21
2ej

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Escuela Nacional de Estudios Profesionales
PLANTEL ARAGON

TCP/IP CONCEPTOS Y APLICACIONES

TESIS PROFESIONAL
Que para optar el título de
INGENIERO EN COMPUTACION
p r e s e n t a

ANTONIO GOMEZ LUVIANO

San Juan de Aragón, Estado de México 1995

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

A mis padres, hermanos, esposa e hijos por todo el cariño y apoyo que siempre me han brindado.

Antonio Gómez Luviano

INDICE

CAPITULO 3 (PROTOCOLO INTERNET)

CAPITULO 4 (RUTEO IP)

CAPITULO 5 PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

CAPITULO 1

CONCEPTOS GENERALES DE REDES

INTRODUCCION

El almacenamiento y análisis de la información ha sido siempre uno de los grandes problemas a los que se ha enfrentado el hombre desde que aparecio la escritura.

Con la invención de la computadora en la década de los 50's , se han ido aminorando estos problemas, sin embargo en el medio ambiente de la computación, son cada vez más necesarios sistemas que nos permitan manipular grandes cantidades de información en intervalos muy reducidos de tiempo. Y aunque a principios de los 80's las microcomputadoras habían revolucionado por completo el concepto de la computación electrónica, así como sus aplicaciones y mercado, el intercambio de información seguía siendo lento para cubrir las necesidades de aquella época, además de inadecuado, puesto que si se trataba de compartir datos que algún otro usuario poseía, lo más natural era copiar esos datos en nuestros diskettes o disco duro, y esto aparte de provocar una relativa pérdida de tiempo, no nos permitia mantener consistente nuestra información debido a que las actualizaciones se realizaban en forma individual.

Por otro lado el uso de impresoras también era muy molesto cuando más de un usuario deseaba hacer uso de ella, puesto que solamente podía conectarse en modo local a una PC, por lo tanto cuando alguién más deseaba utilizarla, debia remplazar a ese usuario de su computadora. El tener una computadora e impresora por cada usuario para contrarrestar estos problemas, sería una solución bastante cara para las empresas.

Los problemas mencionados anteriormente y algunos más son los que la instalación de una red de computadoras pretende resolver, además de crear una base sólida para el futuro crecimiento de las empresas, ya que al realizar un estudio detallado antes de implementar una red local, se deben considerar la situación actal así como los nuevos cambios que la tecnología va presentando para que la inversión inicial no se vuelva absoleta en pocos años.

1.1 Redes de Computadoras

Una red de computadoras es una serie de elementos de computo independientes (Estaciones de trabajo, Microcomputadoras, Minicomputadoras, Impresoras, etc.) equipados para comunicarse entre sí, el concepto de independencia es importante, debido a que cada componente depende solamente de el mismo y no de otro.

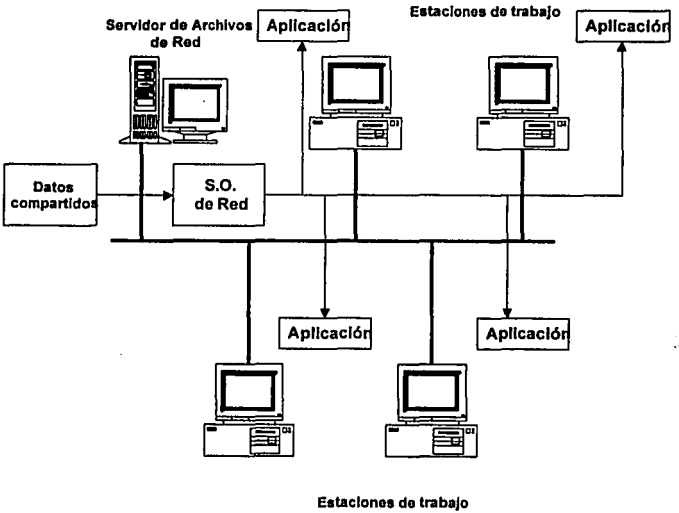

Figura 1.1 Componentes de una red local

1.2 Red de Área Local (LAN)

Una red local (Local Área Network), que en lo sucesivo llamaremos LAN, es por definición "local", lo que implica un límite físico de extensión que abarca desde un metro hasta algunos kilómetros dependiendo del medio de conexión que se utilice (Cable, Rayos Infrarrojos, Microondas, Enlaces Satelitales, etc.).

El objetivo de una LAN es el de compartir los recursos y periféricos disponibles de tal manera que su aprovechamiento sea al máximo. Algunos de estos recursos son:

- Paquetería
- Programas
- Datos
- Dispositivos (Impresoras, Modems, etc).

1.2.1 Componentes de una Red Local

Para el funcionamiento de una red local se necesitan varios componentes, los cuales se mencionan a continuación.

Servidor de Archivos (File server). Es un equipo con características especiales como una mayor cantidad en memoria RAM y en disco duro que los demás elementos que forman la red, ya que es aquí donde se instalan todas las aplicaciones y recursos a los cuáles van a tener acceso todos los usuarios de la red.

Estaciones de trabajo (WS). Son todos aquellos nodos desde los cuáles se puede tener acceso a la red.

Tarjetas de Red (TIR). La tarjeta de red es el dispositivo que permite identificar que un dispositivo pertenece a la red, por lo tanto su elección se ve reflejado en el buen o mal desempeño de la red. Por lo regular en el servidor de archivos que es el que tiene más carga de trabajo, se debe instalar una tarjeta más rápida que en los nodos que la integran.

Actualmente existen diferentes tipos de tarjetas para los diferentes tipos de redes y arquitecturas de computadoras que existen tales como Arquitectura ISA, EISA, MICROCANAL, PCMCIA y también de diferentes velocidades como 8bits, 16bits, o 32 bits.

CABLEADO

El cableado puede llegar a presentar una porción substancial del costo de la instalación total de la red. Elegir un tipo de cable equivocado podría tener un gran impacto sobre el funcionamiento y confiabilidad de la red, ya que está demostrado que de un 60% a un 70% de los problemas que ocurren en la red son debido al cableado.

Los tipos de cable para red se mencionan a continuación:

- Cable Telefónico
- Cable Coaxial
- Fibra Optica

Cable Telefónico

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

Es esta característica la que los distingue con el nombre de par torcido (Twisted Pair). El par torcido a su vez, se encuentra cubierto por una cubierta aislante y protectora en la capa exterior denominada jacket.

Los cables con los conductores de cobre más delgados y menos protegidos por un jacket están dentro de la clasificación de cables tipo UTP(Unshielded Twisted Pair; par torcido sin blindar). Son sumamente baratos, flexibles y permiten manipular una señal a una distancia máxima de 100 metros sin el uso de amplificadores.

Los cables de conductores más gruesos y muy bien cubiertos por un jacket son denominados del tipo STP (Shielded Twisted Pair; cables de par torcido blindado). Estos son más caros y menos flexibles que los UTP, pero tienen un rango de operación mayor.

Algunas de las ventajas del cable telefónico son las siguientes:

- Tecnología conocida
- Facilidad y rapidez de instalación
- Ancho de banda de 16 Mbps
- Distancias de hasta 100 metros sin el uso de repetidores
- Buena tolerancia a interferencias debidas a factores ambientales
- Excelente relación precio-rendimiento

Este tipo de cable es muy fácil de instalar, es el más económico y soporta distancias hasta de 100m. Su desventaja principal es la gran interferencia electrónica que sufre este tipo de cable.

Cable UTP sin blindaje

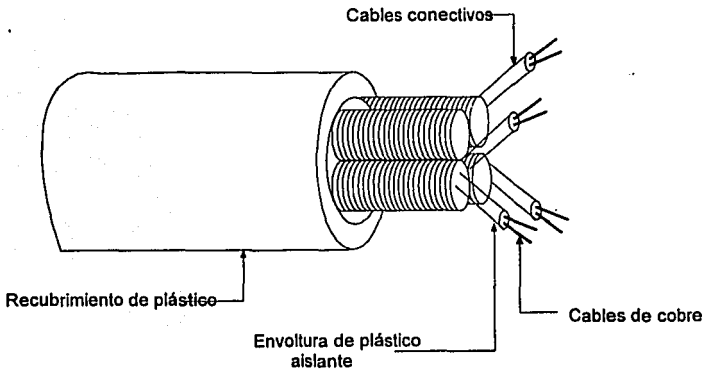

Fig. 1.2 Cable Telefónico

Cable Coaxial

El cable coaxial se forma por un alambre conductor básico cubierto por una capa metálica 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 también aislante, a la que comunmente se le llama jacket.

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 cable grueso suele ser más caro y menos flexible. Por tal razón, cuando tiene que colocarse en instalaciones donde ya existen canales para cableado o conductos con espacio reducido resulta más conveniente utilizar el cable delgado debido a que las nuevas instalaciones de ductos para cable por lo general son muy costosas. Esto puede ser un factor determinante para la implantación de una red local.

El cable coaxial se puede encontrar en dos presentaciones:

- cable coaxial delgado (soporta hasta 185 metros)
- cable coaxial grueso (soporta hasta 500 metros)

Algunas de las ventajas de utilizar cable coaxial son las siguientes:

- Transmisión de voz, video y datos
- Fácil instalación
- Ancho de banda de 10 Mbps
- Distancias de hasta 500m sin necesidad de repetidores
- Buena tolerancia a interferencias debidas a factores ambientales

El cable coaxial es un poco mas caro que el TP, pero soporta mayores distancias, los datos viajan más rápido y es más resistente a las interferencias electromagnéticas.

Cable coaxial

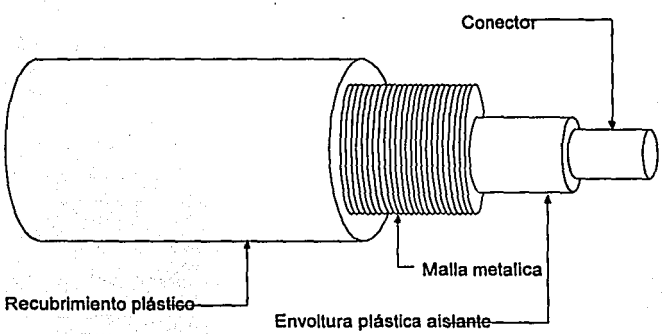

Fig. 1.3 Cable Coaxial

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 donde 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 mayor integridad estructural al cable. Es, sin embargo, extremadamente flexible ya que se pueden realizar giros de hasta 360 grados sin problemas de afectación en el cable.

El diametro de la fibra interior más comunmente usado es de 62.5 micras y el de la fibra exterior, de 125. Presentan una atenuacion máxima de 4 db/km

Para la transmisión de la información en redes locales vía fibra óptica se utiliza una fibra como transmisor y otra como receptor. Es por esto que generalmente se producen en conjuntos de mínimo dos fibras por cable.

Algunas de las ventajas del cable de fibra óptica son las siguientes:

- Transmisión de voz, video y datos por el mismo canal
- Aplicaciones de alta velocidad
- No genera señales eléctricas o magnéticas
- Inmune a interferencias
- Compatibilidad con Ethernet[1] , Token Ring[2] y FDDI[3]
- Ofrece la mayor capacidad de adaptacion a nuevas normas de rendimiento

El uso de la fibra óptica ha comenzado a adquirir importancia económica en los últimos años, aunque su costo sigue restringiendo su uso solo a aplicaciones especiales que justifiquen su instalación.

[1] Marca registrada de Xerox Corp.
[2] Marca registrada de Internacional Business Machines Corp.
[3] Estándar desarrollado por ANSI

Cable de Fibra Optica

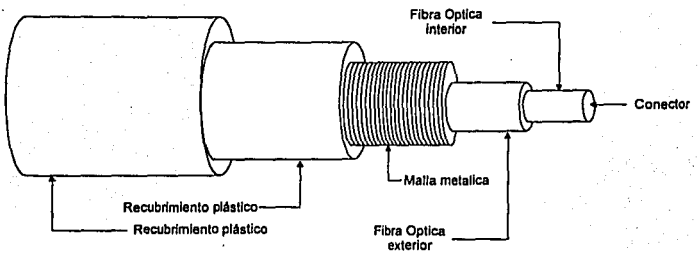

Fig. 1.4 Fibra Optica

Sistema Operativo de Red

El sistema operativo de red es aquel que administra las funciones de la red, entre los más populares tenemos a Netware[4] y Windows NT[5]. Cada uno de ellos presenta ventajas y desventajas por lo que su elección se tiene que hacer de acuerdo a las características actuales y futuras de cada empresa en particular.

Software de Aplicación

Son todos aquellos programas que se instalan en el servidor y que van a poder ser accionados por todos los usuarios que integran la red, entre las principales aplicaciones encontramos:

- Sistemas operativos
- Ambientes gráficos
- Procesadores de textos
- Hojas de cálculo
- Bases de datos

[4] Marca registrada de Novell Inc.
[5] Marca registrada de Microsoft Corp.

1.3 Topologia de Redes

1.3.1 Definición de Topología

Existen diferentes esquemas de distribución en los que las LANs pueden ser cableadas o conectadas; estos esquemas son conocidos como topologías.

Normalmente las redes locales se basan en tres topologías principales:

- Bus (canal)
- Anillo
- Estrella

BUS (CANAL)

Consiste en un diseño simple con un cable de determinada longitud conocido como bus o tronco, que es compartido por todos los dispositivos de la red.

Esta topología se basa en la ausencia de una computadora central. Un nodo no depende de el siguiente para que el flujo de información continúe. Esta topología permite que los mensajes sean transmitidos a todos los nodos simultáneamente a través del bus. Cuando un nodo reconoce que un mensaje va dirigido a él, lo saca del bus. Como consecuencia de esta independencia, aumenta notablemente la confiabilidad propia de la red , pero requiere que cada nodo pueda transmitir, recibir y resolver problemas.

La ventaja de la topología lineal es su econonomía. A diferencia de otras topologías, la única consideración es el cableado del bus, es que el cable pasa por cada dipositivo de la red.

Una desventaja de esta topología es que si el cable falla en cualquier punto, toda la red detendrá su funcionamiento. Dichas fallas en en el cable pueden ser difíciles de localizar en redes grandes, pero con los avances logrados en rutinas de diagnóstico y en softwares de monitoreo de redes, se facilita el localizar estas fallas para tomar las acciones pertinentes.

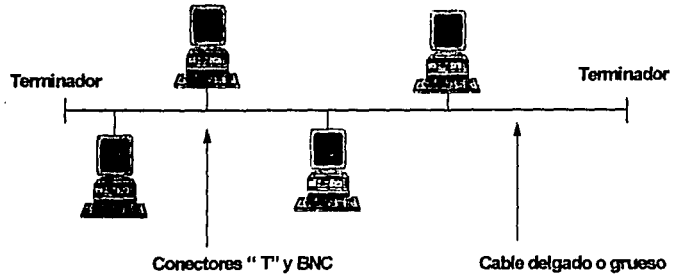

Fig. 1.5 Topología de Bus

ANILLO

En la red en anillo, los nodos se conectan a una unidad central llamada MAU (Media Access Unit) los cuales se conectan entre sí para formar un anillo lógico. El mensaje que entra en una red anillo debe contener un grupo de bits que indique la dirección donde se debe entregar.

Una característica importante de esta topología es que se tiene el control distribuido. En la red en anillo, a excepción de algunas funciones, cada elemento es de igual jerarquía que los demas en lo que respecta a sus facultades de comunicaciones, permitiendo así una mayor flexibilidad y confiabilidad.

La desventaja de la red de anillo es que se necesita conectar cada estación con las dos adyacentes, además de que a medida que se pasan los mensajes , se disminuye notablemente la velocidad de la red, siendo esta una desventaja propia de la configuración en anillo..

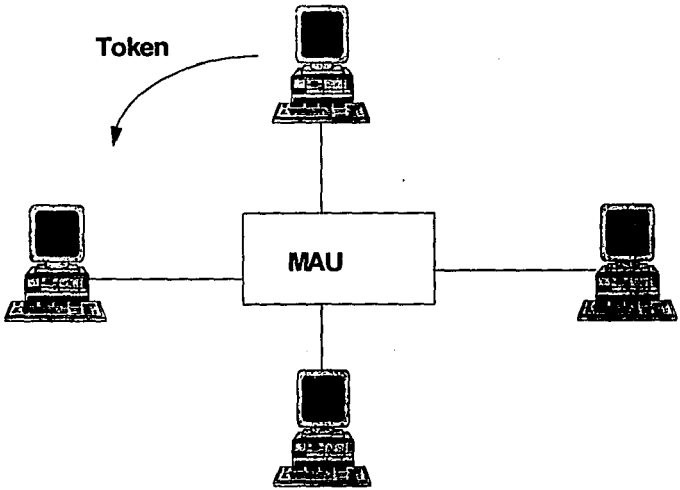

Fig. 1.6 Topología de Anillo

ESTRELLA

Esta topología semeja una estrella con cables saliendo de un punto central. En esta red el punto central es el Servidor de Archivos. La estrella no requiere cables compartidos y cada estación de trabajo tiene su propio cable.

El tamaño de la red está limitado por la capacidad del Concentrador.

Esta topología tiene la ventaja de que la detección de fallas en el cable es muy fácil, debido a que cada estación de trabajo tiene su propio cable, una falla en el cable de cualquier nodo solamente afectará a este y la red continuará funcionando.

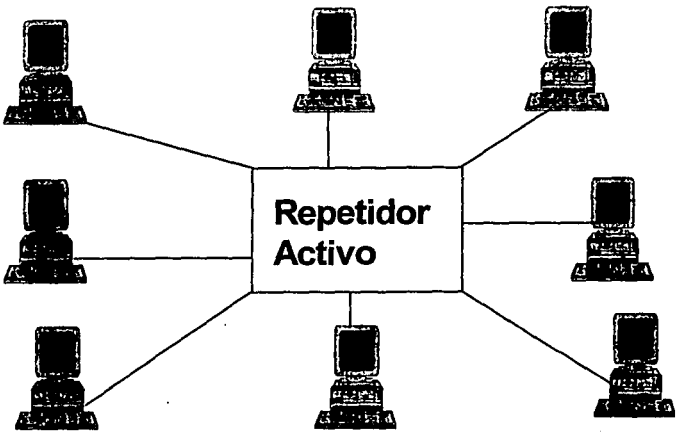

Fig. 1.7 Topología de Estrella

1.4 Protocolos de Comunicación

DEFINICION

Los protocolos son las reglas que determinan el orden en que se les permite a los nodos de la red usar el metodo de comunicación compartido. Las topologías tienen una conexión común, cuyo uso debe distribuirse entre las estaciones. Los principales objetivos de un método de acceso son:

a) **Eficiencia.-** Las reglas de acceso no deben requerir una porción del uso del medio de comunicación o una capacidad de proceso excesivo.

b) **Robustez.-** Los métodos usados para designar el medio de comunicación deben ser capaces de recuperarse de condiciones de error, ya sea en la transmisión o en el orden de paquetes de control o de datos. Si se manejan de manera óptima los mecanismos de recuperación solo afectarán a las estaciones que se estaban comunicando al ocurrir el error.

c) **No Bloqueo.-** Las reglas de acceso deben garantizar que cada estación de la red use una porción del canal, aún en condiciones de carga extrema. Algunas redes están diseñadas para dar a cada estación la misma porción de la capacidad. Otras redes se basan en "prioridades de acceso" y permiten a ciertas estaciones tener el canal más veces que otras.

Existen diferentes protocolos, algunos de ellos propietarios desarrollados únicamente para ejecutarse en los equipos desarrollados por su propio fabricante. Ejemplos de protocolos propietarios y sus correspondientes vendedores podemos citar a los siguientes:

DecNet(DEC)
IPX(Novell)
SNA(IBM)
XNS(Xerox)

Actualmente, en el medio ambiente de la Interconenctividad, estos sistemas propietarios tienden a convertirse en estandares para ser soportados por varios fabricantes.

Existen dos protocolos estandares de fabricantes independientes estos son :
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Open System Interconnect

El TCP/IP es especificado por la junta directiva de actividades Internet (IAB), la cual agrupa un amplio grupo de corporaciones academicas y organizaciones gubernamentales.

Como el modelo del mismo nombre, el Protocolo OSI ha sido definido y aprobado por la International Standars Organization (ISO).

Cuando nos referimos a estandares para Interconectividad, nos estamos refiriendo a sistemas basados en cualquiera de los dos estandares anteriores.

1.5 Niveles de Protocolos

Los protocolos son clasificados en terminos de protocolos de "bajo nivel" y protocolos de "alto nivel"

Protocolos de bajo nivel

Los protocolos de bajo nivel son procesados y operan en:

- La capa física
- La capa de enlace

Los protocolos estandares más comunes de bajo nivel son:

- Ethernet (CSMA/CD)
- Token Ring (Token Passing)
- Token Bus (Token Passing)

Protocolos de alto nivel

Los protocolos de alto nivel operan en:

- La capa de Red
- La capa de Transporte
- La capa de Sesion

Los protocolos más comunes estandares de alto nivel son:

- XNS- Xerox Network System
- TCP/IP- Transfer Control Protocol/Internet Protocol
- OSI- Open System Interconnect

Los protocolos que operan en las primeras capas, permiten a los productos para redes locales compartir el medio seleccionado, pero los protocolos de alto nivel son requeridos para garantizar, deliverar y mantener el orden del flujo de datos entre las estaciones de las redes.

