UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

CAMPUS ARAGÓN

"APLICACIÓN Y FUNCIONALIDAD DE LAS REDES DE DATOS EN INTERNET-WORKING"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A N:

CARLOS ALBERTO MIRELES LOPEZ
C E S A R C R U Z V I D A L

ASESOR:
ING. JUAN CASTALID PEREZ

MÉXICO. **2004**

AGRADECIMIENTOS

A DIOS
Gracias por permitirme haber nacido y darme las fuerzas necesarias para seguir desarrollándome gracias.

A MIS PADRES

DONATO CRUZ TINOCO Y AURELIA VIDAL BOCANEGRA.
Gracias por todo lo que me han dado en la vida, por el apoyo otorgado para la realización de este sueño, gracias por creer en mi por que sabían que podría lograrlo, por todos los buenos consejos, por darme ánimos cuando mas los he necesitado, por que han estado a mi lado ustedes cuando las tormentas y males me han aquejado, sabiendo siempre levantarme después de caído y sobre por todos los buenos principios que me han inculcado durante toda mi vida gracias.

A MIS HERMANOS

JESUS, HERIBERTO E ISABEL

Gracias por estar siempre con migo por apoyarme y creer en mi siempre supieron que podía lograrlo y gracias por estar tan solo con migo gracias.

A MIS AMIGOS

Gracias por estar a mi lado por que me ayudaron muchisimo cuando lo necesite por saber encaminarme y darme buenos consejos y ánimos para seguir siempre adelante.

A LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO.

Gracias por los conocimientos otorgados durante toda mi vida académica.

A MIS PROFESORES

Que supieron transmitirme sus conocimientos a través de todas las materias y por. Saberme encaminar hasta este momento, gracias.

Gracias a todas aquellas personas que aportaron cosas buenas y malas en mi formación académica y personal.

ÍNDICE

INTRODUCCIÓN

Vivimos en la actualidad entre computadoras e información, la mayoría de las personas tienen un acceso directo o indirecto con Internet, de modo que esta a su disposición una computadora y un enlace a la red de redes, pero no por ello todos saben como funciona y de donde procede toda esa información.

Con este tema de tesis, trataremos de explicar al usuario el modo en que la computadora se conecta, así como las rutas que debe de tomar la información desde una fuente hasta un host destino, que es la información que el usuario ve directamente en su computadora, esta tratado de la manera más sencilla para que el usuario sin necesidad de ser especialista en computación, entienda el proceso y este mas familiarizado con el tema.

El crecimiento de la tecnología en estas últimas decadas ha sido sorprendente, estamos avanzando a pasos agigantados y por ello es bueno saber de una manera más simple como ha ido creciendo dicha tecnología, comenzando desde una simple red de computadoras hasta la famosa red de redes conocida como Internet.

Las primeras redes eran las redes en tiempo repartido que utilizaron los chasis y las terminales unidas. Tales ambientes fueron puestos en ejecución por el Systems Network Architecture de la IBM (SNA) y la arquitectura de red digital.

Las redes de área local (LAN), se desarrollaron alrededor de la revolución de la PC. Las redes de área local permitieron a usuarios múltiples en un área geográfica relativamente pequeña intercambiar archivos y mensajes, igual como tener acceso a recursos compartidos tales como servidores e impresoras de archivo. Cada día se crean nuevos métodos para poder conectar redes dispersas.

Hoy, la alta velocidad de las redes de área local y las Internet-Working se están utilizando extensamente, en gran parte porque funcionan a una velocidad muy elevada y apoyan los usos tales de alto ancho de banda como multimedia y videoconferencia.

La Internet se desarrolló como solución a tres problemas dominantes: redes de área local aisladas, duplicación de recursos y de una carencia de la dirección de la red.

Poner una red interna en ejecución funcional no es ninguna tarea simple. Muchos desafíos se deben hacer frente, especialmente en las áreas de la conectividad, de la confiabilidad, de la dirección de la red, y de la flexibilidad. Cada área es dominante en establecer una red interna eficiente y eficaz.

Porque las compañías confían pesadamente en la comunicación de datos, la Internet-Working debe proporcionar cierto nivel de la confiabilidad.

Además, la dirección de la red debe proporcionar la ayuda centralizada y las capacidades de la localización de averías en una red interna. La configuración, la seguridad, el funcionamiento, y otras condiciones se deben tratar adecuadamente para la red interna.

La seguridad dentro de una red interna es esencial. Mucha gente piensa en seguridad de la red de la perspectiva de proteger la red privada contra ataques del exterior. Sin embargo, es justo como importante proteger la red contra ataques internos, especialmente porque vienen la mayoría de las aberturas de la seguridad desde adentro.

Las redes deben también ser aseguradas para no poder utilizar la red interna pues una herramienta para atacar otros sitios externos.

CAPITULO PRIMERO REDES DE DATOS

1.1 Orígenes de las redes de datos

Fig. 1.1

La comunicación ha sido siempre uno de los grandes retos de la humanidad. La necesidad de intercambiar ideas se ha dado desde tiempos remotos y más recientemente la necesidad de comunicarse a grandes distancias ha dado paso al nacimiento de las telecomunicaciones.

Desde el inicio del siglo XX la comunicación ha ido en constante evolución debido a lo que esto significa para el hombre a partir de los años 50´s, con la introducción de la computadora en el mundo de los negocios, ha habido grandes desarrollos en el campo de las telecomunicaciones orientados a conectar entre sí a estos dispositivos y otros muchos más. Las redes de comunicación de datos resultaron de la convergencia de dos tecnologías diferentes: informática y telecomunicaciones, llamada telemática.

En la actualidad sé esta logrando la convergencia total de todos los servicios (voz, datos, video, etc.) sobre una sola red: La Red de Datos. En los años 60´s y principios de los 70´s, el ambiente tradicional de comunicación entre computadoras, era centrado alrededor de una maquina principal (Host / Mainframe). Este ambiente requería líneas de acceso de baja velocidad denominadas terminales tontas que usaban para comunicarse al Host centralizado, actuando como interfaces hombre-maquina a través de la cual se realizan peticiones y se recibe información del Host, con estas terminales nacen también los primeros protocolos para comunicaciones asíncronas.

En 1981 IBM presento la computadora personal (PC) en el mercado, esto brindo a los usuarios la oportunidad de contar con la capacidad de proceso en un puesto individual de

trabajo (stand alone). Y así lo concibió inicialmente IBM para los hogares, pero dentro de una empresa las PC´s deberían de estar conectadas al sistema de computo central.

La introducción de la PC´s revoluciono la comunicación tradicional y las redes de computadoras, y conforme el sector de negocios se dio cuenta de la flexibilidad y poder de estas se incrementó de manera explosiva su uso. Las redes de computadoras de área local (LAN) evolucionaron primeramente para disminuir el costo de dispositivos tales como impresoras de alta velocidad o discos duros de gran capacidad de almacenamiento.

Inmediatamente después se reconoció la importancia estratégica de interconectar estas redes, y las corporaciones empezaron a interconectar LAN´s antes aisladas, esto les proporciono bases para aplicaciones de empresa a nivel nacional y mundial tales como correo electrónico, transferencia de archivos y acceso remoto a redes corporativas, incrementando su productividad y competitividad.

Red de area local

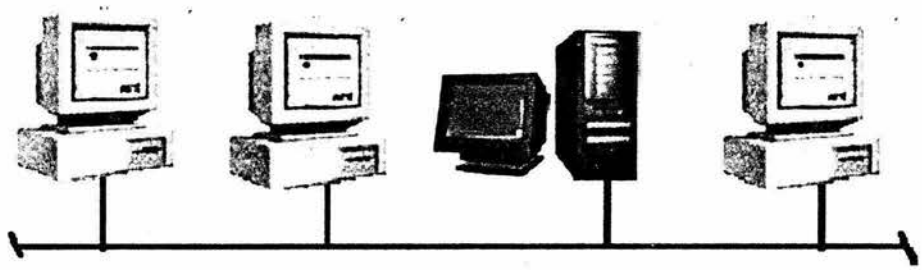

Fig. 1.2 Red de área local

En esta época las minicomputadoras y las redes compartidas de área amplia (WAN) evolucionaron. Las minicomputadoras, generalmente localizadas fuera del centro de datos principal, facilitaron el surgimiento del procesamiento distribuido de datos. Los sistemas VAX de Digital Equipment Corporation (DEC) y las redes DECNet son típicos de esta época, en donde también se desarrollaron varios protocolos de comunicaciones.
A partir de los años 90´s surge el concepto de interconexión e interoperabilidad de redes de computadoras (Internet-working), esto es, redes LAN, redes publicas de datos, líneas privadas y canales de mainframes todos siendo usados para lograr una integración y consistencia de intercambio de información de manera transparente sin importar el patrón de tráfico que sé este usando.

Aprovechando nuevos protocolos y medios de transmisión más eficientes como ISDN, Frame Relay y ATM surgen redes de computadoras de área global (GAN) exigiendo

mayores anchos de banda y sobre todo la convergencia de todos los servicios: voz, video y datos (Multimedia) con un solo acceso y a futuro con una sola terminal. De ahora en adelante se espera una proliferación de redes de este tipo con una convergencia a nivel IP, tomando como base las LAN (ambiente cliente-servidor) evolucionadas hacia fibra óptica, conmutadas y con velocidades de 100 / 1000 Mhz y conmutación ATM.

1.2 Componentes de una red de datos

¿ Que es una red de datos ?

Una red es un conjunto de dispositivos tales como: computadoras (personales, minicomputadoras, mainframes), terminales interactivas, elementos de memoria, impresoras, dispositivos de telecomunicaciones, etc., conectados entre sí, que permiten a los usuarios tener transferencia de datos y compartir recursos de hardware y software.

Fig. 1.3 Componentes de una red de datos

Red de computadoras

En términos generales el objetivo de una red de computadoras es compartir recursos y hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios. En otras palabras, el hecho de que un usuario esta a 1000 Km de distancia de su sistema no deberá impedirle usar sus datos y recursos como si fueran locales, resumiendo, es un intento por acabar con la tiranía geográfica implantada por un cableado entre terminales.

Una segunda meta es lograr una alta confiabilidad al contar con fuentes alternativas de suministro, esto es, varias maquinas en donde se encuentre replicada la información para que en caso de fallas en hardware se pueda acceder a un respaldo sobre la misma red.
Otra de las metas es la de ahorrar dinero ya que las maquinas pequeñas tienen una relación precio-rendimiento mucho mejor que las grandes y con ello se ha orillado a los diseñadores de redes a implementar sistemas compuestos en donde el poder de procesamiento se distribuye en una gran cantidad de computadoras personales y una maquina central encargada de almacenar los datos y programas de todos sus usuarios (clientes), a esto maquina se le llama servidora de archivos (File Server). A este esquema o arquitectura se le denomina: Modelo Cliente – Servidor. Todo lo anterior enfocado a una convergencia de todo tipo de servicios (voz, datos, video, multimedia) en una sola red universal y sobre dispositivos 100% digitales que puedan manejar esta convergencia.

Elementos que conforman la red

- Equipos terminales de datos: computadoras, impresoras, terminales.
- Nodos de comunicación: es en donde se realizan los procesos que hacen posible la transmisión de información por un medio determinado, ya sean tarjetas de red (NIC), módems, NTU, DSU.
- Medios de transmisión: par trenzado, cable coaxial, fibra óptica, microondas, satélite.
- Nodos de conmutación: cualquier punto de la red en la cual los datos son conmutados o enrutados. Accesos a la red telefónica publica, redes publicas y privadas de datos.
- Sistema operativo de red (NOS): Novell, Netware, Windows NT, UNIX / LINUX, Macintosh, etc.

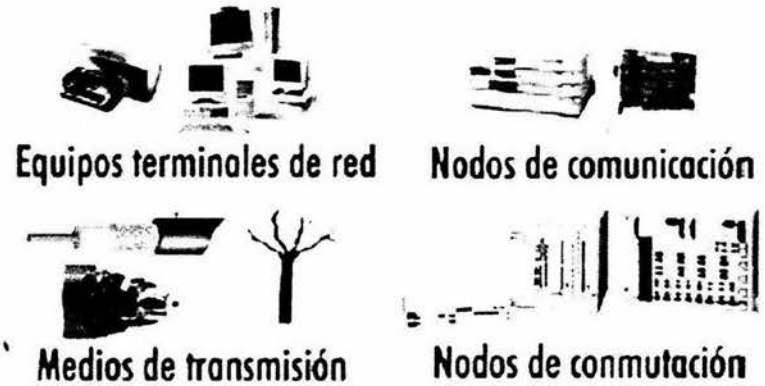

Fig. 1.4 Elementos de una red

1.3 Clasificación de las redes

Tipos de redes

Las redes de computadoras por su cobertura geográfica pueden ser:

- Redes de Área Local (LAN).
- Redes de Área Metropolitana (MAN).
- Redes de Área Amplia (WAM).
- Redes de Área Global (GAM).

Redes de Área Local

Generalmente llamadas LAN (Local Area Network), son redes de propiedad privada dentro de un solo edifico o campus de hasta unos cuantos kilómetros de extensión, se usan para conectar computadoras personales y estaciones de trabajo con el objeto de compartir recursos, se distinguen por su tamaño, tecnología de transmisión y su topología.

Las LAN tradicionales operan a velocidades que van de los 10 a los 100 Mbps y actualmente nuevas LAN ya se están implementando a velocidades del orden de Gbps.

Redes de Área Metropolitana

Una Red de Área Metropolitana o MAN (Metropolitan Área Network) es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas cercanas a una ciudad y podría ser privada o publica.

Una MAN puede manejar datos y voz, e incluso podría estar relacionada con la red de televisión por cable, solo tiene uno o dos cables y no contiene elementos de conmutación, la principal razón para distinguirla es que ha adoptado un estándar que sé esta implementando: DQDB (Distributed Queue Dual Bus) o Bus Dual de Cola Distribuida, estandarizado por la IEEE.

El DQDB cuenta con 2 buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras. Él trafico destinado a una computadora situada a la derecha del emisor usa el bus superior, si es hacia la izquierda usara e bus inferior.

Redes de Área Amplia

Llamada también WAN (Wide Area Network), se extiende sobre un área geográfica extensa, a veces un país o un continente, contiene una colección de maquinas dedicadas a ejecutar programas de aplicación de usuario (Host´s), también denominadas sistema terminal (End System).

Las Hosts están conectadas por una subred de comunicación o simplemente subred, su trabajo es conducir mensajes de una Host a otra. La separación entre los aspectos exclusivamente de comunicación de la red y los aspectos de las aplicaciones simplifican enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión también llamadas circuitos, canales o troncales, mueven bits de una maquina a otra y los elementos de conmutación son maquinas especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, este elemento debe escoger una línea de salida para reenviarlos. Principalmente conocidos como enrutadores (Router´s).

Redes de Área Global

Como consecuencia de la diversificación y crecimiento de los servicios en la llamada red de redes o Internet, surge ahora el concepto de las redes globales, primero desde el punto de vista de cobertura geográfica, al hablar de la aldea global, hablamos de comunicación a nivel mundial con total transparencia desde el punto de vista de tarificación y compatibilidad entre redes de telecomunicaciones de cada país, y desde el punto de vista de servicios, hablamos de la capacidad de generar una comunicación virtual total para negocios, multimedia, transferencia de grandes volúmenes de información con anchos de banda asignados de manera dinámica por encima de los 2 Mbps, la convergencia de servicios de voz sobre redes de datos (VoData), etc.

1.4 Topologías de las redes

El término topología puede definirse como el "estudio de la ubicación". La topología es objeto de estudio en las matemáticas, donde los "mapas" de nodos (puntos) y los enlaces (líneas) a menudo forman patrones.

En si la topología de una red es la forma en como están conectados sus nodos, se podrían definir en dos tipos de conexiones: punto a punto (enlace entre dos nodos) y multipunto (conexión de tres o mas nodos).

Las principales topologías de red son:

Topología en Bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Cada host está conectado a un cable común, en esta topología, los dispositivos clave son aquellos que permiten que el host se "una" o se "conecte" al único medio compartido. Una de las ventajas de esta topología es que todos los hosts están conectados entre sí y, de ese modo, se pueden comunicar directamente. Una desventaja de esta topología es que la ruptura del cable hace que los hosts queden desconectados. Una topología de bus permite que todos los dispositivos de red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja ya que es común que se produzcan problemas de tráfico y colisiones.

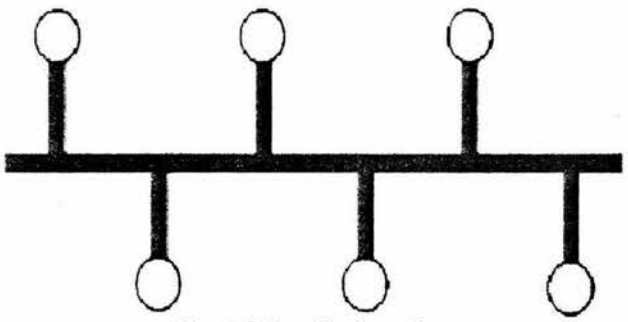

Fig. 1.5 Topología en Bus

Topología en Anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo esta conectado con solo dos nodos adyacentes, la topología muestra todos los dispositivos que están conectados directamente entre sí por medio de cables, para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

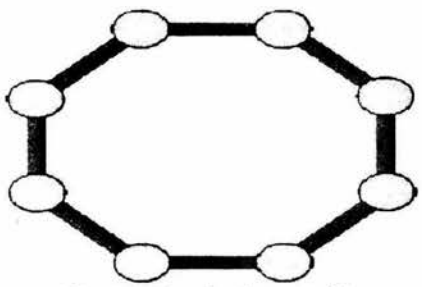

Fig. 1.6 Topología en Anillo

Topología en Estrella

La topología en estrella tiene un nodo central desde el que irradian todos los enlaces hacia los demás nodos y no permite otros enlaces, la ventaja principal es que permite que todos los demás nodos se comuniquen entre si de manera conveniente, la desventaja es que si el nodo central falla, toda la red se desconecta, esto quiere decir que con ella toda la información pasaría entonces a través de un solo dispositivo, esto podría ser aceptable por razones de seguridad o de acceso restringido, pero toda la red estaría expuesta a tener problemas si falla el nodo central de la estrella.

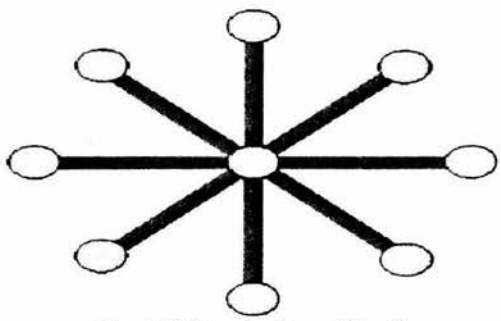

Fig. 1.7 Topología en Estrella

Topología en árbol

Tiene un nodo de enlace troncal desde el que se ramifican los demás nodos, hay dos tipos de topologías en árbol: el árbol binario (cada nodo se divide en dos enlaces) y el árbol backbone (tiene nodos ramificados con enlaces que salen de ellos), el flujo de información es jerárquico.

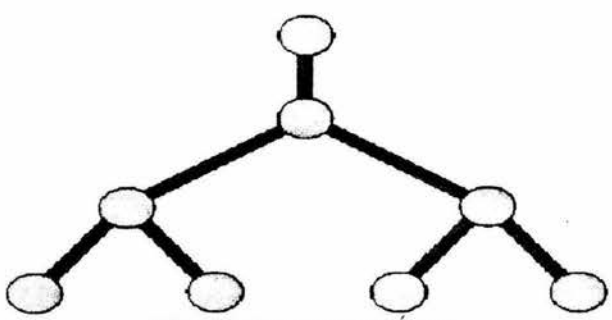

Fig. 1.8 Topología en Árbol

Topología en malla

En una topología de malla cada nodo se enlaza directamente con los demás nodos, este tipo de cableado tiene ventajas y desventajas muy especificas, las ventajas son que cada nodo se conecta físicamente a los demás nodos, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar al destino, además de que permite que la información

circule por varias rutas a través de la red, la desventaja física principal es que solo funciona con una pequeña cantidad de nodos, ya que de los contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones se torna abrumadora, el comportamiento de una topología de malla depende enormemente de los dispositivos utilizados.

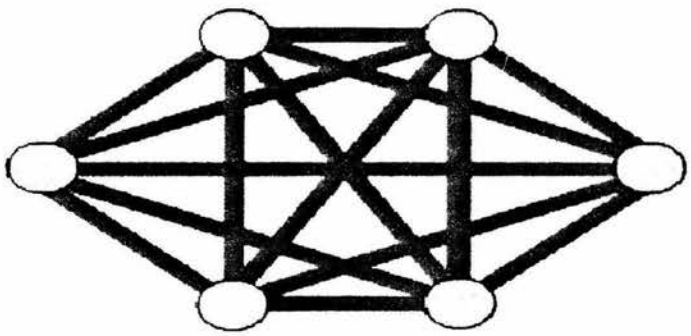

Fig. 1.9 Topología de Malla

1.5 Codificación de datos

Transmisión de señales de voz

La voz es una señal analógica por naturaleza. El teléfono realiza la función de transformar la voz del usuario en una señal adecuada para su transmisión por una red telefónica.

Hasta los años 60´s el teléfono generaba una señal analógica, la cual era transmitida de usuario a usuario a través de la red en forma totalmente analógica.

Debido a que las señales digitales presentan una cierta inmunidad al ruido e interferencias, con lo cual se producen menos errores en su transmisión, a partir de los años 60´s se ha preferido digitalizar la voz humana para transmitirla.

Modulación por codificación de pulsos

El método más simple y más utilizado para convertir una señal analógica a una secuencia digital es el proceso llamado modulación por codificación de pulsos (Pulse Code Modulation; PCM). El PCM fue inventado en los años 30´s pero empezó a ser utilizado en los 60´s cuando dio inicio la comercialización de circuitos integrados.

La teoría en la que se basa la digitalización de señales analógicas es la teoría de Nyquist, la cual especifica que para poder codificar adecuadamente una señal analógica de

determinado ancho de banda W, se necesita por lo menos 2W muestras de la señal por segundo.

Velocidad de un canal telefónico

El rango de frecuencias o ancho de banda en telefonía utilizado es de 300 a 3,400 Hz, pero nominalmente se considera de 4,000 Hz por lo que se toman 8, 000 muestras por segundo. Estas muestras son cuantizadas tomando como base un cierto numero de niveles llamados niveles de cuantización (expresados en números binarios).

A principios de los 60's, en base a estudios psico-acústicos, se determino que para cuantizar la voz en telefonía se necesitan 256 niveles los cuales se podían representar utilizando 8 bits. Esto implica que son necesarios 64,000 bps para codificar en forma digital la voz telefónica, es decir 8 bits por cada una de las 8,000 muestras. Actualmente, estos 64,000 bps son la velocidad nominal de un canal de voz digital.

1.6 Conmutación

Técnicas de conmutación

Existen dos técnicas de conmutación para trafico de datos:

- Conmutación de circuitos
- Conmutación de paquetes

- Conmutación de circuitos

En esta técnica, una trayectoria o circuito físico entre el nodo fuente y el nodo destino debe ser establecida antes de que los datos puedan ser transmitidos. Después de que la conexión es establecida, el uso del circuito es exclusivo y continuo durante el intercambio de información. Cuando este intercambio es completado, el circuito es desconectado y los enlaces físicos entre los nodos están listos para ser usados en otras conexiones.

Como ejemplo el principal uso de la conmutación de circuitos es en la red telefónica publica, cuando una llamada pasa a través de una central de conmutación, se establece una conexión física entre la línea de la que proviene la llamada y una de las líneas de salida.

Particularidades

El tiempo transcurrido entre el momento en que se termina de marcar un numero y el momento en que inicia el sonido del timbre del abonado llamado, puede ser fácilmente de 5 segundos, y más en el caso de llamadas de larga distancia o internacionales.

Durante este intervalo de tiempo, el sistema telefónico se encuentra en la etapa de búsqueda de un camino físico.

Antes de que la transmisión de datos pueda comenzar, la señal de solicitud de llamada deberá propagarse hasta su destino y ser reconocida como tal. Para muchas aplicaciones de computadoras es indeseable tener tiempos de establecimiento de conexión muy largos. Para aplicaciones de transmisión de información del orden de microsegundos y que requieren la capacidad total del canal, como en los sistemas multiusuarios de trafico de datos en ráfagas, la conmutación de circuitos es lenta, relativamente cara e ineficiente. En muchos casos el canal puede estar sin utilizarse una buena porción del tiempo de conexión y permanecer inaccesible para otros usuarios.

Una vez que la conexión es establecida, la transmisión esta garantizada y es secuencial, los retardos son pequeños y constantes, la comunicación toma lugar en tiempo real y no existe congestión.

- Conmutación de paquetes

La conmutación de paquetes se creo con la finalidad de utilizar mas eficientemente los medios de transmisión en sistemas multiusuarios principalmente con trafico de datos en ráfaga. En este tipo de conmutación, los datos de diferentes usuarios o aplicaciones pueden compartir una misma trayectoria física.

Paquete de datos

Es una secuencia continua de bits de un determinado tamaño que es enviada a través de una red como unidad individual. Los paquetes son ensamblados en el nodo destino para obtener la información o mensaje transmitido. Cada paquete que es enviado contiene bits de encabezado (donde se puede encontrar información de la dirección del nodo fuente y del nodo destino, él numero de secuencia del paquete, etc.) y bits de chequeo de errores.

