisión enviada por el transceiver (transmisor/receptor) de regreso al controlador para indicarle que los circuitos de colisiones están funcionales. También se conoce como heartbeat (latido).

STA Algoritmo de árbol de expansión.

T-connector Conector-T. Dispositivo en forma de T con dos conectores BNC hembra y uno macho.

TCP Protocolo que proporciona un servicio de cadena de datos, confiable, full duplex. TCP permite que un proceso de una máquina envíe una cadena de datos de un proceso a otro. Es orientado a conexión en el sentido de que antes de transmitir datos, los participantes deben establecer un acuerdo de transmisión de datos llamado conexión.

Telnet Protocolo estándar Internet de emulación de terminales.

Terminal emulation Emulación de terminales. Aplicación usual de redes en la cual una computadora ejecuta programas que la hacen aparecer ante una máquina anfitriona de la red, como si fuera una terminal simple conectada directamente.

Terminal server Servidor de terminales. Procesador de comunicaciones que conecta dispositivos asíncronos a una red LAN o WAN mediante software emulador de terminales y redes.

Terminator Terminador. Resistencia eléctrica al final de una línea de transmisión, que absorbe las señales, evitando así que sean reflejadas y detectadas de nuevo por las estaciones de la red.

Translation bridging Puenteo de traducción a veces conocido como SR/TLB, es un método de puenteo en el cual las estaciones de rutas fuente pueden

comunicarse con estaciones de puentes transparentes con el auxilio de un puente intermedio que traduce entre los dos protocolos de puenteo.

Throughput Producción, trabajo útil. Cantidad de información que llega y posiblemente pasa, a un punto en particular en un sistema de la red.

TPDU Unidad de datos del protocolo de transporte.

Trailer Elemento de la cola. Información de control añadida a los datos en un paquete.

Transceiver Transmisor/receptor.

Translation bridging Puente traductor. Puenteo entre redes con protocolos de subcapa MAC diferentes.

Transparent bridging Puenteo transparente. Esquema de puenteo preferido por redes Ethernet y IEEE 802.3, en el cual los puentes pasan las tramas un trayecto (hop) a la vez basados en las tablas que asocian nodos terminales con puertos del puente. Se llama así porque la presencia de los puentes es transparente para los nodos terminales de la red.

UDP Es un protocolo que permite a una máquina enviar un datagrama a un programa de aplicación en otra máquina. Hay importantes diferencias entre un datagrama UDP y un datagrama IP. UDP incluye un número de puerto de protocolo, permitiendo al emisor distiguir entre múltiples destinos en la máquina remota.

V.24 Interface de capa física comúnmente empleada en muchos países. Muy similar a EIA-232D y RS- 232C.

X.25 Recomendación CCITT que define el formato de los paquetes para transferencia de datos en redes publicas de datos. Muchos establecimientos tienen redes X.25 que les dan acceso a terminales remotas.

X.28 Recomendación CCITT que define la interface terminal-PAD.

X.29 Recomendación CCITT que define la interface PAD-Host X.25.

X.3 Recomendación CCITT que define varios parámetros de un PAD.

BIBLIOGRAFIA

Tanenbaum, Andrew S.
Redes de Ordenadores
Traduc. Victor Manuel Carbajal Castañeda
Segunda ed.
México, Ed. PRENTICE-HALL, 1991
759 pp.

Comer, Douglas E.
Internetworking with TCP/IP
Vol. I Segunda ed.
New Jersey, Ed. PRENTICE-HALL, 1991
547 pp.

Keiser, Gerd E.
Local Area Networks
Singapore, Ed. McGraw-Hill,1989
420 pp.

Martin, James
Principles of data Communication
USA, Ed. PRENTICE-HALL, 1988
346 pp.

Schwartz, Misha
Transmisión de Información, Modulación y Ruido
Traduc. Caupolicán Muñoz Gamboa
Primera ed.
México, Ed McGraw-Hill, 1994
685 pp.

Taub, Herbert
Principles of Communication Systems
Segunda ed.
Singapore, Ed.McGraw-Hill, 1986
759 pp.

Black, Uyless
Computer Networks Protocols, Standards, and Interfaces
USA, Ed PRENTICE-HALL, 1987
451 pp.

BIBLIOGRAFIA

Tanenbaum, Andrew S.
Redes de Ordenadores
Traduc. Victor Manuel Carbajal Castañeda
Segunda ed.
México, Ed. PRENTICE-HALL, 1991
759 pp.

Comer, Douglas E.
Internetworking with TCP/IP
Vol. I Segunda ed.
New Jersey, Ed. PRENTICE-HALL, 1991
547 pp.

Keiser, Gerd E.
Local Area Networks
Singapore, Ed. McGraw-Hill,1989
420 pp.

Martin, James
Principles of data Communication
USA, Ed. PRENTICE-HALL, 1988
346 pp.

Schwartz, Misha
Transmisión de Información, Modulación y Ruido
Traduc. Caupolicán Muñoz Gamboa
Primera ed.
México, Ed McGraw-Hill, 1994
685 pp.

Taub, Herbert
Principles of Communication Systems
Segunda ed.
Singapore, Ed.McGraw-Hill, 1986
759 pp.

Black, Uyless
Computer Networks Protocols, Standards, and Interfaces
USA, Ed PRENTICE-HALL, 1987
451 pp.

Wandell & Goltermann
DA-30 Multiport Protocol Analyzer Operating
Tercera ed.
USA, Wandell & Goltermann, 1992.
500 pp

Standar Microsytems Corporation SMC
Manual de tarjeta de Red
EtherCard Elite Adapter
NewYork, SMC, 1993
100 pp.

FTP SOFTWARE
PC/TCP Network Software V2.3 DOS/WINDOWS INSTALLATION GUIDE
USA, FTP, 1993
83 pp.

FTP SOFTWARE
PC/TCP Network Software V2.3 DOS/WINDOWS COMMAND REFERENCE
USA, FTP, 1993
120 pp.

Recomendaciones CCITT Libro Azul 1988:

V.24
G.703
G.704
G.711
G.821