En 1980 el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), empezó a trabajar en el estandar 802, el cúal es una familia de estándares para las redes locales. Esta familia de estandares trabajan en conjunto con la capa física y la de enlace del modelo OSI.

802.3 Carrier Sense Multiple Acces/Colition Detection estándar para Ethernet

802.4 Estándar para token Bus

802.5 Estándar para Token Ring

La diferencia principal entre los protocolos CSMA/CD y el Token Passing, es la manera de enviar datos a través de la red.

En el Protocolo Token Passing un mensaje, o ficha (Token) se encuentra siempre circulando en la red para indicar que este está disponible para ser usado por cualquier nodo. Cada estación debe copiar los mensajes que pasen hasta que reciba el Token; entonces, si tiene algún mensaje que transmitir, debe convertir el token en un conector y agregar su propio mensaje inmediatamente despues. El conector difiere del Token solo en el último bit, por lo que la conversion se logra invirtiendo ese bit al retrasmitir el mensaje.

El método de acceso CSMA/CD consiste en que cuando una estación desea mandar un mensaje, debe "monitorear" el canal, esto es, debe checar si otra estación está usándolo. Si este es el caso debe esperar hasta que la otra haya terminado para mandar su mensaje. Si no hay ninguna estación usando el canal, entonces puede transmitir inmediatamente. El término Carrier Sense indica este comportamiento que es "escuchar antes de transmitir".

En el caso de que dos o más paquetes se envíen al mismo tiempo, el protocolo detecta la colisión y pide a las estaciones que envíen nuevamente.

La norma para las redes basadas en el protocolo CSMA/CD de la asociación de ingenieros IEEE 802.3, a la que con frecuencia se le denomina Ethernet, se basa en el principio de que cada estación tiene la misma oportunidad de usar la red. De hecho, la especificación incluye un algoritmo que impide que cualquier estación o grupo de estaciones monopolice a la red. Mientras que por otro lado la Token Passing incluye una capacidad de prioridad, la cúal permite que algunas estaciones tengan más acceso que otras.

Es difícil comparar directamente la eficiencia de las redes de Token Passing contra las de CSMA/CD, unas funcionan mejor en ciertos tipos de ambientes.

El Token Passing ofrece la seguridad de que en el momento de paso de la ficha la estación enviará sus datos, sin embargo esto por lo general se compensa por la mayor velocidad de transferencia de las de CSMA/CD.

Las colisiones son una parte normal de la operación de redes de CSMA/CD. Es verdad que Ethernet tiene colisiones al enviar mensajes, pero estas son una parte integral del método de acceso de contensión.

Estas colisiones son típicamente infrecuentes, y duran unas cuantas millonesimas de segundos. La lógica para manejar las colisiones se integran en los chips del controlador. Como una salvaguarda, si una estación experimenta un nivel anormalmente alto de colisiones, reporta un error y lo remueve de la red.

De los protocolos que operan en las capas de red, transporte y sesión y que son conocidos como protocolos de alto nivel, enfocaremos nuestra atención en el más popular de todos ellos, el TCP/IP.

1.6 Los Orígenes de TCP/IP

El TCP/IP son protocolos de comunicación que fueron originalmente desarrollados por el Departamento de Defensa de los Estados Unidos. Y utilizados inicialmente en la red ARPA (ARPANET), a principios de 1970 y que en aquel entonces unía varias Universidades y Centros de Investigación relacionados con el gobierno de los Estados Unidos.

ARPANET que originalmente había sido diseñada como un experimento para switchear paquetes en redes anchas, al ser todo un exito, derivó en "Internet", que es la red más grande del mundo con millones de nodos en un sinfín de redes locales y enlaces remotos.

A principios de los años 80s, TCP/IP fué incluido como parte integral de UNIX Versión 4.2. Como resultado el protocolo extendió su uso en las redes.

Al ser estandar de comunicación entre las workstations y la proliferación de UNIX 4.2 dió un gran impulso a TCP/IP.

En 1983 , TCP/IP se convirtió en el protocolo estándar para las redes e interconectividad de la carrera militar.

1.7.1 Crecimiento TCP/IP

La aceptación de TCP/IP se debe a varias causas:

- Los productos de OSI están disponibles
- TCP trasciende a ambientes multivendedores, permitiendo a las redes de PC conectarse con minis, mainframes y sistemas basados en UNIX.

En los años recientes, TCP/IP ha ganado un incremento favorable en los negocios de computación. El éxito más importante en la historia del TCP/IP ha sido el hecho de que la Defense Advanced Proyects Research Agency (DARPA) que es un conjunto de Instituciones y Laboratorios de gobierno, dedicados al estudio de la Interconectividad , todos han realizado sus enlaces através de TCP/IP .

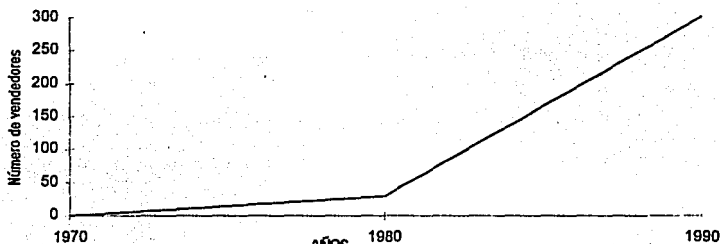

Fig. 1.8 Crecimiento de TCP/IP

1.7.2 Internet

Internet es una gran colección de redes. La Internet con TCP/IP conecta un gran rango de Instituciones incluyendo The National Sience Foundation, la NASA y el Departamento de Energía. En la actualidad engloba a más de 55000 hosts, con un crecimiento del 15% mensual.

Internet empezó a tomar forma en 1980 cuando la Institución de Investigaciones DARPA empezó a hacer la conversión a TCP/IP. La conversión se completo en 1983 cuando el gobierno ordenó que todas las computadoras conectadas a ARPANET usaran TCP/IP.

Algunas de las redes que conforman Internet son:

NSFNET National Science Foundation Network. Una red ancha originalmente desarrollada por la National Science Foundation en 1987. El Backbone de la NSF conecta a sites en Ithaca , NY, Pittsburgh y San Diego entre otros. En 1988 El backbone de la NSFNET fué actualizado al circuito T-1 por la MCI.

DDN Defense Data Network. DDN es actualmente un grupo de redes incluidas, pero no limitadas a ARPANET y a la red MIL (MILNET).

DRI Defense Research Internet (DRI). Esta red es el arma principal de investigación del sistema de redes nacional. Es un proyecto en conjunto de la NFS,DARPA y la NASA, y forma parte de la National Research Education Network (NREN).

1.7.3 RFCs (Request For Comments)

Debido al rápido crecimiento de la Internet ayudando e incrementando la aceptación de TCP/IP como un estándar en la industria, también se fueron creando nuevos problemas. En respuesta a estos problemas la Internet Activities Board (IAB) que es un comite formado por personas altamente calificadas en el mundo de las redes, fué establecido para emitir las direcciones en la futura expansión de Internet.

La IAB solicita los RFCs (Request For Comments) los cuales describen los trabajos internos de Internet. Los RFCs son usados para formalizar protocolos y otros procedimientos que toman lugar en Internet. Los RFCs primero son publicados electrónicamente y comentados por aquellos que quieran tomar parte en la discusión electrónica. El documento es revisado varias veces hasta que se llega a un acuerdo final. Si el documento es aceptado, se le asigna un número y se archiva con los otros RFCs.

Solo algunos de los RFCs actualmente especifican estandares, la mayoría son para información o propósitos de discusión.

Cabe mencionar que en las discusiones de los RFCs el proceso es tan abierto, que no tienen ningún costo y pueden participar en ellos cualquier persona con conocimientos en la materia.

1.8 Capas del Protocolo TCP/IP

Para analizar las capas del protocolo TCP/IP, primero se analizarán las capas del modelo OSI, para distinguir las principales diferencias entre estos dos protocolos estándares.

MODELO OSI

El modelo OSI puede ser visto como un conjunto de módulos funcionales (capas) conteniendo las reglas que los nodos de la red deben seguir para intercambiar informacion y permitir soluciones de Interconectividad entre diferentes fabricantes.

Las reglas que son estandares para diferentes tipos de equipos manufacturados por diferentes fabricantes, son llamados protocolos estándares.

Cada capa del modelo OSI es un módulo.

El modelo OSI está formado por las siguientes siete capas o módulos:

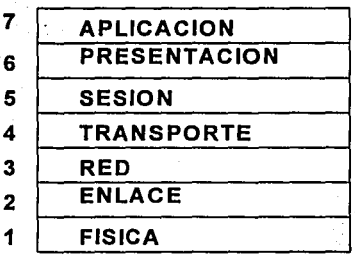

Figura 1.9 Capas del modelo OSI

Capa a nivel Fisico

Esta capa se ocupa de la transmisión de la secuencia de bits sin estructura sobre un medio físico, describe la interfaz a nivel eléctrico, mecánico y funcional, tambien se encarga de transportar las señales para todos los niveles superiores.

Capa de Enlace

Su función principal es la de proporcionar transmisión de información libre de errores sobre el medio físico.
Se encarga de empacar todos los datos, maneja el acceso al canal y el control de flujo, asegura la secuencia correcta de los datos transmitidos.

Capa de Red

La capa de red controla la operación de la subred. Decide cual ruta física deben seguir los datos basados en las condiciones de la red, prioridades de servicios y otros factores. Es la responsable de establecer, mantener y terminar la conección entre las comunicaciones intervenidas. Se encarga del ruteo de paquetes entre diferentes redes.

Capa de Transporte

De la cuarta capa en adelante del modelo OSI, son generalmente referidas como capas altas.

Esta capa se encarga de que las unidades de datos se entreguen sin errores, en secuencia, sin pérdida ni duplicación, segmenta los mensajes recibidos de la capa de sesión y proporciona paquetes a la capa de red, realiza funciones de multiplexaje de varias sesiones en un solo canal, manejo confiable de comunicación y control de flujo.

Capa de Sesión

Permite establecer sesiones entre usuarios en diferentes computadoras, establece conversaciones entre los programas que se ejecutan en diferentes equipos, establece sincronización entre tareas en los equipos de red mediante puntos de chequeo, permite un control de diálogo (quien habla, cuando, por cuanto tiempo, etc)

Capa de Presentación

Formatea los datos para presentarlos a la capa de aplicación, es el "traductor" de la red, realiza funciones de compresión de datos y encriptación.

Capa de Aplicación

Funciona como la ventana para los procesos de aplicación hacia el medio ambiente OSI, representa los servicios que soportan directamente a los usuarios y las tareas de aplicación, contiene una variedad de protocolos que son comunmente usados:

- Terminal Virtual
- Transferencia de archivos
- Acceso remoto de archivos
- Correo electrónico
- Administración de la red

Analizadas las capas del modelo OSI y sus principales funciones, procederemos ahora a analizar las capas del modelo TCP/IP.

En contraste con el modelo OSI que se divide en 7 capas, el software de TCP/IP es organizado dentro de cuatro capas conceptuales.

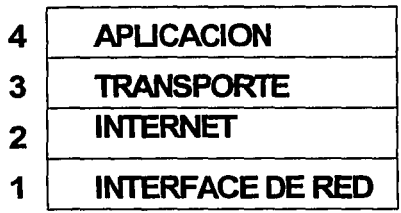

Figura 1.10 Capas del modelo TCP/IP

Capa de Interfaz de Red

Esta capa es la responsable de transmitir los datos sobre el medio físico hacia su destino final. Esto corresponde a las capas física y de enlace del modelo OSI.

Capa Internet

Esta capa corresponde a la capa de red del modelo OSI. Esta capa es responsable de proveer la comunicación entre host y host. Es aquí donde se encapsulan los paquetes dentro de bloques para transmitirlos de la capa de interfaz de la red hacia la red que se este conectando.

Capa de Transporte

Esta capa es la responsable de proporcionar comunicación entre aplicaciones residentes en diferentes hosts; colocando un identificador en los bloques de información, la capa de transporte permite procesar la información.

Capa de Aplicación

En esta etapa se incluyen aplicaciones tales como Telnet, File Transfer Protocol y Simple Mail Transfer Protocol.

1.9 Protocolos de Aplicaciones

El propósito de todos los protocolos de comunicación es el proporcionar servicios para la capa de aplicación. Un número de protocolos de aplicaciones han sido bien definidos en el medio ambiente TCP/IP para soportar el acceso de terminales a la red, transferencia de archivos, correo electrónico y administración de la red. La existencia de estos protocolos estándares de aplicación han permitido el crecimiento de TCP/IP.

TELNET: Provee servicios de terminales virtuales.
Esto permite al usuario conectarse y usar otra computadora de la red, como si su terminal estuviera conectada directamente a la otra máquina.

FTP: Protocolo de transferencia de archivos.
Permite al usuario comunicarse e interactuar con otro host con el propósito de manipular archivos. Esto permite al usuario obtener archivos de otra computadora o enviar archivos a otra computadora.

SMTP: Simple Mail Transfer Protocol
Es un protocolo para transferencia de archivos.

DNS: Domain Name Service
Permite al usuario reconocer nombres en lugar de cadenas numéricas para los direccionamientos de redes.

SNMP: Simple Network Manager Protocol
Administra con sus correspondientes elementos de hardware y software.

1.10 Ventajas de usar TCP/IP

A continuación se mencionaran algunas de las ventajas que se obtienen al trabajar con TCP/IP

- Independencia del fabricante y disponible para un gran número de fabricantes (3COM, IBM,DEC,SUN,HP y otros)

- Para cualquier tamaño de máquina (PCs, Workstations, Minis, Mainframes, etc.)

- Interoperabilidad entre equipos de diferentes fabricantes, facilita la comunicación entre diferentes áreas de la corporación. El uso de un protocolo en lugar de múltiples protocolos simplifica las redes.

- Perfectamente integrado dentro de UNIX

- Soporta la tecnología de ruteadores dinámicos

- Soporta la tecnología cliente-servidor

- Soporta múltiples tecnologías (Ethernet, Token Ring, X.25, etc)

- Las aplicaciones de OSI pueden correr en Internet con TCP/IP

- TCP/IP es una arquitectura punto a punto

CAPITULO 2

DIRECCIONAMIENTO Y SUBREDES

Cualquier sistema global de comunicación requiere un método universal aceptado para identificar a los diferentes dispositivos que estan conectados a este. A los dispositivos o Hosts, en INTERNET se les asigna un unico direccionamiento que los identifique donde estan y como poder llegar a ellos. Estos hosts pueden ser computadoras personales, servidores de terminales, routers, estaciones de administración de redes o hosts de Unix.

Existe algo que todos los hosts tienen en común: cada uno tiene asignado su propio direccionamiento. Algunos dispositivos como los routers los cuales tienen conexiones físicas a más de una red, se les debe asignar una dirección única por cada conexión en red.

Las direcciones usan campos de 32 bits. Los bits en los campos de direccionamiento son números del 0 al 31. Este campo es dividido en dos partes, uno identifica al host, y otra identifica la red en la cual el host reside. Los hosts que pertenecen a la misma red deben compartir en el mismo prefijo común designado para el número de la red.

Existen cuatro clases de direccionamiento para identificar a las redes que pueden ser fácilmente determinadas por el bit que ocupe la posición inicial.

2. 1 Direccionamiento de formato clase A

El formato clase A tiene el bit principal colocado a 0, siete bits para el número de la red y 24 para el direccionamiento de los hosts. 125 redes clase A pueden ser definidas con hasta 16,777,214 hosts
El formato clase A se muestra en la fig. 2.1

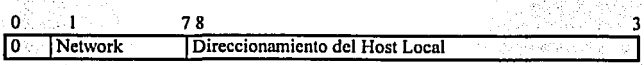

Fig. 2.1 Direccionamiento de formato clase A

2.2 Direccionamiento de formato clase B

El direccionamiento de red clase B tiene los dos bits principales colocados a 1-0, 14 bits para el direccionamiento de hosts locales. 16382 redes clase B pueden ser definidas hasta con 63,534 hosts por red. El direccionmiento clase B se muestra en la fig. 2.2

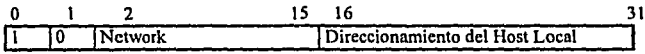

Fig. 2.2 Direccionamiento de formato clase B

2.3 Direccionamiento de formato clase C

El direccionmiento clase C tienen los tres primeros bits colocados a 1-1-0, 21 bits para el número de la red y 8 bits para el direccionamiento de los hosts. 2,097,152 redes clase C pueden ser definidas hasta con 254 hosts por red.

El direccionamiento clase C se muestra en la fig. 2.3

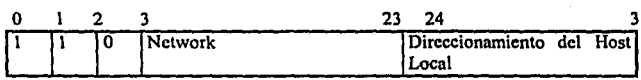

fig. 2.3 Direccionamiento de formato clase C

2.4 Direccionamiento de formato clase D

La clase D es usada como multicast. Los 4 bits principales están colocados a 1-1-1-0. La clase D, como todas las direcciones IP registradas son asignadas por la IAB

Fig. 2.4. Direccionamiento de formato clase D

Centro de Información de redes (NIC)

Para asegurarse que los direccionamientos Internet son únicos, estos son asignados por una autoridad central. Esta organización asigna un número único a la red para cada red que conforman Internet.

La NIC solo asigna una parte de los direccionamientos de la red, asignar un único número al hosts es responsabilidad del Administrador de la red.

2.4.1 Especificaciones de direccionamientos en las conexiones de redes

Para resumir las clases de direccionamiento, decimos que un direccionamiento Internet identifica al Host, pero esto no es totalmente estricto. Considerando que el gateway puede unir dos redes físicas.

Cuando las computadoras convencionales tienen dos o mas conexiones físicas, son llamadas hosts multi-homed. Los hosts multi-homed y los gateways requieren múltiples direcciones IP. Cada direccionamiento corresponde a una de las conexiones de la red.

2.4.2 Notación Decimal

Para hacer más facil que el usuario de redes entienda las direcciones Internet, estas son usualmente escritas con 4 números decimales separadas por un punto. Este formato es llamado notación decimal con punto.

Esta notación divide los 32 bits en campos de 8 bits llamados octetos, especificando el valor de campo independiente como un número decimal.

Por ejemplo, si tenemos un formato clase B especificado por los siguientes bits:

10000100	10001111	00000010	00000010

El valor de cada octeto es el siguiente:

132	147	2	2

La dirección completa Internet puede ser especificada en notación decimal con punto como:

132.47.2.2

El número de red valido para cada clase de direccionamiento es dado a continuación. Las "hhh" representan la parte de direccionamiento del host los cuales los puede asignar el Administrador de la red.

CLASE A	126.hhh.hhh.hhh
CLASE B	191.254.hhh.hhh
CLASE C	223.255.254.hhh
CLASE D	239.255.255.255

2.4.3 Direccionamiento Recursivo

En la clase A, EL DIRECCIONAMIENTO 127.0.0.0 es reservado para recursión y es diseñado para probar un inter-proceso de comunicación en una máquina local. Cuando algún programa usa el direccionamiento recursivo para enviar datos, el software del protocolo en la computadora regresa los datos sin enviar tráfico através de la red. Por lo tanto un paquete enviado al direccionamiento de red 127 nunca debe aparecer en ninguna red. Además, un host o un gateway nunca deben enviar información a la red 127; este NO es un direccionamiento de red.

2.4.4 Direccionamientos de Redes y Mensajes

Hemos citado las principales ventajas de decodificar la información en direccionamientos; haciendo posible el ruteo eficiente. Otra ventaja es que los direccionamientos Internet pueden referirse a las redes así como a los hosts. Por convención, el identificador host 0 nunca es asignado a un hosts individual. En lugar de esto, una dirección IP con el identificador host cero es usado para referirse a la red propia.

2.5 Estructura de una Red usando el Formato Clase B

Los segmentos conectados por puentes comparten los mismos campos de la red mientras tengan diferentes campos en los hosts. Los segmentos interconectados por ruteadores deben tener diferentes campos para la red como se muestra en la figura 2.5

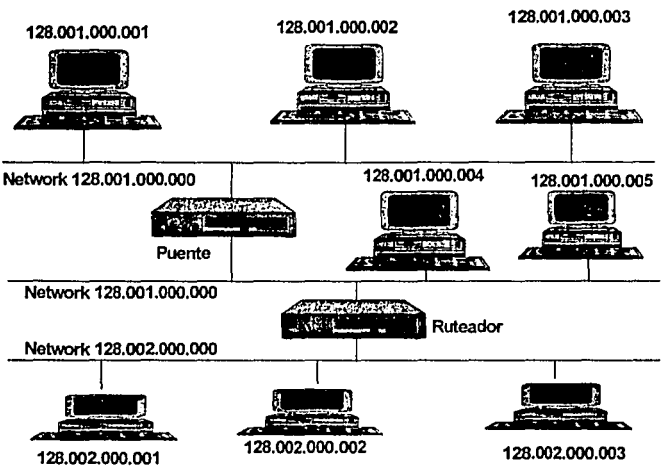

Fig. 2.5 Ejemplo de redes usando el formato de direccionamiento clase B

2.6 Direccionamientos de Subredes

Las subredes son subdivisiones lógicas de un número de red que pertenezca a Internet. Por razones técnicas o administrativas, en muchas organizaciones se divide una red dentro de diferentes redes. Esas redes independientes son entonces conectadas por ruteadores. Sin embargo, cada organización que desea conectarse a la Internet debe obtener un número individual de red.