Sistema de conmutación de paquetes

Un sistema de conmutación de paquetes acepta paquetes de un nodo fuente, los almacena en el buffer de memorias de un conmutador y luego los retransmite a otro conmutador del sistema donde la misma operación de almacenaje-retransmisión ocurre, esto se repite hasta que los paquetes llegan al nodo destino.

Un sistema de este tipo no necesita que una trayectoria física dedicada sea establecida de antemano entre el emisor y el receptor.

Mensaje de acuse de recibo

Generalmente existe un mensaje de acuse de recibo (acknowledgment) de que los paquetes llegaron bien, entre conmutadores adyacentes. Los paquetes tienen que ser retransmitidos cuando el nodo emisor no recibe este mensaje en cierto lapso de tiempo o recibe un mensaje de acuse de recibo negativo que indica que se detecto un error.

Particularidades

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

Debido a que los circuitos nunca están dedicados a una tarea especial en la conmutación de paquetes, estos pueden ser utilizados por paquetes de otro origen o por paquetes con destino que no tengan ninguna relación. Sin embargo y precisamente porque los circuitos no están dedicados a una tarea especial, la aparición de una sobrecarga repentina en el tráfico de entrada puede llegar a trastornar un conmutador, excediendo su capacidad de almacenamiento y ocasionando la perdida de paquetes.

En la conmutación de paquetes, por lo general, el costo se basa tanto en él numero de paquetes transportados, como en el tiempo de conexión. La distancia de transmisión no importa demasiado, con excepción quizás de las distancias internacionales. Con la conmutación de circuitos, el cargo se basa solamente en la distancia y en el tiempo y no en el trafico.

Técnicas de conmutación de paquetes

La conmutación de paquetes se puede realizar de dos formas: utilizando circuitos virtuales o utilizando datagramas.

Circuitos virtuales: Por lo general se utilizan en redes cuyo servicio principal esta orientado a conexión. La idea que respalda a los circuitos virtuales es la de evitar que se tengan que hacer decisiones de enrutamiento para cada paquete transmitido. A cambio de esto. Cuando se establece una conexión, se selecciona una ruta que va desde el nodo origen hasta el nodo destino como parte del proceso de conexión. Esta ruta se utiliza para todo él trafico que circule por la conexión, exactamente de la misma manera como trabaja el sistema telefónico. Cuando se libera la conexión, se deshace el circuito virtual.

Aunque se establezca un circuito virtual para determinar transmisión de datos de un usuario, el medio físico utilizado por este circuito puede ser compartido por paquetes de otros usuarios al mismo tiempo o inclusive por datos de otros circuitos virtuales del mismo usuario. Utilizando circuitos virtuales, los paquetes llegan al nodo destino en la misma secuencia con la que los manda en nodo fuente.

Como los paquetes que circulan por un circuito virtual dado siguen siempre la misma ruta a través de la red, cada conmutador deberá recordar hacia donde expedirlos para cada uno de los circuitos virtuales establecidos que pasa a través de el.

Cada conmutador debe mantener una tabla donde se especifique el nodo del que proviene, él numero del circuito virtual y el nodo al que se tiene que enviar el paquete para cada circuito virtual establecido.

Cada paquete que viaja a través de la red, deberá contener un campo con el numero de circuito virtual en su encabezado o cabecera, además del numero de secuencia, el código de redundancia, etc. Cuando llegue un paquete a un conmutador, este conocerá la línea por la que llego, así como él numero del circuito virtual, basándose exclusivamente en esta información, los paquetes deberán expedirse al siguiente conmutador correctamente.

Datagramas: Con datagramas ninguna ruta se determina en forma anticipada. Cada paquete se cinta independientemente de sus predecesores. Los paquetes sucesivos pueden seguir caminos diferentes para llegar al mismo destino. Al mismo tiempo que las redes datagrama tienen que hacer un mayor trabajo, también son más robustas y se adoptan con mayor facilidad a los fallos y a la congestión que las redes de circuitos virtuales.

Al utilizar datagramas, los conmutadores emplean una tabla de enrutamiento para saber hacia cual nodo destino se deberá lanzar cada paquete, esto depende de la dirección destino que cada paquete trae indicado en su encabezado. Estas tablas, también son necesarias cuando se usan circuitos virtuales, pero solo se emplean en el primer paquete, para determinar la ruta que se utilizara para la totalidad de los paquetes restantes.

Cada datagrama contiene la dirección completa del nodo fuente y del nodo destino. Debido a que los datagramas pueden seguir rutas diferentes, es posible que lleguen en una secuencia diferente a la enviada por lo que se hace necesario que sean ordenados en el nodo destino para obtener la información transmitida.

Los datagramas se pueden utilizar para servicios orientados a conexión como en el caso del TCP (Protocolo de control de transmisión) o para servicios orientados a no-conexión como en el caso del IP (Protocolo de interred).

Ventajas y desventajas

Tanto los circuitos virtuales como los datagramas presentan ventajas y desventajas. Los circuitos virtuales permiten que los paquetes contengan números de circuitos en lugar de direcciones completas de origen y destino. Si los paquetes tienden a ser muy pequeños, el hecho de tener direcciones completas en cada paquete puede representar una sobrecarga bastante significativa y, por consiguiente, un desperdicio notable de ancho de

banda. El precio que se paga por el uso de circuitos virtuales, es el espacio de memoria que ocupa la tabla que se emplea dentro de los conmutadores.

La perdida de una línea de comunicación resulta fatal para los circuitos virtuales que la están utilizando, pues la comunicación se pierde totalmente; en cambio, si se usan datagramas esta perdida se puede solucionar con relativa facilidad conmutando los datagramas hacia otro link con el mismo destino, en el proceso solo se pierden unos cuantos datagramas, el uso del datagrama también permite que los conmutadores balanceen él trafico a través de la red, gracias a que las rutas se pueden modificar a mitad de una conexión, es decir, se actualizan de una manera dinámica para conocer las condiciones actuales del trafico en la red.

Asunto	Red Datagrama	Red de Circuito Virtual
Establecimiento del circuito	No es posible	Requerido
Direccionamiento	Cada paquete contiene la dirección completa de la fuente y del destino	Cada paquete contiene un numero corto de CV
Enrutamiento	Cada paquete sé enruta independientemente	Ruta seleccionada cuando el CV se establece, todos los paquetes siguen esa ruta
Efecto a las fallas en un nodo (perdida de memoria)	Ninguno, con excepción de los paquetes que se perdieron durante la falla	Todos los CV's que pasan a través del equipo que fallo se terminan
Secuenciamiento de paquetes	No garantizado	Garantizado
Complejidad	En la capa de transporte	En la capa de red
Adecuado para	Servicio orientado a conexión y a no-conexión	Servicio orientado a conexión (protocolo X.25)

Tabla 1.1

1.7 Organizaciones de normalización

Organizaciones normativas

Con la finalidad de establecer normas o estándares en el campo de las telecomunicaciones para que diferentes fabricantes pudieran producir artículos bajo una misma filosofía asegurando de esta forma la interoperatividad de los mismos y diversos

proveedores pudieran proporcionar sus servicios siguiendo parámetros comunes, se crearon varias organizaciones de normalización. A continuación se explica lo que efectúa cada una de las principales organizaciones.

IEEE (Institute of Electrical and Electronics Engineers)

Esta organización es responsable de estándares específicos relacionados con los sistemas de comunicación privada, por ejemplo: el estándar IEEE 802 se refiere a las redes de área local (LAN´s).

EIA (Electronic Industries Association)

Este cuerpo de normalización de la industria electrónica de los Estados Unidos de América es responsable de los estándares involucrados en el nivel físico. Los estándares originados por esta organización inician con las letras RS, como por ejemplo el RS232-C.

ISO (International Standards Organization)

Es un grupo de varias organizaciones de normalización, es responsable de la normalización de una gran variedad de artículos. Específicamente, el comité técnico numero 97 es el responsable de los estándares de las comunicaciones de datos, por ejemplo: las recomendaciones relacionadas con el HDLC y el modelo OSI.

ANSI (American National Standards Institute)

Es una organización no gubernamental que representa a los Estados Unidos de América ante los organismos internacionales de normalización y es miembro de la ISO. Entre sus trabajos de normalización se encuentran los estándares de la tecnología de conmutación rápida de datos Frame Relay.

CCITT (Comité Colsultatif International de Telephonie et Telegraphie)

Esta organización actualmente conocida como ITU (International Telecom Union), define estándares relacionados con telefonía, telegrafía y comunicación de datos. Tiene periodos de estudio de 4 años, los cuales concluyen con la publicación de un conjunto de libros, conocidos anteriormente como recomendaciones del CCITT.

Por otra parte cuenta con varios grupos de estudio los cuales tienen tareas especificas. Todas las recomendaciones del CCITT inician con una letra seguida de un numero de máximo 4 cifras. Las letras indican el área a la que pertenece el estándar.

Grupo de Estudio	Area	Letra
VII	Redes publicas de comunicación de datos	X
VIII	Equipo terminal telegráfico	S
VIII	Equipo terminal para servicio telemático	T
XI	Señalización en redes telefónicas	Q
XV	Conexiones y circuitos telefónicos internacionales Sistemas de transmisión	G
XVII	Comunicación de datos en redes telefónicas analógicas	V
XVIII	Red digital de servicios integrados (ISDN)	I

Tabla 1.2

1.8 Modelo de Referencia OSI

Modelo OSI

En 1929, ISO definió su modelo de arquitectura de red OSI (Interconexión de sistemas abiertos). Este modelo fue adoptado en 1980 por el CCITT en su recomendación X.200. La comunicación de datos comprende 2 aspectos principales:

El transporte: involucra todas las funciones relacionadas con la transparencia entre dos usuarios finales.

La manipulación de datos: los datos deben ser liberados en una forma inteligible, en algunos casos los datos deben ser convertidos.

Ambos aspectos se dividieron en subfunciones, por lo que finalmente entre el trasporte de datos y la manipulación de los mismos se definió una función que se encargara de monitorear el sistema de transporte.

Consideraciones de diseño para las capas

Algunos de los problemas clave en el diseño de redes de computadoras se presentan en varias capas. A continuación se mencionan las más importantes:

Cada capa necesita un mecanismo para identificar emisores y receptores. Puesto que una red normalmente tiene muchas computadoras, las cuales pueden tener múltiples procesos, se requiere un mecanismo para que un proceso de una maquina especifique

con quien quiere conversar. Como consecuencia de tener múltiples destinos, se necesita alguna forma de direccionamiento que permita determinar un destino especifico (Ruteo). Se tienen que definir las reglas de transferencia de datos:

- Comunicación Simplex
- Comunicación Half Duplex
- Comunicación Full Duplex

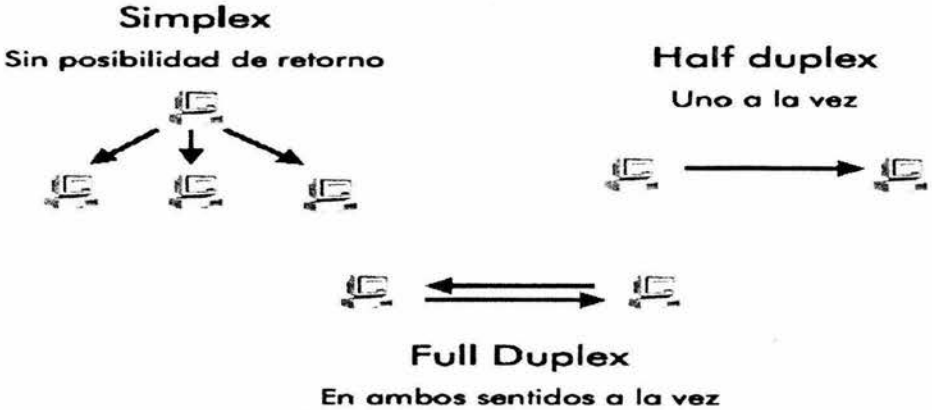

Fig. 1.10 Tipos de comunicaciones

Definiéndose también la cantidad de canales de comunicación que serán asignados y de que manera serán usados.

El control de errores es una consideración importante porque los circuitos de comunicación físicos no son perfectos. Se conocen muchos códigos de detección y de corrección de errores, pero ambos extremos de la conexión deben acordar cual se va a usar. De igual manera se deberá establecer un método que garantice la secuencia correcta de los mensajes enviados y recibidos para su posterior reensamble en el destino.

Otra consideración en todos los niveles es como evitar que un emisor rápido sature de datos a un receptor lento, esto mediante retroalimentación en cuanto al estado de la red o de los equipos en los extremos.

Otro problema a resolver es la incapacidad de ciertos sistemas a procesar mensajes de longitud arbitraria, lo que requiere de la definición de procesos de segmentación / reensamble de la información en mensajes que se ajusten a la capacidad de cada sistema procesador, y con el fin de hacer mas eficientes el uso de los medios físicos, se deberán definir procesos de múltiplexación y demultiplexación para múltiples conversiones.

Las 7 capas del modelo OSI

Fig. 1.11 Capas del modelo OSI

El modelo OSI comprende 7 funciones, representadas por 7 capas o niveles en la arquitectura de la red. En la parte inferior se encuentra el enlace físico entre ambos usuarios y en la parte superior se encuentran los usuarios finales con sus peticiones de comunicación de datos y sus datos. Cada capa cumple una tarea especifica y para la ejecución de sus funciones asume que las capas inferiores o superiores, según el flujo de la información, han realizado su función correctamente.

A continuación se describen las capas definidas en le modelo OSI:

Capa Física (Physical Layer) (Capa 1)

Es responsable del transporte de bits. Dependiendo del tipo de enlacé físico los bits se representan de una manera en que puedan ser transportados a través del medio. Define voltajes, tiempos de duración de los pulsos, él numero de pines que tiene el conector de la interfaz y sus funciones, la forma de establecer la conexión inicial y de interrumpirla, etc., algunos la conocen como la interfaz eléctrico – mecánica. Aquí se definen medios de transmisión, velocidades, anchos de banda, topología física de red, técnicas de conversión análoga / digital, modulación y múltiplexación, así como los métodos de conmutación utilizados.

- *Voltajes*
- *Sincronía*
- *Interfaces*

Capa de Enlace de Datos (Data Link Layer) (Capa 2)

Utilizando un medio de transmisión común y corriente, su función es asegurar que la información sea transmitida sin errores entre nodos adyacentes de la red. Esta capa maneja tramas de datos como unidad de transmisión. Como la capa física básicamente acepta y trasmite un flujo de bits sin tener en cuenta su significado o estructura, recae sobre la capa de enlace de datos la creación o reconocimiento de los limites de la trama. Además resuelve los problemas de daño, perdida o duplicidad de datos y participa en la regulación de flujo. Las redes de difusión tiene una consideración adicional en esta capa: como controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos se encarga de este problema, la Subcapa de Control de Acceso al Medio (MAC).

- *Detección y corrección de errores*
- *Creación y reconocimiento de tramas*
- *Control de congestión*

Capa de Red (Network Layer) (Capa 3)

Es la encargada de que los datos sean enviados a su correcto destino, determinando la ruta de transmisión. La unidad de transmisión de datos en esta capa es el paquete de datos. También participa en el control de congestión de la red. En muchas ocasiones se introduce una función de contabilidad en la capa de red, el software deberá saber cuantos paquetes o bits se enviaron a cada cliente con objeto de producir información de facturación. Además la responsabilidad de resolver problemas de interconexión de redes heterogéneas recaerá, en todo caso, en esta capa. En las redes de difusión el problema del Ruteo es simple y la capa de red con frecuencia es muy delgada o incluso inexistente.

- *Determina la ruta de transmisión*
- *Discrimina (información local o de paso)*
- *Distribuye a diferentes aplicaciones*

Capa de Transporte (Transport Layer) (Capa 4)

Su función principal consiste en aceptar los datos de la capa de sesión, dividirlos siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos lleguen correctamente a su destino. Todo lo anterior se debe hacer de una manera eficiente y en forma que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware. A partir de la capa de red, las cuatro capas superiores restantes manejan mensajes como unidad de transmisión de datos.

En condiciones normales, esta capa crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión, sin embargo, si se requiere un alto volumen

de trafico, esta capa puede crear múltiples conexiones de red, dividiendo los datos. También tiene la capacidad de multiplexar varias conexiones de transporte en una conexión de red para reducir costos, estas conexiones se denominan: Circuitos Virtuales. En todos los casos la Capa de Transporte debe lograr que la múltiplexación sea transparente para la capa de sesión. Esta capa determina el tipo de servicio que le proveerá tanto a la sesión como a los usuarios de la red, por ejemplo:

- Canal punto a punto libre de errores, que entregue mensajes o bytes en el orden en que se enviaron.
- Un servicio de transporte de mensajes aislados sin confirmación.
- Un servicio de difusión de mensajes.

Esta capa es de extremo a extremo, del origen al destino, ya que un programa en la maquina fuente sostiene una conversación con un programa similar de la maquina destino, haciendo uso de los encabezados de los mensajes y de los mensajes de control.

- *Define tipo de servicio*
- *Administra la conexión o conexiones*
- *Hace que los cambios HW no afecten al SW*

Capa de Sesión (Sesion Layer) (Capa 5)

Es un tipo de sistema operativo para la comunicación de datos. Permite que los usuarios de diferentes computadoras puedan establecer sesiones entre ellos. Uno de los servicios de la capa de sesión consiste en la realización del control del dialogo. Las sesiones permiten que él trafico vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado. Si él trafico solo puede ir en una sola dirección en un momento dado, la capa de sesión ayudara en el seguimiento de quien tiene el turno. Otro de los servicios de la capa de sesión es la sincronización, esta capa proporciona una forma de insertar puntos de verificación en el flujo de datos, con objeto de que solamente tengan que retransmitirse los datos que se encuentran enseguida del ultimo punto de verificación cuando se reanuda el servicio después de una caída de la red.

- *Inserta puntos de verificación en el flujo de datos*
- *Control de dialogo*

Capa de Presentación (Presentation Layer) (Capa 6)

Permite a computadoras que intercambian información, entenderse o interpretarse entre ellas independientemente de la codificación que utilicen para los caracteres. Esta capa es responsable de convertir los datos transmitidos a una forma inteligible. Después de pasar este nivel los datos recibidos están disponibles en una forma que la computadora

entenderá. Esta capa esta relacionada también con otros aspectos de representación de la información, por ejemplo: la comprensión de datos se puede utilizar aquí para reducir él numero de bits que tiene que transmitirse y la criptografía se necesita usar frecuentemente por razones de privacidad y autenticación.

- *Formatea la información de manera que esta sea legible al usuario*

Capa de Aplicación (Aplication Layer) (Capa 7)

Contiene una variedad de protocolos que hacen posible ofrecer una serie de aplicaciones al usuario final, por ejemplo: correo electrónico, transferencia de archivos, conexión de terminales, directorio telefónico, y en la actualidad también se encarga de los sistemas de cifrado (encriptado) de la información del usuario.

- *Protocolos que permiten ofrecer aplicaciones*

Transmisión de Datos en el Modelo OSI

Como se ha estado viendo a través del análisis de las diferentes capas que integran el modelo OSI, existe una comunicación real y una comunicación virtual entre capas iguales (PEER to PERR), esto se logra mediante la adición de encabezados por cada una de las capas que progresivamente y en orden descendente van armando el paquete a transmitir y que en el sentido de recepción servirán para definir que capa debe de procesar que información de dicho paquete y de esta manera establecer las conversaciones entre capas par.

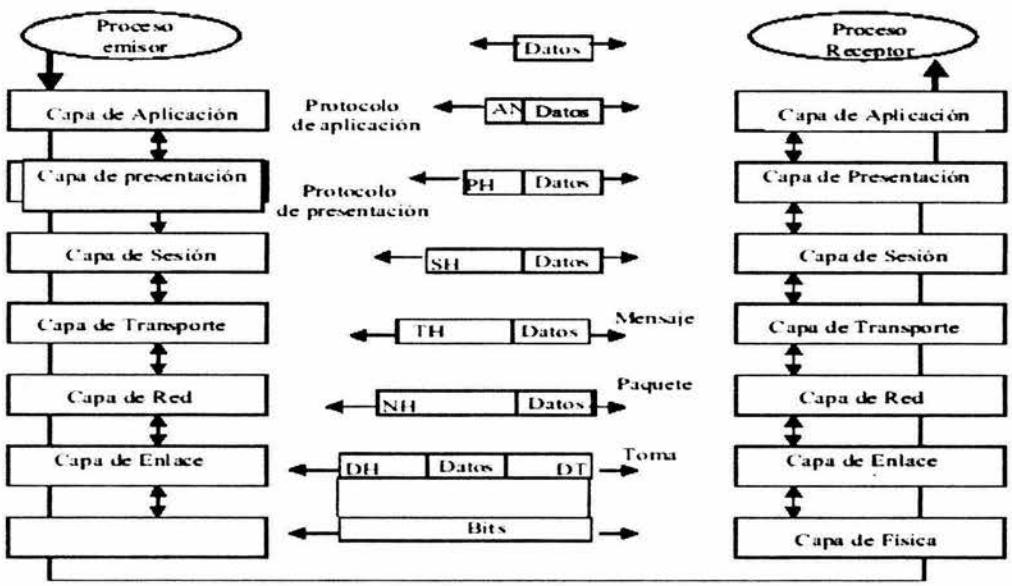

Fig. 1.12 Transmisión de Datos

1.9 X.25 y su relacion con el modelo OSI

Aun cuando fue diseñado para proporcionar un modelo conceptual y no una guía de implementación, el esquema de estratificación por capas de OSI ha sido la base para la implementación de varios protocolos. Entre los protocolos comúnmente asociados con el modelo OSI, el conjunto de protocolos conocido como X.25 es probablemente el mejor conocido y el más ampliamente utilizado. X.25 fue establecido como una recomendación de la Telecommunications Section de la International Telecommunications Union (ITU-TS), una organización internacional que recomienda estándares para los servicios telefónicos internacionales. X.25 ha sido adoptado para las redes públicas de datos y es especialmente popular en Europa. Consideraremos a X.25 para ayudar a explicar la estratificación por capas de OSI.

Dentro de la perspectiva de X.25, una red opera en gran parte como un sistema telefónico. Una red X.25 se asume como si estuviera formada por complejos conmutadores de paquetes que tienen la capacidad necesaria para el ruteo de paquetes. Los anfitriones no están comunicados de manera directa a los cables de comunicación de la red. En lugar de ello, cada anfitrión se comunica con uno de los conmutadores de paquetes por medio de una línea de comunicación serial. En cierto sentido la comunicación entre un anfitrión y un conmutador de paquetes X.25 es una red miniatura que consiste en un enlace serial. El anfitrión puede seguir un complicado procedimiento para transferir paquetes hacia la red.

- Capa física. X.25 especifica un estándar para la interconexión física entre computadoras anfitrión y conmutadores de paquetes de red, así como los procedimientos utilizados para transferir paquetes de una máquina a otra. En el modelo de referencia, el nivel 1 especifica la interconexión física incluyendo las características de voltaje y corriente. Un protocolo correspondiente, X.21, establece los detalles empleados en las redes publicas de datos.

- Capa de enlace de datos. El nivel 2 del protocolo X.25 especifica la forma en que los datos viajan entre un anfitrión y un conmutador de paquetes al cual esta conectado. X.25 utiliza él termino trama para referirse a la unidad de datos cuando esta pasa entre un anfitrión y un conmutador de paquetes (es importante entender que la definición de X.25 de trama difiere ligeramente de la forma en que la hemos empleado hasta aquí). Dado que el hardware, como tal, entrega solo un flujo de bits, el nivel de protocolos 2 debe definir el formato de las tramas y especificar cómo las dos maquinas reconocen las fronteras de la trama. Dado que los errores de transmisión pueden destruir los datos, el nivel de protocolos 2 incluye una detección de errores (esto es, una suma de verificación de trama). Finalmente, dado que la transmisión es no confiable, el nivel de protocolos 2 especifica un intercambio de acuses de recibo que permite a las dos máquinas saber cuando se ha transferido una trama con éxito.

- Capa de red. El modelo de referencia OSI especifica que el tercer nivel contiene funciones que completan la interacción entre el anfitrión y la red. Conocida como capa de red o subred de comunicación, este nivel define la unidad básica de transferencia a través de la red e incluye el concepto de direccionamiento de destino y ruteo. Debe recordarse que en el mundo de X.25 la comunicación entre el anfitrión y el conmutador de paquetes esta conceptualmente aislada respecto al trafico existente. Así, la red permitiría que paquetes definidos por los protocolos del nivel 3 sean mayores que el tamaño de la trama que puede ser transferida en el nivel 2. El software del nivel 3 ensambla un paquete en la forma esperada por la red y utiliza el nivel 2 para transferido (quizás en fragmentos) hacia el conmutador de paquetes. El nivel 3 también debe responder a los problemas de congestionamiento en la red.

- Capa de transporte. El nivel 4 proporciona confiabilidad punto a punto y mantiene comunicados al anfitrión de destino con el anfitrión fuente. La idea aquí es que, así como en los niveles inferiores de protocolos se logra cierta confiabilidad verificando cada transferencia, la capa punto a punto duplica la verificación para asegurarse de que ninguna máquina intermedia ha fallado.

- Capa de sesión. Los niveles superiores del modelo OSI describen cómo el software de protocolos puede organizarse para manejar todas las funciones necesarias para los programas de aplicación. El comité OSI considera el problema del acceso a una terminal remota como algo tan importante que asignó la capa 5 para manejarlo. De hecho, el servicio central ofrecido por las primeras redes publicas de datos consistía en una terminal para la interconexión de anfitriones. Las compañías proporcionaban en la red, mediante una línea de marcación, una computadora anfitrión de propósito especial, llamada Packet Assembler and Disassembler (Ensamblador y desensamblador de paquetes o PAD, por sus siglas en ingles). Los suscriptores, por lo general de viajeros que transportaban su propia computadora y su módem, se ponían en contacto con la PAD local, haciendo una conexión de red hacia el anfitrión con el que deseaban comunicarse.

- Capa de presentación. La capa 6 de OSI esta proyectada para incluir funciones que muchos programas de aplicación necesitan cuando utilizan la red. Los ejemplos comunes incluyen rutinas estándar que comprimen texto o convierten imágenes gráficas en flujos de bits para su transmisión a través de la red. Por ejemplo, un estándar OSI, conocido como Abstract Svntax Notation 1 (Notación de sintaxis abstracta 1 o ASN 1, por sus siglas en ingles), proporciona una representación de datos que utilizan los programas de aplicación. Uno de los protocolos TCP/IP, SNMP, también utiliza ASN 1 para representar datos.

- Capa de aplicación. Finalmente, la capa 7 incluye programas de aplicación que utilizan la red. Correo electrónico y programas de transferencia de archivos.

1.10 Modelo de referencia TCP / IP

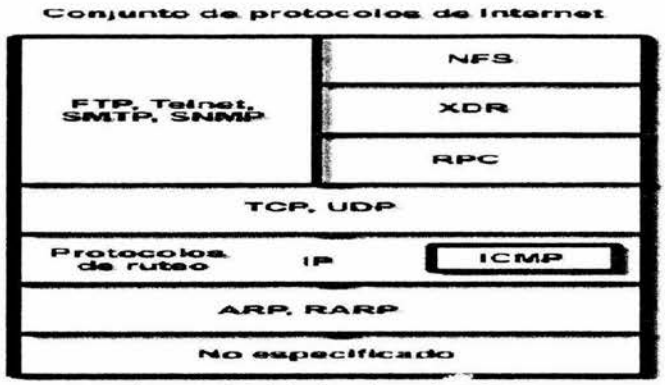

Fig. 1.13 Modelo de referencia TCP/IP

Pasemos ahora del modelo de referencia OSI al modelo que se usa en la "abuela" de todas las redes de computadoras, la ARPANET, y su sucesora más moderna y famosa, la Internet Mundial. Patrocinada por el DoD (Department of Defense) de los EUA, requería de un conjunto de protocolos que permitieran la interconexión de varios tipos de plataformas de manera transparente para los usuarios y sobre todo generar un nivel de respaldo de los costosos elementos de red y subred de la milicia que le permitiera a sus redes seguirse comunicando en caso de un atentado a dichos elementos o a las vías de transmisión. Todos esto requerimientos condujeron a la elección de algo denominado el modelo de referencia TCP / IP sobre una red de conmutación de paquetes basada en una capa de interred carente de conexiones, esta capa es el eje que mantiene unida toda la arquitectura de este modelo.

1.14 Capas principales del modelo TCP/IP

Capa de red

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete

IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI.

En este modelo las dos primeras capas del enlace físico y lógico no están definidas, esto es, para TCP / IP, el tipo de red y el medio de transmisión son transparentes, ya que esta diseñada para realizar funciones de enrutamiento y servicios a aplicaciones, no para transporte.

Capa de interred (IP)

Esta capa es el eje que mantiene unida toda la arquitectura de este modelo, su misión es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino. Los paquetes pueden llegar incluso en un orden diferente a aquel en que se enviaron, en cuyo caso corresponde a las capas superiores reacomodarlos. Es una analogía con el sistema de correos, si envió varias cartas internacionales, con suerte casi todas llegaran a su país de destino como o cuando, no lo sabré hasta que me contesten. La capa de interred define un formato de paquete y protocolo oficial llamada IP (Internet Protocol, protocolo de interred). El trabajo de esta capa es entregar paquetes IP a donde se supone deben ir, aquí la consideración más importante es claramente el ruteo de los paquetes, y también evitar la congestión. Su similar OSI seria la funcionalidad de la capa de Red (3).

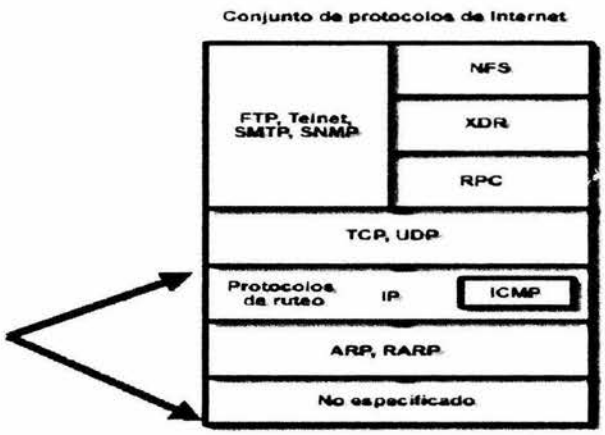

Fig. 1.15

Capa de transporte

Esta capa se diseño para permitir que las entidades pares en los nodos de origen y destino de transporte de OSI. Para esto se definieron 2 protocolos de extremo a extremo:

- TCP (Transmisión Control Protocol): el protocolo de control de transmisión, es un protocolo confiable orientado a la conexión que permite que una corriente de

bytes originada en una maquina se entregue sin errores en cualquier otra maquina de la interred. Este protocolo fragmenta la corriente entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino el proceso TCP receptor reensambla los mensajes recibidos en secuencia para formar la misma corriente de salida, también controla el flujo de trafico.

- El protocolo de datagrama de usuario, es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia de control ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo se usa ampliamente en ambientes cliente – servidor donde se manejan consultas de petición y respuesta de una sola ocasión. También se usa en aplicaciones en donde la pronta entrega es más importante que la entrega precisa, como transmisiones de voz o video.

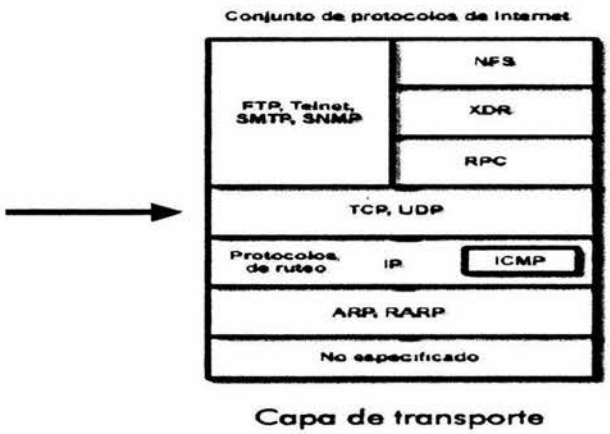

Fig. 1.16

Capa de aplicación

El modelo TCP / IP no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias, y la experiencia dio la razón, ya que se utilizan muy poco en la mayor parte de las aplicaciones y redes actuales. Encima de estas se encontraría la capa de aplicación, que contiene todos los protocolos de alto nivel, algunos de ellos:

TELNET – Terminal virtual para sistemas multiusuario

FTP – File Transfer Protocol (Protocolo de transferencia de archivos)

SMTP – Simple Mail Transport Protocol (Protocolo de transporte de correo simple)

DNS – Servicio de nombres de dominio para direcciones IP

NNTP – Protocolo de transferencia de artículos de noticias

HTTP - Protocolo de transferencia de hipertexto (paginas WEB)

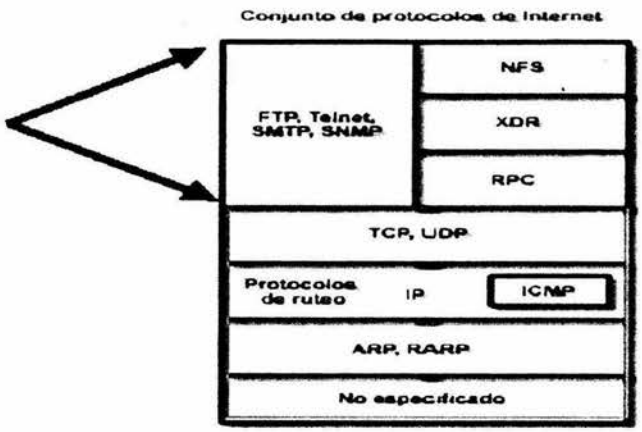

Fig. 1.17

CAPITULO SEGUNDO PROTOCOLOS TCP / IP

2.1 Historia de TCP / IP

TCP / IP (Transfer Control Protocol / Internet Protocol)

Es un conjunto de protocolos diseñado para la comunicación entre computadoras de tal modo para que estas compartan recursos en un ambiente de red. También se le conocen con el nombre de Suite de Protocolos de Internet, donde el termino Internet se le aplica a la totalidad de las redes formada por las redes locales, regionales e internacionales, del sector educativo, privado, centros de investigación, etc.

TCP/IP surge como la solución de integración para múltiples plataformas dentro del proyecto militar ARPANET. En 1970 se lograron enlazar entre sí 4 universidades: Stanford, UCLA, UCSB y la Universidad de Utah.

Posteriormente en 1973 la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA) en EUA inicia un proyecto en forma, que pretendió encontrar tecnologías que permitieran la transmisión de paquetes de datos entre redes que usarán diferentes tecnologías y protocolos, este proyecto buscaba la interconexión de redes de datos.

Tal proyecto tuvo como frutos un conjunto de protocolos de comunicación y servicios conocidos como TCP/IP, de tal manera que estos funcionan como un estándar de comunicaciones en lo que ahora conocemos como la Internet (La Red de Redes).

ARPA

La ARPA (Agencia de Proyectos de Investigación Avanzada), fue la primera en comenzar a trabajar con una tecnología de red de redes a mediados de los años setenta; su arquitectura y protocolos tomaron su forma actual entre 1977 y 1979.

En este tiempo ARPA era conocida como la principal agencia en proporcionar fondos para la investigación de redes de paquetes conmutados y fue pionera de muchas ideas sobre la conmutación de paquetes con su bien conocida ARPANET.

ICCB

La ICCB (Junta de Control y Configuración de Internet), fue formada por la ARPA en 1979 debido a que había muchos investigadores involucrados en el desarrollo de TCP/IP, y esto con el fin de coordinar y guiar el diseño de los protocolos y la arquitectura del Internet que surgía, dicha junta se reunió con regularidad hasta 1983, año en que fue organizada.

ARPANET

ARPANET fue la creada por la ARPA, la cual fue la columna vertebral de Internet, y fue utilizada para realizar muchos de los experimentos con el TCP/IP. La transición hacia la tecnología Internet se completo en enero de 1983, cuando la Oficina del Secretario de Defensa ordenó que todas las computadoras conectadas a redes de largo alcance utilizaran el TCP/IP.

DCA

La DCA (Agencia de Comunicación de la Defensa), dividió ARPANET en dos redes separadas, una para la investigación futura y otra para la comunicación militar. La parte de investigación conservo el nombre de ARPANET; la parte militar, que era un poco más grande, se conoció como red militar MILNET.

UNIX BSD

El UNIX BSD (Distribución Berkeley de Software), era el sistema operativo mas utilizado por los departamentos universitarios de ciencias de la computación, así que ARPA proporciono fondos para que se implementaran los protocolos de TCP/IP con el UNIX BSD, lo cual llegó en un momento significativo ya que muchos de estos departamentos estaban comprando una o dos computadoras mas y les permitió ponerlas en red.

La distribución Berkeley de software se volvió popular ya que ofrecía mucho mas que los protocolos básicos de TCP/IP. Además de los programas normales de aplicación TCP/IP, Berkeley ofrecía un grupo de utilidades para servicios de red que se parecían a los servicios de UNIX utilizados en una sola maquina.

Socket

El socket es una abstracción de sistema operativo proporcionado por UNIX BSD, la cual permite que programas de aplicación accedan a protocolos de comunicación. Su introducción fue muy importante ya que permitió a los programadores utilizar protocolos TCP/IP sin mucho esfuerzo. Por los tanto, alentó a los investigadores a experimentar con el TCP/IP.

2.2 Crecimiento de TCP / IP

Éxito de TCP/IP

El éxito de la tecnología TCP/IP y de Internet entre los investigadores de ciencias de la computación guió a que otros grupos la adoptaran. Dándose cuenta de que la

comunicación por red pronto seria una parte crucial de la investigación científica, la Fundación Nacional de Ciencias tomo un papel activo al expandir el Internet TCP/IP para llegar a la mayor parte posible de científicos.

Crecimiento de TCP/IP

En 1985 la Fundación Nacional de Ciencias, comenzó con un programa para establecer redes de acceso distribuidas alrededor de sus seis centros de supercomputadoras, en 1986 se creo una nueva red de columna vertebral de área amplia, llamada NSFNET, que eventualmente alcanzo todos los centros con supercomputadoras y los unió a ARPANET.

Crecimiento de Internet

Desde su concepción, Internet ha crecido hasta abarcar cientos de redes individuales localizadas en los Estados Unidos y Europa. Inicio conectando computadoras de universidades, así como a centros de investigación privados y gubernamentales. El tamaño y la utilización de Internet ha seguido creciendo mucho más rápido de lo esperado. A finales de 1987, se estimo que el crecimiento había alcanzado un 15% mensual. En 1994, la Internet incorporaba mas de 3 millones de computadoras en 61 países.

Adopción de TCP/IP

La adopción de los protocolos TCP/IP y el crecimiento de Internet no se ha limitado a proyectos con fondos del gobierno. Grandes corporaciones computacionales se conectaron a Internet, así como muchas otras grandes corporaciones, incluyendo: compañías petroleras, automovilísticas, electrónicas, farmacéuticas y de telecomunicaciones.

IAB

La IAB (Junta de Arquitectura de Internet), es quien establece la dirección técnica y decide cuando los protocolos se convierten en estándares. IAB se formo en 1983.

Esto quiere decir que el grupo de protocolos TCP/IP no surgió de una marca comercial especifica o de una sociedad profesional reconocida. La IAB proporciona el enfoque y coordinación para gran parte de la investigación y desarrollo subyacentes de los protocolos TCP/IP, y también guía la evolución de Internet. Decide que protocolos son parte obligatoria del grupo y establece políticas oficiales. Es importante comentar que la IAB no maneja un gran presupuesto, aunque establecía las directivas, no proporcionaba fondos para la mayor parte de la investigación e ingeniería que realizaba, por el contrario, eran los voluntarios los que realizaban casi todo el trabajo.

2.3 TCP/IP vs OSI

La suite de Protocolos Internet especifica funciones correspondientes a las capas del modelo OSI por encima de la capa de enlace de datos. La omisión de protocolos de la capa inferior se diseño intencionalmente para permitir a los protocolos Internet interoperar con diversas tecnologías físicas y de enlace.

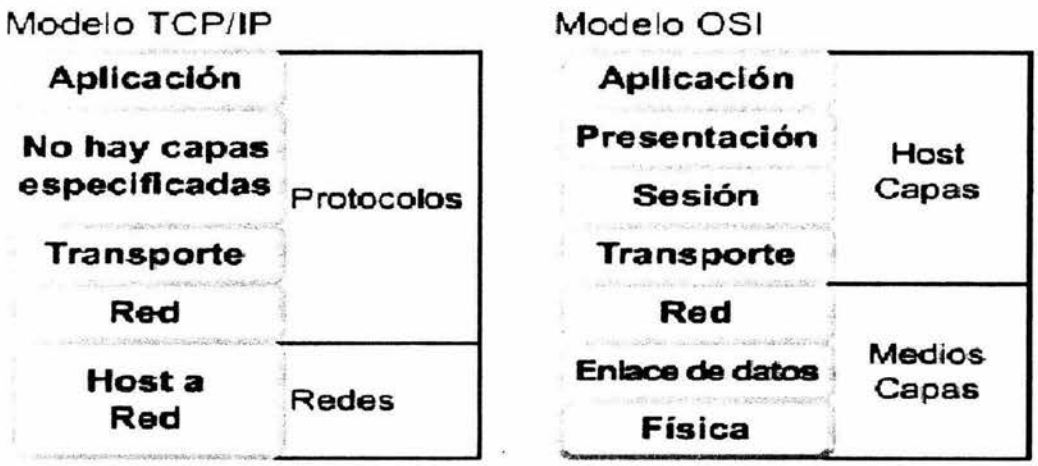

Fig. 2.1 TCP/IP vs OSI

La comparación se debe de tomar con reservas ya que el modelo TCP/IP precede al modelo OSI. La comparación es de acuerdo a la funcionalidad de las capas de TCP/IP con las capas del modelo OSI.

Conceptualmente, enviar un mensaje desde un programa de aplicación en una maquina hacia un programa de aplicaciones en otra, significa transferir el mensaje hacia abajo, por las capas sucesivas del software de protocolo en la maquina emisora, transferir un mensaje a través de la red y luego, transferir el mensaje hacia arriba, a través de las capas sucesivas del software de protocolo en la maquina receptora.

En la practica, el software es mucho más complejo de lo que se muestra en el modelo. Cada capa toma decisiones acerca de lo correcto del mensaje y selecciona una acción apropiada con base en el tipo de mensaje o la dirección de destino. Por ejemplo, una capa en la maquina de recepción debe decidir cuándo tomar un mensaje o enviarlo a otra maquina. Otra capa debe decidir que programa de aplicación deberá recibir el mensaje.

2.4 Niveles del modelo TCP/IP

Toda arquitectura de protocolos se descompone en una serie de niveles, usando como referencia el modelo OSI. Esto se hace para poder dividir el problema global en subproblemas de más fácil solución. A diferencia de OSI el cual esta conformado por 7

capas, el TCP/IP se descompone en cinco niveles, cuatro niveles de software y un nivel de hardware que veremos a continuación.

Nivel Físico

El nivel de red física corresponde al hardware, y su definición eléctrico mecánica, puede ser un cable coaxial, par trenzado, fibra óptica o una línea telefónica.
TCP/IP no considera oficialmente el nivel físico como componente especifico de su modelo y tiende a agrupar el nivel físico con el nivel de red.

Los protocolos principales de este nivel son:

- ARP (Address Resolution Protocol): se encarga de convertir las direcciones IP en direcciones de red física que puedan ser utilizadas por los manejadores, esto a través de tablas de direcciones ARP.
- RARP (Reverse Address Resolution Protocol): se utiliza al momento de la inicialización de las computadoras para que estas, enviando un mensaje con su dirección de red física obtengan de un servidor RARP su dirección IP correspondiente.

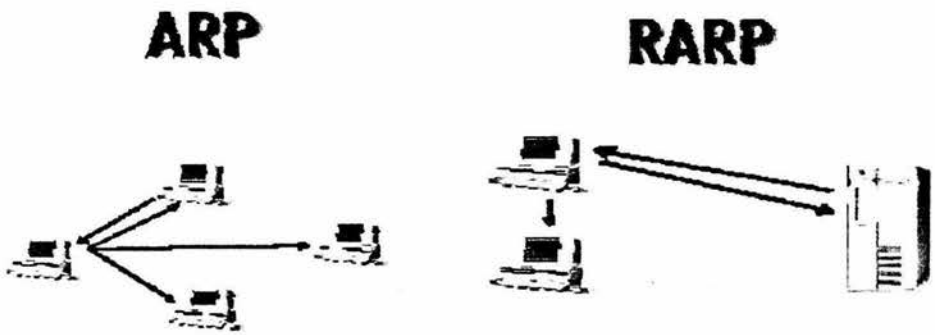

Fig. 2.2 Nivel Físico

Nivel de Enlace

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC(IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las maquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP

conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

El nivel de enlace independiente del medio que utilice necesitara una tarjeta de red especifica que a su vez requerirá un driver o software controlador de dispositivo. Proporciona fiabilidad en la distribución de datos que pueden adoptar diferentes formatos. Aunque TCP/IP no especifica ningún protocolo para este nivel, los más notables usados son:

- SLIP (Serial Line Internet Protocol): es un protocolo antiguo desarrollado para UNIX. Opera sin control de errores, de flujo o seguridad, pero consigue un buen rendimiento con bloques pequeños de datos.
- PPP (Point to Point Protocol): es un protocolo SLIP mejorado con control y recuperación de errores, este protocolo puede ser compartido por otros protocolos como IPX.
- PPTP (Point to Point Tunneling Protocol): no es un protocolo de TCP/IP, sino que fue incorporado por Windows NT, para trabajar en redes privadas multi-protocolos para permitir a los usuarios remotos acceder de manera segura a redes de empresas a través de la Internet, con las siguientes ventajas:

    - Costos de transmisión más bajos.
    - Menos inversión de hardware.
    - Mayor nivel de seguridad sobre redes publicas.

Los datos enviados en PPTP son encapsulados en paquetes PPP cifrados que se envían a través de Internet. Pero también puede ser usado para transportar trafico de acceso remoto IPX y NETBEUI.

Nivel de Iterred (Internet)

El nivel de Internet se superpone a la red física creando un servicio de Red Virtual independiente de aquella. No es fiable y no es orientada a conexión. Se encarga de direccionamiento y encaminamiento de los datos hasta la estación receptora.

En este nivel se encuentran 2 protocolos principales:

- ICMP (Internet Control Message Protocol): es un protocolo de mantenimiento / gestion de red que ayuda a supervisar la red. Se utiliza para encontrar la ruta optima de transmisión para los datagramas.

Su objetivo principal es proporcionar la información de error o control entre nodos, a través de mensajes generados por TCP/IP y no por el usuario, hay 4 tipos de mensajes

ICMP: Mensaje de destino no alcanzable, Mensaje de control de Congestión, Mensaje de redireccionamiento, Mensaje de tiempo excedido.

Una utilidad de diagnostico que usa este protocolo es la utilidad PING de UNIX para verificar si una computadora esta conectada a la red.

- IP (Internet Protocol): se encarga de seleccionar la trayectoria a seguir por los datagramas, pudiendo también realizar tareas de fragmentación y reensamblado.

No tiene un control de secuencia, recepción ni verificación de datagramas enviados a través de la red, esto se delega a protocolos de la capa transporte. Los datagramas IP contienen una cabecera con información para el nivel IP y los datos del usuario. Estos datagramas se encapsulan en tramas de longitud determinado por el tipo de red física a utilizar.

Al atravesar por diferentes redes la longitud de los paquetes puede variar, por lo que se establece un tamaño máximo permitido en cada red, denominado MTU (Maximun Transmisión Unit), si el paquete excede este tamaño, deberá ser fragmentado o reensamblado según la dirección de transmisión. El nivel de direccionamiento de TCP/IP se genera aquí, los procedimientos, tipos de direcciones y su resolución se analizaran posteriormente.

El protocolo de Interred (IP) proporciona envío de paquetes de la capa de transporte también llamados Unidades de datos del Protocolo de Transportes (TPDU) a través de una Internet, es un protocolo ruteado ya que es capaz de proveer la información y los medios para hacer que un mensaje o datagrama llegue a su destino final.

Fig. 2.3 TPDU-1

Si los TPDUs deben pasar por un ruteador o a través de un tipo de red, IP puede fragmentar TPDUs en partes mas pequeñas y reensamblarlas en un estación intermedia (usualmente un ruteador) o en el host destino. Cada TPDU o fragmento es adoptado con un encabezado IP y transmitido como un cuadro por los protocolos de la capa mas baja.

Varias rutas pueden estar disponibles entre en host fuente y el destino. IP basa su decisión de ruta en las tablas de ruteo. IP mueve datagramas un salto a la vez. Diferentes fragmentos de un TPDU pueden tomar diferentes rutas a lo largo de una internet. Esto puede causar que un fragmento llegue fuera de orden, en este caso IP reensambla los fragmentos en secuencia en el host destino.

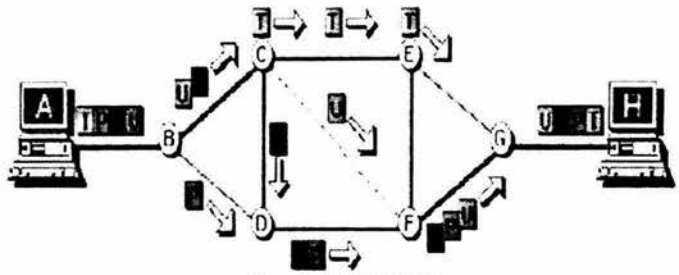

Fig. 2.4 TPDU-2

Nivel de Transporte

El nivel de transporte suministra a las aplicaciones servicios de comunicaciones desde la estación emisora hasta la receptora.

Fig. 2.5 Nivel de transporte

Utiliza 2 tipos de protocolos:

- TCP (Transmission Control Protocol): es un protocolo orientado a conexión que utiliza los servicios del nivel Internet, consta de 3 fases:

  - Establecimiento de la conexión y numero de secuencia inicial.
  - Transferencia de datos por segmento a los que agrega un encabezado con el numero de secuencia y un código de control, la fiabilidad se logra con la confirmación de recepción, y los temporizadores de espera de confirmación y la retransmisión de segmentos.
  - Liberación de la conexión en ambos sentidos.

TCP permite Múltiplexación, es decir, una conexión, puede ser utilizada por varios usuarios a la vez, para esto se definen puertos para cada aplicación o usuario, un puerto es una palabra de 16 bits que direcciona la aplicación destino de los datos.

Puerto origen	Puerto destino
Longitud	Checksum
Bytes de datos	
. . . . .	

Tabla 2.1

Puerto origen: indica el numero de puerto del proceso que envía los datos.