Si múltiples redes TCP/IP son interconectadas por ruteadores, se deba asignar un diferente número a cada red. Sin embargo, si la red es parte de la Internet, no se puede arbitrariamente seleccionar cualquier número de red, dado que los números de red deben ser asignados por la NIC. Los direccionamientos de subredes permiten a una organización usar un único número de red de la Intenet para múltiples redes físicas. Las subredes pueden ser usadas con cualquier clase de formato de direccionamiento, excepto la clase D (MULTICAST).

En la fig. 2.6 se han creado las subredes de una red de formato clase B. El administrador usa el tercer octeto de direccionamiento para identificar las dos subredes de la red 135.1.5.0.0.

El ruteador recive todo el tráfico para la red 135.013.000.000 y se selecciona la interface correcta basada en el tercer octeto (del identificador de la subred) del direccionamiento.

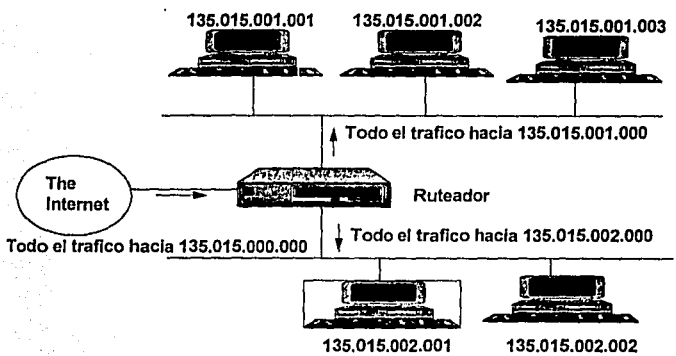

Fig. 2.6 Direccionamiento de subredes

El enmascaramiento de la subred permite a la parte del host del direccionamiento Internet ser dividido en dos partes. Una parte es para identificar el número de la subred, y la otra parte es para identificar el host en la subred.

El host o router usa el bit principal del direccionamiento IP para determinar la clase. Una vez que la clase de direccionamiento es determinada, el host puede fácilmente distinguir entre el bit usado para identificar la parte de direccionamiento del host. Esto es debido a que los 32 bits de la máscara de la subred son configurados para permitirle al host hacer esa distinción.

Los bits en la máscara de la subred y en el direccionamiento Internet tienen correspondencia uno a uno.

Los bits en la máscara de la subred son colocados a 1 si el dispositivo está examinando el direccionamiento debe tratar al correspondiente bit en el direccionamiento Internet como parte original del número de red o como parte del número de subred. Los bits en la máscara son colocados a 0 si el dispositivo debe tratar al bit como parte de la subred del número de host. En otras palabras, después de que la clase de direccionamiento IP es determinada, cualquier bit de número original del host que tenga un bit correspondiente colocado en la misma máscara de la subred es usado para identificar el número de subred.

La figura 2.7 muestra un enmascaramiento de subred

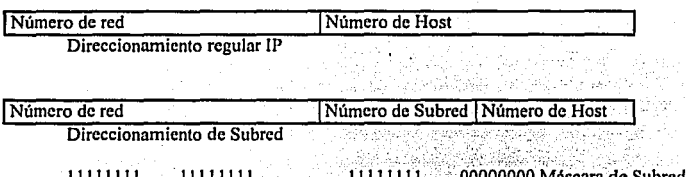

Fig. 2.7 Máscara de Subred

2.7 Subredes: Diagrama 1

Supongamos que la NIC asigna el siguiente direccionamiento clase B 128.001.000.000.
Se necesita establecer 254 subredes con cada subred capaz de soportar hasta 254 hosts.

Lo anterior es una simple forma de subdireccionamiento, el primero y segundo octetos del direccionamiento IP identifica a la red, el tercer octeto identifica a la subred, y el cuarto octeto identifica al host en la subred.

Solución

Podemos expresar el direccionamiento asignado por la NIC en formato binario quedando:

128.001.000.000= 10000000.00000001.00000000.00000000

Los dígitos binarios subrayados representan la parte de la red en el direccionamiento Imterner asignado por la NIC.

Ocho dígitos binarios son requeridos para definir 254 subredes. Las subredes deben ser numeradas de la 1 a la 254.

En la tabla 2.8 se ilustra la conversión de Decimal a binario

Decimal	Binario
1	00000001
2	00000010
.	.
.	.
.	.
254	11111110

Fig. 2.8 Direccionamiento de subredes en decimal y binario

En este caso seleccionamos los ocho bits más significativos en la parte del host del direccionamiento Internet para definir las subredes. Estos bits son desplegados a continuación en texto en negritas:

128.001.000.000 = 10000000.00000001.**00000000**.00000000

Debemos definir un enmascaramiento en la subred tal que todos los bits en la red y en el futuro campo de la subred sean colocados a 1 y todos los bits en los futuros campos de los hosts sean colocados a 0.

Número de red = 10000000.00000001.**00000000**.00000000 = 128.001.000.000
Máscara en la subred=11111111.11111111.11111111.00000000 =255.255.255.000

Esta máscara en la subred debe ser configurada en cada host y son definidas para cada ruteador. Debes de usar la misma máscara para todo el conjunto de redes físicas que comparten el mismo direccionamiento Internet.

Las 254 subredes deben tener los siguientes direccionamientos:

Subred # 1 10000000.00000001.**00000001**.00000000 = 128.001.001.000
Subred # 2 10000000.00000001.**00000010**.00000000 = 128.001.002.000
Subred # 3 10000000.00000001.**00000011**.00000000 = 128.001.003.000

.
.
.

Subred # 254 10000000.00000001.**11111110**.00000000 = 128.001.254.000

El rango que se le debe asignar a la subred # 1

Subred # 1 10000000.00000001.**00000001**.00000000 = 128.001.001.000
Direc. mín. 10000000.00000001.**00000001**.00000001 = 128.001.001.001
Direc. máx. 10000000.00000001.**00000001**.11111110 = 128.001.001.254

Mensajes IP: Mensajes limitados y directos

Mensajes limitados

Un paquete enviado a la dirección IP 255.255.255.255 o a la dirección 0.0.0.0 es clasificado como un paquete de "mensaje limitado". En un mensaje el paquete destino para la red local, la parte identificadora de la red y la parte identificadora del host del direccionamiento destino si para ambos todos son unos (255.255.255.255) o para la misma implementación todos ceros (0.0.0.0)

Los mensajes limitados nunca deben pasar através de un ruteador.

El único dispositivo por el cuál pueden a través son los repetidores.

Mensajes Directos

Un paquete que es enviado a la dirección IP donde solo la porción del host del direccionamiento IP son todos unos o todos ceros tales como (180.100.255.255 ó 180.100.0.0) es clasificado como un paquete de "mensaje dirigido".

Los mensajes dirigidos pueden pasar a través de un ruteador y pueden enviar mensajes a todos los hosts de la red destino.

2.8 Esquema sin subredes

A través de intercambio de información de ruteo, tal como se muestra en la fig. 2.9, cada uno de los ruteadores conoce acerca de las tres redes que forman la pequeña Internet IP.

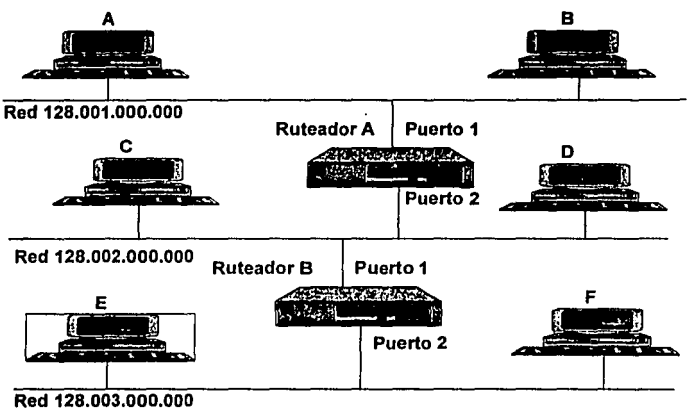

Fig. 2.9 Modelo de mensajes IP sin subredes

La tabla 2.10 despliega dos receptores de los mensajes transmitidos porel Host. C.

Remitente	Dirección destino IP	Recibidor
Host C	255.255.255.255	Host D, RTR_A Port 2, Rtr_b Port 1
Host C	128.1.255.255	Host A, Host B, Rtr_A Port
Host C	128.2.255.255	Host D, Rtr_A Port 2, Rtr_B Port 1
Host C	128.3.255.255	Host E, Host F, Rtr_B PORT 2

Fig. 2.10 Ejemplo de bloques de datos recibidos por el Host C

2.9 Diagrama con subredes

Un mensaje directo puede ser enviado a una subred específica.
Un mensaje directo no puede ser enviado a todas las subredes .
Para intentar enviar bloques de datos a todas las subredes, es necesario permitir reenvío de mensajes limitados a través del ruteador.

En el siguiente ejemplo en la figura 2.11, asumimos una mascara de subred 255.255.255.0

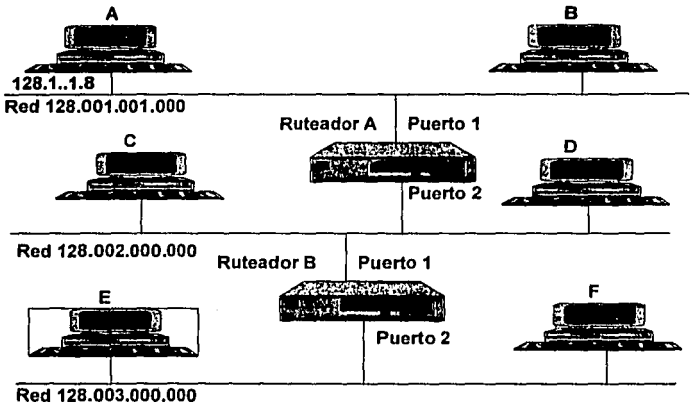

Fig. 2.11 Ejemplo de mensajes IP sin subredes

En la tabla 2.12 se despliegan ejemplos de los receptores de los mensajes transmitidos por el host C .

Remitente	Dirección destino IP	Recibidor
Host C	255.255.255.255	Host D, RTR_A Port 2, Rtr_b Port 1
Host C	128.1.1.255	Host A, Host B, Rtr_A Port 1
Host C	128.1.2.255	Host D, Rtr_A Port 2, Rtr_B Port 1
Host C	128.1.3.255	Host E, Host F, Rtr_B PORT 2

Fig.. 2.12 Ejemplo de bloques de datos recibidos por el Host C

2.10 Protocolo de Dirección de Resolución (ARP).

Si en una red dada, dos host desean comunicarse, ambos deben conocer más uno del otro que solo la dirección Internet. También deben conocer uno del otro el direccionamiento físico, por lo tanto pueden usar protocolos de la capa de enlace para transmitir bloques sobre el medio local.

Los diseñadores de ethernet asignarón 48 bits para el direccionamiento ethernet. Cada controlador ethernet viene con un direccionamiento asignado de fábrica. Los vendedores que manufacturan equipo ethernet tienen que registrarlo con una autoridad central para asegurarse que los números que asignaron no entren en conflicto con el de algún otro fabricante.

Desafortunadamente, no existe una relación entre direcccionamiento ethernet y direccionamiento Internet.

ARP: Operación básica

La Figura 2.13 ilustra como ARP es usado para resolver el problema de direccionamiento dinámico

- El Host A desea comunicarse con el Host B pero no conoce el direccionamiento de este
- El Host A ha aprendido la dirección del Host B a través del nombre de servicio (Name Service)
- El Host A conoce que ambos dispositivos están conectados a la misma red física, dado que tienen el mismo campo de red en su direccionamiento Internet. Si no comparten el mismo campo en la red, el destinatario debe estar localizado en otra red. Si este fuera el caso, el Host A debe enviar el paquete al ruteador default y dejar que los ruteadores liberen el mensaje a la red apropiada.

2.10 Protocolo de Dirección de Resolución (ARP).

Si en una red dada, dos host desean comunicarse, ambos deben conocer más uno del otro que solo la dirección Internet. También deben conocer uno del otro el direccionamiento físico, por lo tanto pueden usar protocolos de la capa de enlace para transmitir bloques sobre el medio local.

Los diseñadores de ethernet asignarón 48 bits para el direccionamiento ethernet. Cada controlador ethernet viene con un direccionamiento asignado de fábrica. Los vendedores que manufacturan equipo ethernet tienen que registrarlo con una autoridad central para asegurarse que los números que asignaron no entren en conflicto con el de algún otro fabricante.

Desafortunadamente, no existe una relación entre direccionamiento ethernet y direccionamiento Internet.

ARP: Operación básica

La Figura 2.13 ilustra como ARP es usado para resolver el problema de direccionamiento dinámico

- El Host A desea comunicarse con el Host B pero no conoce el direccionamiento de este
- El Host A ha aprendido la dirección del Host B a través del nombre de servicio (Name Service)
- El Host A conoce que ambos dispositivos están conectados a la misma red física, dado que tienen el mismo campo de red en su direccionamiento Internet. Si no comparten el mismo campo en la red, el destinatario debe estar localizado en otra red. Si este fuera el caso, el Host A debe enviar el paquete al ruteador default y dejar que los ruteadores liberen el mensaje a la red apropiada.

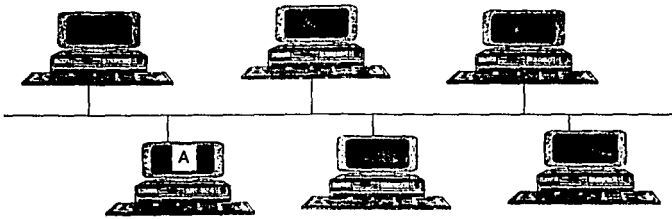

Fig. 2.13 Resolución de problemas de direccionamiento dinámico a través de ARP

2.11 Requerimientos del ARP

El Host A está preguntando que el Host con el direccionamiento Internet requerido responda con su direccionamiento Ethernet. Todos los Hosts de la red reciben el requerimiento, pero solo el Host B responderá.

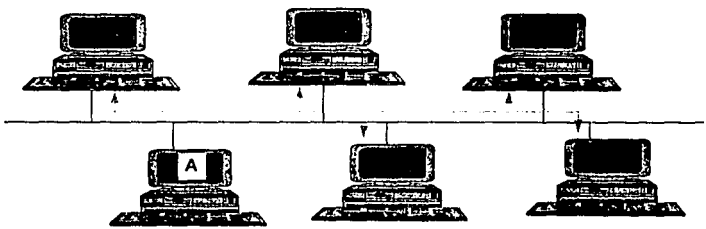

Fig. 2.14 Requerimiento ARP

2.12 Respuesta ARP

El Host B reconoce el direcionamiento Internet y responde el requerimiento del Host A enviando una respuesta ARP que contiene el direccionamiento Ethernet.

El Host A conoce ahora el direccionamiento Ethernet que necesita para enviar paquetes al Host B sobre la red física

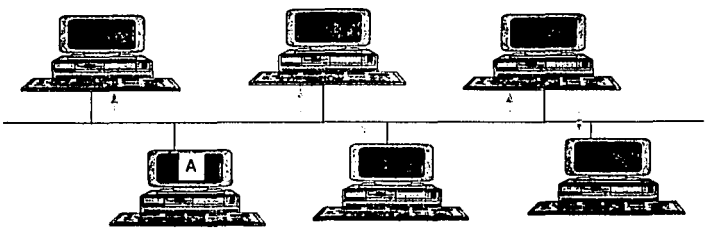

Fig. 2.15 Respuesta ARP

Protocolo de resolución de direccionamiento recursivo

Una máquina con un direccionamiento Internet es usualmente configurada por el administrador de la red cuando el software de comunicación es inicialmente instalado. El direccionmiento Internet de la máquina es almacenado en un archivo de configuración en un disco donde el sistema operativo puede encontrar el boot. La máquina sin disco únicamente identifica a su servidor propio usando su direccionamiento Ethernet.

La máquina requerida debe esperar hasta que reciba respuesta de uno o más servidores localizados en la red. Una vez que la máquina aprende su direccionamiento Internet, puede comunicarse a través de Internet.

El protocolo que las máquinas sin disco usan para los requerimientos al servidor para que este les proporcione su direccionamiento Internet es llamado Protocolo de Resolución de Direccionamiento Recursivo (RARP). Este protocolo usa la misma estructura que el ARP

2.13 RARP: Operación

El siguiente ejemplo ilustra como un Host sin disco usa RARP para determinar su direccionamiento Internet

RARP: Requerimiento

En la figura 2.16 el Host A envía mensajes de requerimientos RARP incluyendo su direccionamiento Ethernet en el campo de direccionamiento del Hardware destino. Todas las máquinas en la red reciben el requerimineto dado que se trata de un mensaje.

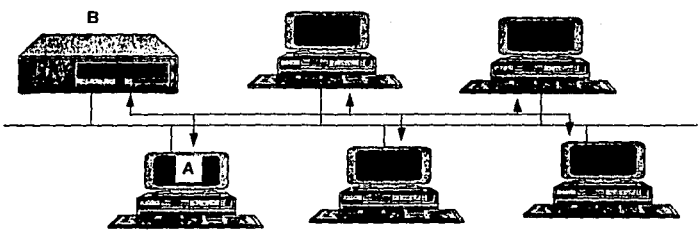

Fig. 2.16 Requerimiento RARP

2.14 RARP: Respuesta

En la figura 2.17, el server B procesa el requerimiento y envía una respuesta. Para que el RARP sea un éxito, la red debe contener por lo menos un server RARP porque el requerimiento puede no ser enviado por el ruteador al server localizado en otra red.

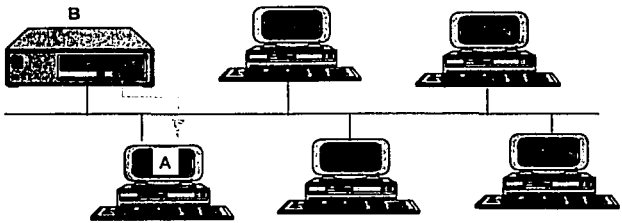

Fig. 2.17 Respuesta RARP

CAPITULO 3

PROTOCOLO INTERNET (IP)

Este capítulo considera los fundamentos principales de conexión que proporciona el protocolo Internet (IP), uno de los dos principales protocolos usados en interconectividad.

IP proporciona tres importantes definiciones :

1.- IP define la unidad básica de transferencia de datos usada a través de Internet TCP/IP. Esto es, especifica el formato exacto de datos que pasan a través de la red Internet.

2.- El Software de IP ejecuta las funciones de ruteo eligiendo la ruta por la cual los datos serán enviados.

3.- IP incluye un conjunto de reglas que incorporan la idea de liberación de paquetes. Las reglas caracterizan como los hosts y los gateways deben procesar los paquetes, como y cuando los mensajes de error deben ser generados, y las consideraciones bajo las cuales los paquetes puedan ser desertados.

El protocolo IP es responsable de transferir bloques de datos a través de un conjunto de redes interconectadas. IP recibe esos bloques de protocolos de alto nivel tales como TCP o UDP, y entonces los transmite a través de Internet.

IP provee servicios de desconexión entre estaciones finales, cada datagrama transporta el direccionamiento destino y es ruteado a través del sistema independiente de el resto de los datagramas.

No se establecen conexiones o circuitos lógicos.

IP también proporciona un mecanismo de fragmentación y reensamble de datagramas para la transmisión a través de redes en las cuales el máximo tamaño del paquete es más pequeño que el tamaño del datagrama.

El modulo de Software IP reside en todos los hosts y ruteadores del sistema Internet. Estos módulos comparten reglas comunes para interpretación de campos de direccionamiento y fragmentación y ensamble de dataramas a través de Internet. Adicionalmente, estos módulos tienen procedimientos para hacer decisiones de ruteo y otras funciones de ayuda, tales como mensajes ARP o ICMP.

CAPITULO 3

PROTOCOLO INTERNET (IP)

Este capítulo considera los fundamentos principales de conexión que proporciona el protocolo Internet (IP), uno de los dos principales protocolos usados en interconectividad.

IP proporciona tres importantes definiciones :

1.- IP define la unidad básica de transferencia de datos usada a través de Internet TCP/IP. Esto es, especifica el formato exacto de datos que pasan a través de la red Internet.

2.- El Software de IP ejecuta las funciones de ruteo eligiendo la ruta por la cual los datos serán enviados.

3.- IP incluye un conjunto de reglas que incorporan la idea de liberación de paquetes. Las reglas caracterizan como los hosts y los gateways deben procesar los paquetes, como y cuando los mensajes de error deben ser generados, y las consideraciones bajo las cuales los paquetes puedan ser desertados.

El protocolo IP es responsable de transferir bloques de datos a través de un conjunto de redes interconectadas. IP recibe esos bloques de protocolos de alto nivel tales como TCP o UDP, y entonces los transmite a través de Internet.

IP provee servicios de desconexión entre estaciones finales, cada datagrama transporta el direccionamiento destino y es ruteado a través del sistema independiente de el resto de los datagramas.