Puerto destino: numero de puerto al cual va dirigido el mensaje en la maquina destino.

Longitud: tamaño del encabezado y de los datos en bytes.

Checksum: verificación del datagrama UDP.

Hay aplicaciones que tienen puertos reservados pues actúan como servidores de servicios.

Un Socket es un par de números que identifica de manera única a cada aplicación. Cada Socket se compone de dos campos:

La dirección IP de la computadora en el que se esta ejecutando la aplicación.

El puerto a través del cual la aplicación se comunica con TCP/IP.

- UDP (User Datagram Protocol): es un protocolo que se basa en el intercambio de datagramas, orientado a no conexión, permite el envío de datagramas a través de la red sin antes haber establecido una conexión, ya que el propio datagrama contiene en su encabezado información suficiente de enrutamiento, por lo tanto es mucho mas rápido. Tiene el inconveniente de que no hay confirmación de recepción ni de secuencia correcta, dejando estas tareas a las terminales destino. Al igual que TCP utiliza puertos y sockets para identificar las aplicaciones destino y también permite la multiplexación.

Nivel de Aplicación

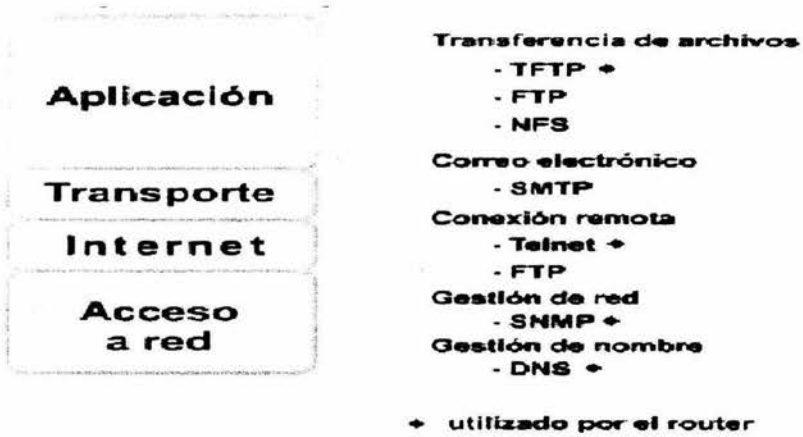

Fig. 2.6 Nivel de aplicación

- HTTP (Hyper Text Transport Protocol): es uno de los protocolos mas recientes. Se utiliza para manejar la consulta de hipertextos y el acceso a datos con WWW (World Wide Web) browser's. El trafico generado por este protocolo ha pasado, debido a la influencia de Internet, a ser muy grande.

- NFS (Network File System): desarrollado por Sun Mycrosystems Inc., permite a los usuarios el acceso en línea a archivos que se encuentran en sistemas remotos, como si fueran locales. La mayoría del trafico NFS es ahora un caso especial del protocolo RPC.

- NTP (Network Time Protocol): permite que todos los sistemas sincronicen su hora con un sistema designado como servidor horario.

- RPC (Remote Procedure Call): es una llamada a un procedimiento que se ejecuta en un sistema diferente (servidor) del que se realiza la llamada. Existen dos tipos de servidores:

    - Iterativo, un solo proceso a la vez.
    - Concurrente, varios procesos remotos a la vez.

- SMTP (Simple Mail Transfer Protocol): maneja el correo electrónico, especificando formato de mensajes, y su direccionamiento, así como servicios de notificación y administración de cuentas.

- SNMP (Simple Network Management Protocol): sirve para administrar los sistemas de forma remota, también se puede utilizar para supervisar el trafico de la red.

- TELNET: permite que un usuario, desde su terminal, o emulando una desde su PC, acceda a los recursos y aplicaciones de otras computadoras. Su sintaxis es:

  - telnet (nombre o dirección IP del host remoto)
  - telnet solaris
  - telnet 168.255.115.7
  - solicita username y password e indica la connexion con un prompt >

Una vez que la conexión queda establecida, actúa de intermediario entre ambas computadoras.

Se fundamenta en tres principios:

- El concepto de Terminal Virtual de Red (NVT), que define el formato de los datos intercambiados, códigos de control, y secuencia de comandos para permitir una comunicación entre sistemas heterogéneos.
- La simetría entre terminales y procesos.
- Permite que el cliente y el servidor negocien sus opciones.

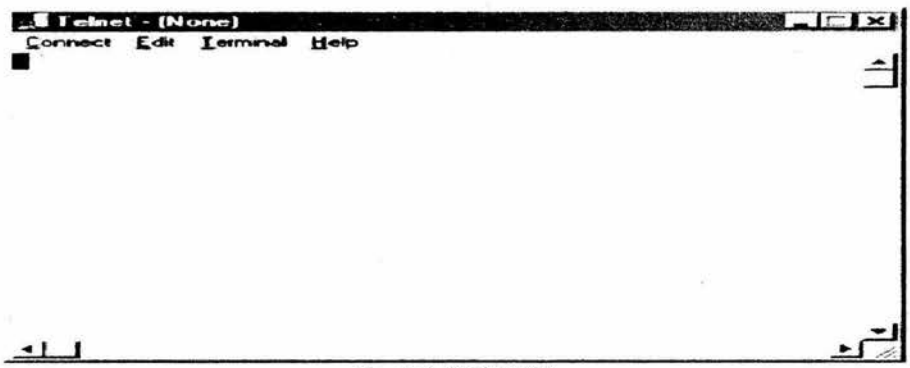

Fig. 2.7 TELNET

- TFTP (Trivial File Transfer Protocol): es un protocolo similar a FTP solo que en lugar de utilizar TCP utiliza UDP.

Envía los datos en paquetes con numero de secuencia y un paquete de manos de 512 bytes indicara fin de archivo.

La mayoría de los protocolos antes mencionados son utilizados con plataformas UNIX, sistema operativo siempre vinculado con TCP/IP.

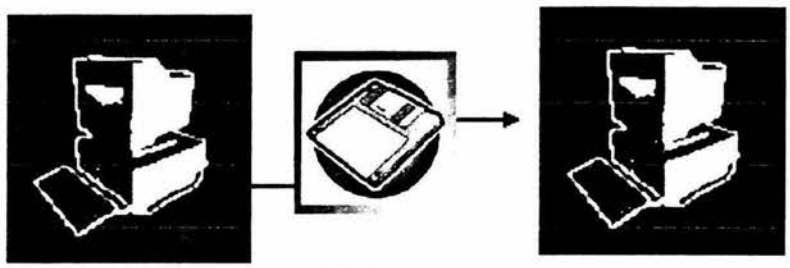

Fig. 2.8 FTP

2.5 MTU (Unidad Máxima de Transferencia)

El formato de encabezado de IP no especifica el formato del área de datos, lo que permite ser usado para transportar cualquier tipo de datos, y para determinar el tamaño del paquete, se hace referencia al MTU, la cual es diferente para cada arquitectura de red utilizada.

Características de la MTU

Las características más importantes de la MTU son:

- La mayoría de las arquitecturas de red manejan un tamaño de paquete máximo conocido como MTU.
- El protocolo IP considera el MTU cuando manda un paquete.
- Si el datagrama es mayor que el MTU, IP lo fragmentara y lo reensamblara en el punto destino.
- Si cualquier fragmento se pierde, el paquete entero es descartado.
- Los protocolos son libres de considerar el MTU en caso de ser necesario, por ejemplo TCP sabe cual es le MTU de la capa física y limita sus paquetes de acuerdo a esta medida.
- Es posible que los datagramas IP sean fragmentados en ruta. Esto sucede si la red intermedia tiene una MTU inferior que el origen.

2.6 Datagrama IP

El Protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico. IP es el protocolo de red que usa Internet. A medida que la información fluye por las distintas capas del modelo OSI, los datos se encapsulan en cada capa. En la capa de red, los datos se encapsulan en paquetes (también denominados datagramas). IP determina la forma del encabezado del paquete IP (que incluye información de direccionamiento y otra información de control) pero no se ocupa de los datos en sí (acepta cualquier información que recibe desde las capas superiores).

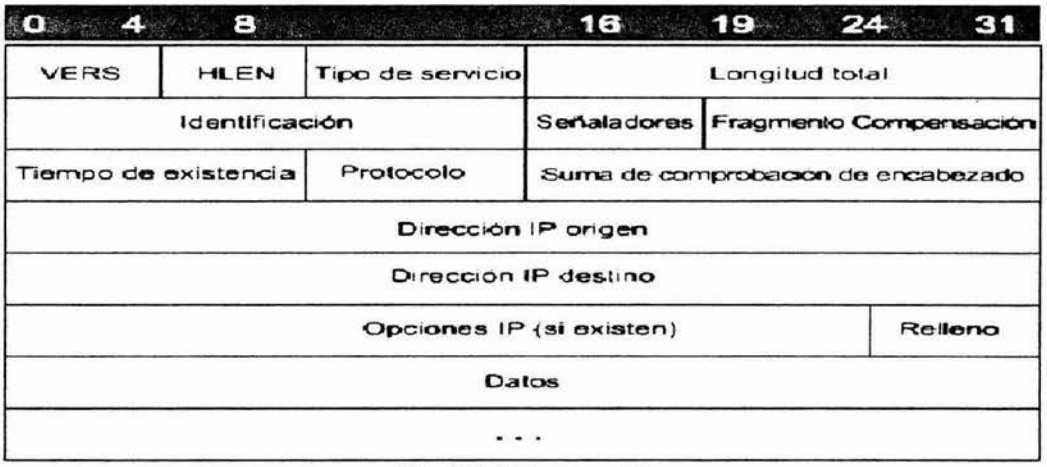

Fig. 2.9 Datagrama IP

Versión: Indica la versión del protocolo IP del datagrama.
HLEN: Longitud del encabezado de IP en múltiplos de 32 bits.
Tipo de servicio: Tipo de servicio que requiere al originador del datagrama.
Longitud total: Numero de bits en el paquete.
Identificación: Campo utilizado para reconocer un fragmento de un datagrama.
Señaladores: Indicadores que controlan si debe o no fragmentarse.
Compensación de fragmentos: ayuda a recuperar fragmentos del datagrama.
Tiempo de existencia: tiempo de vida. Contador que limita la vida de un paquete.
Protocolo: Especifica si el protocolo de la capa superior es TCP o UDP.
Suma de composición de encabezado: Verificador de la integridad del encabezado.
Dirección de origen: especifica el nodo emisor.
Dirección destino: especifica en nodo receptor.
Datos: contiene información de capa superior.
Relleno: se agregan 0's adicionales para asegurar 32 bits.

Los ruteadores también implementan el protocolo Internet para transportar y direccionar datagramas entre redes. Estos a su vez también usan protocolos Gateway a Gateway (GGP) entre ellos para coordinar el ruteo y otras informaciones Internet.

2.7 Direccionamiento IP

Direccionamiento

Antes de empezar debemos saber que la capa de red es responsable por el desplazamiento de datos a través de un conjunto de redes. Los dispositivos utilizan el esquema de direccionamiento de la capa de red para determinar el destino de los datos a medida que se desplazan a través de las redes.

Los protocolos que no tienen capa de red sólo se pueden usar en redes internas pequeñas. Estos protocolos normalmente sólo usan un nombre para identificar el computador en una red. El problema con este sistema es que, a medida que la red aumenta de tamaño, se torna cada vez más difícil organizar todos los nombres como, por ejemplo, asegurarse de que dos computadores no utilicen el mismo nombre.

Los protocolos que soportan la capa de red usan una técnica de identificación que garantiza que haya un identificador exclusivo. Las direcciones de capa de red utilizan un esquema de direccionamiento jerárquico que permite la existencia de direcciones exclusivas más allá de los límites de una red, junto con un método para encontrar una ruta por la cual la información viaje a través de las redes.

Los esquemas de direccionamiento jerárquico permiten que la información viaje por una internet-work, así como también un método para detectar el destino de modo eficiente.

La red telefónica es un ejemplo del uso del direccionamiento jerárquico. El sistema telefónico utiliza un código de área que designa un área geográfica como primera parte de la llamada (*salto*). Los tres dígitos siguientes representan el intercambio a la central local (segundo salto). Los últimos dígitos representan el número Telefónico destino individual que por supuesto, constituye el último salto.

Los dispositivos de red necesitan un esquema de direccionamiento que les permita envíar paquetes de datos a través de la internetwork (un conjunto de redes formado por múltiples segmentos que usan el mismo tipo de direccionamiento). Hay varios protocolos de capa de red con distintos esquemas de direccionamiento que permiten que los dispositivos envíen datos a través de una internet-work.

Hay dos razones principales por las que son necesarias las redes múltiples: el aumento de tamaño de cada red y el aumento de la cantidad de redes.

Cuando una LAN, MAN o WAN crece, es posible que sea necesario o aconsejable que el control de tráfico de red la divida en porciones más pequeñas denominadas segmentos de red (o simplemente segmentos). Esto da como resultado que la red se transforme en un grupo de redes, cada una de las cuales necesita una dirección individual.

En este momento existe un gran número de redes, las redes de computadores separadas son comunes en las oficinas, escuelas, empresas, negocios y países. Si bien resulta útil que las redes separadas (o sistemas autónomos, si cada una está controlada por un administrador de red) se comuniquen entre sí a través de Internet, deben hacerlo con sistemas de direccionamiento y dispositivos de internet-working apropiados. De no ser así, el flujo de tráfico de red se congestionaría seriamente y ni las redes locales ni Internet funcionarían.

Una analogía que puede ayudarlo a entender la necesidad de la segmentación de las redes es imaginar un sistema de autopistas y los vehículos que las utilizan. A medida que la población en las áreas cercanas a las autopistas aumenta, las carreteras quedan sobrecargadas de vehículos. Las redes operan en gran parte de la misma manera. A medida que las redes aumentan de tamaño, aumenta también la cantidad de tráfico. Una solución podría ser aumentar el ancho de banda, al igual que, en el caso de las autopistas, la solución puede ser aumentar los límites de velocidad o la cantidad de carriles. Otra solución puede ser utilizar dispositivos que segmenten la red y controlen el flujo de tráfico, así como una autopista puede usar dispositivos tales como semáforos para controlar el tráfico.

Direcciones IP

El Protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico. IP es el protocolo de red que usa Internet. A medida que la información fluye por las distintas capas del modelo OSI, los datos se encapsulan en cada capa. En la capa de red, los datos se encapsulan en paquetes (también denominados datagramas). IP determina la forma del encabezado del paquete IP (que incluye información de direccionamiento y otra información de control) pero no se ocupa de los datos en sí (acepta cualquier información que recibe desde las capas superiores).

El protocolo IP usa direcciones lógicas para identificar a las computadoras que están conectadas a una red. Así mismo, un ruteador en una red toma como base la dirección destino en un paquete de datos para decidir a que nodo debe transferirlo en la red. Mas específicamente, una dirección IP se asigna a la tarjeta NIC, que conecta a la computadora a la red, mas que a la computadora misma.

Las direcciones IP se expresan como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos (un octeto es un grupo de 8 bits). El valor decimal máximo de cada octeto es 255 (el número binario de 8 bits más alto es 11111111, y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total).

El número de red de una dirección IP identifica la red a la que se conecta un dispositivo, mientras que la parte de una dirección IP que corresponde al host identifica el dispositivo específico de esa red. Como las direcciones IP están formadas por cuatro octetos separados por puntos, se pueden utilizar uno, dos o tres de estos octetos para identificar el número de red. De modo similar, se pueden utilizar hasta tres de estos octetos para identificar la parte del host de una dirección IP.

Tipos de direcciones IP

Hay cinco clases de direcciones IP pero en realidad solo se usan tres clases de direcciones que una organización puede recibir de parte del Registro Estadounidense de Números de Internet (ARIN) o ISP de la organización: Clase A, B y C. En la actualidad, ARIN reserva las direcciones de Clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de Clase B para las medianas empresas. Se otorgan direcciones de Clase C para todos los demás solicitantes.

Hay cinco clases de direcciones IP, como se muestra en la siguiente tabla:

Clase	1er octeto								2° Octeto	3° Octeto	4° Octeto	Rango de direcciones de red	Numero de Host
A	**0**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**H**	**H**	**H**	**0 a 127**	**16,777,216**
B	**1**	**0**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**H**	**H**	**128 a 191**	**65,536**
C	**1**	**1**	**0**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**H**	**192 a 223**	**256**
D	**1**	**1**	**1**	**0**	**R**	**R**	**R**	**R**	**R**	**R**	**H**	**224 a 239**	Se emplea para multicast
E	**1**	**1**	**1**	**1**	**0**	**R**	**R**	**R**	**R**	**R**	**H**	**240 a 255**	Reservada para investigación

Nota: R: Numero asignado por el NIC H: Numero asignado por el Administrador

Tabla 2.2

Dirección Clase A

Las direcciones de clase A, tienen las siguientes características:

Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección de Clase A siempre es 0. Un ejemplo de una dirección IP de clase A es 124.95.44.15. El primer octeto, 124, identifica el número de red asignado por

ARIN. Los administradores internos de la red asignan los 24 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase A es verificar el primer octeto de su dirección IP, cuyo valor debe estar entre 0 y 126. (127 comienza con un bit 0, pero está reservado para fines especiales).

Todas las direcciones IP de Clase A utilizan solamente los primeros 8 bits para identificar la parte de la red de la dirección. Los tres octetos restantes se pueden utilizar para la parte del host de la dirección. A cada una de las redes que utilizan una dirección IP de Clase A se les pueden asignar hasta 2 elevado a la 24 potencia (2^{24}) (menos 2), o 16.777.214 direcciones IP posibles para los dispositivos que están conectados a la red.

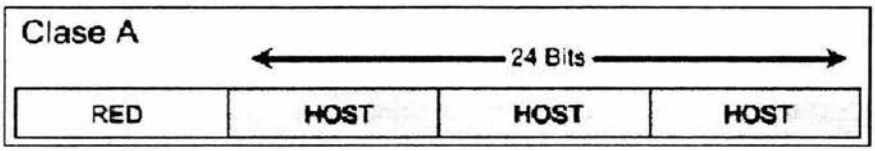

Fig. 2.10 Dirección clase A

Dirección Clase B

Las direcciones de clase B, tienen las siguientes características:

Los primeros 2 bits de una dirección de Clase B siempre son 10 (uno y cero). Un ejemplo de una dirección IP de Clase B es 151.10.13.28. Los dos primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 16 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase B es verificar el primer octeto de su dirección IP. Las direcciones IP de Clase B siempre tienen valores que van del 128 al 191 en su primer octeto.

Todas las direcciones IP de Clase B utilizan los primeros 16 bits para identificar la parte de la red de la dirección. Los dos octetos restantes de la dirección IP se encuentran reservados para la porción del host de la dirección. Cada red que usa un esquema de direccionamiento IP de Clase B puede tener asignadas hasta 2 a la 16ta potencia (2^{16}) (menos 2 otra vez), o 65.534 direcciones IP posibles a dispositivos conectados a su red.

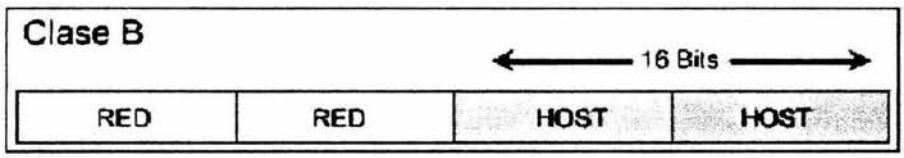

Fig. 2.11 Dirección clase B

Dirección Clase C

Las direcciones de clase C, tienen las siguientes características:

Los 3 primeros bits de una dirección de Clase C siempre son 110 (uno, uno y cero). Un ejemplo de dirección IP de Clase C es 201.110.213.28. Los tres primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 8 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase C es verificar el primer octeto de su dirección IP. Las direcciones IP de Clase C siempre tienen valores que van del 192 al 223 en su primer octeto.

Todas las direcciones IP de Clase C utilizan los primeros 24 bits para identificar la porción de red de la dirección. Sólo se puede utilizar el último octeto de una dirección IP de Clase C para la parte de la dirección que corresponde al host. A cada una de las redes que utilizan una dirección IP de Clase C se les pueden asignar hasta 2^8 (menos 2), o 254, direcciones IP posibles para los dispositivos que están conectados a la red.

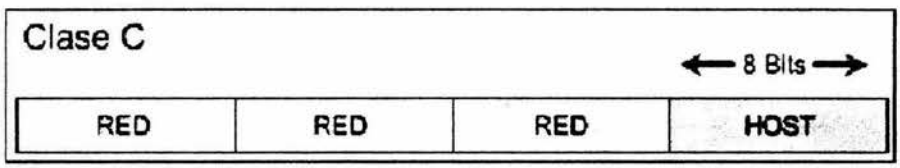

Fig. 2.12 Dirección clase C

Dirección Clase D

Las direcciones clase D se emplean para multicast, es decir, para que un conjunto de computadoras comparta una dirección, los cual permite que una copia de un mensaje con una dirección multicast se entregue a cada una de las computadoras que comparten esa dirección.

Dirección Clase E

Estas direcciones se reservan para la investigación.

Las direcciones IP identifican un dispositivo en una red, y la red a la cual se encuentra conectado. Para que sea fácil recordarlas, las direcciones IP generalmente están escritas en notación decimal punteada (4 números decimales separados por puntos, por ejemplo, 166.122.23.130; tenga en cuenta que un número decimal es un número de base 10, el tipo de número que usamos diariamente).

Cada clase de red permite una cantidad fija de hosts. En una red de Clase A, se asigna el primer octeto, reservando los tres últimos octetos (24 bits) para que sean asignados a los

hosts, de modo que la cantidad máxima de hosts es 2^{24} (menos 2: las direcciones reservadas de broadcast y de red), o 16.777.214 hosts.

En una red de Clase B, se asignan los dos primeros octetos, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} (menos 2), o 65.534 hosts.

En una red de Clase C, se asignan los tres primeros octetos, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^8 (menos 2), o 254 hosts.

Recuerde que la primera dirección en cada red está reservada para la dirección de red (o el número de red) en sí y la última dirección en cada red está reservada para los broadcasts.

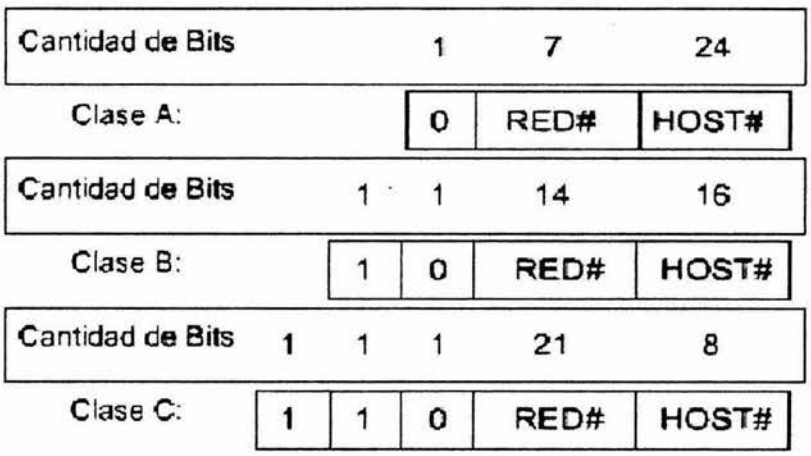

Fig. 2.13 Cantidad de bits en las direcciones

2.8 Subredes

Los administradores de redes a veces necesitan dividir las redes, especialmente las de gran tamaño, en redes más pequeñas denominadas subredes, para brindar mayor flexibilidad. Las subredes, son pequeñas redes en que se pueden dividir las redes IP.

La creación de subredes representa varias ventajas para el administrador de la red, entre ellas tenemos:

- Mayor flexibilidad
- Uso mas eficiente de las direcciones de red
- Capacidad de manejar trafico de difusión

De manera similar a lo que ocurre con la porción del número de host de las direcciones de Clase A, Clase B y Clase C, las direcciones de subred son asignadas localmente,

normalmente por el administrador de la red. Además, tal como ocurre con otras direcciones IP, cada dirección de subred es única.

Las direcciones de subred incluyen la porción de red de Clase A, Clase B o Clase C además de un campo de subred y un campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original para toda la red.

La capacidad de decidir cómo dividir la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad para el direccionamiento al administrador de red.

Para crear una dirección de subred, un administrador de red pide prestados bits de la parte original de host y los designa como campo de subred.

Los componentes de una subred son:

- Dirección de red o de Internet
- Dirección de la subred
- Dirección de host

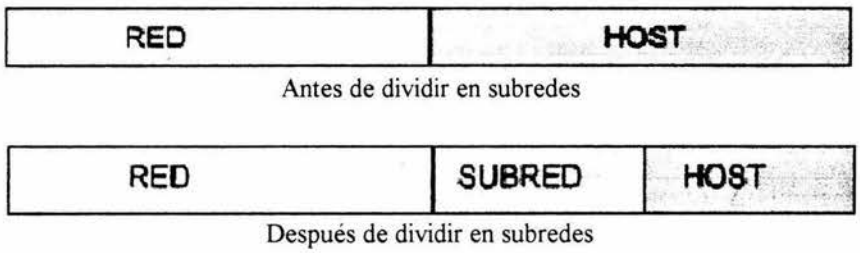

Fig. 2.14 División de la dirección IP

Con ello la dirección de red o Internet identifica a la red perteneciente a la empresa dentro del conjunto mundial de redes, la dirección de subred identifica una red LAN o WAN, y la dirección host identifica a un host dentro de la subred.

El incremento en el uso de redes de datos pequeñas provoco problemas que no fueron visualizados al aparecer TCP/IP. Se requiere de mucho trabajo administrativo para manejar las direcciones de red. Las tablas de ruteo de los ruteadores se hacen cada vez mas grandes, el espacio para las direcciones se acabara eventualmente.

La solución al problema fue, que dos o más redes pequeñas compartan una misma dirección IP.

- Por medio de la utilización de subredes
- Y utilización de las mascaras de subred

Sabemos que una dirección IP de 32 bits tiene una porción de red de redes y una porción local. La parte de red identifica una localidad o conexión, posiblemente con muchas redes físicas, la porción local identifica una red física y un anfitrión en dicha localidad.

Para permitir una máxima flexibilidad al particionar las direcciones de subred, el estándar TCP/IP de subred permite que la interpretación se escoja de forma independiente para cada red física.

Una vez seleccionada una partición de subred, todas las maquinas la debe utilizar. Además de que otras localidades en Internet puedan manejar las direcciones como el esquema original.

El direccionamiento de subred también permite asignaciones mas complejas tomando en cuenta la cantidad de subredes y el numero de anfitriones de cada uno de ellos, así como el crecimiento futuro de estas, para lograr esto se emplean las mascaras de subred de 32 bits para cada red.

La máscara de subred (término formal: prefijo de red extendida), le indica a los dispositivos de red cuál es la parte de una dirección que corresponde al campo de red y cuál es la parte que corresponde al campo de host. Una máscara de subred tiene una longitud de 32 bits y tiene 4 octetos, al igual que la dirección IP.

Los bits de la mascara de subred se indican como "1", si la red trata al bit correspondiente de la dirección IP como parte de la dirección de red, y como "0", si se trata al bit como parte de identificador del anfitrión.

Para determinar la máscara de subred para una dirección IP de subred particular, siga estos pasos:

1) Exprese la dirección IP de subred en forma binaria.
2) Cambie la porción de red y subred de la dirección por todos unos.
3) Cambie la porción del host de la dirección por todos ceros.
4) Como último paso, convierta la expresión en números binarios nuevamente a la notación decimal punteada.

Por defecto, si no se pide ningún bit prestado, la máscara de subred para una red de Clase B sería 255.255.0.0, que es el equivalente en notación decimal punteada de los 1s en los 16 bits que corresponden al número de red de Clase B.

Si se pidieran prestados 8 bits para el campo de subred, la máscara de subred incluiría 8 bits 1 adicionales y se transformaría en 255.255.255.0.

Fig. 2.15 Mascara

Siempre que se pidan prestados bits del campo del host, es importante tomar nota de la cantidad de subredes adicionales que se están creando cada vez que se pide prestado un bit. Usted ya ha aprendido que no se puede pedir prestado solamente 1 bit, la cantidad menor que se puede pedir prestada es 2 bits.

Al pedir prestados 2 bits, se crean cuatro subredes posibles (2^2) (pero siempre debe tener en cuenta que hay dos subredes no utilizables / reservadas). Por lo tanto se le debe de restar 2. Cada vez que se pide prestado otro bit del campo de host, la cantidad de subredes que se han creado aumenta por una potencia de 2.

Las ocho subredes posibles que se crean pidiendo prestados 3 bits es igual a 2^3 (2 x 2 x 2). Las dieciséis subredes posibles que se crean pidiendo prestados 4 bits es igual a 2^4 (2 x 2 x 2 x 2).

A partir de estos ejemplos, es fácil darse cuenta de que cada vez que se pide prestado otro bit del campo de host, la cantidad de subredes posibles se duplica.

Ahora veamos un ejemplo para entender esto mejor:

Supongamos que tiene una red de Clase B, con el número de red 172.16.0.0. Después de analizar las necesidades de la red, decide pedir prestados 8 bits para crear subredes. Como ha aprendido anteriormente, si pide prestados 8 bits en una red de Clase B, la máscara de subred es 255.255.255.0.

Alguien, desde fuera de la red, envía datos a la dirección IP 172.16.2.120. A fin de determinar dónde enviar los datos, el router realiza la operación AND con esta dirección y la máscara de subred. Cuando se ha realizado la operación AND de los dos números, la porción del host del resultado siempre es 0. Lo que resta es el número de red, incluyendo la subred. De este modo, los datos se envían a la subred 172.16.2.0 y solo el último router se da cuenta de que el paquete se debería haber enviado hacia el host 120 de esa subred.

	Red	Subred	Host
Dirección IP del host 172.16.2.120	10101100 00010000	00000010	01111000
Máscara de subred 255.255.255.0 /7:	11111111 11111111	11111111	00000000
Subred	10101100 00010000 172 16	00000010 2	00000000 0

Fig. 2.16 Ejemplo 1

Ahora, supongamos que tenemos la misma red, 172.16.0.0. Sin embargo, esta vez decide pedir prestados solamente 7 bits para el campo de subred. La máscara de subred en números binarios sería 11111111.11111111.11111110.00000000.

Nuevamente alguien, desde fuera de la red, envía datos hacia el host 172.16.2.120. Para determinar dónde se deben enviar los datos, el router realiza la operación AND de esta dirección y la máscara de subred. Como en el caso anterior, cuando se realiza la operación AND de los dos números, la porción del host del resultado es 0. Todo parece ser igual (al menos en la notación decimal).

La diferencia radica en la cantidad de subredes disponibles y en la cantidad de hosts que se pueden ubicar en cada subred, y que solamente lo puede ver si compara las dos máscaras de subred distintas.

Si hay 7 bits en el campo de subred, solamente puede haber 126 subredes. ¿Cuántos hosts puede haber en cada subred? ¿Qué longitud tiene el campo de host? Si hay 9 bits para los números de host, puede haber 510 hosts en cada una de esas 126 subredes. Lo sabemos porque (2x2x2x2x2x2x2)-2= 126 que es el numero de subredes y en binario 111111111 = 510, que es el numero de host.

	Red	Subred	Host
Dirección IP del host 172.16.2.120	10101100 00010000	00000010	01111000
Máscara de subred 255.255. .0 /7:	11111111 11111111		00000000
Subred	10101100 00010000 172 16	00000010	00000000 0

Fig. 2.17 Ejemplo 2

Si las mascaras no son definidas, el software IP toma las siguientes mascaras por default:

Tipo de red	Decimal	Binario
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Tabla 2.3 Mascaras por default

CAPITULO TERCERO INTERNET-WORKING

3.1 Infraestructura de Internet

Durante los últimos siglos, los gobiernos tuvieron una participación fundamental en la construcción y regulación de la infraestructura del transporte, de las comunicaciones y de la energía. En una palabra, la política impulsaba la tecnología. Aunque ese factor estimuló el pasaje de una sociedad agrícola a una industrial, en la actualidad esta obstaculizando la transición de la sociedad industrial a la informática. Hoy es el sector privado el que impulsa la tecnología, y los gobiernos cada vez tienen mas problemas para mantenerse actualizados con respecto a los últimos desarrollos y así crear las regulaciones del caso.

En las ultimas décadas, la privatización de muchas industrias, como la del transporte (aerolíneas y ferrocarriles), la de las comunicaciones (empresas de correo y telefónicas) y la de la energía (plantas eléctricas y estaciones de combustible), han promovido la separación entre la economía y la política.

En el caso de Internet, hay cuatro áreas tecnológicas que desempeñan un papel preponderante para la futura expansión de la red: las empresas tradicionales de telecomunicaciones, los proveedores de tecnología satelital, los de redes inalámbricas y las empresas de cable.

Las empresas tradicionales de telecomunicaciones se están transformando rápidamente: a partir de su origen como proveedoras de servicios simples, por ejemplo, la telefonía básica, se están convirtiendo en compañías tecnológicas que proveen soluciones para todo tipo de clientes. Están desarrollando nuevas tecnologías para comunicaciones de mayor ancho de banda a través de las redes existentes, gracias a desarrollos como el xDSL y centrales más veloces. Por otra parte, las empresas de software han desarrollado nuevas tecnologías de compresión que reducen la cantidad de datos que se envían a la red.

No solo se están mejorando las redes existentes, sino que se están instalando nuevos tipos de redes: las de fibra óptica, que utilizan amplificación óptica y centrales de fotones, son más poderosas y eficientes. No solo las empresas de telecomunicaciones están instalando este tipo de cableado: las compañías eléctricas están invirtiendo mucho dinero en la provisión de un backbone de fibra óptica para Internet.

Las compañías satelitales están construyendo nuevas redes de banda ancha con alcance global. Estas empresas en estrecha colaboración con las corporaciones electrónicas y aeroespaciales para poner los satélites en funcionamiento.

Mediante estas nuevas redes se podrá proveer conexión a las personas que viven en áreas en las que no se cuenta con servicio telefónico normal de cableado de cobre. Con

menores y mayor velocidad, estas redes posibilitaran el acceso a Internet a personas de bajos recursos.
En las ultimas décadas, la mayoría de los países industrializados invirtió grandes sumas en la construcción de redes de cable para televisión, que pueden tener otros usos: muchos proveedores de televisión por cable comenzaron a acondicionar sus redes para trafico de internet de dos vías, mediante la introducción de las llamadas set-top boxes que funcionan como conversores y separadores del trafico de entrada y salida para la transmisión conjunta de datos, voz y video.
Recientemente se han comenzado a modificar las redes inalámbricas para uso de internet. En poco tiempo, todos los hogares contaran con redes locales inalámbricas, mediante las que se podrían comunicar todos los dispositivos entre si utilizando protocolos de Internet específicos. Los nuevos estándares para la telefonía móvil aumentarán la velocidad de transferencia de datos; de hecho, ya existen teléfonos celulares que reciben y transmiten trafico de voz, datos y de internet.

3.2 Arquitectura de Internet

En realidad, Internet es una red de computadoras. No esta constituida por una sola red, sino por muchas redes separadas que se conectan únicamente en puntos muy específicos. Toda red que desee conectarse a Internet debe utilizar un conjunto de protocolos de comunicación denominados IP.

Las redes están constituidas por nodos y canales que proveen la infraestructura básica de comunicación. Existen dos tipos básicos de nodos: los terminales y los intermediarios. En la mayoría de los casos, los nodos terminales son los servidores y los clientes, que proveen o solicitan un conjunto de servicios. Generalmente, los clientes son computadoras que los usuarios utilizan para comunicarse con otros nodos, mientras que los servidores son proveedores de servicios centralizados que, entre otras cosas, ofrecen funciones de servidor web o de correo a los clientes.

Los nodos intermediarios suelen ser computadoras de funciones reducidas que reenvían trafico entre segmentos de red. Estos dispositivos, que se denominan routers o bridges, pueden utilizarse en algunas ocasiones para filtrar ciertas solicitudes o para restringir el acceso a ciertos tipos de una red. Sin embargo, ni los clientes ni los servidores pueden acceder a los servicios que ofrece un nodo intermediario.

No es necesario utilizar otros dispositivos como nodos terminales o intermediarios: los servidores también pueden funcionar como clientes o como routers en forma simultanea. Cada nodo cuenta con un identificador único llamado dirección IP. Los sistemas de mayor envergadura pueden llegar a tener varias direcciones IP, a las que se les suele asignar un nombre de dominio para que sean más fáciles de recordar.
Los canales necesarios para la comunicación entre nodos pueden implementarse de diferentes formas, en la mayoría de los casos se utiliza un sistema de cables que conecta dos terminales a través de los intermediarios. El cable utilizado puede ser coaxial , de

fibra de vidrio o el tradicional de cobre. Las velocidades de conexión varían de acuerdo al tipo de cable utilizado. No obstante, dado que se utilizan los mismos protocolos de transmisión, no es necesario volver a escribir las aplicaciones para los diferentes canales. Además de las conexiones físicas, es posible transmitir en forma inalámbrica. Estas transmisiones electromagnéticas se realizan en diferentes frecuencias: sistemas infrarrojos, links de microondas, telefonía celular y comunicación por link satelital.
En líneas generales, todos los nodos se comunican entre si a través de internet, dado que esto no siempre es deseable, algunos nodos intermediarios pueden denegar la conexión con ciertos nodos. Estos dispositivos, denominados firewalls, impiden que el publico acceda a las redes exclusivas de empresas. Debido a que las intranets utilizan el mismo conjunto de protocolos, cualquiera podría proteger datos de los gobiernos y todo tipo de información que se desee incluir en una red para el uso de un grupo en particular.

Internet ofrece, en casi todos los casos, mas de una forma de acceso para cada conexión entre dos nodos. Si se produce una falla en un nodo intermediario, la conexión puede redirigirse a través de otros segmentos de la red sin necesidad de interacción con el usuario: la red cuenta con la capacidad de reorganizarse a si misma.

Teniendo en cuenta que Internet aparentemente no pertenece a nadie, resulta sorprendente que todavía funcione a la perfección. Una de las razones para ello es que en la actualidad las redes ya no se conectan en forma directa entre si, sino que utilizan backbones. Estos sistemas son conexiones de alta velocidad que vinculan segmentos de red separados y que ofrecen conexiones a redes ajenas mediante puntos de intercambio o gateways. En realidad, se puede decir que los backbones de Internet son la verdadera autopista informática. Las redes locales son mas como ciudades, en las que las calles están mas congestionadas y son mas estrechas.

Los protocolos de internet se planifican y controlan en forma jerárquica. Aunque cualquiera puede contribuir al desarrollo de nuevas tecnologías y protocolos, solo unas pocas organizaciones tienen influencia sobre lo que se incluye en el grupo de protocolos de internet.

3.3 ¿Qué es Internet?

Internet es una red de computadoras que utiliza convenciones comunes a la hora de nombrar y direccionar sistemas. Es una colección de redes independientes interconectadas; no hay nadie que sea dueño o active Internet al completo.

Las computadoras que componen Internet trabajan en UNIX, el sistema operativo Macintosh, Windows 95 y muchos otros. Utilizando TCP/IP y los protocolos veremos dos servicios de red:

- Servicios de Internet a nivel de aplicación
- Servicios de Internet a nivel de red

Servicios de Internet a nivel de aplicación

Desde el punto de vista de un usuario, una red de redes TCP/IP aparece como un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación. Utilizamos el término interoperabilidad para referirnos a la habilidad que tienen diversos sistemas de computación para cooperar en la resolución de problemas computacionales. Los programas de aplicación de Internet muestran un alto grado de interoperabilidad. La mayoría de usuarios que accesan a Internet lo hacen al correr programas de aplicación sin entender la tecnología TCP/IP, la estructura de la red de redes subyacente o incluso sin entender el camino que siguen los datos hacia su destino. Sólo los programadores que crean los programas de aplicación de red necesitan ver a la red de redes como una red, así como entender parte de la tecnología. Los servicios de aplicación de Internet más populares y difundidos incluyen:

- Correo electrónico. El correo electrónico permite que un usuario componga memorandos y los envíe a individuos o grupos. Otra parte de la aplicación de correo permite que un usuario lea los memorandos que ha recibido. El correo electrónico ha sido tan exitoso que muchos usuarios de Internet depende de él para su correspondencia normal de negocios. Aunque existen muchos sistemas de correo electrónico, al utilizar TCP/IP se logra que la entrega sea más confiable debido a que no se basan en compradoras intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su máquina local, se habrá recibido de manera exitosa en el sitio de destino.

- Transferencia de archivos. Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado principalmente para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, el cual permite que lo usuarios envíen o reciban archivos arbitrariamente grandes de programas o de datos. Por ejemplo, al utilizar el programa de transferencia de archivos, se puede copiar de una máquina a otra una gran base de datos que contenga imágenes de satélite, un programa escrito en Pascal o C++, o un diccionario del idioma inglés. El sistema proporciona una manera de verificar que los usuarios cuenten con autorización o, incluso, de impedir el acceso. Como el correo, la transferencia de archivos a través de una red de redes TCP/IP es confiable debido a que las dos máquinas comprendidas se comunican de manera directa, sin tener que confiar en máquinas intermedias para hacer copias del archivo a lo largo del camino.

- Acceso remoto. El acceso remoto permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva. El acceso remoto hace aparecer una ventana en la pantalla del

usuario, la cual se conecta directamente con la máquina remota al enviar cada golpe de tecla desde el teclado del usuario a una máquina remota y muestra en la ventana del usuario cada caractér que la computadora remota lo genere. Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

Servicios de Internet a nivel de red

Un programador que crea programas de aplicación que utilizan protocolos TCP/IP tiene una visión totalmente diferente de una red de redes, con respecto a la visión que tiene un usuario que únicamente ejecuta aplicaciones como el correo electrónico. En el nivel de red, una red de redes proporciona dos grandes tipos de servicios que todos los programas de aplicación utilizan. Aunque no es importante en este momento entender los detalles de estos servicios, no se deben omitir del panorama general del TCP/IP:

- Servicio sin conexión de entrega de paquetes. La entrega sin conexión es una abstracción del servicio que la mayoría de las redes de conmutación de paquetes ofrece. Simplemente significa que una red de redes TCP/IP rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden. Como por lo general se introduce directamente en el hardware subyacente, el servicio sin conexión es muy eficiente.

- Servicio de transporte de flujo confiable. La mayor parte de las aplicaciones necesitan mucho más que sólo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una "conexión" con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si fuera permanente y directa del hardware.

  Muchas redes proporcionan servicios básicos similares a los servicios TCP/IP, pero existen unas características principales que los distingue de los otros servicios:

- Independencia de la tecnología de red. Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos

TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular.

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

- Acuses de recibo punto-a-punto. Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aún cuando las dos máquinas no estén conectadas a la misma red física.
-
- Estándares de protocolo de aplicación. Además de los servicios básicos de nivel de transporte (como las conexiones de flujo confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto. Por lo tanto, cuando se diseñan programas de aplicación que utilizan el TCP/IP, los programadores a menudo se encuentran con que el software ya existente proporciona los servicios de comunicación que necesitan.

3.4 Internet-Working

Actualmente existen varias arquitecturas de red que aunque son compatibles en cierta forma con el modelo OSI no especifican el mismo tipo de capas y los protocolos que utilizan son diferentes. A este tipo de arquitectura se les llama propietarias debido a que están diseñadas tomando en cuenta sólo los productos de un fabricante y no son compatibles con los de otros. Las arquitecturas de red propietarias más conocidas son:

- SNA (System Network Architecture) de IBM

- XNS (Xerox Network System)

- DNA (Digital Network Architecture) o también conocido como DECNET de Digital Equipment Corporation

Y existe una gran cantidad de estas redes, así como LAN's que no están basadas en el modelo OSI. Para poder interconectar redes y hacerlas ínter operables se han desarrollado diferentes tipos de dispositivos que cumplen funciones especificas y cuya complejidad dependerá fundamentalmente de que tan parecidas sean las redes por conectar, en términos de estructura de datos de tramas, paquetes, mensajes y protocolos (grado de compatibilidad).

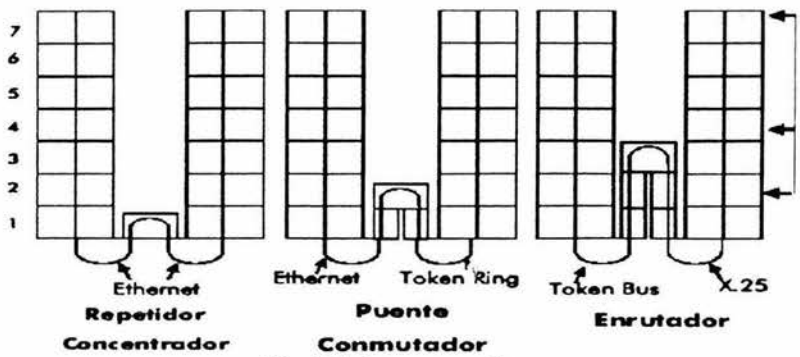

Fig. 3.1 Internetworking

El Internet-Working puede ser citada como una metodología que permite estructurar una red de forma coherente distribuyendo o centralizando la información de la forma mas adecuada, independientemente de su localización geográfica; también puede proporcionar anchos de banda dedicados e interconectar segmentos de diferente tecnología.

Los dispositivos de Internet-Working permiten a las LAN seguir extendiéndose por encima de las distancias máximas y se pueden usar para dividir grandes LAN en varias más pequeñas para aumentar las prestaciones globales del sistema. Hay varias maneras diferentes de lograr interconexiones LAN a LAN. Para entender totalmente los diversos métodos de interconexión, es importante entender las diferentes capas del modelo OSI (Interconexión de Sistemas Abiertos - Open Systems Interconnect):

Las comunicaciones de datos en una LAN pueden ser examinadas usando el modelo OSI. La comunicación de datos consiste en paquetes de información. Cada paquete puede contener información para cada sección del modelo OSI.

Las diferentes secciones se muestran a continuación. Los niveles bajos, del 1 a 3, se usa principalmente para comunicaciones de datos en la LAN. Los niveles superiores, se usan internamente para conexiones del host a la LAN y no contribuyen directamente a la comunicación de la LAN.

Capa física

La capa física describe el método de transmisión de datos al nivel físico ("cableado") del medio de transmisión.

Capa de enlace de datos

La capa de enlace de datos describe el método de empaquetar datos en unidades llamadas tramas o paquetes y enviar estas tramas de una interfaz en la LAN a otra interfaz en la misma LAN. Dentro de cada LAN la capa de enlace de datos se emplea para la transmisión de los datos.

Capa de red

La capa de red describe el método de transferir tramas entre dispositivos en redes diferentes. Usando la capa de red es posible separar una LAN en redes distintas.
La capa de red a veces se denomina "sin conexión" porque cada trama se encamina independientemente, sin que el protocolo de la capa de red proporcione ninguna garantía de la transmisión de los datos. La capa de red se limita a enviar la trama a la siguiente red en la ruta hacia la red de destino.

Capa de transporte

La capa de transporte describe el método de proporcionar transferencias fiables de datos entre los dispositivos LAN. La capa de transporte es usada principalmente para la transmisión de tramas entre los protocolos de las capas superiores entre dispositivos diferentes en la red. La capa de red se usa para conseguir que los datos lleguen a la red destino apropiada y la capa de transporte para asegurar la entrega garantizada de los datos.

Protocolos de LAN más frecuentes

Los protocolos usados para comunicación entre ordenadores pueden ser muy diversos. Uno de los protocolos más comunes es el denominado Protocolo de Internet (IP o Internet Protocol). Otros dos ejemplos de protocolos de red son IPX y DECNET. Estos protocolos funcionan dentro de la capa 3 del modelo OSI.
Como se puede ver en el diagrama siguiente, un protocolo de red en la capa 3 puede existir tanto en una LAN Ethernet como en una LAN Token Ring. Las capas 1 y 2 se ocupan de la toma de comunicación física para cada tipo de LAN. Es factible por tanto generar una trama IP en una LAN Ethernet y enviarla a través de la red para llegar a un ordenador en una LAN Token Ring. Esta comunicación entre plataformas cruzadas es posible debido a que la capa de red es la misma en ambas LAN.

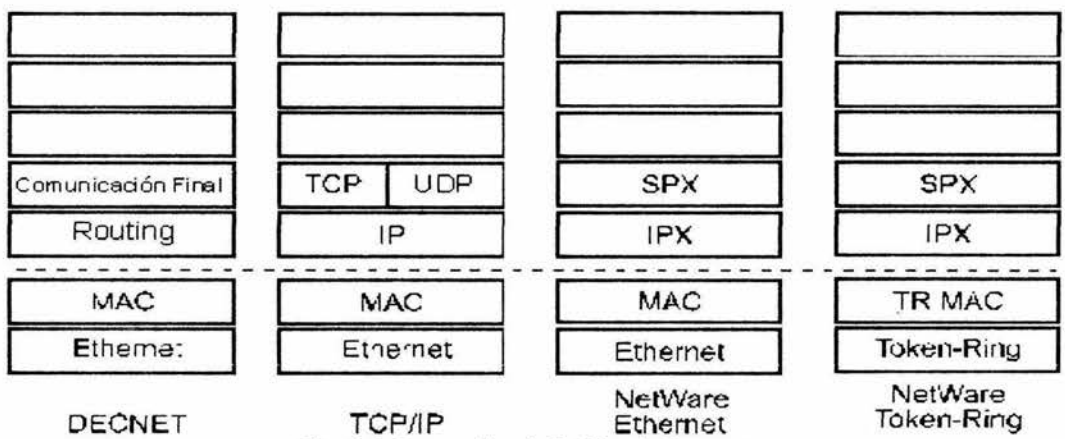

Fig. 3.2 Protocolos de LAN más frecuentes

3.5 Unidades en Internet-Working

El Internet-Working se realiza mediante las Internet-Working Units (IWU) que engloban una amplia gama de dispositivos entre los que se cuentan:

- Repetidores / Concentradores (Repeaters / Ruteadors): operan en el nivel 1 del modelo OSI. Su función básica es la de incrementar el tamaño físico de la red, regenerando las señales para superar los efectos de la atenuación e interferencias del medio de transmisión y así aumentar la distancia entre nodos. En el caso de los Hubs además, permite la centralización de las topologías de red, actuando como puntos de dispersión a centros de alambrado, cuentan con una inteligencia de enrutamiento.

- Puentes: operan en el nivel 2 del modelo OSI ejecutando funciones de Relay en el nivel MAC para conectar redes homogéneas. Su modo de funcionamiento es similar al de un filtro de direcciones, capturando las tramas que tienen como destino otro segmento y dejando pasar el resto. Son rápidos, transparentes e independientes de los niveles superiores de protocolo permitiendo el diseño flexible de redes.