No se establecen conexiones o circuitos lógicos.

IP también proporciona un mecanismo de fragmentación y reensamble de datagramas para la transmisión a través de redes en las cuales el máximo tamaño del paquete es más pequeño que el tamaño del datagrama.

El modulo de Software IP reside en todos los hosts y ruteadores del sistema Internet. Estos módulos comparten reglas comunes para interpretación de campos de direccionamiento y fragmentación y ensamble de dataramas a través de Internet. Adicionalmente, estos módulos tienen procedimientos para hacer decisiones de ruteo y otras funciones de ayuda, tales como mensajes ARP o ICMP.

La comunicación en Internet es posible a través del paso de datos del módulo Internet de una máquina, al módulo Internet de otra máquina, hasta que el datagrama alcanza su destino final.

El datagrama es ruteando de una máquina a otra basada en el direccionamiento Internet transportado en el encabezado antes de alcanzar su destino final.

3.1 El Datagrama Internet

La analogía entre una red física y Internet TCP/IP es muy fuerte. En una red física, la unidad de transferencia es el frame que contiene el encabezado y los datos, donde el encabezado proporciona información como el direccionamiento origen y destino. La red Internet llama a esta unidad de transferencia básica como datagrama Internet, algunas veces referida también como datagrama IP. Como un típico frame físico de la red, el datagrama es dividido dentro de una área de encabezado y datos. También como un frame, el encabezado del bloque contiene el direccionamiento origen y destino así como el tipo de campo que identifica el contenido del bloque. La figura 3.1 muestra la forma de un datagrama.

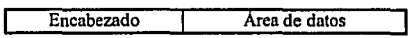

Fig. 3.1 Datagrama IP

3.2 IP y el modelo de Referencia OSI

La figura 3.2 muestra la capa dentro de la cual el protocolo IP trabaja dentro del módulo OS1.

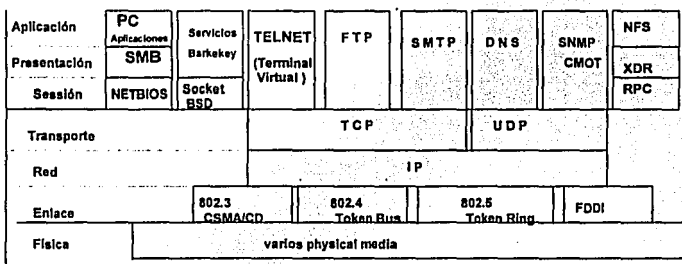

Fig. 3.2 Posición de IP en el STACK de Protocolos TCP/IP

Como se puede observar en la figura anterior, al trabajar en la capa de red, el protocolo IP es el encargado de asignar la dirección, el ruteo y la fragmentación de los paquetes de datos de una estación a otra.

3.2.1 Direccionamiento

El propósito fundamental del IP es el mover datagramas a través de conjuntos de redes interconectadas. Los datagramas son ruteados de un módulo Internet a otro a través de redes individuales basadas en la interpretación de direccionamientos Internet. Por lo tanto, una importante característica del IP es la implementación y reconocimiento del direccionamiento Internet.

Como se vio en el capítulo 2, el direccionamiento Internet está formado por campos de 32 bits divididos en campos de cuatro octetos. El direccionamiento propio consiste en dos partes:

. La parte de la red
. La parte del host

Existen cuatro clases de direccionamientos de formatos, A,B,C, y D.

3.3 Demultiplexando Protocolos de Transporte

Multiplexar es un proceso que coloca múltiples tipos de señales de comunicación sobre un canal de comunicación. Por otro lado, demultiplexar se refiere a la práctica de separar una entrada dentro de varias salidas,como se muestra en la figura 3.3

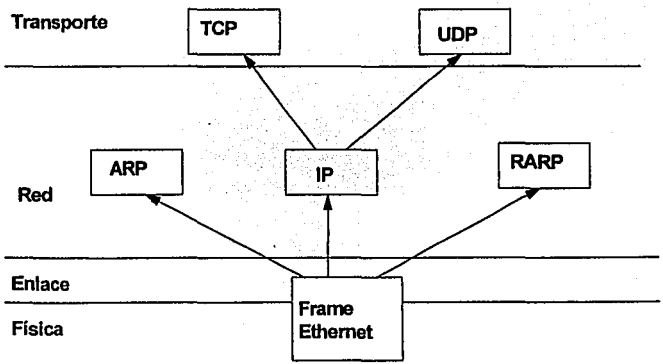

Fig. 3.3 Demultiplexando Protocolos de transporte

Los datagramas entrantes son demultiplexados y enviados al protocolo apropiado de la capa de transporte basados en el valor contenido en el campo "Protocolo" del encabezado IP.

El datagrama original IP coloca un valor en el campo de Protocolo para indicar si el protocolo de la capa de transporte original fue TCP o UDP . La máquina receptora usa esta información para reenviar los datagramas al proceso correcto de la capa de Transporte.

3.4 Tamaño de los Datagramas y Fragmentación

En un caso ideal, el bloque completo de datos IP cabe dentro de un frame físico, haciendo transmisiones a través de una red física eficiente. Para alcanzar tal eficiencia los diseñadores de IP tienen que seleccionar un tamaño máximo del datagrama tal que los datagramas siempre deben de caber dentro de un frame. Para entender el problema, necesitamos conocer acerca del hardware de la red, ya que cada tecnología de switcheo de paquetes permite un número máximo de datos que pueden ser transferidos dentro de un frame físico. Nos referimos a estos límites de red como unidad de transferencia máxima (MTU). Los tamaños de los MTU pueden ser muy pequeños: algunas tecnologías de hardware limitan transferencias de 128 octetos o menos.

Limitar a los bloques de datos a caber dentro del MTU más pequeño posible dentro de Internet realiza transferencias ineficientes cuando esos datagramas pasan a través de redes que pueden transportar frases de gran tamaño.

El software de TCP/IP elige el tamaño inicial más concerniente del datagrama y arregla la forma de dividir bloques de datos grandes dentro de piezas pequeñas cuando el datagrama necesita viajar a través de una red que tiene pequeños MTU.

Las piezas pequeñas dentro de las cuales los bloques de datos son divididos son llamados fragmentos, y el proceso de dividir un datagrama es conocido como fragmentación.

En la figura 3.4 se ilustra la fragmentación, la cual ocurre en los gateway colocados a lo largo de la ruta entre el datagrama origen y el último destino. El gateway recibe un datagrama de la red con un largo MTU y debe rutear a través de la red para la cual el MTU es más pequeño que el tamaño del datagrama.

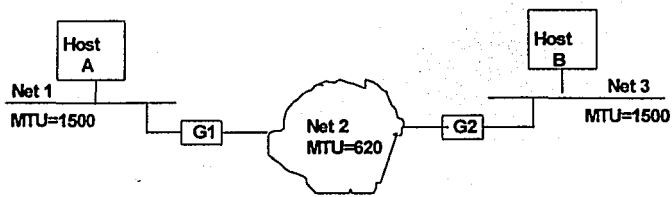

Fig. 3.4 Fragmentación

En la figura anterior, ambos hosts están conectados directamente a las Ethernets las cuales tienen un MTU de 1500 octetos. Esto es, ambos hosts pueden generar y enviar bloques de datos hasta de 1500 octetos de longitud. La ruta entre ellos, sin embargo, concluye una red con un MTU de 620. Si el host A envía al host B un datagrama mayor a 620 octetos, el gateway G1 fragmenta el datagrama. Similarmente si el host B envía un datagrama grande a A, el gateway G2 fragmentaría el datagrama. Los fragmentos deben ser reensamblados para producir una copia completa del datagrama original antes de que pueda ser procesada a su destino.

3.4.1 Reensamblando los Fragmentos

En Internet TCP/IP, una vez que el datagrama ha sido fragmentado, los fragmentos viajan en bloques separados hacia su destino final donde serán reensamblados.

Preservar todos los fragmentos hacia su destino final tiene dos desventajas. Primero, porque el datagrama no es reensamblado inmediatamente despúes de atravesar la red con un MTU pequeño, los pequeños fragmentos deben ser transportados de el punto de fragmentación hacia su destino final. Reensamblar los bloques de datos en el destinatario puede ser ineficiente. Segundo, si se perdió algún fragmento el datagrama no puede ser reensamblado.

La máquina que está recibiendo empieza a reensamblar cuando recibe el fragmento inicial. Si el tiempo expira antes de que todos los fragmentos arriben, la máquina receptora descarta las piezas restantes sin procesar el bloque.

3.4.2 Campos que controlan la Fragmentación

Cuatro campos en el encabezado IP son usados para controlar la fragmentación y reensamble de datagrama:

. Identificación	Proporciona un número entero único que identifica dos fragmentos del datagrama. El origen del datagrama asigna este valor al datagrama original sin fragmentar. Si el datagrama es fragmentado por un ruteador, este valor es copiado dentro del campo de identificación de todos los fragmentos resultantes.

. Longitud Total — La longitud de los bloques de datos (medida en octetos) incluyendo el encabezado y el dato. Todos los hots deben de estar preparados para aceptar bloques de datos hasta de 576 octetos. Los Hots sólo deben enviar bloques de datos mayores de 576 octetos cuando el administrador de la red está seguro que el destinatario está preparado para aceptar bloques de datos grandes.

. Fragment Offset — Indica adonde pertenece el fragmento dentro del bloque de datos original. El valor está medido en unidades de 8 octetos desde el comienzo del datagrama original. El primer fragmento debe ser colocado a cero.

. Flags — Controlan la fragmentación. El conjunto de estos bits determina donde debe ser la fragmentación de los bloques de datos. Si el datagrama es fragmentado, el campo FLAG es usado para indicar donde hay más fragmentos o si ese es el último fragmento de una serie de fragmentos.

3.5 Tipo de Servicio (TOS)

El campo de tipo de servicio es usado para indicar la calidad de servicio deseada por el emisor del datagrama. Desafortunadamente no hay garantía de que el receptor responda con el tipo de servicio requerido. En la figura 3.5 se muestra el campo de tipo de servicio.

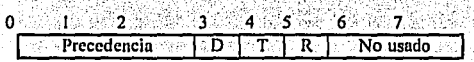

Fig. 3.5 Campo de Tipo de Servicio

3.6 BITS PROCEDENTES.

Los Bits procedentes en el campo TOS son usados por el host fuente para transmitir a otro dispositivo de Internet la importancia del datagrama.

Esos bits fueron originalmente diseñados para proporcionar un mecanismo que permitiera al ruteador tratar ciertos bloques de datos como más importantes que otros tipos de tráficos. Tres bits son usados para especificar la procedencia del datagrama. El valor de este campo debe caer dentro de un rango de 0 (bajo) a 7 (alto). La tabla 3.6 despliega los valores y significados de los bits procedentes.

Valor	Precedencia
111	Control de red
110	Control de la interred
101	CRITIC/ECP
100	Flash Override
011	Flash
010	Inmediato
001	Prioridad
000	Rountine

Fig. 3.6 Valores de los bits precedentes

3.6.1 Tiempo de Vida (TTL)

El campo de tiempo de vida es colocado por el host fuente y especifica el tiempo que el datagrama tiene permitido para circular en el sistema Internet. El valor para este campo es especificado en segundos. El tiempo máximo de vida es 255 segundos.

Estimar el tiempo exacto es difícil porque los gateways usualmente no conocen el tiempo de tránsito en las redes físicas. Algunas reglas simplifican el procesamiento y hacen más fáciles el manejo de datagrama sin usar relojes en sincronía. Primero, cada gateway a lo largo de la ruta entre el origen y el destino decrementa el campo TTL en 1 cuando este procesa el encabezado de el datagrama. Además para manejar los casos de sobrecarga los gateways que introducen retardos largos, cada gateway registra el tiempo local cuando el datagrama arriba, y decrementa el TTL por el número de segundos que el datagrama permanece dentro de el gateway esperando para el servicio.

Cuando el campo TTL alcanza el 0, el gateway descarta el datagrama y envía un mensaje de error hacia el origen. Guardar un tiempo máximo de vida para los datagramas es interesante porque garantiza que el datagrama nunca viajara a través de Internet indefinidamente, aunque las tablas de ruteo se corrompan y dos gateways ruteen datagramas en círculos.

3.6.2 Opciones para Datagramas Internet

El campo opciones IP puede o no aparecer en un datagrama individual, Sin embargo, deben estar implementados por todos los módulos IP que residen en los hosts y en los ruteadores. El principal propósito del campo opciones es el de proporcionar al administrador de la red una herramienta para probar y depurar la red. El procedimiento de las opciones es una parte integral del protocolo IP, sin embargo, todas las implementaciones standares deben incluirlo.

La longitud del campo opciones varían dependiendo de que opciones sean seleccionadas.

Algunas opciones ocupan un octeto de longitud; estos consisten de un octeto de código de opciones. Otros campos de opciones tienen longitud variable.

Cuando las opciones son presentadas en datagramas, estas aparecen contínuas, sin separadores especiales a través de ellas.

3.7 Opciones de Registrar Rutas

Las opciones de ruteo y registro del tiempo, son forma de monitorear o controlar como los gateways rutean los datagramas .

La opción de registrar rutas permite al hosts reservar espacio para la lista vacía de direccionamientos IP. Cada ruteador que procesa el datagrama es requerido para añadir direcciones a la lista de direcciones IP. Esta opción es útil para mantener la ruta del datagrama como es ruteada através de Internet . Figura 3.7

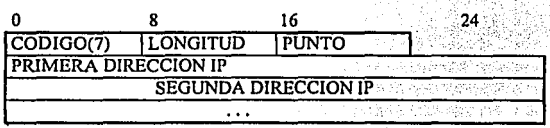

Fig. 3.7 Formato de registro de un datagrama IP

3.8 Opciones de Ruteo Fuente

La opción de ruteo fuente proporciona un método al host fuente para especificar la ruta a través de Internet. Los lugares a los que se envía se encuentran en una lista secuencial de direccionamientos Internet que los datagramas deben seguir para alcanzar su destino. Por supuesto, este ruteo solamente es útil para la gente que conoce la topología de la red.

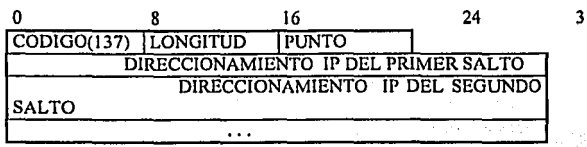

Fig. 3.8 Opciones de ruteo fuente

3.9 Encapsulación del Frame IP

La figura 3.9 muestra como el datagrama IP es encapsulado como una porción del dato del frame Ethernet.

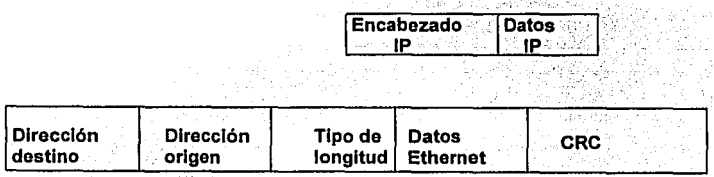

Fig. 3.9 Paquete Ethernet

3.10 Formato del Encabezado IP y Descripción de Campos

La fig. 3.10 muestra el formato del encabezado IP y las descripciones de campo, las cuales son descritas a continuación:

Versión	IHL	Tipo de Servicio	Longitud Total	
Identificación			Flags	Fragmento
Tiempo de vida		Protocolo	Encabezado IP	
Direccionamiento IP Origen				
Dirección IP Destino				
Opciones				Padding

Fig. 3.10 Formato del encabezado IP

Versión — Indica el formato del encabezado en Internet.

IHL — (Internet Header Length) Es la longitud del encabezado en la Internet. Debe ser usado para localizar el inicio del datagrama porque el tamaño del encabezado puede ser dependiente de que opciones sean seleccionados.

Tipo de servicio — Especifican la procedencia y el TOS requerido por el HOST origen .

Longitud total — Es la longitud del datagrama en octetos, incluyendo el encabezado y el dato Internet. Todos los hosts aceptan bloques de datos hasta 576 octetos.

Banderas — Usado para controlar la fragmentación en los datagrmas .

Tiempo de vida (TTL) — Indica el tiempo máximo que el datagrama tiene permitido permanecer en el sistema Internet.

Protocolo	El campo protocolo es usado para demultiplexar los protocolos de alto nivel.
Direccionamiento fuente	Es la dirección IP de 32 bits del host fuente.
Direccionamiento Destino	Es la dirección IP de 32 bits a la cual será enviada el bloque de datos.

CAPITULO 4

RUTEO IP

4.1 Arquitectura de Internet

El sistema Internet puede ser visto como una colección de Hosts y redes interconectadas a través de ruteadores IP . El protocolo IP fue diseñado para soportar comunicaciones entre hosts heterogéneos o redes heterogéneas. Los ruteadores son dispositivos que conectan dos o más redes y controlan el tráfico de datos entre ellas.

Dos hosts en la misma red son capaces de enviar paquetes uno al otro. También , cada red es capaz de aceptar paquetes de una red remota y liberarlos hacia un destino específico de la red local.

Si dos hosts en diferentes redes desean comunicarse, el host origen envía el paquete al ruteador apropiado. El ruteador reenvía cada paquete a través del sistema de ruteadores y redes hasta alcanzar al ruteador conectado en la misma red del host destino. Este ruteador final debe transmitir el paquete a la dirección física del host destino.

Los ruteadores envían paquetes basados en el número de red destino, y no en la dirección física de los hosts destino. Dado que el ruteo es basado en números de red, el promedio de información que el ruteador necesita es proporcional al número de redes que forman Internet, no el número de máquinas.

En la fig. 4.1 , el Host A puede comunicarse directamente con el Host B porque están conectados a la misma red física. Sin embargo, si el Host A desea comunicarse con el Host C, el Host A debe transmitir el datagrama al ruteador de salida más cercano. Este ruteador inserta el datagrama dentro del sistema de ruteadores que conectan Internet. El datagrama es enviado de un ruteador a otro hasta alcanzar al ruteador que está conectado a la misma red física del Host C. Este ruteador final usa los servicios provistos por la red local para deliberar el paquete de datos al Host C.

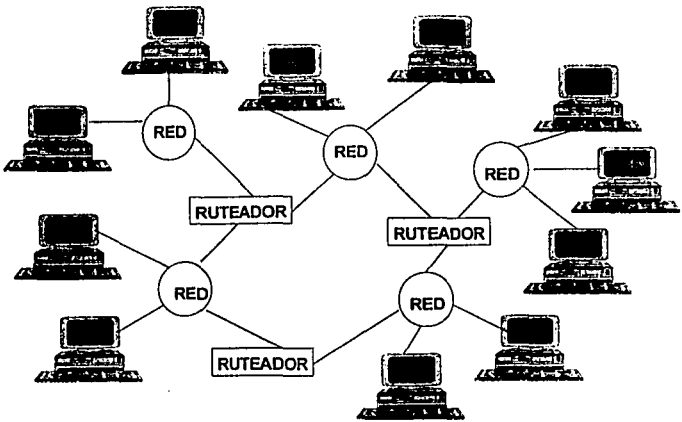

Figura 4.1 Arquitectura de Internet

4.2 Ruteando dentro de Internet

En el sistema de ruteo de paquetes, rutear se refiere al proceso de elegir la ruta sobre la cual enviar los paquetes, y ruteador se refiere al dispositivo que realiza la tárea.

El ruteo ocurre en diferentes niveles. Por ejemplo, en una red de área local con múltiples conexiones físicas, la red es responsable de rutear los paquetes desde que entran hasta que salen. Dado que el ruteo interno esta contenido en el interior de la red de área ancha. Los dispositivos en el exterior no pueden participar en las decisiones; ellos solamente ven a la red como una entidad que libera paquetes.

Rutear dentro de Internet puede resultar difícil, especialmente entre dispositivos con múltiples conexiones físicas . Idealmente, el software de ruteo debe examinar condiciones como carga de tráfico en la red, longitud del datagrama, o el tipo de servicios especificando en el encabezado del datagrama cuando se elige la mejor ruta.

4.3 Ruteo Directo

El ruteo se puede dividir en dos formas : ruteo directo y ruteo indirecto. En el ruteo directo la transmisión de paquetes dentro de una misma red de una máquina a otra es directa y no requiere los servicios de un ruteador.

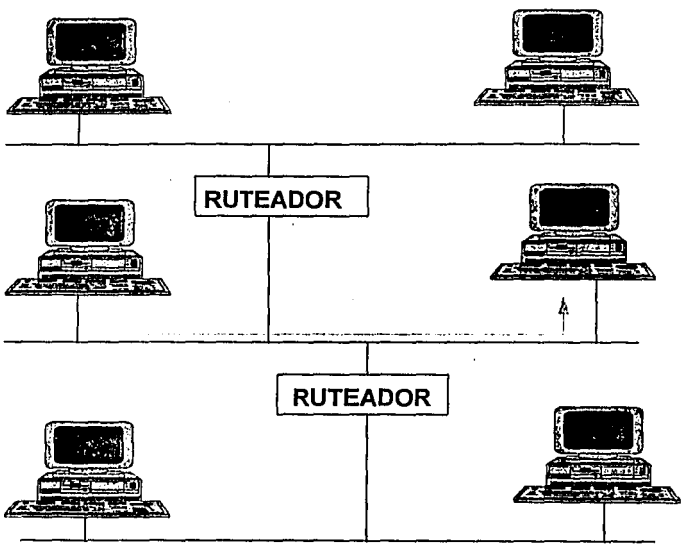

Fig. 4.2 Ruteo Directo

4.3.1 Liberación de paquetes sobre una misma red

Sabemos que una misma máquina conectada en una red puede enviar un tramo directamente a otra máquina en la misma red. Para transmitir un datagrama IP, el transmisor encapsula el datagrama dentro de un frame físico, mapea la dirección IP destino dentro de un direccionamiento físico y usa el hardware de la red para deliberarlo. En este caso , el direccionamiento fuente IP y el direccionamiento Ethernet fuente son asignados al host fuente y los direccionamientos IP y Ethernet destino son asignados al host destino.

La distribución es el paso final en la transmisión de datagramas , aunque el datagrama atraviese muchas redes y ruteadores intermediarios.

El ruteador final a lo largo de la ruta entre el datagrama origen y su destino lo conectará a la misma red física del destinatario. Esto es, el ruteador que finalmente libera el datagrama usa ruteo directo.

Ruteo indirecto

El ruteo indirecto ocurre cuando el destinatario no está directamente conectado a la red. Esto requiere que el host origen envíe el datagrama a un ruteador para que lo libere. Este tipo de ruteo es más complejo debido a que el host fuente debe identificar no solamente el destinatario final, sino también el ruteador a través del cual debe pasar el datagrama. Es entonces trabajo del ruteador enviar el datagrama hacia la red destino.

Para visualizar como trabaja el ruteo indirecto, imaginemos una gran red con varias redes interconectadas con ruteadores pero con solo dos hosts en los extremos. Cuando un host quiere enviarle al otro, encápsula el datagrama y lo envía al ruteador más cercano. Una vez que el frame alcanza al ruteador, el software extrae el datagrama encapsulado, y la rutina del ruteo IP selecciona el próximo ruteador a lo largo de la ruta hacia el destinatario. El datagrama es nuevamente colocado dentro de un frame y enviado sobre la siguiente red física al segundo ruteador, y asi sucesivamente hasta que pueda ser deliberado directamente.

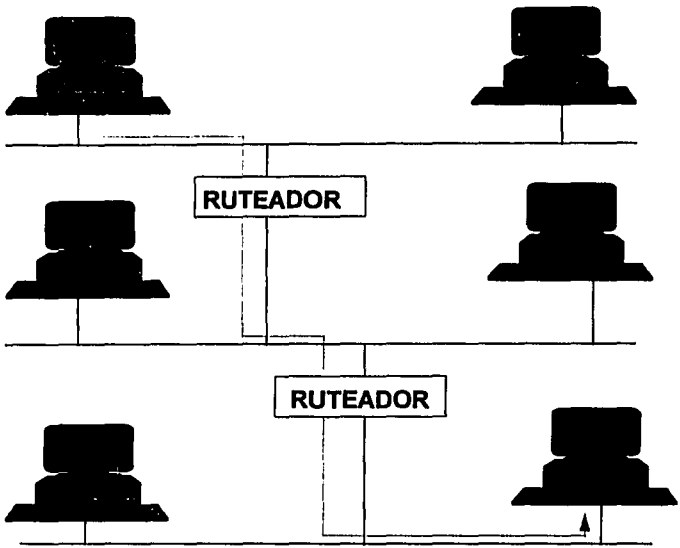

Fig. 4.3 Ruteo Indirecto

4.4 Tablas de ruteo

Un ruteador IP toma la decisión de transmitir los datagramas buscando en sus tablas de ruteo. El ruteador ejecuta esta tárea usando una clave de búsqueda, la cuál consiste en el número de red IP obtenido del campo de direccionamiento de cualquier datagrama IP .

Si el destinatario está directamente conectado a la red, el ruteador libera al paquete directamente sin usar los servicios de otro ruteador. Si el destinatario esta en una red remota, el ruteador debe enviar el paquete a otro ruteador cerca del destino final .

Mantener correctamente las tablas de información de todos los ruteadores en una red Internet grande es una tárea difícil. Las tablas de ruteo deben mantenerse dinámicas para reflejar la topología actual del sistema Internet. Para cumplir esta tárea el ruteador normalmente participa en ruteos distribuidos y algorítmos con otros ruteadores.

Algunos de los protocolos de ruteo usados para intercambiar información en la red incluyen al Protocolo de Información de Ruteo (Rip), el Open Shortest Path First Protocol (OSPF), el Exterior Gateway Protocol (EGP) y el Border Gateway Protocol (BGP) . Dependiendo de la estructura de Internet, algunos ruteadores pueden participar en más de un protocolo de ruteo IP.

La figura 4.4 ilustra una pequeña Internet compuesta de cuatro redes y tres ruteadores.

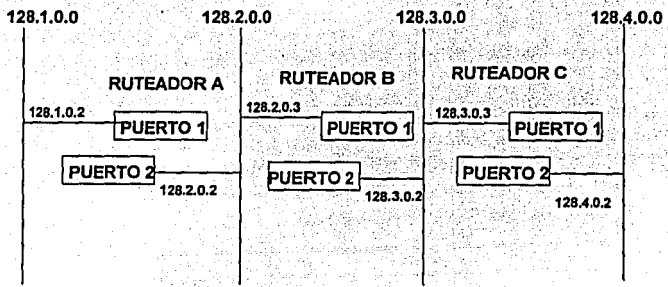

Fig. 4.4 Ejemplo de una Internet pequeña

El ruteador A usa el Protocolo de Resolución de Direccionamiento (ARP) para encontrar el direccionamiento físico que corresponda al direccionamiento Internet para cualquier host o ruteador que este directamente conectado a su red.

Las tablas de ruteo para la figura anterior son desplegadas de las tablas 4.5 a la 4.7 : Las tablas de ruteo contienen una fila para cada ruteador . Las columnas de las tablas de ruteo incluyen el número de red IP destino, el direccionamiento IP del siguiente salto del ruteador, y la métrica la cuál es usada para seleccionar el menor costo de ruteo si existe más de una ruta existente para la red destino.

Red destino	Siguiente salto del ruteador	Metrica(saltos)
128.1.0.0	Directo al puerto 1	0
128.2.0.0	Directo al puerto 2	0
128.3.0.0	128.2.0.3	1
128.4.0.0	128.2.0.3	2

tabla 4.5 Tablas de ruteo para el Ruteador A

Red destino	Siguiente salto del ruteador	Metrica(saltos)
128.1.0.0	128.2.0.2	1
128.2.0.0	Directo al puerto 1	0
128.3.0.0	Directo al puerto 2	0
128.4.0.0	128.3.0.3	1

tabla 4.6 Tablas de ruteo para el Ruteador B

Red destino	Siguiente salto del ruteador	Metrica(saltos)
128.1.0.0	128.3.0.2	2
128.2.0.0	128.3.0.2	1
128.3.0.0	Directo al puerto 1	0
128.4.0.0	Directo al puerto 2	0

tabla 4.7 Tablas de ruteo para el Ruteador C

4.5 Modelo de Operación

El modelo de operación para transmitir un datagrama de un host a otro sobre Internet se muestra en la figura 4.8. Este ejemplo involucra al host origen (Host A), y al host destino (Host B), tres ruteadores intermedios y cuatro distintas redes físicas. Internet y el direccionamiento Ethernet para cada host y cada punto del ruteador también son desplegados.

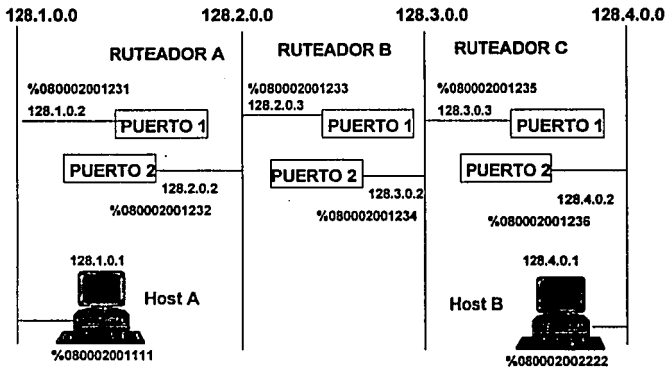

Fig. 4.8 Ejemplo de transmision sobre la Internet

La ruta que el datagrama toma no es determinado por el ruteador central, es el resultado de examinar cada una de las tablas de rutas usados en la jornada. Cada ruteador define solo el siguiente ruteador y así sucesivamente para enviar el paquete IP.

Host A

El Host A en la red 128.1.0.0 desea conectarse con el Host B en la red 128.4.0.0 usando el protocolo Telnet. Como el paquete es mandado de un ruteador a otro, el encabezado IP definido por el Host A permanece constante. El único direccionamiento que cambia al mover los paquetes hacia su destino final son el direccionamiento Ethernet origen y destino.

Paquetes en la red 128.1.0.0

Dado que el Host A y el Host B radican en diferentes redes, el Host A debe ejecutar ruteo indirecto y usar los servicios de un ruteador IP. Al final de la inicialización, el Host A ha aprendido que el direccionamiento IP del Defaul Gateway es el 128.1.0.2.

Como resultado, el Host A sabe que debe usar al ruteador A para transmitir paquetes a cualquier Host residente en una red diferente. Si el Host A no tiene ninguna entrada en su cache ARP para el dispositivo 128.1.0.2, debe enviar un requerimiento ARP y esperar que el ruteador A responda .

Dado que existen mapeos de direccionamiento, el Host A transmite un frame Ethernet con un direccionamiento MAC destino % 080002001231 (Ruteador A), el direccionamiento MAC origen % 080002001111 (Host A), y un tipo de campo 0800h (IP). La estructura del paquete colocado en la red 128.1.0.0 se muestra en la fig. 4.9

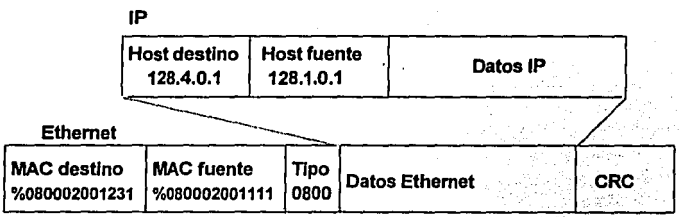

Fig. 4.9 Paquete en la Red 128.1.0.0

Paquetes en la red 128.2.0.0

Después de recibir el paquete, el ruteador A remueve el encabezado Ethernet y pasa el datagrama a un proceso IP. El proceso IP examina el número de red destino contenido en el encabezado IP, y localiza la ruta hacia la red 128.4.0.0 en las tablas de ruteo (tabla 4.5).

El ruteador A sabe que la red destino está a dos saltos aún, y que debe enviar el datagrama al ruteador B a la dirección IP 128.2.0.3. El ruteador A debe hacer un requerimiento ARP y esperar que el Ruteador B si este no tiene el direccionamiento mapeado en su cache ARP. Finalmente, el ruteador A transmite un frame Ethernet sobre el puerto 2 con el direccionamiento MAC destino % 080002001233 (Ruteador B), al direccionamiento MAC fuente %080002001232 (puerto 2 del ruteador A) y al tipo de campo 0800h (IP). La estructura del paquete anterior se muestra en la fig. 4.10

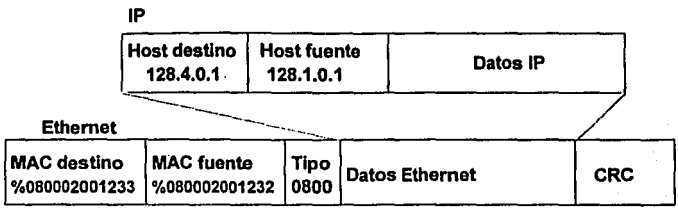

Fig. 4.10 Paquete en la Red 128.2.0.0

Paquetes en la red 128.3.0.0

Después de recibir el paquete, el ruteador B remueve el encabezado Ethernet y pasa el datagrama a un proceso IP. El proceso de rutas IP examina el número de red destino contenido en el encabezado IP y localiza la ruta a la red 128.4.0.0 en la tabla de ruteo (tabla 4.6). El Ruteador B aprende que la red destino está a un salto aún, y que debe enviar el datagrama al Ruteador C a la dirección IP 128.3.0.3.

El ruteador B debe hacer un requerimiento ARP, y esperar que el ruteador C responda si no tiene la dirección mapeada en su cache ARP. Una vez que el mapeo es obtenido, el Ruteador B transmite un frame Ethernet sobre el puerto 2 con el direccionamiento MAC destino % 080002001235 (Ruteador C), al direccionamiento MAC fuente % 080002001234 (Puerto 2 del ruteador B), y al tipo de campo 0800h (IP). La estructura del paquete para la red 128.3.0.0 se muestra en la fig. 4.11

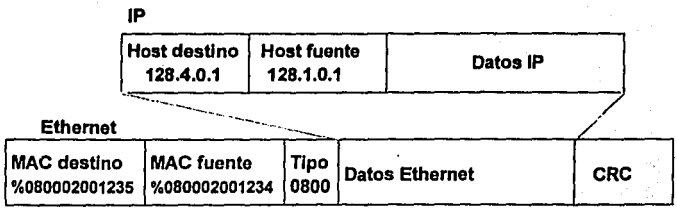

Fig. 4.11 Paquete en la Red 128.3.0.0

Paquetes en la red 128.4.0.0

Después de recibir el paquete, el Ruteador C remueve el encabezado Ethernet y pasa el datagrama al proceso IP. El proceso IP examina el número de red destino en el encabezado IP y localiza la ruta a la red 128.4.0.0 en la tabla de ruteo (tabla 4.7). El ruteador C descubre que la red destino está directamente conectada al puerto 2, y que no necesita enviar el datagrama a otro ruteador. El ruteador C puede liberar el datagrama directamente.

El Ruteador C debe hacer un requerimiento ARP y esperar que el Hots B responda (si este no tiene el direccionamiento mapeado en su cache ARP). Una vez el mapeo es obtenido, el Ruteador C transmite el frame Ethernet sobre el puerto 2 con la dirección MAC destino % 080002002222 (Host B), a la dirección MAC fuente % 08002001236 (Puerto 2 del Ruteador C), y el tipo de campo 800h (IP). La estructura del paquete colocado en la red 128.4.0.0 se muestra en la figura 4.12

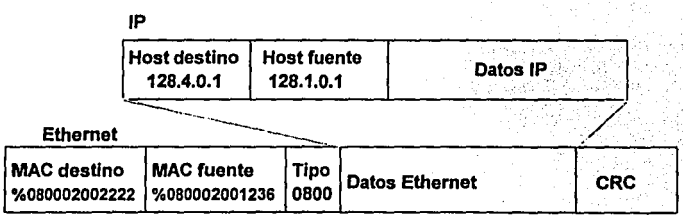

Fig. 4.12 Paquete en la Red 128.4.0.0

Host B

El Host B recibe el paquete, remueve el encabezado Ethertnet, y pasa el requerimiento al módulo IP. El proceso IP determina que el datagrama es direccionado al host local, remueve el encabezado IP, y pasa esto a TCP para futuros procesos. TCP examina el número de puerto y pasa el datagrama a la entrada de la cola para el proceso Telnet.

4.6 Rutas Default

El ruteador debe examinar sus tablas de ruteo para encontrar la ruta para cada datagrama. Si la ruta para el datagrama no puede ser localizado, el ruteador descarta el paquete.

El direccionamiento especial 0.0.0.0 es usado para describir una ruta default . Si la ruta a la red destino no puede ser localizada y la ruta default ha sido definida, las rutinas de ruteo no deben descartar el datagrama, sino enviarlo a la ruta default.

Las rutas default son generalmente usadas para reducir el tamaño de las tablas de ruteo. Como resultado el ruteo es simplificado, dado que este consiste de algunas pruebas para las redes locales y una de default para todos los otros destinos. Otra ventaja de usar las rutas default es que el tamaño de las tablas de ruteo de actualización de mensajes entre los ruteadores pueden ser sustancialmente reducidas. Algunas de las desventajas incluyen la posible creación de múltiples rutas, la creación de loops y configuraciones perdidas.

4. 7 Internet Control Message Protocol (ICMP)

El Protocolo de Control de Mensajes en Internet (ICMP) es un requerimiento del Protocolo Internet (IP) esto significa que todos los hosts que implementan IP deben implementar ICMP.

La función basica del ICMP es proveer un mecanismo que permita a los ruteadores o hosts destino reportar si existe un error en el proceso de envio de bloques de datos.

Algunos ejemplos de cuando usar los mensajes de ICMP son:

- Cuando el ruteador debe descartar un datagrama porque la cuenta del tiempo de vida expiro
- Cuando el ruteador no tiene la capacidad de buffers para reenviar el datagrama
- Cuando el host o ruteador descubren un error en el encabezado IP
- Cuando el ruteador no tiene una ruta para la red destino en su tabla de ruteo

La función principal del ICMP es proporcionar retroalimentación entre varios problemas que pudieran ocurrir en el medio-ambiente de la comunicación

Los mensajes de ICMP son encapsulados como una porción de los datos del datagrama IP. Como resultado, son ruteados como cualquier otro datagrama IP . Como los mensajes ICMP son transmitidos en datagrama IP, el transmisor no puede garantizar que estos serán liberados hasta su último destino.

Dado que los mensajes ICMP no pueden ser considerados confiables, no existe garantía de que que puedan ser perdidos o descartados.

4.7.1 Encapsulación ICMP

El ICMP es un miembro de la capa de enlace de la arquitectura del protocolo TCP/IP. Cada mensaje ICMP es encapsulado como una porción de los datos del bloque IP.

IP encapsula el mensaje con un encabezado IP y transmite el bloqe de datos resultantes sobre la red física a el host o ruteador destino. La razón por que IP fué seleccionado para liberar mensajes IP es que el mensaje puede necesitar atravesar varios ruteadores y redes hasta alcanzar su destino final.

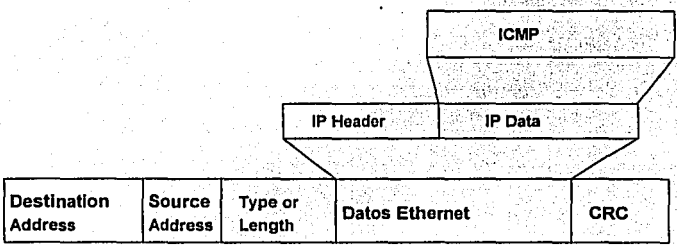

Fig. 4.13 Encapsulado ICMP

CAPITULO 5

PROTOCOLO DE CONTROL DE TRANSMISIONES (TCP)

El Protocolo de Control de Transmisión es una de las dos capas principales de protocolos de transporte que recide en la cima del Protocolo Internet (IP). El otro protocolo es el UDP

TCP es un protocolo confiable de circuito virtual orientado a conexión. Proporciona una alta confiabilidad de comunicación host-to-host entre dos computadoras conetadas a la misma red o unidas a un sistema interconectado de redes. Las principales características proporcionadas por TCP incluyen:

- El establecimiento y terminación de la conexión
- Mantenimiento confiable de los paquetes liberados
- Secuencia de los paquetes liberados
- Control de flujo para proteger al host de sobreflujos
- Recuperación de errores por pérdida o duplicado de datos

Los principales clientes de TCP son las siguientes capas de protocolos de aplicación:

- Telnet
- Protocolo de Transferencia de Archivos (FTP)
- Protocolo de Transferencia de Correo Sencillo (SMTP)

TCP es un cliente del Protocolo Internet(IP). IP proporciona el medio para que TCP ENVÍE Y RECIBA INFORMACIÓN. Los principales servicios que IP proporciona a TCP incluyen:

- Direccionamiento para identificar la estación origen y la destino en redes diferentes:
- La habilidad de rutear bloques de datos a través de Internet
- La habilidad de fragmentar y posteriormente reensamblar bloques de datos para transmitirlos a través de pequeños paquetes en la red.

- Un campo de tiempo de vida para limitar el periodo de tiempo que un datagrama permanece activo en Internet.
- Un campo de Tipo de servicio que indica la calidad de servicio que el ruteador deberá proporcionar.

5.1 Interfaces

TCP tiene interfaces en la cima del proceso de aplicación del usuario y en la parte baja de la capa de red tal como el protocolo IP. La aplicación del usuario transmite datos haciendo llamadas a TCP y pasando buffers de datos como argumentos. TCP enpaqueta el paquete de entrada dentro de segmentos y llama al modulo IP para transmitir cada segmento al host destino. Al recibirlos TCP coloca los datos del segmento dentro de buffers, y notifica a la aplicación destino.

5.1.1 TCP /Interface de Aplicación

La interface entre el proceso de aplicación y TCP consiste de un conjunto de funciones de llamadas bien definidas. Estas llamadas son similares a las funciones de un sistema operativo estandar que abren, cierran, leen o escriben un archivo. Estas llamadas permiten a la aplicación Abrir o Cerrar la conexión. Enviar o Recibir datos, u obtener el Status de la conexión.

5.1.2 TCP/Interface Internet

La interface entre TCP y los protocolos de nivel bajo no está especificada. Usualmente el protocolo de nivel bajo define la especificación de la interface.