- Conmutadores (Switch): operan en el nivel 2 del modelo OSI y proporcionan la posibilidad de interconectar diferentes segmentos de una LAN. Por operar en el mismo nivel, comparten con los puentes algunas características como velocidad, transparencia, etc.

- Ruteadores (Ruteadors): operan en el nivel 3 del modelo OSI, lo que significa que implementan protocolos de red como TCP/IP, Appletalk; que los convierte en dispositivos mas específicos que los puentes. Son sofisticados y han de ser direccionados explícitamente. Se suelen utilizar para conformar Backbones de LAN conectados a través de una WAN o entornos LAN de cierta complejidad (Switched LAN).

- Ruteador – Puente: implementan funciones de puente y de ruteador combinando las posibilidades de ambos dispositivos. Funcionan como puente con unos protocolos y como un ruteador con otros. Es una buena solución cuando en la red existen protocolos no enrutables.

- Compuerta o pasarela (Gateway): soportan los niveles superiores de comunicación para permitir la interconexión de redes con arquitecturas diferentes. Son totalmente específicos de los recursos que interconectan, llegando a soportar varios esquemas de direccionamiento. Se utilizan por ejemplo para permitir el trafico entre una red privada SNA y la Red Global Internet.

3.6 Funcionamiento

Desde el punto de vista del análisis de Internetworking los elementos mas interesantes, podrían ser los puentes, los ruteadores y las compuertas, pues involucran el uso de protocolos de capa, esto es, la lógica que actualmente nos permite tener redes interfuncionando entre si de manera transparente y he aquí lo interesante... ¿cómo lo hacen?

- **Repetidor (Repeater):** simplemente reexpido bits de una red hacia otra, haciendo que los dos se vean lógicamente como una sola red, es decir, se encarga de recibir, amplificar y retransmitir señales en ambas direcciones.

  A menudo las redes se dividen en dos o mas segmentos, como consecuencia de las restricciones de máxima longitud del cable de cada segmento individual, los repetidores son poco inteligentes. Los repetidores se pueden usar para conectar segmentos LAN y crear una LAN física más grande.

  Un repetidor opera en la capa física de una LAN y se limita a aceptar bits de datos en un lado y retransmitirlos al otro lado. Con este proceso, se permite a las señales originales recorrer una distancia más larga. En la especificación Ethernet, un solo segmento esta limitado a 500 metros. Usando repetidores, Ethernet puede extenderse hasta 1.500 metros (usando un máximo de dos repetidores según Ethernet Versión 1), o 2.800 metros (usando un máximo de cuatro repetidores, según la Versión 2/IEEE 802.3).

  Es importante observar que los segmentos conectados al repetidor constituyen una LAN física y todo el tráfico está presente en cada segmento.

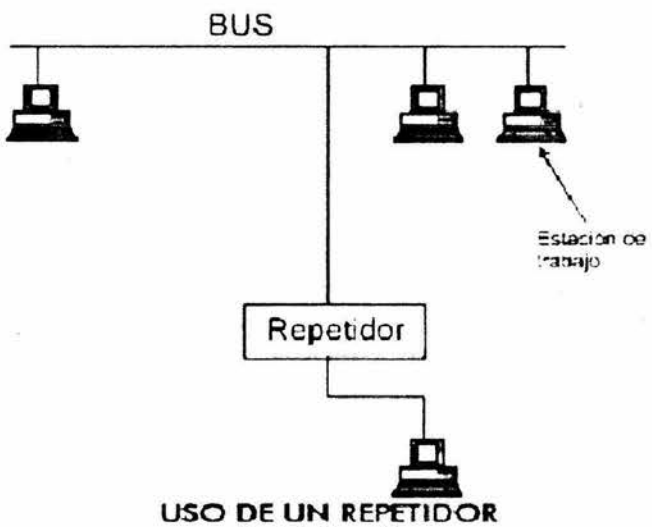

Fig. 3.3 Repetidor

- **Concentrador (Hub):** la aparición de los Hubs significa el primer paso hacia la unificación topológica de las redes Token Ring y Ethernet. Los hubs configuran redes en estrella mediante conexiones alámbricas punto a punto desde la estación al hub sin que la red deje de ser lógica y eléctricamente un bus, un anillo o un árbol. La ventaja de una topología centralizada en estrella es admitida por todos, ya que es mas confiable y manejable ante rupturas y permite el uso de funciones centralizadas de control. A través de la integración de SW (inteligencia) ha adquirido nuevas funcionalidades como: detección de colisiones, cierre lógico de anillo e incluso funciones de puente y ruteador. Tal inteligencia facilita también la segmentación de redes LAN heterogéneas a través de sus puertos.

  El propósito de un hub es regenerar y retemporizar las señales de red. Esto se realiza a nivel de los bits para un gran número de hosts (utilizando un proceso denominado concentración. Podrá observar que esta definición es muy similar a la del repetidor, es por ello que el hub también se denomina repetidor multipuerto. La diferencia es la cantidad de cables que se conectan al dispositivo.

  Las razones por las que se usan los hubs son crear un punto de conexión central para los medios de cableado y aumentar la confiabilidad de la red. La confiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. Esta es la diferencia con la topología de bus, en la que si un cable falla, esto causa una interrupción en toda la red. Los hubs se consideran dispositivos de la Capa 1 dado que sólo regeneran la señal y la envían por medio de un broadcast de ella a todos los puertos (conexiones de red).

  En networking, hay distintas clasificaciones de los hubs. La primera clasificación corresponde a los hubs activos o pasivos. La mayoría de los hubs modernos son activos; toman energía desde un suministro de alimentación para regenerar las señales de red. Algunos hubs se denominan dispositivos pasivos dado que simplemente dividen la señal entre múltiples usuarios, lo que es similar a utilizar un cable "Y" en un reproductor de CD para usar más de un conjunto de auriculares. Los hubs pasivos no regeneran los bits, de modo que no extienden la longitud del cable, sino que simplemente permiten que uno o más hosts se conecten al mismo segmento de cable.

  Otra clasificación de los hubs corresponde a hubs inteligentes y hubs no inteligentes. Los hubs inteligentes tienen puertos de consola, lo que significa que se pueden programar para administrar el tráfico de red. Los hubs no inteligentes simplemente toman una señal de networking entrante y la repiten hacia cada uno de los puertos sin la capacidad de realizar ninguna administración.

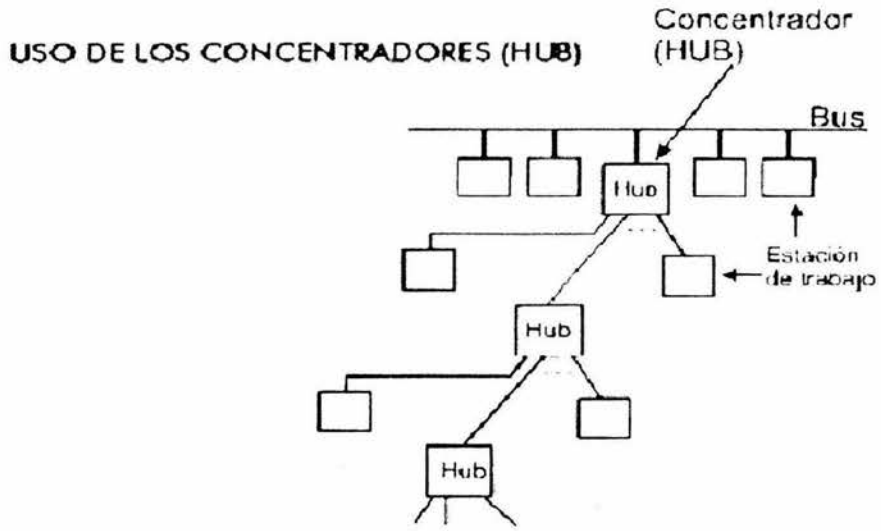

Fig. 3.4 Concentrador

- **Puente (Bridg):** los puentes permiten extender de forma transparente los limites de los segmentos de una LAN si importar los protocolos de niveles superiores de las redes. Los puentes se emplean para conectar segmentos LAN, para crear una LAN lógica más grande. Un puente opera en la capa de enlace de datos de una LAN e inteligentemente acepta bits de datos en un lado y selectivamente los retransmite al otro lado. En el proceso, un puente aísla tráfico local LAN en cada segmento y sólo deja pasar tráfico dirigido a un dispositivo situado en el siguiente segmento LAN. Esto evita que los mismos datos LAN sean transmitidos innecesariamente por la LAN completa y mejora sus prestaciones globales.

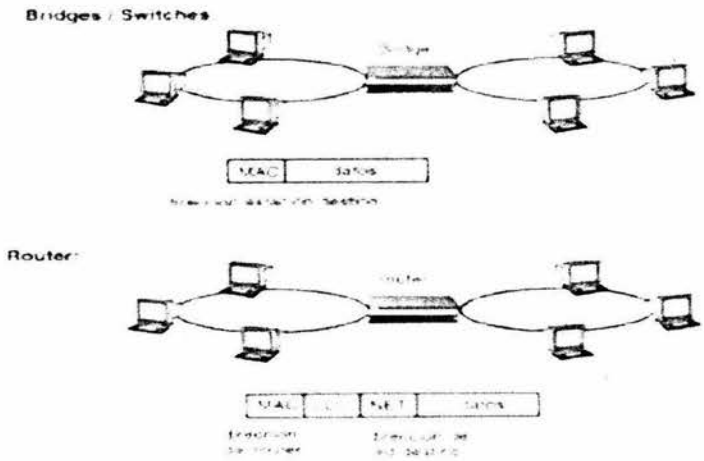

Fig. 3.5 Puente (1)

En la mayoría de los casos, la opción entre usar un puente o un encaminador es simple. Generalmente, si dos LAN simplemente van a ser conectadas como una

continuación de la red LAN actual, se debe usar un Puente para unir los dos segmentos. Si se trata de unir dos LAN distintas y predefinidas, debe usarse un Router para mantener la singularidad de cada LAN.

Existen versiones con capacidad de unir segmentos geográficamente distantes utilizando puentes remotos, que permiten una extensión de las LAN sin necesidad de modificar el software instalado. Podemos diferenciar varios tipos:

- Transparent Bridging
- Spanning Tree Algorithm
- Source Routing Bridging
- Source Routing Transparent Bridging
- Translational Puentes

- Transparent Bridging (TB)

Conectan dos o mas segmentos de LAN utilizando las direcciones MAC de 48 bits. La decisión de reenviar una trama de acuerdo a unas tablas topológicas que indican el segmento donde se encuentra cada estación. Estas tablas son auto-construidas por los puentes monitorizando los enlaces.

Cuando leen una dirección fuente que no tienen registrada, crean una nueva entrada en la tabla indicando el segmento donde ha sido leída. Las direcciones destino son buscadas en la tabla; si se encuentran en el mismo enlace donde fueron leídas, dejan pasar la trama, la encuentran y es reenviada al enlace perteneciente al otro segmento.

Una característica básica de los puentes TB es que evitan la necesidad de que los nodos de la red tengan conocimiento de la topología, resultando su existencia "transparente" a las estaciones de trabajo.

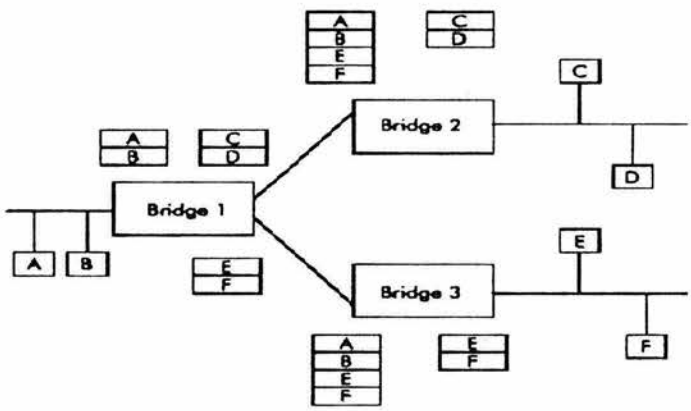

Fig. 3.6 Puente (2)

- Spanning Tree Algorithm (STA)

La tecnología Ethernet funciona muy bien con topologías en bus o árbol pero no tolera redes con bucles (loops) que provocan conflictos de rutas, para evitar este problema los puentes intercombinan entre si BPDU (Puente Protocol Data Units) que contienen la información acerca de la topología de la red, siendo "spanning tree" un algoritmo que describe los mecanismos para detectar bucles y elegir, mediante ponderaciones por cada puente y por cada enlace, de entre todas las vías posibles, un enlace primario que no contenga bucles, por el que se realizara el "bridging".

El algoritmo STA se ejecuta permanentemente, por lo que es posible detectar caídas de enlaces o de puentes, de forma que es posible rediseñar el árbol utilizando los enlaces no primarios que quedan como respaldos. Las redes Ethernet que funcionan sobre una topología STA, se pueden configurar como tolerantes a fallas. En redes internas medias y grandes, cuando se usan puentes adicionales para conectar un número creciente de segmentos de LAN, es muy probable que se creen múltiples caminos entre los segmentos LAN interconectados. La creación de caminos múltiples causa "bucles activos" qué resultan en una rápida degradación de la actuación de la red global, porque múltiples puentes estarán transmitiendo el mismo tráfico entre los segmentos de LAN interconectados.

El Spanning Tree Protocol fue creado para superar automáticamente el problema de caminos múltiples entre los segmentos. Con todos los puentes en la red ejecutando STP, los puentes adicionales que esten creando un camino redundante, negociarán y sólo uno de ellos se usará para transferir el tráfico. Si el puente activo falla, un puente ocioso se apercibirá y empezará a transferir el tráfico en su lugar. Obsérvese que, de este modo, se puede emplear un puente redundante para proteger segmentos de la red críticos. Cuando existe más de un camino de puente entre los segmentos LAN, el STP definirá un puente activo y el resto se pondrá en modo ocioso. El puente activo continúa enviando mensajes STP a la red de puentes STP para indicar que todavía está vivo. Si el puente activo falla, el STP reconfigurará la red automáticamente y activará un puente redundante previamente ocioso para asegurar que los datos continúan fluyendo.

- Source Routing Bridging (SRB)

Es una tecnología diseñada por IBM para las redes Token Ring. A diferencia de los TB, aquí las estaciones son las que conocen que ruta seguirán las tramas para llegar a su destino mientras que los puentes se limitan a consultar la cabecera de la trama para saber si deben o no pasar la trama al anillo adyacente. La información de ruta, contenida en el campo de información de enrutamiento (RIF) consiste en una secuencia de identificadores de anillos y puentes que la trama debe seguir.

El conocimiento de la topología por parte de las estaciones requiere un periodo de aprendizaje por parte de las mismas. Para hacer esto, el algoritmo SRB realiza dos búsquedas:

- Búsqueda de la estación destino dentro del propio segmento: lanza una trama TEST o XID con identificador Non-Broadcast.

- Búsqueda de la estación destino fuera del propio segmento: se lanza una trama TEST o XID pero con los bits Broadcast activados, para hacer una difusión a todos los ruteadores o bien una difusión a un solo ruteador.

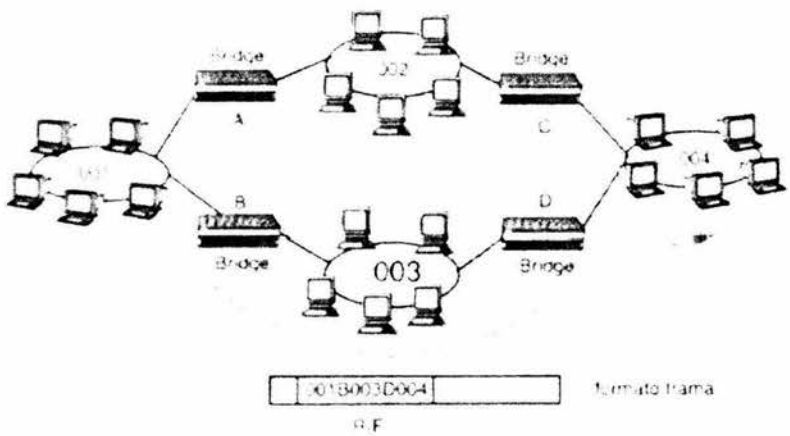

Fig. 3.7 Puente (3)

- Source Routing Transparent Bridging (SRTB)

Es similar al SRB con la diferencia de que si un Puente de estas características recibe un Frame sin información de Ruteo, se le aplica el mecanismo de los TB para reenviar el Frame necesario. Es un estándar utilizado en redes Ethernet, Token Ring y FDDI.

- Translational Puentes

Se utilizan para interconectar redes locales de diferentes tipos, como una Token Ring conectada a una Ethernet. El método mas utilizado para este tipo de interconexiones es el mismo empleo de ruteadores, pero existen situaciones donde un puente puede aportar mas ventajas que un ruteador. El trabajo fundamental es el de realizar la conversión de formato de tramas a nivel MAC.

El puente traductor puede y debe realizar las siguientes funciones:

- Conversión de formatos de tramas

- Manejar diferentes velocidades de red:

  - 10 Mbps
  - 4 o 16 Mbps

- Procesar diferentes longitudes de paquetes de datos:

  - 802.3 1518 bytes
  - 802.4 8191 bytes
  - sin limite, usualmente 5000 bytes

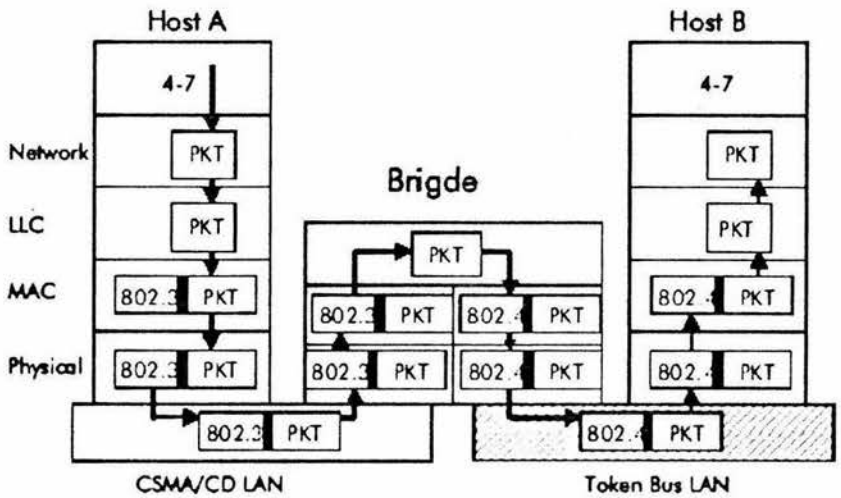

Fig. 3.8 Puente (4)

- **Conmutadores (Switchs):** los conmutadores son dispositivos de reciente aparición y que amplían la gama de posibilidades existentes para interconectar LAN's. Por sus características son mas asimilables a un puente que a un ruteador ya que operan el en nivel 2 y son trasparentes a los protocolos que transportan.

  Existen diversos tipos de conmutadores dependiendo del tipo de red que soportan, así, existen conmutadores para tramas TR, Ethernet, FDDI y aun mas, ya que son capaces de procesar también celdas ATM por lo que a menudo también realizan funciones de backbone soportando los diferentes segmentos de LAN existentes.

  Como principal ventaja que presenta su instalación, es que protegen la base instalada, pues la mayor parte de la NIC ya instaladas pueden seguir siendo usadas, hacen mas eficiente la asignación de ancho de banda a cada usuario haciendo mas eficientes las redes que pasan de ser redes LAN compartidas o

ruteadas a ser redes LAN conmutadas, y la lógica requerida para esto permite también la generación lógica de grupos de trabajo en redes virtuales (VLAN).

Un switch, al igual que un puente, es un dispositivo de la capa 2. De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión, dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red). La diferencia entre un hub y un switch está dada por lo que sucede dentro del dispositivo.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total (la velocidad de transmisión de datos en el backbone de la red).

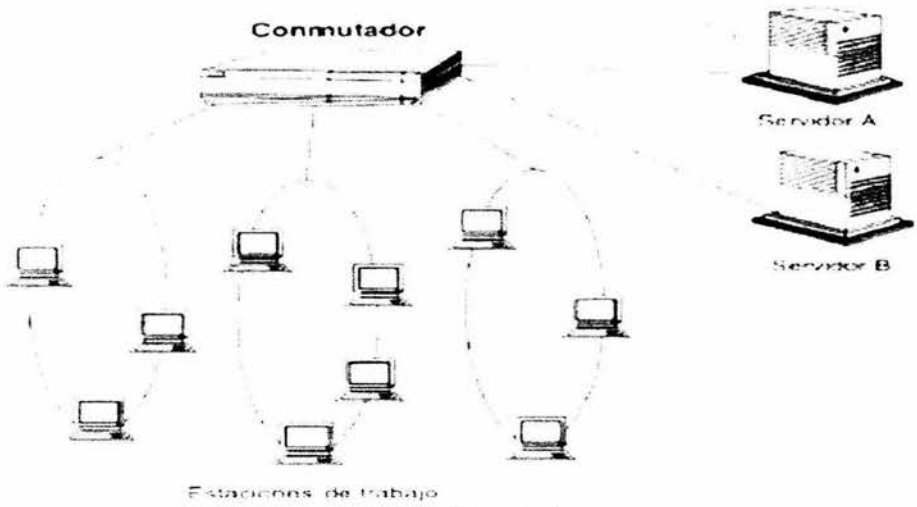

Fig. 3.9 Conmutador

- **Ruteador (Router):** estos dispositivos tienen como función principal el encaminar paquetes de información hasta una estación destino utilizando el nivel

de red (3) del modelo OSI. Los ruteadores deben de conocer la dirección de los mismos para poder acceder a nodos remotos. Esta es una característica que los diferencia de los puentes, cuyas estaciones conectadas no necesitan conocer las direcciones de los mismos, lo único importante es la dirección de la estación remota con la que quieren hablar.

Los ruteadores proporcionan servicios mas sofisticados que los puentes: pueden seleccionar una ruta basándose en parámetros tales como la latencia de los enlaces, el estado de congestión en la red, la distancia entre nodos, etc., de modo que pueden aplicar diferentes políticas según los requerimientos específicos de cada aplicación permitiendo unas topologías mas complejas y descentralizadas ya que pueden manejar diversos esquemas de direccionamiento, diferentes velocidades y tamaños de trama. No obstante todos ejecutan funciones similares:

- Eligen el camino más adecuado. Mantienen tablas internas que proporcionan información de los enlaces de la red, estas tablas son fundamentales, pues en ellas basan la decisión para realizar el enrutamiento.
- Disponen de mecanismos para el control de flujo. La congestión es algo común cuando las redes de diferente velocidad están interconectadas, pues la más rápida excede la capacidad de la mas lenta. Cuando esto ocurre y es detectado, el ruteador envía una señal a la estación fuente, indicando congestión e invitándole a reducir la velocidad de transmisión.
- Unen redes heterogéneas. Los ruteadores pueden conectar redes de diferente nivel MAC (Token Ring, Ethernet,...), su tarea es la de mapear las direcciones del protocolo de comunicaciones (por ejemplo, IPX) en las direcciones destino de la red utilizada (por ejemplo, Frame Relay), siendo esta una de las razones que dificultan las funciones multicasting pues las WAN suelen estar orientadas a conexión.

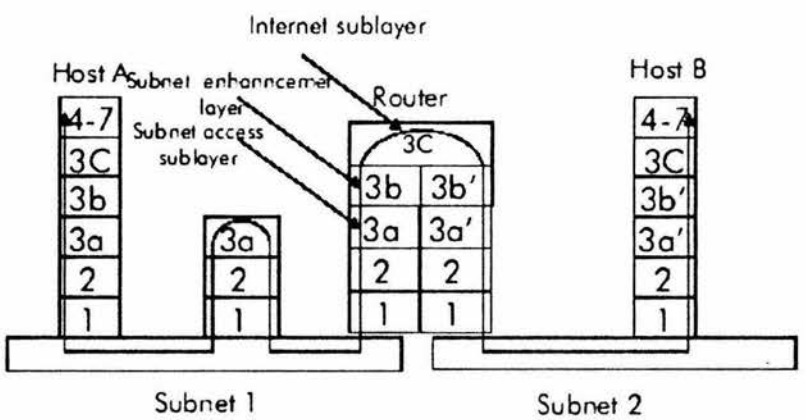

Fig. 3.10 Ruteador

3.7 Enrutamiento

En la mayoría de los casos un host determina que tiene que enviar un paquete a otro host. Habiendo adquirido una dirección física de un ruteador por medios que después analizaremos, el host origen envía un paquete direccionado hacia una dirección física MAC de un ruteador, pero también la dirección del protocolo a usar en el host destino.

Examinando la dirección destino del paquete, el ruteador determina si puede o no enviar el paquete al siguiente punto de conmutación o salto, esto mediante la comparación de la dirección obtenida con las direcciones contenidas en una tabla de enrutamiento.

Si el ruteador no sabe como reenviar el paquete simplemente lo desecha, si lo sabe y tiene dirección de salida, cambia la dirección física del paquete por la del siguiente hop y transmite el paquete. Es posible que el siguiente hop no sea el ultimo para llegar al otro host, por lo tanto la dirección física de destino en el paquete ira cambiando conforme se vaya adentrando en la red y pasando de ruteador a ruteador hasta llegar al final de su trayectoria.

Proceso de Enrutamiento

El mecanismo básico explicado anteriormente requiere de varias definiciones:

- Mecanismo / Proceso de Enrutamiento (Usando la tabla de enrutamiento): son las actividades realizadas por un nodo o host para determinar como se manejara un paquete en base a una dirección de red destino.

- Protocolo de Enrutamiento (Crea la tabla de enrutamiento): es el conjunto de reglas (en realidad el lenguaje) usadas entre ruteadores para compartir información de la red y tomar decisiones.

- Tabla de Enrutamiento: una tabla que contiene información acerca de los posibles destinos en base a direcciones de red especificas.

Las tablas de enrutamiento sobre las que se basan las decisiones de enrutamiento pueden ser configuradas de dos modos:

1- Estáticamente: definidas en el momento de la instalación y manipulables por los administradores de la red. Los ruteadores que se utilizan son eficientes, aunque obligan a un procedimiento de configuración largo y tedioso. El enrutamiento estático se administra manualmente. El administrador de red introduce la ruta en la configuración del router. El administrador debe actualizar manualmente esta entrada de ruta estática siempre que un cambio en la topología de la red requiera una actualización. El enrutamiento estático reduce el gasto porque no se envían actualizaciones de enrutamiento.

2- Dinámicamente: utilizando algoritmos automáticos. Los ruteadores son mas fáciles de configurar, pero pueden llegar a incrementar el "overhead" de la red por los continuos intercambios de información de control entre los ruteadores instalados. El enrutamiento dinámico funciona de manera diferente. Después de que un administrador de red introduce los comandos de configuración para empezar el enrutamiento dinámico, el conocimiento de la ruta se actualiza automáticamente a través de un proceso de enrutamiento siempre que se reciba nueva información de la red. Los cambios en el conocimiento dinámico se intercambian entre routers como parte del proceso de actualización.

Actividades de Enrutamiento

Encontrar información concerniente al destino de un paquete, el cual tiene que ser transmitido; la dirección del registro es comparada con los registros de la tabla de enrutamiento para decidir por cual interfaz será transmitida.

Actualización de la Tabla de Enrutamiento

Puede ser echo manualmente, directo sobre las áreas de configuración de redes en el sistema operativo utilizado por un operador o administrador de la red, como por ejemplo la configuración del gateway por omisión para TCP/IP en Windows 95, o automáticamente por medio de protocolos de enrutamiento.

Protocolos de Enrutamiento (Routing Protocols)

En general un RP esta compuesto de dos partes:

1- La comunicación con sus ruteadores y host vecinos para investigar que estaciones están conectadas a que parte de la red.

2- Después de recolectar esta información, filtrarla y correr un algoritmo para decidir cuales partes de esta información son usadas para cambiar o actualizar la tabla de enrutamiento.

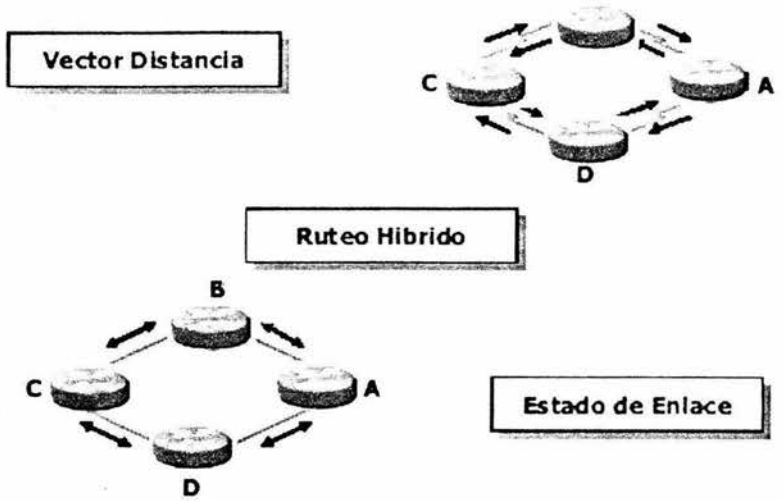

Fig. 3.10 Protocolos de enrutamiento

Los algoritmos mas usados en los actuales protocolos de ruteo son:

- RIP: Protocolo de enrutamiento por vector distancia
- OSPF: Protocolo de enrutamiento de estado de enlace.
- EIGRP: Protocolo de enrutamiento híbrido balanceado.

La mayoría de los protocolos de enrutamiento se pueden clasificar dentro de uno de dos tipos básicos: vector distancia o estado de enlace El protocolo de enrutamiento por vector distancia determina la dirección (vector) y distancia hacia cualquier enlace en la red. El protocolo de estado de enlace (también denominado primero la ruta libre más corta - SPF) recrea la topología exacta de toda la red (o por lo menos la partición en la que se ubica el router). Un tercer tipo de protocolo, el protocolo híbrido balanceado, combina aspectos de los protocolos de estado de enlace y por vector distancia.

El protocolo de estado de enlace es le mejor en términos de estabilidad, velocidad de actualización, manejo de overhead, etc., por lo tanto en mas comúnmente usado, de hecho, salvo casos muy especiales el protocolo por vector distancia.

Enrutamiento por vector distancia

Los protocolos de enrutamiento por vector de distancia envían copias periódicas de una tabla de enrutamiento desde un router a otro. Cada router recibe una tabla de enrutamiento de los routers directamente vecinos. Por ejemplo, el Router B recibe información del Router A. El Router B agrega un número de vector de distancia (tal como el número de saltos), aumentando de esta manera el vector de distancia y luego transfiere esta nueva tabla de enrutamiento a su otro vecino, el Router C. Este mismo proceso paso a paso se produce en todas las direcciones entre los routers directamente vecinos. De este modo, el protocolo acumula distancias de red para que pueda mantener

una base de datos de información de la topología de la red. Los protocolos por vector de distancia no permiten que el router conozca la topología exacta de la red.

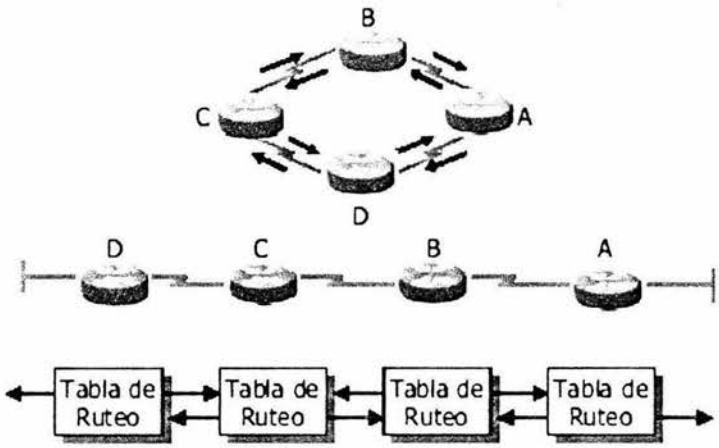

Fig. 3.11 Enrutamiento por vector distancia

Los ruteadores descubre en mejor camino a sus destinos a través de cada vecino.

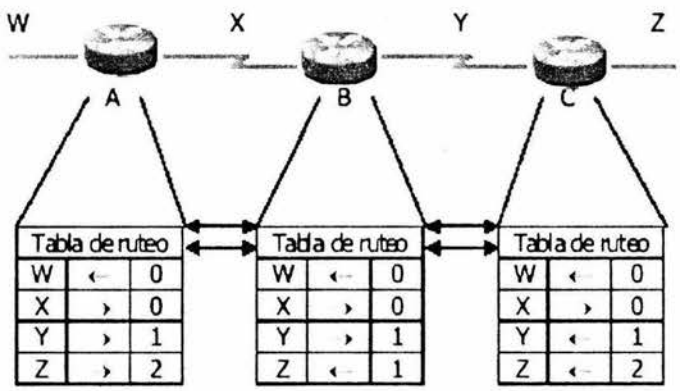

Fig. 3.12 Vector distancia con tabla de ruteo

Para cambiar de topología el proceso de actualización paso por paso de ruteador a ruteador.

RIP (Routing Information Protocolo): Esta basado en el protocolo de vector de distancia, el principio es el siguiente, un ruteador llama a cada ruteador vecino para enviar toda o una porción de su tabla de ruteo. Dicha tabla contiene un vector de distancias (conteo de hops) y cada ruteador actualiza su tabla basándose en estos vectores de distancia que recibe de sus vecinos. El envío de esta información se hace por broadcasting y este

continua mientras el ruteador este en línea en la red. El objetivo de su algoritmo es, una vez que llega un paquete, se analiza su dirección destino y se asigna la trayectoria mas optima en base a la distancia mas corta que se tenga en las posibles interfaces de salida.

Enrutamiento de estado de enlace (Link–State)

El segundo protocolo básico utilizado para el enrutamiento es el protocolo de estado de enlace. Los protocolos de enrutamiento de estado de enlace mantienen una base de datos compleja con información de topología. Mientras que el protocolo por vector distancia posee información no específica acerca de las redes distantes y ningún conocimiento acerca de los routers distantes, un protocolo de enrutamiento de estado de enlace conoce perfectamente los routers distantes y cómo se interconectan.

El enrutamiento de estado de enlace utiliza publicaciones de estado de enlace (LSA), una base de datos topológica, el protocolo SPF, el árbol SPF resultante y, por último, una tabla de enrutamiento de rutas y puertos hacia cada red. Los ingenieros han implementado este concepto de estado de enlace en el enrutamiento OSPF.

Cuando nos encontramos en estado de enlace después del primer flood, se pasan pequeñas actualizaciones del estado en enlace generadas por eventos a todos los ruteadores.

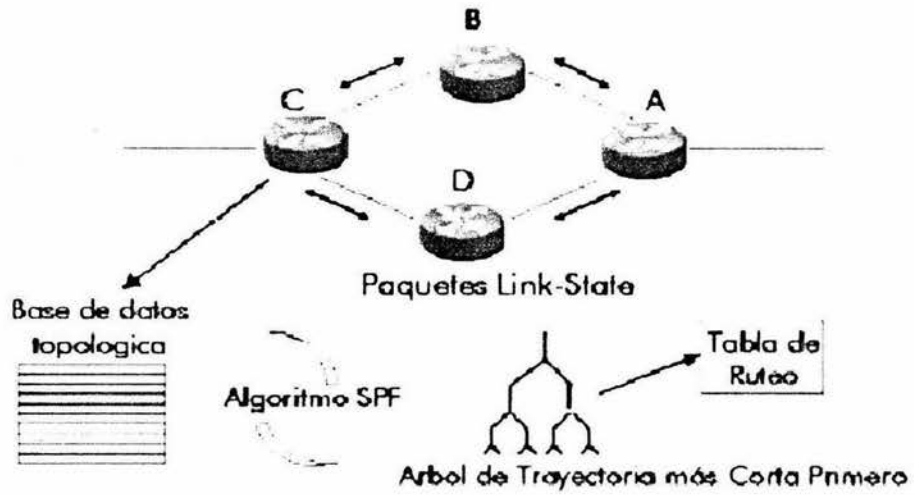

Fig. 3.13 Enrutamiento por estado de enlace

Los ruteadores calculan el camino mas corto a los destinos en paralelo.

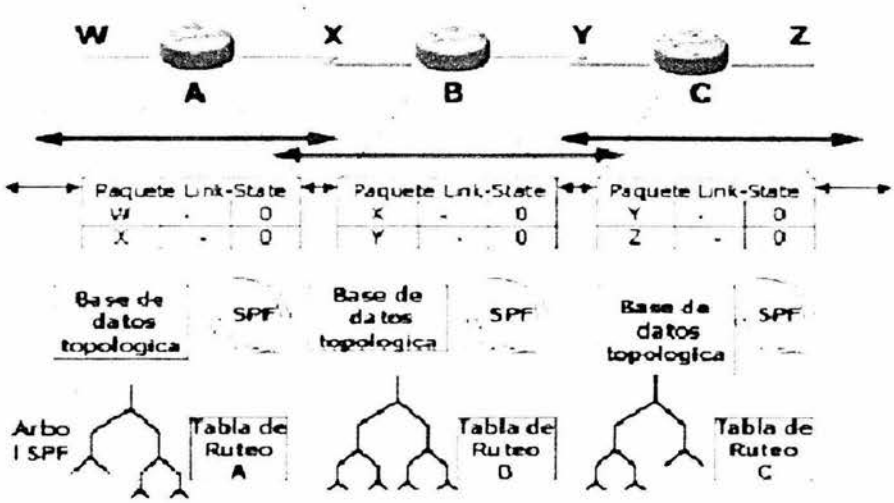

Fig. 3.14 Estado de enlace con tablas de enlace

Unas de las preocupaciones de Link-State es su procesamiento y la memoria requerida para estar en estado de enlace, así como el ancho de banda que se necesita para ser consumido por el flood inicial, además de contar con algunos problemas como actualizaciones desincronizadas y decisiones inconsistentes de rutas, también tiene algunas fallas al tratar de sincronizar redes grandes y al arrancado del ruteador la orden de inicio altera la topología aprendida.
Para este tipo de problemas se pueden aplicar algunas soluciones como reducir la necesidad de recursos, con esto la frecuencia de actualización amortiguada, intercambiar resúmenes de rutas en bordes de área y coordinar algunas actualizaciones usando tiempos de rechazo, actualizando numeración y contadores, así como llevando un manejo particionado usando un área de jerarquía.

OSPF (Open Shortest Path First): Esta basado en el algoritmo de Estado de Enlace, en el cual un ruteador prueba continuamente el estado de sus enlaces hacia cada uno de sus vecinos y envía esta información a tales vecinos, los cuales a su vez la propagan a través de todo el sistema autónomo o dominio, de tal manera que cada ruteador forma esta información y construye una tabla de ruteo completa de toda la red.

Para hacer lo anterior, en un proceso de inicialización de la red, un ruteador generara un mensaje: Link-State advertisement que representa la recolección del estado de todos los enlaces de ese ruteador.

Cada ruteador vecino recibirá esta información, guardara una copia en su base de datos y la retransmitirá a los siguientes ruteadores con los que tenga enlaces, sumando su propia información, mediante un proceso de inundación. Una vez que cada ruteador tenga la información completa, calculara un árbol de ruta mas corta para todos sus destinos, con el algoritmo que calcula para cada destino su costo y el siguiente hop para alcanzarlos.

Desde el punto de vista de la Internet y considerando su tamaño y acelerado crecimiento se tienen que jerarquizar los niveles de enrutamiento para que no necesariamente, en le caso de OSPF todos los ruteadores deban de conocer el estado de la totalidad de la red, lo que implicaría la creación y manejo de bases de datos gigantescos.

Por esta razón diferentes tipos de ruteadores pueden ser identificados:

- Ruteadores Backbone: usan un protocolo de ruteo de backbone y solo necesitan saber de enrutamiento entre AS (Sistemas Autónomos o dominios), en donde por cuestiones de seguridad se establecen trayectorias fijas ha de ser seguidas por un paquete.

- Ruteador Interior: son usados dentro de los dominios o AS. Si tienen una pasarela por omisión, debe de apuntar a un ruteador frontera del mismo AS.

- Ruteadores frontera: proveen la interfaz entre el backbone y el AS, deben de conocer tanto la estructura interna y la conexión de AS al backbone, por lo tanto deberá correr dos protocolos.

3.8 Pasarela / Gateway

Las pasarelas como se definió anteriormente tienen su funcionalidad desde el nivel 4 hasta el nivel 7 de OSI. En esencia esto significa que las pasarelas pueden examinar también el contenido de los paquetes de los datos de aplicación.

Las pasarelas son usadas para varias funciones:

- Servicios Proxy
- Traducción de Direcciones
- Compuertas de Acceso
- Seguridad

Algunas veces se hace una separación entre las pasarelas de transporte los cuales están involucrados solo en los mecanismos de transporte, por ejemplo: establecimiento de conexión y traducción de direcciones y las pasarelas de aplicación los cuales examinan los paquetes.

Servicios Proxy

- La definición de un Servidor Proxy es: hacer algo en beneficio de alguien mas, esto significa que, puesto un requerimiento a algún servidor, este no es respondido por el servidor al que se requirió sino por un agente intermedio, esto puede ser, en un momento dado trasparente para el usuario.

- Las motivaciones para tener un servidor proxy son:

  1- El servidor proxy puede responder mas rápidamente.
  2- Es usuario no conoce al verdadero servidor, por lo tanto el proxy puede buscarlos por el.

Web Proxy Server

Es usado para tener una respuesta mas rápida y mayor capacidad cuando se navega por paginas Web en Internet. La idea es comparable con "caching", de paginas Web recuperadas. Cuando una pagina Web es requerida varias veces por un usuario, en lugar de traerla siempre desde el site original, cuando se pide por segunda vez o posterior, se recupera de la memoria cache del proxy.

Esto es, el servidor proxy generara en memoria una lista de las paginas que se han cargado de Internet, y cada que un usuario intente traer la conexión, pasara por el proxy, que verificara si la pagina esta en memoria, si es así, se la enviara al usuario sin necesidad de crear la conexión, acelerando de esta manera el acceso y de paso disminuyendo el trafico de salida real hacia Internet.

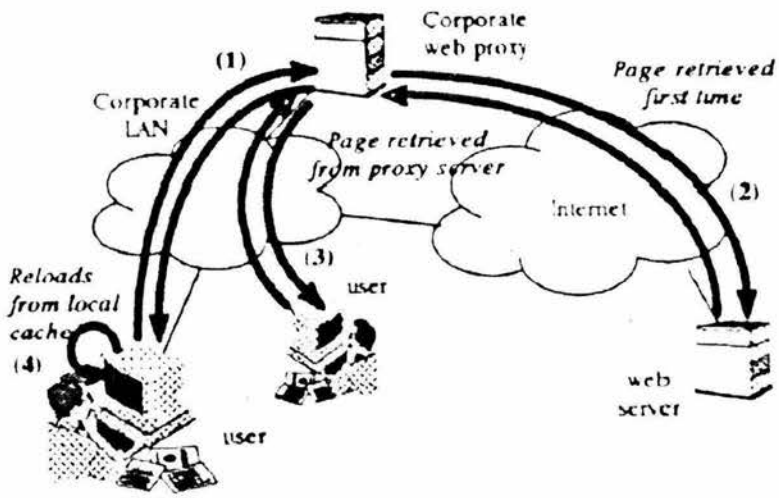

Fig. 3.15 Web Proxy Server

SMC Proxy Server

El centro de administración de servicios del servidor proxy se encarga de almacenar las grandes bases de datos para la autenticación y autorización de los usuarios que desean conectarse a redes de tipo corporativas a través de redes de acceso (RAN), por ejemplo; ni las redes corporativas ni un operador que proporciona el acceso tiene la intención de mantener tales bases de datos, de manera que se dividen en varios SMC's de acuerdo a la función que desempeñaran, de autorización o de autenticación. De tal manera que

cuando un usuario pide conectarse a una red a través de una red de acceso, será en realidad atendido primero por el SMC del operador que lo enrutara al SMC corporativo correspondiente a la red destino, el cual lo autorizara y autenticara para entonces si proceder a generar la conexión.

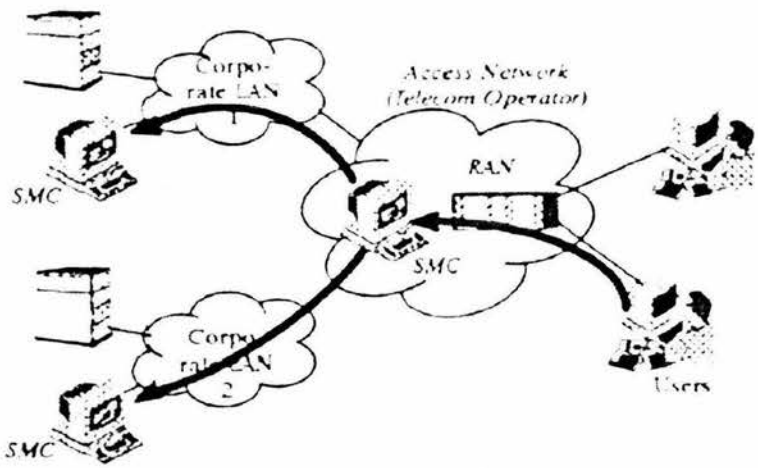

Fig. 3.16 SMC Proxy Server

Network Address Translation (NAT) Proxy Server

Es un método para conectar múltiples a la Internet (a cualquier otra red IP) usando solo una dirección IP oficial. Esto permite a los usuarios residenciales y de pequeñas empresas conectar su red a la Internet de una manera eficiente y sobre todo barata compartiendo un acceso IP. Este método también agrega un cierto nivel de seguridad a la red detrás del NAT Proxy Server, pues desde Internet solo ven la dirección IP asignada al proxy y no a las terminales o host que están detrás. La asignación de direcciones IP "privadas" puede ser echo de manera dinámica mediante un DHCP (Dynamic Host Configuration Protocol) en el momento en que se enciende una terminal. El propósito básico es por lo tanto multiplexar trafico interno hacia la Internet y viceversa, esto mediante el uso de puertos asignados a las direcciones IP locales y representados en un encabezado en cada paquete.

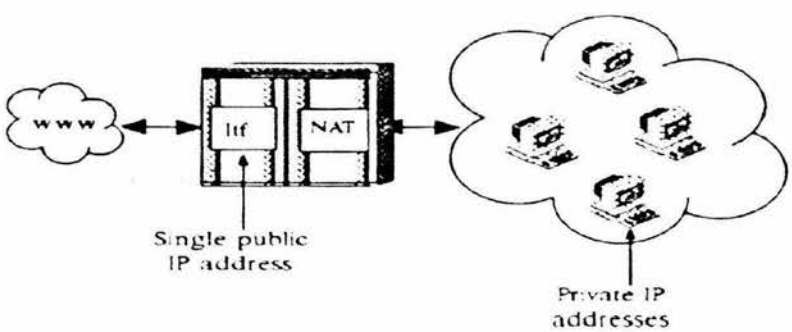

Fig. 3.17 Network Address Translation

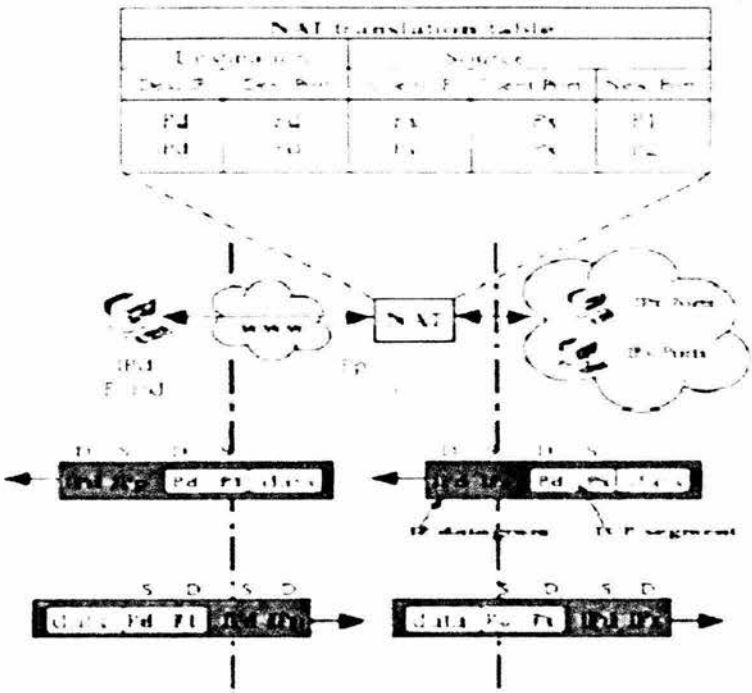

Fig. 3.18 NAT Tabla

CONCLUSIONES

Ahora ya sabemos todo el proceso que la información tiene que pasar para que nos llegue a la computadora, parece sencillo pero son muchos años de trabajo, claro que todo esto no funcionaría sin la revolución de las computadoras y la necesidad para intercambiar información por medio de ellas, por ello recordamos que en el capitulo primero hablamos un poco de una red de datos, y las primeras interconexiones entre computadoras en un mismo lugar llamadas LAN, su forma de conexión y sus topologías.

Del mismo modo conocimos las organizaciones que regulan la Internet y por ultimo el modelo OSI con el cual se lleva una estructura desde recibir la información hasta procesarla y presentarla en una pantalla, gracias a ello podemos contar con Internet en nuestras casas.

Claro que falta todo el proceso de direccionamiento que se hace con el protocolo TCP/IP con el cual le damos una dirección única a cada computadora para evitar errores de envío y de llegada, es una especie de dirección como la de nuestra casa, sin la cual no podríamos recibir correspondencia y no podríamos mandarla tampoco sin conocer al destinatario.

Por ultimo vimos el proceso de la información en Internet-Working con las Internet Working Units que son las unidades que conforman el Internet y las decisiones que deben de tomas para enviar o desechar información, así como regenerarla y darle total alcance de ella al usuario.

Ahora que ya sabemos mejor como funciona, tal vez comprendamos por que a veces algunas pequeñas fallas y uno que otro retardo en la información, esperemos que la tecnología continúe en esta gran evolución y pronto contaremos con sistemas más rápidos y más eficaces, al alcance de cualquier persona en el planeta.

Con el desarrollo de nuevas tecnologías van a ir desapareciendo muchos de estos términos o pasos a seguir, pero por el momento es lo que se utiliza para este servicio, por lo tanto hay que seguir actualizándose en las nuevas tecnologías de la información y no quedarnos obsoletos nosotros, lo que debe quedar en el pasado solo son las maquinas que se van convirtiendo en antiguas y no nuestro capacidad para desarrollar y entender las nuevas tecnologías.

GLOSARIO

Acuse de recibo

Notificación enviada por un dispositivo de la red a otro para comunicar que se produjo un evento determinado.