La interface actual para la red física es controlada por un dispositivo de driver, TCP no hace llamadas directas al dispositivo de driver de la red. En lugar de esto, TCP hace llamadas al modulo IP el cúal hace la llamada directa al dispositivo driver.

5.2 Operación Fundamental

El proposito primario de TCP es proporcionar un servicio confiable orientado a conexion entre procesos residentes en diferentes hosts.

El Protocolo de Control de Transmisión (TCP) debe proporcionar servicios en las siguientes áreas:

- Transferencia Básica de Datos
- Confiabilidad
- Control de Flujo
- Multiplexación
- Conexiones

5.2.1 Transferencia Básica de Datos

La unidad básica de transferencia entre el software TCP en dos hosts es llamado segmento .

TCP ve a las cadenas de datos como una secuencia de bytes u octetos que son agrupados dentro de segmentos para su transmisión. Cada segmento es transmitido a través de Internet como un campo de datos de un simple datagrama IP. Cada IP en la conexión determina a su propia conveniencia cuando enviar o bloquear datos para la transmisión de IP.

El TCP local determina el número de octetos a incluir en un segmento particular.

A veces, la aplicación del usuario necesita garantizar que todos los datos pasados al TCP local hayan sido transmitidos. La función " Push" forza la liberación de datos aunque no completen el buffer de transmisión. En el lado fuente la función "Push" requiere del TCP local para transmitir todos los datos que han sido generados, sin esperar el buffer de salida para llenarlo. En el lado destino la función "Push" requiere del TCP local para inmediatamente liberar los datos a la aplicación destino sin esperar a recibir el buffer para llenarlo.

5.2.2 Confiabilidad

TCP debe ser capaz de recuperar datos que han sido dañados, perdidos, duplicados o liberados fuera de secuencia.

TCP asigna un número secuencial a cada octeto (byte) que es transmitido, y requiere que un reconocimiento (ACK) sea devuelto por el destinatario TCP. Si el ACK no es recibido en un periodo específico, el dato es retransmitido por la estación origen. La estación destino usa el número secuencial para corregir segmentos que pudieron haber sido liberados fuera de orden , y eliminar el problema de duplicarlos.

5.2.3 Control de Flujo

TCP provee un mecanismo para la estación destino para controlar el promedio de datos enviados por la estación fuente. La ventana recibida es devuelta con cada ACK indicando que tantos octetos adicionales la estación destino está dispuesta a aceptar de la estación origen. La ventana de reconocimiento puede variar en tamaño según las circunstancias. En respuesta a una ventana de reconocimiento grande, el originador incrementa el tamaño de los buffers a enviar, si la ventana de reconocimiento es pequeña, el originador detiene el envio de octetos

La ventaja de usar ventanas variables en tamaño es que provee un control de flujo así como una transferencia confiable. Tener un mecanismo para un control de flujo es esencial en un medio ambiente internet, donde maquinas de diferentes velocidades y tamaños se comunican a través de redes y gateways de varias velocidades y capacidades

5.2.4 Multiplexamiento

Como el protocolo UDP(User Datagram Protocol), TCP incorpora la idea de puertos para identificar el último destino . TCP provee un conjunto de puertos en cada host para permitir múltiples procesos con un solo host para usar servicios de comunicación TCP simultáneamente.

Un socket es creado con la combinación de la dirección internet del host con el número de puerto. Los Sockets son el último destino de todo el tráfico TCP. El par de sockets (uno para cada host) unicamente identifica cada conexión. Sin embargo, un socket puede ser usado simultaneamente en más de una conexión.

El proceso de enlace de puertos es manejado independientemente por cada host

5.2.5 Conexiones

La seguridad y control de flujo requieren que TCP inicialice y mantenga un status de información importante para cada datagrama. La conexión es la combinación de esta información. Esta incluye número de sockets, secuencia de números e información de administración. Cada conexión es únicamente identificada por un par de sockets que identifica cada lado del circuito virtual.

Cuando dos procesos desean comunicarse, el primer proceso TCP en cada host será establecer la conexión . El proceso de la conexión causa que la información del status sea inicializada por cada lado del circuito virtual. Despues de que el intercambio de datos es completado, la conexión es terminada para liberar los recursos para otros usuarios.

Durante la transferencia de datos, los procesos en cada host se comunican para verificar que los datos están siendo recibidos sin errores o pérdidas. Si la conexión establecida llega a fallar debido a problemas de la red, ambas máquinas detectan la falla, y reportan esto al programa de aplicación correspondiente.

5.2.6 Secuencia de números

TCP percibe los datagramas como una secuencia de octetos (o bytes) que son agrupados dentro de segmentos para su transmisión. Cada octeto de datos es asignado a un único número secuencial. El número de secuencia asignado a cada primer octeto en el datagrama es determinado cuando la conexión es establecida. La secuencia de números es entonces incrementada para cada subsequente octeto en el datagrama.

Dado que los octetos individuales son agrupados dentro de segmentos para su transmisión, un número secuencial individual es proporcionado para cada segmento. El número de secuencia colocado en el encabezado de cada paquete es el número secuencial que fûe asignado al primer octeto de datos en el segmento.

Dado que cada octeto es numerado, es posible reconocer cada octeto en la cadena de datos. Sin embargo este no es el método utilizado para reconocimientos de TCP. Un mecanismo acumulativo de reconocimientos es utilizado. Esto significa que el conocimiento de un número secuencial X indica que todos los octetos excluyendo el número secuencial X han sido recibidos por el host destino. La ventaja de esta técnica es que la pérdida de un reconocimiento no necesariamente forza la retransmisión.

Cada lado de la conexión full duplex tiene sus propios conjuntos de secuencia de números. Cuando la conexión es establecida por primera vez; un número secuencial inicial debe ser definido para cada lado de la conexión. Para que la conexión sea establecida, los dos TCPs deben sincronizarse en cada número secuencial inicial. Si la sincronización no se lleva a cabo, será imposible para cada lado enviar o recibir datagramas . La figura 5.1 muestra la secuencia de números

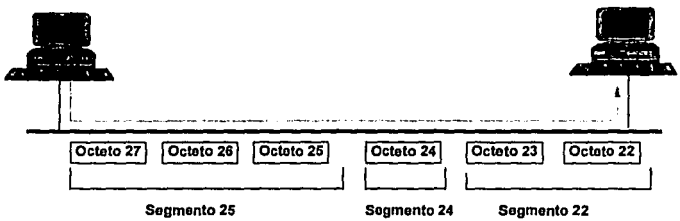

Figura 5.1 Números secuenciales

5.2.7 Puertos

Como el User Datagram Protocol (UDP), TCP usa el concepto de número de puerto como el último destino del host. Cuando se establece la conexión, el TCP local debe especificar no solo la dirección Internet del host destino, sino también el número de puerto de el proceso de aplicación que se desea accesar.

Los servidores tienen números de puertos bien conocidos que los otros dispositivos pueden abrir conexiones a ellos, y empezar a enviar comandos. Además números de puertos específicos se reservan para procesos especiales que simplifican la espera para los requerimientos del cliente . Estos procesos incluyen:

- Nombre del servicio
- Servicio de transferencia de archivos
- Acceso desde una terminal remota
- Correo
- Administración de redes

Los puertos anteriores se conocen como " puertos bien conocidos " y se ilustran el la fig. 5.2

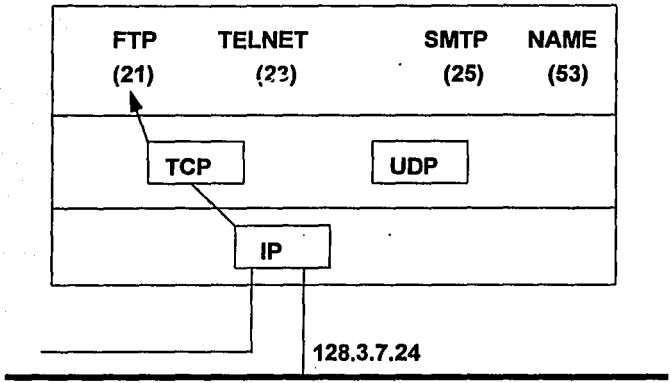

FIG. 5.2 "Puertos bien conocidos"

5.2.8 Sockets

Una conexión es actualmente definida por un conjunto de cuatro números: La dirección Internet en cada lado, y el número de puerto TCP en cada lado. Cada datagrama contiene estos cuatro números. La dirección Internet es colocada en el encabezado IP, y el número de puerto es incluido en el encabezado TCP. Dos conexiones no pueden tener el mismo conjunto de números. Sin embargo es suficiente con tener un solo número diferente.

En la fig. 5.3, dos conexiones simultáneas existen entre dos hosts en Internet.
Dado que las mismas máquinas son involucradas, las direcciones Internet son idénticas. Dado que ambas conexiones son TELNET, el final de la conexión involucra un puerto bien conocido para TELNET(23). La única área que difiere es el número de puerto para el lado del cliente de la conexión Telnet.

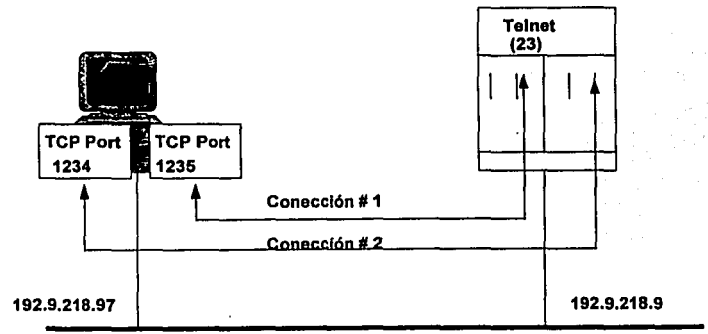

Fig. 5.3 Conexión a un dispositivo

5.2.9 Estableciendo Conexión

La LLAMADA hecha por el proceso de aplicación para abrir una conexión especifica donde la conexión será activa o donde será un requerimiento pasivo.

Entrada Pasiva

Una ENTRADA pasiva indica que el proceso que esta haciendo la LLAMADA está lista para aceptar un requerimiento en lugar de intentar iniciar una conexión. La conexión puede ser hecha con cualquier proceso que requiera una conexión con un puerto bien conocido.

Entrada Activa

Cuando un cliente necesita establecer una conexión con un servidor remoto, este crea un proceso TCP para iniciar el circuito. Entonces emite un requerimiento de Entrada activa.

Las conexiones son establecidas después de un intercambio exitoso de sincronía de paquetes entre los dos procesos para sincronizar los números de secuencia inicial, y el control básico de información que ambos lados necesitan acordar antes de que los datos puedan ser transferidos sobre la conexión.

Funciones de conexiónes establecidas

El establecimiento de conexiónes provee cuatro funciones principales:

- Asegura a cada lado de la conexión que el otro existe a través de intercambios de requerimientos de conexiónes y respuesta de paquetes.
- Proporciona para intercambio de parametros opcionales tales como tamaño del paquete, tamaño de la ventana y la calidad del servicio.
- Asigna recursos de transporte como espacio en el buffer
- Crea una entrada en la tabla de conexión.

5.3 Transmisión de datos

Secuencia de Números

Una vez que la conexión ha sido establecida, cada lado envía y recibe datos como un flujo de octetos. Dado que TCP es un protocolo de flujo de bytes, cada octeto de datos tiene un número secuencial y las fronteras del paquete son arbitrarias.

Cada lado de la conexión tiene su propio conjunto de secuencia de números. La primera secuencia de números para cada lado de la conexión es especificado cuando la conexión es primeramente establecida. El flujo de datos puede ser visto como dos flujos independientes siguiendo en direcciones opuestas entre ambas terminaciones de la conexión .

La liberación de octetos del destinatario TCP hacia la aplicación receptora es exactamente en el mismo orden en que los octetos fueron pasados hacia el fuente TCP del programa de aplicación emisor.
El proceso anterior se ilustra en la figura 5.4

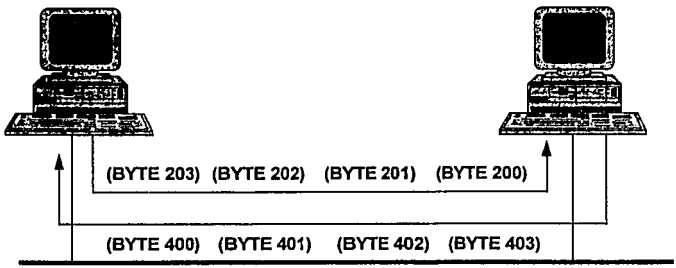

Fig. 5.4 Transmisión de datos: Números secuenciales

5.4 Segmentos

Cuando TCP recibe datos de su cliente, este abre los datos del correo del cliente hacia la cola de salida actual. Si la ventana emisora es abierta, TCP envía tantos datos como quepan dentro de la ventana. El número de secuencia incluido en el paquete es el número de secuencia asignado al primer byte del dato que es colocado en el paquete.

Dado que TCP es un protocolo de cadenas de bytes, este es libre de dividir la cadena de bytes dentro de segmentos de cualquier tamaño para su transmisión. El tamaño de cada segmento es independiente del datagrama que el programa de aplicación proporciona.
En la figura 5.5 se ilustran los segmentos

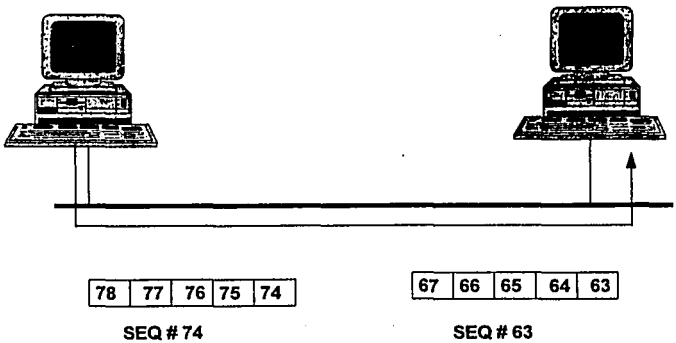

Fig. 5.5 Transmisión de datos: Segmentos

5.5 Banderas de empuje y Banderas urgentes

Existe una gran cantidad de comunicaciones con pérdida de ancho de banda cuando los segmentos contienen solo algunos bytes o datos de usuarios. Esto es porque el paquete que transmite el segmento debe proveer la información del encabezado. Un paquete típico TCP/IP debe contener 24 bytes de información de encabezado TCP y un mínimo de 20 bytes de información de encabezado IP. Para hacer una transferencia de datos más eficiente y para minimizar el tráfico de la red, TCP usualmente colecta los suficientes bytes de la cadena de bytes dentro de un buffer para hacer un segmento rasonablemente largo. TCP entonces transmitirá el segmento a través de Internet.

TCP provee un mecanismo para forzar la liberación de datos aunque no haya los suficientes bytes para llenar el buffer.

Bandera de enpuje

Incluido como parte de la información del encabezado TCP. Normalmente, TCP decide cuando han sido acumulados suficientes datos para formar un segmento. La aplicación fuente puede requerir TCP para transmitir todos los datos pendientes y etiquetarlos con una bandera de ENPUJE, esta no tiene que esperar más datos antes de pasar los datos hacia su proceso destinatario.

El propósito de la función de enpuje y la bandera dé ENPUJE es enpujar los datos del proceso origen hacia el proceso destinatario. Este mecanismo puede ser implementado para usuarios de terminales interactivas quienes esperan una respuesta inmediata para cada presión de tecla.

Bandera Urgente	Informa al proceso destino que existe un importante o "urgente" dato en la cadena de datos entrantes. Es función del proceso destino de determinar la acción apropiada y asegurarse que los datos sean rápidamente enviados hacia el proceso fuente.

5.6 Reconocimiento y Retransmisión

Una vez que la conexión es establecida, cada paquete de intercambio entre los dos procesos TCP deben de tener una bandera de reconocimiento, y deben de contener un número válido de reconocimiento. El número de reconocimiento es el número secuencial para el siguiente byte del dato que el proceso receptor espera.

El proceso TCP origen debe retener todos los datos transmitidos hasta que reciba un reconocimiento. Si el reconocimiento no es recibido dentro del tiempo límite especificado por el usuario, dentro del término de retransmisión, el TCP remitente asume que el dato ha sido perdido o corrompido, TCP retransmitira los datos empezando con el primer byte no reconocido. Despues de alcanzar el número configurado por el usuario de retransmisiones sin reconocimiento, TCP abortará la conexión.

El esquema de reconocimiento TCP es llamado acumulativo porque este reporta que tanto de las cadenas han sido acumuladas.

5.7 Tiempo agotado y Retransmisión.

Una de las más importantes y complejas ideas de TCP es la forma en la que maneja el tiempo de expiración y la retransmisión. Cada vez que se envía un segmento, TCP activa un contador de tiempo y espera para recibir un reconocimiento. Si el tiempo expira antes que el dato en el segmento haya sido reconocido, TCP asume que el dato ha sido perdido o corrompido y lo retransmite.

El algoritmo de retransmisión de TCP difiere de muchos de los algoritmos usados por los otros protocolos de red ya que TCP se utiliza en medios ambientes de Internet. Dentro de una internet, los segmentos viajan entre un par de máquinas que pueden estar en la misma LAN o que pueden estar en dos redes separadas por varios puentes. Esto hace imposible saber que tan rápido regresará el reconocimiento hacia el origen. Además el retardo entre cada puente varía según el tráfico que encuentre, por lo tanto el tiempo en recibir el reconocimiento varía mucho entre una red y otra.

5.7.1 Control de flujo

Ventanas variables

El control de flujo fin-a-fin es alcanzado a través del uso de ventanas variables de tamaños. Cada proceso TCP notifica a su contraparte remota que ha recibido la ventana. La ventana "recibida" es el rango de numeros secuenciales que esta dispuesta a recibir. Normalmente el tamaño de la ventana decrece cuando los datos son recibidos, y se incrementa cuando los datos son pasados exitosamente hacia el cliente.

Ventana recibida "Cero"

TCP acepta y reconoce únicamente aquellos segmentos que caben dentro de una ventana. Si el proceso no puede aceptar más datos, este cierra la ventana de recibimientos enviando un paquete de reconocimiento con un anuncio en la ventana que esta tiene un tamaño cero. Dado que TCP no puede cerrar su buzón mientras recibe datos, este puede seguir recibiendo datos después de que se ha cerrado la ventana. Estos segmentos no serán reconocidos.

Un proceso TCP con una ventana de envío cero, debe periodicamente probar paquetes con secuencias inválidas y números de reconocimientos con un byte de datos inválidos. El proceso TCP receptor responde enviando un ACK inmediatamente. El proceso de la prueba es asegurar que abriendo la ventana es confiablemente reportada hacia el otro lado de la conexión.

Terminación de la Conexión

Las conexiones TCP son full-duplex, lo que significa que la conexión tiene dos cadenas de datos independientes. Hay una cadena de datos en cada dirección originando para ambos el final de la conexión. Para terminar la conexión, ambas cadenas deben ser cerradas.

5.7.2 Iniciando el requerimiento de Desconexión

Cuando TCP desea cerrar una conexión transmite un paquete que contiene un bit de FIN (bit de terminación) al TCP remoto. El TCP que inicio el servicio debe seguir aceptando datos del TCP remoto hasta que el TCP remoto responda con un paquete de terminación.

Cuando el TCP remitente recibe un paquete de terminación del TCP remoto, este envia un mensaje de desconexión a sus clientes, cierra sus cajas de correo y espera el tiempo de terminación. Cuando este tiempo expira, el TCP remitente libera sus recursos y termina la sesión.

5.7.3 Respondiendo el requerimiento de Desconexión

Cuando el TCP remoto recibe un paquete de terminación del lado que inicio la desconexión, envía una señal a sus clientes con un mensaje de desconexión. El TCP remoto continua aceptando y transmitiendo datos a sus clientes hasta que el TCP remitente termina la conexión.

El TCP remoto envía un mensaje de desconexión a sus clientes TCP una vez que todos los datos han sido enviados. En este punto, el TCP remoto cierra sus buzones de correo para ya no recibir más datos de sus clientes.

5.8 Reseteando la conexión- recuperación de errores

Algunas veces, ocurre algun evento que forza al programa de aplicación o al software de comunicación a abortar la conexión. Por ejemplo, si al recibir un datagrama este no es reconocido en un periodo dado, el TCP origen continua con la retransmisión del datagrama desconocido. Al llegar al número de retransmisiones desconocidas configuradas, TCP aborta la conexión. TCP proporciona una operación de reseteo de conexión para terminar con estas ocurrencias anormales.

El TCP origen inicia el reset transmitiendo un segmento con un bit de caracter de control RST colocado a 1. El otro lado de la conexión debe responder a un requerimiento de reset con un aborto de sesión. El lado receptor también informa a sus aplicaciones que ha ocurrido un reset. Como resultado, la transferencia de datos en ambas direcciones es inmediatamente detenida, y todos los recursos son liberados.

5.9 Encapsulación del Frame TCP

El mensaje completo TCP, incluyendo el encabezado y los datos, son encapsulados en un datagrama IP y viajan a través de Internet. El esquema anterior se muestra en la figura *5.6*

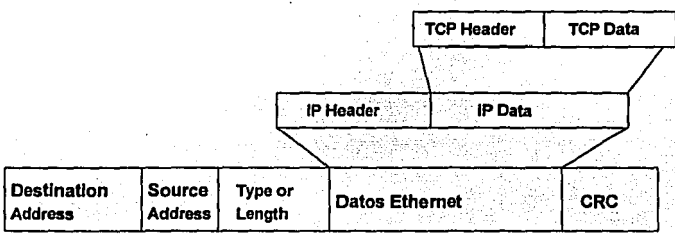

Fig. 5.6 Frame Ethernet

La capa Ethernet es responsable de transferir entre los dos hosts o routers en la misma red física.

La capa IP es responsable para transmitir datos a traves de routers, entre dos hosts en Internet.

La capa TCP es responsable de proporcionar una cadena de servicios para la capa de aplicación. TCP proporciona una conexión full-duplex entre las máquinas permitiendoles intercambiar grandes volumes de datos eficientemente.

5.9.1 Formato del Encabezado TCP

En la fig. 5.7 se ilustra el formato del encabezado TCP

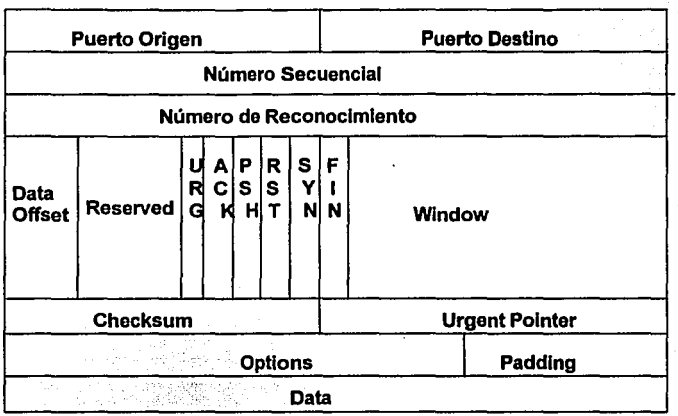

Fig. 5.7 Formato del encabezado TCP

Puerto origen	Identifica la aplicación, con el host que origina la transmisión
Puerto destino	Identifica la aplicación, con el host al cual la transmisión será liberada
Número de secuencia	El número secuencial del primer octeto de datos en el segmento (excepto cuando SYN está presente). Cuando SYN está presente, el número secuencial es el número de la secuencia inicial (ISN) y el primer octeto de datos es ISN+1.
Número de reconocimiento	Aplica solamente si el bit de control ACK es colocado. El número ack Es el siguiente número secuencial que el remitente del segmento está esperando recibir. Si la conexión es establecida, este valor siempre es enviado.

Data Offset	Especifica el número de 32 bits en el encabezado TCP. Este indica donde el dato empieza en el segmento.
Reservado	Los siguientes 6 bits al campo Data Offset son reservados y son siempre cero.
Checksum	Verifica que el segmento haya sido transmitido sin errores. Si un error es detectado, el segmento es descartado.
Opciones	Es un campo de longitud variable para indicar las opciones de TCP. Este campo puede ser usado, por ejemplo, para indicar el tamaño máximo de segmento que el remitente está dispuesto a acceptar.
Padding	Especifica el número de ceros añadidos para asegurarse que el encabezado termina en las fronteras

5.9.3 Rendimiento TCP

Como se ha visto, TCP es un protocolo complejo que administra comunicaciones sobre una gran variedad de tecnologías de red. Experimentos han demostrado que TCP conectado a una Internet pueden deliverar hasta 8 Mbps entre dos estaciones en una red Ethernet de 10 Mbps.

5.10 Interior y Exterior Gateway Protocol

Dos routers que intercambian información son referidos como "vecinos". Los ruteadores pertenecientes al mismo sistema autónomo son llamados "vecinos interiores", y los pertenecientes a diferentes sistemas autónomos son llamados "vecinos exteriores".

5.10.1 Interior Gateway Protocol (IGP)

Los ruteadores con un solo sistema autónomo de comunicación usan uno de varios de los protocolos de ruteo, conocido generalmente como Interior Gateway Protocol (IGP). La comunicación continua es necesaria para actualizar dinámicamente el ruteo e intercambiar información con cada ruteador, ya que esto reflejará el estado de la topología de red actual.

El rendimiento es la clave principal del IGP. El algoritmo de ruteo debe responder inmediatamente a fallas, y debe encontrar la ruta de costo más baja hacia la red destino.
Dos ejemplos del Interior Gateway Protocol son el Routing Information Protocol (RIP) y el Open Shortest Path First Protocol (OSPF).

5.10.2 Exterior Gateway Protocol

La comunicación entre ruteadores pertenecientes a diferentes sistemas autónomos requieren un protocolo adicional. Este tipo de protocolo es llamado Exterior Gateway Protocol (EGP). Los ruteadores que ejecutan EGP, también deben de ejecutar IGP para obtener información acerca de su propio dominio. Cada sistema autónomo es libre de seleccionar el IGP que mejor cubra sus necesidades, pero todos los sistemas de comunicación autónomos deben usar el mismo EGP.

La figura 5.8 muestra la comunicación entre vecinos exteriores en dos diferentes sistemas autónomos.

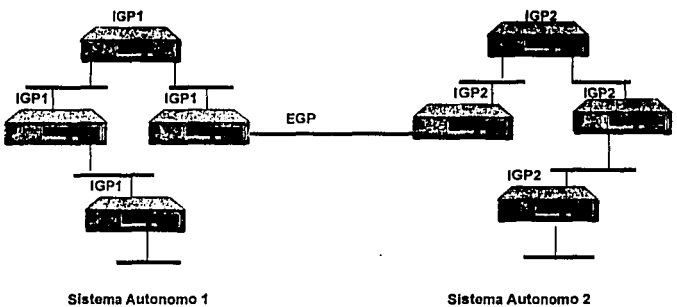

Fig. 5.8 Exterior Gateway Protocol (EGP)

Cuando se rutea entre diferentes sistemas autónomos, existe generalmente una peqeña coordinación de administración entre las regiones. También existe algo de falsedad en la información obtenida de otros sistemas autónomos. Por ejemplo, el administrador de la red no puede prevenir fallas a ocurrir en otras redes privadas. Como resultado,se deben crear barreras para prevenir los efectos de tales fallas y su esparcimiento hacia otras redes privadas.

Existen mayores políticas de ruteo y control para EGP que para IGP. Dos de los más populares EGPs son la revisión para el primer Exterior Gateway Protocol (EGP2) y el Border Gateway Protocol (BGP).

5.10.3 Algorítmos de ruteo estático vs ruteo dinámico

Hay dos técnicas básicas usadas por los hosts y ruteadores para obtener la información almacenada en sus tablas de ruteo. Los algorítmos de ruteo pueden variar en sus respuestas, de usar rutas estáticas teniendo los cambios en las rutas dinámicamente en respuesta a los cambios en el estado operacional de los recursos de la red.

5.10.3.1 Algorítmo de ruteo estático

- El administrador de la red guarda una tabla de las redes, y manualmente actualiza estas tablas siempre que exista un cambio en el dominio del ruteo
- El sistema estático no opera bien en un medioambiente de rápido crecimiento o rápido cambio. Las tablas de ruteo no pueden ser completamente responsables en caso de fallas dado que los ruteadores de respaldo pueden necesitar usar los recursos o dispositivos de la red dañada.
- Cuando son añadidas nuevas redes, la topología física cambia, cada ruteador en el dominio debe de tener estas tablas actualizadas manualmente. Esto puede requerir una gran cantidad de tiempo de parte del administrador de la red.
- Los errores de configuración en las tablas de ruteo estático en grandes redes, pueden ser difíciles de encontrar o corregir.

5.10.3.2 Algorítmo de ruteo dinámico

- Los algorítmos de ruteo dinámico responden automáticamente a los cambios en la topología de la red.
- Los esquemas de ruteo dinámico automáticamente incorporan estos cambios añadiendo o borrando entradas de sus tablas de ruteo.

Construyendo las tablas de ruteo

Típicamente, la mayoría de ruteadores usan una combinación de técnicas estáticas y dinámicas para obtener información de las tablas de ruteo.

Cada ruteador primero establece un conjunto inicial de rutas. Esta información es usualmente obtenida leyendo las tablas de ruteo del disco de arranque. La información de esta tabla es proporcionada por el administrador de la red y generalmente incluyen las redes conectadas y posiblemente algunas rutas estáticas de redes remotas.

Una vez que las tablas de ruteo se han convertido en residentes de la memoria, el ruteador debe tener la habilidad de responder a las nuevas rutas o cambios en la topología de red. En una red pequeña, la tabla de ruteo puede ser actualizada y administrada por el administrador de la red.

Algorítmos de ruteo Dinámico

Dos tipos de algorítmo de ruteo dinámico son usados por las redes de computadoras manteniendo sus tablas de ruteo y calculando la ruta más corta hacia el destino. Estos son " algorítmo distancia-vector" y algorítmo "link-state" (también conocido como Primera Ruta más corta o "Dijkstra").

Todos los algoritmos deben usar métricas para seleccionar la mejor ruta hacia el destinatario. La ruta más corta entre redes es determinada examinando todas las rutas hacia el destinatario y seleccionando la ruta que tenga la métrica más corta. .

Algoritmos de Vector-Distancia

Operación Básica

En los algoritmos de vector-distancia, el ruteador envía a sus vecinos las distancias de sus vectores (sus tablas de ruteo). Esto es, cada ruteador conoce la longitud de la ruta más corta de cada uno de sus ruteadores vecinos hacia todas las redes destinos. Los ruteadores usan esta información para registrar las rutas más cortas hacia cada destino eligiendo al vecino con la ruta más corta disponible.

Desventajas

Dependiendo del tamaño de la red, el promedio de información intercambiada entre vecinos puede ser damasiado grande.

En los algoritmos de ruteo de vector-distancia, cada ruteador transmite información hacia sus vecinos acerca de las rutas de cada otro destino de la red. Es imposible para otros ruteadores checar esta información con precisión. Como resultado, es difícil para un ruteador ignorar automáticamente la información proporcionada por un ruteador dañado o desincronizado. También, dado que la información transmitida por cada ruteador está en la información que recibe de sus vecinos inmediatos, la identificación de ruteadores corrompidos o mal sincronizados puede ser bastante difícil..

Un cambio en la tabla de ruteo de algún ruteador puede traer como resultado una cadena de actualizaciones. Puede tomar bastante tiempo para que esta información alcance a todos los ruteadores del dominio.

Finalmente, un algoritmo de vector-distancia no es adecuado en grandes redes.

Ventajas

Los algoritmos de ruteo vector-distancia han sido usados por muchos años. Por lo tanto, muchas implementaciones están disponibles y son bien conocidos por los desarrolladores de software.

Los algoritmos de vector-distancia requieren solo un pequeño número de ciclos de CPU para determinar la ruta más corta hacia la red apropiada.

Algorítmos Link-State

Operación Básica

En los algorítmos de ruteo link-state, cada ruteador debe conocer completamente la topología de red antes de registrar la ruta más corta hacia cada destino de la red. Cada ruteador envía mensajes de actualización a cada ruteador del dominio. Estos mensajes contienen la metrica y el estado de cada uno de los ruteadores conectados al enlace. Las rutas son consistentes por que cada ruteador esta usando el mismo algorítmo de ruteo en bases de datos idénticas. Cada cambio en la topología es detectado por el ruteador local y reportado a todos los otros ruteadores del dominio. Cada nodo tiene toda la información requerida para calcular la ruta de mínimo costo por si mismo hacia cualquier otra red en el dominio de ruteo.

Desventajas

Una gran cantidad de memoria puede ser requerida en grandes redes dado que cada ruteador debe mantener actualizada la base de datos que contiene la completa topología de la red.

El algorítmo Link-State reqiere más promedio de tiempo de uso de CPU para calculos comparado con el algorítmo de ruteo vector-distancia.

Ventajas

Cada ruteador mantiene una vista consistente de la red, esto elimina los problemas de loops y ajustes lentos en los cambios de condiciones de la red.

Los ruteadores corrompidos son fáciles de detectar cuando se usa un algorítmo de link-state por que cada ruteador mantiene una base de datos idénticas.

Los algorítmos de Link-State pueden eleminar los problemas que ocurren en redes muy grandes debido a la habilidad de particionarse en áreas de sistemas autónomos.

5.10.3.3 Tablas de ruteo

Un ruteador examina sus tablas de ruteo para determinar como enviar un paquete. Si el destinatario está directamente conectado a la red, el ruteador libera el paquete sin usar los servicios de otros ruteadores. Si el destinatario está en una red remota, el ruteador debe enviar el paquete hacia otro ruteador más cerca del destinatario final. La ruta hacia una red remota puede ser configurada estáticamente, o aprender dinámicamente a través de un protocolo de ruteo tales como RIP, OSPF o EGP.

La figura 5.9 ilustra un ejemplo de entradas en una tabla de ruteo.

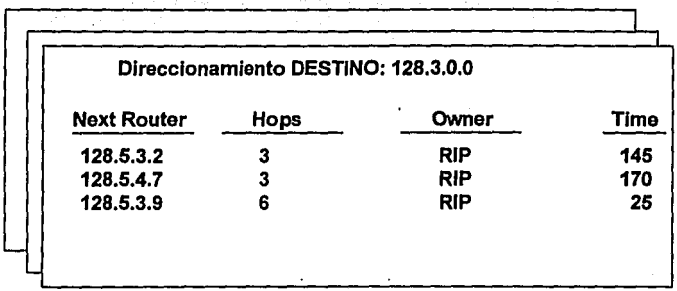

Fig. 5.9 Tabla de Ruteo

Cada entrada en la tabla de ruteo incluye la siguiente información que determina como un paquete es ruteado hacia una ruta particular seleccionada.

Destination Address	La dirección IP de la red destino, subred o host
Next Router	La dirección IP del ruteador remoto al cual el ruteador local debe enviar el paquete antes de que el paquete sea ruteado hacia su destino.
Hop Count	El número de saltos entre el ruteador y el destinatario.
Owner	El nombre del protocolo de ruteo que proporciona esta entrada a la tabla de ruteo.
Timer	El promedio de tiempo desde que la entrada fue actualizada.

5.10.3.4 Ruteo Multi-rutas

Para cada dirección destino (red, subred o host), algunos ruteadores soportan multiples rutas. Esto significa que el ruteador puede enviar paquetes hacia el destinatario a través de varias rutas. Estas rutas, aprendidas o configuradas, son almacenadas en una tabla de ruteo. La habilidad de rutear paquetes a través de diferentes rutas es llamado "ruteo multi-rutas".

Algunas de las ventajas del ruteo multi-rutas son:

- Si la ruta primaria falla, el ruteador puede seguir enviando paquetes usando una ruta alternativa. Como resultado, el ruteador puede responder inmedintamente a los cambios en la topología de la red.
- Si existe más de una ruta apropiada, el administrador puede seleccionar la más adecuada mediante el método de round-robin.

5.10.3.5 Rutas Default

El ruteador debe descartar un paquete si no encuentra una ruta hacia el destinatario en su tabla de ruteo. Sin embargo, si una ruta default ha sido definida, el ruteador debe enviar el datagrama hacia el ruteador identificado con la ruta default. La ruta default es identificada como una ruta hacia la red 0.0.0.0. Todo el trafico destinado para un destinatario que no está explicitamente listado en la tabla de ruteo debe enviarlo hacia el ruteador con la métrica más baja hacia la red 0.0.0.0.

Las rutas default son normalmente definidas cuando no se desea listar cada red en los mensajes de actualización de las tablas de ruteo.

En la fig. 5.10 el Ruteador D aprende la ruta default a través del Ruteador C. El ruteador D debe considerar al Ruteador C como su ruta default. Esto es, el Ruteador D necesita rutear un paquete hacia un destino que no esta en su tabla de ruteo, este envia el paquete hacia el ruteador C. El Ruteador C debe continuar enviando el paquete hacia la ruta default.

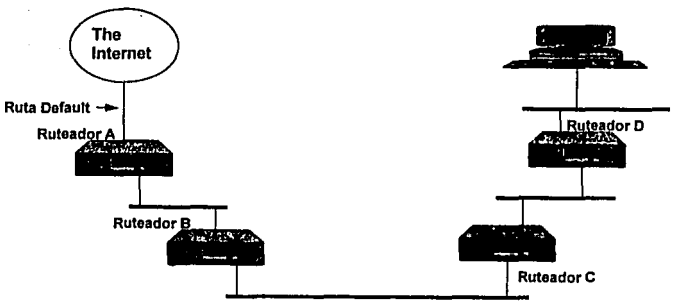

Fig. 5.10 Rutas Default

CAPITULO 6

PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED

ANTECEDENTES

En los últimos años, Internet ha crecido al incluir cientos de redes con cientos o miles de hosts incluyendo un gran número de puentes, ruteadores, servidores de comunicación, etc de diferentes proveedores.

El explosivo crecimiento de Internet y de las redes privadas ha demandado la necesidad de un aprovechamiento de la administración de las redes entre diferentes fabricantes. Aquellas que aún no son administradas, tendrán muchos problemas durante su crecimiento para proporcionar servicios confiables a los usuarios que se vayan incorporando.

En 1988 como un requerimiento de Internet Activities Board (IAB), quien fijo las políticas y estándares para las redes basadas en TCP/IP que estaban conectadas a Internet, un comite fue llamado para revisar las opciones de administración de Internet. La conclusión del comite fué que el Simple Network Manager Protocol (SNMP) debería ser adaptado para el uso de Internet.

6.1 Operación Básica

El modelo de administración de redes en el cual SNMP está basado consiste en la administración de estaciones y elementos de la red.

- La administración de las estaciones de la red son responsables de ejecutar la administración de las aplicaciones que monitorean y controlan los elementos de la red.
- Los elementos de la red tales como concentradores, puentes y ruteadores ejecutan agentes que son responsables para la ejecución de funciones de administración de la red requeridas por la estación de administración.
- SNMP es el medio por el cual la estación de administración y los elementos de la red se comunican. Este está diseñado para ser un protocolo que permita al administrador inspeccionar o alterar variables en los elementos de la red desde una estación de administración remota.
- La estación de administración polea a los elementos de la red para obtener información (GET) o para cambiar una variable en el elemento de la red (Set).

6.2 Funciones de Administración de redes

La administración de la red puede ser definida en términos de cinco funciones de administración identificadas por la Organización Internacional de Estandarización (ISO). Estas funciones incluyen:

- Configuración y Administración: El monitoreo y mantenimiento del estado actual de la red .Instalación, inicialización o modificación en la configuración del hardware y software.

- Fallas en la Administración: La detención, aislamiento y corrección de condiciones anormales. Problemas en la red; localización y corrección de componentes dañados

- Seguridad en la administración: Proporciona autorización, control de acceso, encriptación y claves de administración.

- Rendimiento de la Administración: Habilita el mantenimiento y rendimiento de la red en niveles aceptables. Monitoreando la capacidad de carga de los elementos de la red, tales como segmentos de área local y equipos de interconectividad para predecir futuras necesidades y requerimientos o actualizaciones de equipos.

- Contabilidad en la Administración: Habilita el establecimiento de cargos por usos de recursos de la red.

Las cinco funciones anteriores aplican para redes LAN o WAN. Sin embargo no todas las funciones necesitan estar presentes en la implementación de la administración de la red para tener un sistema efectivo de administración.

6.3 Requerimientos Básicos

Debido al tamaño y complejidad de las grandes redes empresariales, es necesario verlas como sistemas complejos. Con tales controles, el control de los elementos es lo más importante.

- Funciones de Administración: El sistema de administración de red debe ejecutar una o más de las cinco funciones: fallas, configuración, seguridad, conteo y administración del rendimiento.

- Interface del Usuario: La administración de la red en la interface del usuario debe ser clara, consistente, y orientado a graficos. La orientación gráfica permite entradas a través de menús o iconos y la salida de información en forma de diagramas o graficas.

- Estándares de la Industria: Para romper las barreras de los sistemas propietarios y asegurar la integración de diferentes fabricantes de redes, la solución de administración de redes deben soportar estándares de la industria tales como TCP/IP.
- Integración de productos: Los proveedores de sistemas de administración de redes o herramientas deben proporcionar elementos con capacidad de ser administrados.
- Comunicaciones con el Host: El sistema de administración debe tener una interface que permita comunicarse con el host central.

6.4 Arquitectura SNMP

6.4.1 Elementos de la arquitectura

La administración de la red a través de SNMP consiste de varios elementos que trabajan unidos. Entre estos tenemos a los elementos administrables, el administrador y los medios por los cuales se comunican. La figura 6.1 muestra estos elementos.

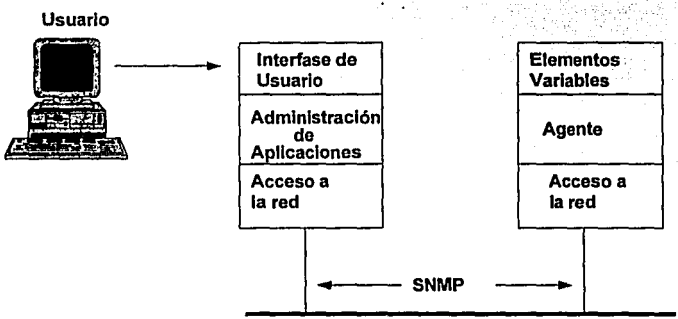

Fig. 6.1 Arquitectura SNMP

6.4.1.1 Estación de Administración.

La estación de administración ejecuta las aplicaciones de administración las cuales monitorean y controlan los elementos de la red. La estación de administración reportan directamente al Administrador.

6.4.1.2 Elementos administrables

Son dispositivos tales como concentradores, puentes, ruteadores, o cualquier otro dispositivo "inteligente" que tenga un agente de administración (software instalado). Estos elementos son responsables de ejecutar las funciones de administración de red requeridas por la estación de administración de la red.

6.5 Protocolo Simple De Administración de Red (SNMP)

El Protocolo Simple de Administración de Red (SNMP) es un simple protocolo de requerimiento/respuesta que intercambia información de administración entre la estación de administración de red y los agentes residentes en los elementos de la red. El protocolo no define los objetos que pueden ser administrados. SNMP puede ser usada con cualquier variable de administración de red que pueda ser inspeccionada o alterada.

6.5.1 Agentes SNMP

Las aplicaciones SNMP son implementadas en elementos de red via el uso de Agentes. Los agentes residen en los elementos de la red y tienen acceso a los datos de las Bases de Administración de la Red (MIB). Estos son responsables de actuar como servidores para ejecutar las funciones de administración requeridas por el administrador de la red.

Los Agentes son Elementos simples y la mayor parte son pasivos. Estos ejecutan operaciones solo bajo la dirección de un proceso de administación de red. Solo cuando una condición de error bien definida ocurre, el agente toma una acción por su propia cuenta. Estos eventos son llamados traps, el uso de traps es limitado.

Los Agentes solo administran un conjunto específico de recursos de un elemento dado de la red. Este simple alcance hace a un agente relativamente simple y barato de instalar.

La fig. 6.2 muestra los Agentes SNMP.

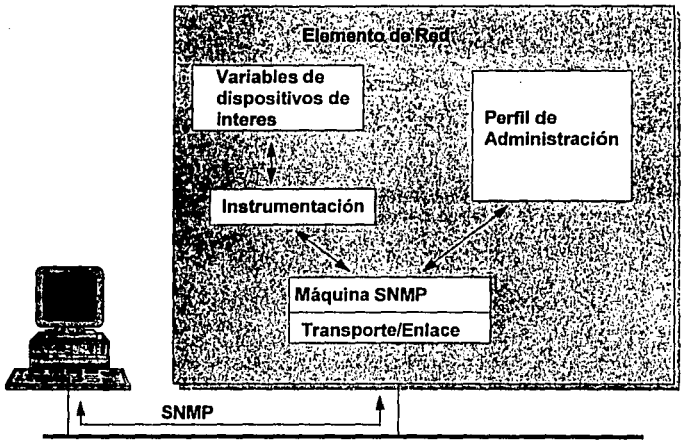

Fig. 6.2 Agentes SNMP

Una típica implementación de un Agente incluye cuatro recursos:

- Protocolo de Transporte: Provisto para la transmisión (envío y recepción) de datagrama entre dispositivos de la red.
- Máquina SNMP: Implementa SNMP; responsable del intercambio de mensajes punto-a- punto entre el administrador y el agente.
- Instrumentación: Proporciona al protocolo de administración el acceso hacia los agentes con variables de interés. Esto es usualmente alcanzado por un mecanismo de comunicación interno en la cuál la estructura de datos para el dispositivo puede ser accesado y manipulado al ser requerido por el protocolo de administración.

- Management Profile: Son el conjunto de reglas que definen el acceso hacia las variables de interés. Cada objeto en la mascarilla tiene un modo de acceso SNMP que puede ser READ-ONLY, READ-WRITE, o NOT ACCESSIBLE.

6.5.2 SNMP Agentes Proxy

Otro aspecto poderoso de la arquitectura SNMP es el uso de Agentes Proxy. Estos sirven como traductores entre SNMP y sistemas propietarios de administración. Los agentes Proxy SNMP reciven directrices SNMP de los procesos de administración, traducen las directrices dentro de operaciones propietarias, colectan información, y responden a los procesos de administración con mensajes estándares SNMP y traps.

La fig. 6.3 muestra los agentes SNMP Proxy

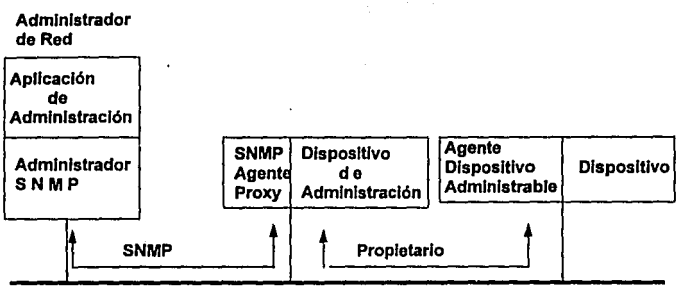

Fig. 6.3 Agentes proxy SNMP

Existen diferentes razones para el desarrollo de los agentes proxy SNMP

- El sistema de administración es limitado en memoria o recursos de procesamiento y además no puede soportar el agente requerido.
- El acceso del protocolo de administración para la administración del sistema no es soportado por el administrador.
- El sistema de administración tiene señas especiales de contraseñas.
- El protocolo de transporte no puede proporcionar una ruta entre el administrador y el agente.

6.5.3 Estación de Administración SNMP

Un Administrador SNMP es una aplicación que controla un grupo de agentes. Los administradores tienen la capacidad de dirigir agentes individuales para liberar información o cambiar la operación de elementos particulares.

Los Administradores son más complejos que los agentes. Pueden tomar información de un conjunto de agentes, analizar la información y entonces elaborar un conjunto de directrices que coordinen la actividad del conjunto de agentes.

La fig. 6.4 muestra los componentes de una estación de Administración.

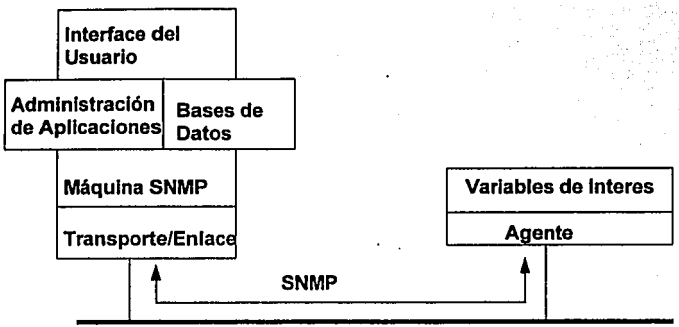

Fig. 6.4 Estación de Administración SNMP

Una implementación típica de Administración de Redes incluye cinco componentes:

- Interface del Usuario: Habilita al operador a introducir comandos de administración y recibir respuestas. Las respuestas de los agentes pueden ser solicitadas o no solicitadas.

- Aplicaciones de Administración: Asiste en el análisis de la información obtenida del proceso de los agentes en la administración de redes.

- Bases de datos: Contiene toda la configuración, rendimiento y datos auditables.
- Máquina SNMP: Es el proceso que implementa SNMP, intercambia mensajes SNMP y permite la administración del sistema vía remota.
- Transporte/Enlace: Permite el acceso hacia los datos.

6.5.4 Administración de la Información Base (MIB)

El MIB es una colección de información de todos los datos bajo el control de un administrador o agente en particular.

6.5.5 Objetos Administrables

Los objetos son representaciones de recursos actuales que están siendo administrados bajo un ambiente SNMP. Actualmente, existen cientos de objetos que han sido definidos y registrados como miembros estándares de los MIBs Internet.

6.6 Grupos de Objetos MIB

Los MIB han colectado los objetos de administración dentro de grupos relacionados para facilitar y simplificar las funciones de administración. La siguiente lista nombra los grupos de objetos SNMP.

Grupo de Sistemas (1)

La implementación de un grupo de Sistemas es obligatorio para todos los dispositivos. La descripción de cada sistema incluye el tipo de máquina, número serial, sistema operativo, recursos disponibles y otros atributos.

Interface de Grupo (2)

La implementación de una interface de grupo es requerida por todos los sistemas. Algunos de los atributos incluyen el número total de interfaces y una tabla de interfaces. Esta tabla incluye el tipo de interface, velocidad de transmisión, tamaño máximo de unidad de transmisión, dirección física, estado de la interface, y varios contadores estáticos.

Grupo traductor de Direcciones (3)

La implementación de un grupo Traductor de Direcciones es obligatorio para todos los sistemas. Este grupo monitorea el servicio proporcionado por el Protocolo de Resolución de Direcciones (ARP). Este contiene una tabla indexada compuesta por los mapeos de las direcciones Internet hacia las direcciones físicas.

Grupo IP (4)

La implementación del grupo IP es requerido en cada sistema. Este define los parámetros de configuración para cada máquina con Protocolo Internet. Este grupo también incluye dos tablas. La tabla de direcciones IP contiene la información de los dispositivos con direccionamiento IP. La tabla de ruteo IP contiene una entrada para cada ruta conocida hacia el dispositivo.

Grupo ICMP (5)

La implementación del grupo ICMP es obligatorio para todos los sistemas. Este grupo define los parámetros de configuración para la máquina del Control de Mensajes del Protocolo Internet. Este contiene las estadísticas de entrada y salida ICMP para cada tipo de mensaje ICMP.

Grupo TCP (6)

La implementación del grupo TCP es obligatorio para todos los sistemas que implementan el protocolo TCP. Los objetos seleccionados incluyen el número máximo de conexiones soportadas, el número actual de conexiones establecidas y una tabla conteniendo información de conexiones específicas (estado de la conección, dirección local, dirección remota y puerto remoto).

Grupo UDP (7)

La implementación del grupo UDP es obligatorio para todos los sistemas que inplementan el protocolo UDP. Los objetos seleccionados incluyen el número total de transmisiones y recepciones de datagrama UDP y un contador de errores.

Grupo EGP (8)

La implementación del grupo EGP es obligatorio para todos los sistemas que inplementan el protocolo EGP. Este grupo consiste de varios contadores de mensajes y de una tabla de vecinos EGP.

CONCLUSIONES

1.- El manejo, procesamiento y manipulación de grandes cantidades de información, ha propiciado el crecimiento acelerado de los equipos de cómputo.

2.- La incursión de la informática en todas las áreas, ha obligado que el procesamiento jerárquico de los años 60s y 70s, se este migrando a computadoras personales que son más sencillas en su operación para los usuarios.

3.- La necesidad de compartir información y recursos entre los usuarios de equipos de cómputo, han impulsado el origen y crecimiento de las redes locales de computadoras.

4.- La aceptación e implementación de redes locales de computadoras a nivel mundial, ha captado la atención de grandes fabricantes que enfocan gran parte de sus recursos de investigación en elaborar sistemas operativos de red cada vez más sofisticados y amigables para los usuarios.

5.- De los diferentes tipos de redes que existen actualmente, Ethernet es el tipo de red más utilizado a nivel mundial.

6.- Durante la instalación de una red local de computadoras, los puntos más importantes son la elección del servidor de archivos , el tipo de red y el tipo de cableado.

7.- La gran diversidad de los sistemas operativos con que normalmente cuentan las empresas (MS-DOS, NETWARE, UNIX, OS/2, etc), y la necesidad de que estos puedan convivir de una manera trasparente para el usuario, ha originado la creación de las herramientas necesarias (protocolos) para lograr tales objetivos.

8.- Dentro de la gran variedad de protocolos que existen actualmente (IP, IPX, UDP, TCP, ARP, RARP, FTP, ICMP, RIP, OSPF, SNMP), el conjunto de protocolos TCP/IP es el más utilizado en las comunicaciones a nivel mundial debido a las ventajas que ofrece sobre los demás protocolos.

9.- La gran aceptación y crecimiento del sistema operativo UNIX a nivel mundial en equipos multiusuarios, ha impulsado el crecimiento del protocolo TCP/IP, ya que todas las versiones de UNIX traen incorporado este protocolo de una forma nativa.

10.- Debido a la gran aceptación y uso de TCP/IP en redes de área local (LAN) y en redes de área extendida (WAN), este se ha convertido en un protocolo estándar para la industria, por lo que todos los fabricantes lo incorporan dentro de sus equipos, lo que garantiza su buen funcionamiento para interconectar las más diversas familias y tamaños de computadoras.

11.- En un enlace TCP/IP cada nodo tiene una dirección IP de 4 bytes

12.- Las direcciones de red obedecen a un plan general de asignación de acuerdo a redes y subredes

13.- IP es un protocolo no orientado a conexión, que solo se encarga de ver por donde irán los paquetes, pero no de garantizar su llegada.

14.- TCP es un protocolo orientado a conexión, que garantiza la llegada de los paquetes a través de números de secuencia y reconocimiento de los mismos.

15.- De los servicios que ofrece el conjunto de protocolos TCP/IP (Telnet, FTP, Mail, etc), el más utilizado es el File Transfer Protocol (FTP) para el intercambio de información entre quipos de cómputo diferentes.

16.- Debido al crecimiento en el número de nodos que integran una red LAN o una red WAN y los servicios que estas ofrecen, cada vez es más laborioso para el personal de sistemas la administración de estas, por lo que han surgido herramientas (analizadores de protocolos, software de monitoreo de redes, etc), para apoyar a los administradores de red a realizar de una manera más eficiente sus actividades.

17.- Para que los diferentes softwares de monitoreo de redes puedan convivir de una manera transparente para los usuarios, se desarrollo el Simple Network Manager Protocol (SNMP) como el protocolo estándar para las funciones de administración.

18.- Debido a la necesidad de intercambiar información entre usuarios que se encuentran ubicados en diferentes localidades del mundo, se ha creado "Internet", que es la red más grande del mundo, con millones de nodos en un sinfín de redes locales y enlaces remotos.

GLOSARIO

Agente:	En SNMP, la palabra agente se refiere al sistema administrado.
Ancho de banda:	(Bandwidth): Gama de frecuencias que pasa por un circuito. Cuando mayor el ancho de banda, más información puede enviarse por el circuito en un lapso determinado.
ANSI:	American National Standards Institute: Instituto Nacional Norteamericano de Estándares. Instancia coordinadora de grupos voluntarios de fijación de estándares en los Estados Unidos.
Baudios:	Unidad de velocidad de transmisión que es igual al número de cambios de una señal por segundo.
Bit:	Contracción de "Binary Digit" (digito binario), la menor unidad de información en un sistema binario. Un bit representa un uno o un cero.
Buffer:	Dispositivo de almacenamiento. Usado corrientemente para compensar diferencias en la velocidad de transmisión de datos o temporización de eventos cuando se transmite de un dispositivo a otro. Se usa también para eliminar el Jitter.
Bus:	Vía o canal de transmisión. Tipicamente, un bus es una conexión eléctrica de uno o más conductores en el cual todos los dispositivos ligados reciben simultáneamente todo lo que se transmite.
Byte:	Grupo de bits que una computadora puede leer (cadenas de 8 bits).
CSMA/CD:	(Carrier Sense Múltiple Access/collisión detection . Detección por portadora de acceso múltiple/colisíon). En este protocolo las estaciones escuchan al bus y sólo transmiten cuando el bus está desocupado. Si se produce una colisión el paquete es transmitido tras un intervalo (time-out)aleatorio. El CSMA/CD se usa en Ethernet.
Dirección:	(Address): Representación codificada del origen o destino de los datos.
Dirección Internet:	(Internet Adrress). También denominada IP Address. Dirección de 32 bits independiente del hardware que se asigna a computadoras centrales bajo el conjunto de protocolos TCP/IP.

Ethernet:	Diseño de red de área local normalizada como IEEE 802.3. Utiliza transmisión a 10 Mbps, y el método de acceso CSMA/CD.
FDDI:	(Fiber Distributed Data Interface- Interface de datos distribuidos por fibra), Norma ANSI para enlaces por fibra óptica con velocidades hasta 100 Mbps.
Fibra óptica:	Delgados filamentos de vidrio o plástico que llevan a un haz de luz transmitido (generado por un LED o láser).
IEEE:	(Institute of Electrical and Electronic Engineers - Instituto de Ingenieros en Electricidad y Electrónica). Organización profesional Internacional que pública sus propias normas. La IEEE es miembro de ANSI e ISO. 802.3- especificación de la IEEE para las LAN CSMA/CD. IEEE 802.5- especificación de la IEEE para las LAN.Token-Ring.
ISO:	(International Standards Organization-Organización de Normas Internacional)- Organización Internacional involucrada en la formulación de normas de comunicaciones.
MAC:	(Media Access Control-Control de Acceso a Medio). Protocolo que define las condiciones bajo las cuales las estaciones de trabajo acceden al medio de transmisión; su uso está más difundido en lo que hace a las LAN. En las LAN tipo IEEE, la capa MAC es la subcapa más baja del protocolo de la capa de enlaces de datos.
MIB:	(Management Information Base- Base de Información de Administración). Colección de objetos a los que se puede acceder a través de un protocolo de administración de redes tal como SNMP, los objetos representan valores que pueden ser leídos o modificados.
NIC:	Network Information Center : Centro de información de redes. Localidad que controla el acceso a los RFC e información sobre Internet.
Nodo:	Estación de trabajo que puede ser una computadora personal.
OSI:	(Open Systems Interconnection) Model - Modelo de referencia de siete capas de red de comunicaciones desarrollado por la ISO.
Paquete:	Grupo ordenado de señales de datos y de control transmitido por una red y que es un subconjunto de un mensaje más grande.

Paquetes:	Son sucesiones de bytes de tamaño fijo (de 64 a 1024). Al dividir cada mensaje en paquetes se evita que algún nodo monopolice un canal.
Protocolo:	Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en que los dispositivos de una red intercambian información.
Puente:	(Bridge)- Dispositivo que interconecta redes de área local (LANs), en la Capa de Enlace de Datos OSI. Filtra y retransmite tramas según las direcciones a nivel MAC (Media Access Control).
Rendimiento:	(Throughput)- Cantidad total de datos generados o transmitidos durante un cierto lapso.
Repetidor:	Dispositivo que automáticamente amplifica, restaura o devuelve la forma a las señales para recompensar la distorsión y/o atenuación antes de proceder a retransmitir.
RFC:	Request For Comments: Solicitud de comentarios. Documetos empleados como el medio primario de comunicación de información sobre Internet. Algunos RFC son designados por IAB como " Estándares Internet " . La mayoría documentan especificaciones de protocolos como Telnet y FTP. Están disponibles a través de los Centros de Información de la Red Internet.
RMON:	(Remote Monitoring). El MIB de monitoreo remoto que permite que un dispositivo de monitoreo de red sea configurado y leído a distancia.
Router:	Enrutador. Dispositivo de la capa 3 OSI que puede decidir cuál de varios caminos debe seguir el tráfico de la red, basándose en alguna métrica óptima.
Routing:	Enrutamiento. Proceso de encontrar un camino hacia el anfitrión de destino. En las grandes redes el enrutamiento es muy complejo debido a los muchos destinos intermedios potenciales que un paquete puede alcanzar antes de llegar a su anfitrión de destino.
SNMP:	(Simple Network Management Protocol- Protocolo de administración de Redes Simples). El protocolo de administración de redes del conjunto de protocolos TCP/IP.

TCP/IP:	(Transmisión Control Protocol/Internet Protocol-Protocolo de Control de Transmisión/Protocolo Internet).Conocido también como Internet Protocol suite. Este conjunto de protocolos se utiliza en Internet y se ha generalizado su uso para la interconexión de redes heterogéneas.
Token Ring:	Red de área local normalizada como IEEE 802.5. Una trama supervisora (token) es pasada secuencialmente entre estaciones adyacentes. Las estaciones que desean acceder a la red deben esperar a que les llegue el " token" antes de poder transmitir datos.

BIBLIOGRAFIA.

Douglas E. Cower
Internetworking with TCP/IP Vol. 1 y 2
Prentice Hall,1991.

Mark A. Miller
Troubleshouting TCP/IP
M&T Books

Andrew S. Tanen
Computer Networks
Prentice Hall, 1988.

Rowland Archer
The practical guide to local Área Networks
Osborne Mc Graw-Hill, 1986.

Michel Santifaller
TCP/IP and NFS
Internetworking in a UNIX enviroment
Addison Wesley,1991.

3 COM Corporation
Network Architectures, Standars, and Protocols

3 COM Corporation
Introduction to Simple Network Management Protocol (SNMP)

R.J. Cypser
Communications for Cooperating Systems OSF, SNA, and TCP/IP
Addison Wesley, 1991.

Internet Network Information Center
"Structure and Identification of management Information", RFC 55

Internet Network Information Center
"A Simple Network Management Protocol (SNMP)", RFC 1157

Revista RED
Colección de boletines técnicos Vol. 1, 1991

Mark A. Miller
A Guide to Network Comunications LAN to LAN; LAN to WAN
M&T Publishing Inc., 1991.

Dand M. Piscitello & A. Lyman Chapin
Open Systems Networking
TCP/IP and OSI
Addison- Wesley, 1993.

Willian Stallings
Networking Standards
A Guide to OSI, ISDN, LAN , and MAN standards
Addison Wesley, 1993.