Administración de errores

Una de las cinco categorías de administración de red definidas por ISO para la administración de las redes OSI. La administración de errores pretende asegurar la detección y el control de las fallas de red.

Ancho de banda

Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. También se utiliza este término para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

Anillo

Conexión de dos o más estaciones en una topología circular lógica. La información se pasa de forma secuencial entre estaciones activas. Token Ring, FDDI y CDDI se basan en esta topología.

Anillo dividido

Arquitectura LAN basada en una topología de anillo en la cual el anillo está dividido en ranuras que circulan continuamente. Las ranuras pueden estar vacías o llenas, y las transmisiones deben comenzar al inicio de una ranura.

ANSI

Instituto Nacional Americano de Normalización. Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones normalizadoras internacionales. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la ISO (Organización Internacional para la Normalización).

Área

Conjunto lógico de segmentos de red (basados en CLNS, DECnet u OSPF) y sus dispositivos conectados. Las áreas habitualmente se conectan entre sí mediante routers, formando un sistema autónomo único.

ARP

Protocolo de Resolución de Direcciones. Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826.

ARP inversa

Protocolo de resolución de direcciones inversas. Método de desarrollo de rutas dinámicas en una red. Permite que un servidor de acceso descubra la dirección de red de un dispositivo asociado con un circuito virtual.

ARPA

Agencia de Proyectos de Investigación Avanzada. Organización de investigación y desarrollo que forma parte del Departamento de la Defensa de los EE.UU. ARPA es responsable por numerosos avances tecnológicos en comunicaciones y networking. ARPA se convirtió en DARPA, pero volvió a ser ARPA (en 1994).

ARPANET

Red de la Agencia de Proyectos de Investigación Avanzada. Una red de conmutación de paquetes de gran importancia establecida en 1969. ARPANET fue desarrollada durante los años 70 por BBN y financiada por ARPA (y luego DARPA). Eventualmente dio origen a la Internet. El término ARPANET se declaró oficialmente en desuso en 1990.

Arquitectura cliente / servidor

Término utilizado para describir sistemas de red (de procesamiento) de informática distribuida, en los que las responsabilidades por las transacciones se dividen en dos partes: el cliente (front-end) y el servidor (Back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos en sí. También se denomina *informática distribuida.*

Asignación de direcciones

Técnica que permite que diferentes protocolos interoperen convirtiendo direcciones de un formato a otro. Por ejemplo, al enrutar IP en X.25, las direcciones IP deben asignarse a las direcciones X.25 para que la red X.25 pueda transmitir los paquetes IP.

Backbone

Parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de, y se destina a, otras redes.

Banda ancha

Sistema de transmisión que multiplexa varias señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que un canal de grado de voz (4 kHz). En la terminología de las LAN, un cable coaxial en el que se usa señalización analógica. También se denomina *banda amplia.*

Banda base

Característica de una tecnología de red donde sólo se utiliza una frecuencia portadora. Ethernet es un ejemplo de una red de banda base. También denominada *banda angosta.*

BER

1. **Índice de error binario**. La proporción de bits recibidos que contienen errores.
2. **Normas de codificación básica**. Normas para unidades de codificación descritas en el estándar de ISO ASN.1.

Binario

Sistema de numeración compuesto por unos y ceros (1 = encendido; 0 = apagado).

Bit

Dígito binario utilizado en el sistema numérico binario. Puede ser 0 ó 1.

bps

Bits por segundo.

broadcast

Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican mediante una dirección de broadcast.

Broadcast de IP

Técnica de enrutamiento que permite que el tráfico de IP se propague desde un origen hasta una serie de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, un paquete se envía a un grupo de broadcast identificado a través de una sola dirección IP de grupo de destino.

Bucle

Ruta donde los paquetes nunca alcanzan su destino, sino que recorren repetidamente una serie constante de nodos de red.

Búfer

Área de almacenamiento utilizada para manejar datos en tránsito. Los búferes se usan en la internetworking para compensar las diferencias en velocidad de procesamiento entre dispositivos de red. Se pueden almacenar ráfagas de datos en los búferes hasta que los dispositivos de procesamiento más lentos las puedan manejar. A veces se denomina *búfer de paquetes.*

Bus

Ruta de señales físicas comunes compuesta por cables y otros medios a través de los cuales las señales se envían de una parte de un computador a otro. A veces se denomina *autopista.*

Byte

Término utilizado para hacer referencia a una serie de dígitos binarios consecutivos sobre los que se opera como una unidad (por ejemplo, un byte de 8 bits).

Byte

Término utilizado para hacer referencia a una serie de dígitos binarios consecutivos sobre los que se opera como una unidad (por ejemplo, un byte de 8 bits).

Cable

Medio de transmisión de alambre de cobre o fibra óptica que se envuelve en una cubierta protectora.

Cable coaxial

Cable compuesto por un conductor cilíndrico externo hueco, que reviste un conductor con un solo cable interno. Actualmente se usan dos tipos de cable coaxial en las LAN: el cable de 50 ohmios, utilizado para la señalización digital y el cable de 75 ohmios, utilizado para señales analógicas y para la señalización digital de alta velocidad.

Cable de fibra óptica

Medio físico que puede conducir la transmisión modulada de luz. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otro lado no es susceptible a la interferencia electromagnética y permite mayores velocidades de transmisión de datos. A veces se le denomina *fibra óptica.*

Cable de par trenzado

Medio de transmisión de velocidad relativamente baja, que consta de dos cables aislados colocados según un patrón de espiral regular. Los cables pueden ser blindados o no blindados. El par trenzado se utiliza comúnmente en las aplicaciones de telefonía y su uso en las redes de datos se está tornando cada vez más común.

Canal

1. Una ruta de comunicación. Se pueden multiplexar múltiples canales en un solo cable en ciertos entornos.
2. En IBM, la ruta específica entre computadores de gran tamaño (como los mainframes) y dispositivos periféricos conectados.
3. Tipo de conducto con cubierta móvil montado en la pared utilizada para soportar el cableado horizontal. El canal es lo suficientemente grande como para contener varios cables.

Canal de envío

Ruta de comunicación que transporta la información desde el iniciador de la llamada hasta el que recibe la llamada.

Capa ATM

Subcapa independiente de servicio de la capa de enlace de datos en una red ATM. La capa ATM recibe los segmentos de carga de 48 bytes de la AAL y adjunta un encabezado de 5 bytes a cada uno, produciendo celdas estándar ATM de 53 bytes. Estas celdas se pasan a la capa física para su transmisión a través del medio físico.

Capa de aplicación

Capa 7 del modelo de referencia OSI. Esta capa brinda servicios a procesos de aplicación (como por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que se encuentran fuera del modelo de referencia OSI. La capa de aplicación identifica y establece la disponibilidad de los dispositivos con los que se pretende establecer comunicación (y de los recursos requeridos para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece la concordancia de procedimientos para la recuperación de errores y el control de la integridad de los datos.

Capa de control de enlace de datos

Capa 2 del modelo de arquitectura SNA. Es responsable por la transmisión de datos a través de un enlace físico en particular. Corresponde aproximadamente a la capa de nelace de datos del modelo de referencia OSI.

Capa de control de ruta

Capa 3 del modelo de arquitectura SNA. Esta capa ejecuta servicios de control secuencial relacionados con el reensamblaje correcto de los datos. La capa de control de ruta también es responsable por el enrutamiento. Equivale aproximadamente a la capa de red del modelo OSI.

Capa de control de transmisión

Capa 4 del modelo de arquitectura SNA. Esta capa tiene la responsabilidad de establecer, mantener y terminar las sesiones SNA, secuenciar mensajes de datos y controlar el flujo de nivel de sesión. Equivale a la capa de transporte del modelo OSI.

Capa de control físico

Capa 1 del modelo de arquitectura SNA. Esta capa es responsable por las especificaciones físicas de los enlaces físicos entre sistemas finales. Equivale a la capa física del modelo OSI.

capa de enlace de datos

Capa 2 del modelo de referencia OSI. Proporciona tránsito confiable de datos a través de un enlace físico. La capa de enlace de datos se ocupa del direccionamiento físico, topología de red, disciplina de línea, notificación de errores, entrega ordenada de las tramas y del control de flujo. IEEE dividió esta capa en dos subcapas: la subcapa MAC y la subcapa LLC. A veces se le denomina simplemente *capa de enlace.*

Capa de presentación

Capa 6 del modelo de referencia OSI. Esta capa asegura que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. La capa de presentación también se ocupa de las estructuras de datos que usan los programas y, por lo tanto, negocia la sintaxis de transferencia de datos para la capa de aplicación.

Capa de red

Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es la capa en la que se produce el enrutamiento

capa de sesión

Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina las sesiones entre aplicaciones y administra el intercambio de datos entre las entidades de la capa de presentación

Capa de transporte

Capa 4 del modelo de referencia OSI. Esta capa es responsable por la comunicación confiable de red entre nodos finales. Proporciona mecanismos para el establecimiento, el mantenimiento y la terminación de circuitos virtuales, la detección y recuperación de fallas de transporte y el control del flujo de información.

Capa física

Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

CCITT

Comité Consultivo Internacional Telegráfico y Telefónico. Organización internacional responsable por el desarrollo de estándares de comunicación. Actualmente ha pasado a llamarse UIT-T.

Codificación

1. Técnicas eléctricas utilizadas para transportar señales binarias.
2. Proceso a través del cual los bits son representados por voltajes.

Colisión

En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de los dos dispositivos chocan y se dañan cuando se encuentran en los medios físicos.

Conductor

Cualquier material con baja resistencia a la corriente eléctrica Cualquier material que puede transportar una corriente eléctrica.

Configuración base

La información mínima de configuración que se introduce cuando se instala un nuevo router, switch, u otro dispositivo de red configurable en una red. La configuración básica de un switch ATM LightStream2020, por ejemplo, incluye direcciones IP, la fecha y los parámetros para por lo menos una línea troncal. La configuración básica permite que el dispositivo reciba una configuración completa del NMS.

Congestión

Tráfico que supera la capacidad de la red.

Conmutación de circuitos

Sistema de conmutación en el que debe existir una ruta de circuito física dedicada entre el emisor y el receptor durante la duración de la "llamada". Se utiliza ampliamente en la red telefónica comercial

Conmutación de mensajes

Técnica de conmutación que incluye la transmisión de mensajes de nodo a nodo a través de la red. El mensaje se almacena en cada nodo hasta que se encuentre disponible una ruta de envío

Conmutación de paquetes

Método de networking en el cual los nodos comparten el ancho de banda entre sí enviando paquetes.

Control de paridad

Proceso para controlar la integridad de un carácter. Un control de paridad implica agregar un bit que hace que la cantidad total de dígitos 1 binarios de un carácter o una palabra (excluyendo el bit de paridad) sea impar (para la *paridad impar*) o par (para la *paridad par*).

Correo electrónico

Aplicación de red de uso generalizado en la que los mensajes de correo se transmiten electrónicamente entre usuarios finales en diferentes tipos de redes, utilizando diferentes protocolos de red. A menudo se denomina *e-mail*.

DARPA

Agencia de Proyectos de Investigación Avanzada para la Defensa. Agencia gubernamental de los EE.UU. que financió la investigación y la experimentación con la Internet. Antiguamente denominada ARPA, volvió a utilizar ese nombre a partir de 1994.

Datagrama

Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información de la Internet. Los términos trama, mensaje, paquetes y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Datos

Datos de protocolo de capa superior.

DECnet

Grupo de productos de comunicaciones (incluyendo un conjunto de protocolos) desarrollado y soportado por Digital Equipment Corporation. DECnet/OSI (también denominado DECnet Phase V) es la iteración más reciente y soporta protocolos OSI y protocolos Digital propietarios. Phase IV Prime soporta direcciones inherentes MAC que permiten que los nodos DECnet coexistan con sistemas que ejecutan otros protocolos que tengan restricciones de dirección MAC.

Demodulación

Proceso de devolver una señal modulada a su forma original. Los módems realizan la demodulación capturando una señal analógica y devolviéndola a su forma original (digital).

Dirección

Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular.

Dirección de broadcast

Dirección especial reservada para enviar un mensaje a todas las estaciones. Por lo general, una dirección de broadcast es una dirección MAC de destino compuesta exclusivamente por todos los números uno.

Dirección de multicast

Dirección única que se refiere a los dispositivos de múltiples redes. Sinónimo de *dirección de grupo.*

Dirección de origen

Dirección de un dispositivo de red que envía datos.

Dirección de red

Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada *dirección de protocolo.*

Dirección de subred

Parte de una dirección IP especificada como la subred por la máscara de subred.

Dirección IP

1. Dirección de 32 bits asignada a los hosts que usan TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host.. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet.
2. Instrucción utilizada para establecer la dirección de red lógica de esta interfaz.

Direcciones IP de origen y de destino

Campo dentro de un datagrama IP que indica las direcciones de origen y de destino de 32 bits.

DNS

Sistema de denominación de dominio. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DoD

Departamento de Defensa. Organización gubernamental de los EE.UU., responsable por la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

Dominio

1. En la Internet, una parte del árbol jerárquico de denominación que se refiere a agrupamientos generales de redes basados en un tipo de organización o geografía.
2. En SNA, un SSCP y los recursos que controla.
3. En IS-IS, un conjunto lógico de redes.

Dominio de broadcast

Conjunto de todos los dispositivos que recibirán tramas de broadcast que se originan en cualquier dispositivo dentro del conjunto. Los dominios de broadcast se encuentran normalmente delimitados por routers, debido a que los routers no envían tramas de broadcast.

Dominio de colisión

En Ethernet, el área de la red en la que se propagan las tramas que colisionan. Los repetidores y los hubs propagan las colisiones; los switches de LAN, puentes y routers no lo hacen.

Enrutamiento

Proceso de descubrimiento de una ruta hacia el host de destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host de destino.

Estándar

Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Explorador proxy

Técnica que reduce al mínimo el tráfico del paquete explorador que se propaga a través de una red SRB al crear un caché de respuesta del paquete explorador, cuyo contenido se vuelve a utilizar cuando paquetes exploradores subsiguientes deben encontrar el mismo host.

Firewall

Router o servidor de acceso o varios routers o servidores de acceso designados como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de acceso así como otros métodos para garantizar la seguridad de la red privada.

Flujo

Corriente de datos que viaja entre dos puntos finales a través de una red (por ejemplo, de una estación LAN a otra). Varios flujos se pueden transmitir a través de un mismo circuito.

Fragmentación

Proceso de dividir un paquete en unidades más pequeñas cuando se está transmitiendo en un medio de red que no puede soportar el tamaño original del paquete.

Frame Relay

Estándar de la industria, protocolo de capa de enlace de datos con conmutación que maneja múltiples circuitos virtuales mediante una forma de encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se le considera generalmente un reemplazo.

FTP

Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP utilizado para la transferencia de archivos entre nodos de red. El FTP se define en RFC 959.

Full dúplex

Capacidad de transmisión de datos simultánea entre la estación emisora y la estación receptora.

Gateway

En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término *router* se utiliza para describir nodos que desempeñan esta función y *gateway* se refiere a un dispositivo especial que realiza una conversión de capa de aplicación de la información de una pila de protocolo a otro.

Grupo de multicast

Grupo determinado dinámicamente de hosts IP identificados por una dirección de multicast IP única.

Hipertexto

Texto almacenado electrónicamente que permite el acceso directo a otros textos a través de enlaces codificados. Los documentos de hipertexto se pueden crear utilizando HTML y generalmente integran imágenes, sonido y otros medios que se pueden visualizar normalmente utilizando un navegador de la Web.

Host

Sistema informático en una red. Similar al término *nodo*, salvo que *host* normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y routers.

HTML

Lenguaje de etiquetas por hipertexto. Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo una aplicación de visualización, como por ejemplo un navegador de la Web, debe interpretar una parte determinada de un documento.

Hub

1. Por lo general, se usa este término para describir un dispositivo que sirve como centro de una red con topología en estrella.
2. Dispositivo de hardware o software que contiene múltiples módulos independientes pero que están conectados a los equipos de red y de internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten las señales sino simplemente dividen las señales enviadas a través de ellos).
3. En Ethernet y IEEE 802.3, un repetidor multipuerto de Ethernet que se conoce a veces como *concentrador*.

I/O

Entrada/salida.

IAB

Comité de Arquitectura de Internet. Comité de investigadores de internetworking que discute temas relativos a la arquitectura de Internet. Responsables por designar una serie de grupos relacionados con Internet, como IANA, IESG e IRSG. El IAB es nombrado por integrantes de la ISOC.

IEEE 802,1

Especificación IEEE que describe un algoritmo que evita los bucles de puenteo creando un spanning tree (árbol de extensión). El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo Digital y el algoritmo IEEE 802.1 no son exactamente iguales, ni tampoco son compatibles.

IEEE.

Instituto de Ingeniería Eléctrica y Electrónica. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares que predominan en las LAN de la actualidad.

Interfaz

1.Conexión entre dos sistemas o dispositivos.
2.En terminología de enrutamiento, una conexión de red.
3.En telefonía, un límite compartido definido por características en común de interconexión física, características de señal y significados de las señales intercambiadas.
4. Límite entre capas adyacentes del modelo de referencia OSI.

Internet

Término utilizado para referirse a la internetwork más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó *Internet DARPA*. No debe confundirse con el término general *internet*.

Internetwork

Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (en general) como una sola red. A veces denominada una *internet*, que no se debe confundir con la *Internet*.

Internetworking

Término general utilizado para referirse a la industria que ha surgido en torno de la cuestión de la conexión de redes entre sí. El término se puede referir a productos, procedimientos y tecnologías.

Interoperabilidad

Capacidad de los equipos de informática de diferentes fabricantes para comunicarse entre sí con éxito en una red.

IP

Protocolo Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientada a la conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad.

ISO

Organización Internacional para la Normalización. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a la networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.

LAN

Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y la señalización en la capa física y la capa de enlace de datos del modelo de referencia OSI. Ethernet, FDDI y Token Ring son tecnologías de LAN ampliamente utilizadas.

MAC

Control de acceso al medio. Capa inferior de las dos subcapas de la capa de enlace de datos, según la define el IEEE. La subcapa MAC maneja el acceso a los medios compartidos, por ejemplo, si se utilizara la transmisión o la contención de tokens.

Malla

Topología de red en la cual los dispositivos se organizan de manera administrable, segmentada, con varias interconexiones, a menudo redundantes, colocadas de forma estratégica entre los nodos de la red. Ver

Máscara de dirección

Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se la llama simplemente *máscara*.

Máscara de subred

Máscara de dirección de 32 bits que se usa en IP para indicar los bits de una dirección IP que se utilizan para la dirección de subred. A veces se denomina simplemente *máscara*.

Mensaje

Agrupación lógica de información de la capa de aplicación (Capa 7), a menudo compuesta por una serie de agrupaciones lógicas de las capas inferiores, por ejemplo, paquetes

MILNET

Red militar. Porción sin clasificar de la DDN. Operada y mantenida por la DISA.

modelo de referencia OSI

Modelo de referencia para interconexión de sistemas abiertos. Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, por ejemplo, direccionamiento, control de flujo, control de errores, encapsulamiento y transferencia confiable de mensajes. La capa superior (la capa de aplicación) es la más cercana al usuario; la capa inferior (la capa física) es la más cercana a la tecnología de medios. Las dos capas inferiores se implementan en el hardware y el software, y las cinco capas superiores se implementan sólo en el software. El modelo de referencia OSI se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red.

MTU

Unidad máxima de transmisión. Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

multicast

Paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de direcciones de destino.

NET

Título de entidad de la red. Direcciones de red, definidas mediante la arquitectura de red ISO y que se usa en redes basadas en CLNS.

Networking

Interconexión de cualquier grupo de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NFS

Sistema de archivos de red. Se utiliza comúnmente para designar un conjunto de protocolos de sistema de archivos distribuido, desarrollado por Sun Microsystems, que permite el acceso remoto a archivos a través de una red. En realidad, NFS es sólo un protocolo del conjunto.

NIC

Tarjeta de interfaz de red. Placa que proporciona capacidades de comunicación de red hacia y desde un computador. También llamada *adaptador*.

Nodo

1. Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales, pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra *dispositivo*. Ver también *host*.
2. En SNA, el componente básico de una red y el punto en el que una o más unidades funcionales conectan canales o circuitos de datos.

Número de host

Parte de una dirección IP que designa a qué nodo de la subred se realiza el direccionamiento. También denominada *dirección de host*.

Número de red

Parte de una dirección IP que especifica la red a la cual pertenece el host.

Orientado a conexión

Término utilizado para describir la transferencia de datos que requiere el establecimiento de un circuito virtual.

OSI

interconexión de sistemas abiertos. Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

PDU

Unidad de datos del protocolo. Término OSI equivalente a paquete.

ping

Instrucción utilizada por el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red. Este es un mecanismo de prueba sumamente básico.

PPP

Protocolo punto a punto. Sucesor del SLIP que suministra conexiones router a router y host a red a través de circuitos síncronos y asíncronos .

Protocolo

1. Descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información.
2. Campo dentro de un datagrama IP que indica el protocolo de capa superior (Capa 4) que envía el datagrama.

Protocolo de enrutamiento

Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. IGRP, OSPF y RIP son ejemplos de protocolos de enrutamiento.

Protocolo de spanning tree

Protocolo de puente que usa el algoritmo de spanning tree (árbol de extensión) y permite que un puente con aprendizaje evite los bucles de forma dinámica en una topología de red con conmutación, creando un árbol de extensión. Los puentes intercambian mensajes BPDU con otros puentes para detectar bucles y luego eliminarlos al desactivar las interfaces de puente seleccionadas. Se refiere al estándar IEEE 802.1 de Protocolo de spanning tree y al Protocolo de spanning tree más antiguo, de Digital Equipment Corporation, en el cual se basa. La versión de IEEE soporta dominios de puente y permite que el puente desarrolle una topología sin bucles a través de una LAN extendida. Generalmente, se prefiere la versión de IEEE en lugar de la versión de Digital. A veces abreviado *STP*.

Protocolo enrutado

Protocolo que puede ser enrutado por un router. Un router debe poder interpretar la internetwork lógica según lo que especifica dicho protocolo enrutado. AppleTalk, DECnet e IP son ejemplos de protocolos enrutados.

PTT

Administración postal, de telégrafos y teléfonos. Entidad gubernamental que suministra servicios telefónicos. Las PTT existe en la mayoría de las áreas fuera de América del Norte y suministran servicios telefónicos locales y de larga distancia.

Puente

Dispositivo que conecta y transmite paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (Capa 2) del modelo de referencia OSI. En general, un puente filtra, envía o inunda la red con una trama entrante sobre la base de la dirección MAC de esa trama.

Puerto

1. Interfaz en un dispositivo de internetworking (por ejemplo, un router).
2. En la terminología IP, un proceso de la capa superior que recibe información de las capas inferiores.

RARP

Protocolo inverso de resolución de direcciones. Protocolo en la pila TCP/IP que brinda un método para encontrar direcciones IP en base a las direcciones MAC.

Red

1.) Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de un medio de transmisión.
2.) Instrucción que asigna una dirección basada en la NIC con la cual el router está directamente conectado.
3.) Instrucción que especifica cualquier red conectada directamente que se desee incluir.

Redundancia

1. En internetworking, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla.
2. En telefonía, la porción de la información total contenida en un mensaje que se puede eliminar sin sufrir pérdidas de información o significado esencial.

Relay

Terminología OSI para un dispositivo que conecta dos o más redes o sistemas de red. Un relay de capa de enlace de datos (Capa 2) es un puente; un relay de capa de red (Capa 3) es un router.

Repetidor

Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

RFC

Petición de comentarios. Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFC pueden encontrarse en línea en distintas fuentes.

RIP

Protocolo de información de enrutamiento. IGP provisto con los sistemas UNIX BSD. El IGP más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

Router

Dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Envía paquetes desde una red a otra basándose en la información de la capa de red. De vez en cuando denominado *gateway* (aunque esta definición de gateway se está tornando obsoleta).

Salto

Término que describe el pasaje de un paquete de datos entre dos nodos de red (por ejemplo, entre dos routers).

Segmento

1. Sección de una red limitada por puentes, routers o switches
2. En una LAN que usa topología de bus, un segmento es un circuito eléctrico continuo que a menudo está conectado a otros segmentos similares a través de repetidores.
3. En la especificación TCP, una unidad única de información de capa de transporte.

Sesión

Conjunto relacionado de transacciones de comunicaciones entre dos o más dispositivos de red.

SMTP

Protocolo de transferencia de correo simple. Protocolo Internet que suministra servicios de correo electrónico.

Subred

1. En redes IP, una red que comparte una dirección de subred específica. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina *subnet*
2. En redes OSI, un conjunto de sistemas finales y sistemas intermedios bajo el control de un dominio administrativo único y que utiliza un protocolo de acceso de red exclusivo.

Switch

1. Dispositivo de red que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.
2. Término general que se aplica a un dispositivo electrónico o mecánico que permite que una conexión se establezca según sea necesario y se termine cuando ya no haya ninguna sesión para soportar.

Tabla de enrutamiento

Tabla almacenada en un router o en algún otro dispositivo de internetworking que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TCP

Protocolo para el control de la transmisión. Protocolo de la capa de transporte orientado a conexión que proporciona una transmisión confiable de datos de full dúplex. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP

Protocolo de control de transporte/Protocolo Internet. Nombre común para el conjunto de protocolos desarrollados por el DoD de los EE.UU. en los años '70 para soportar el desarrollo de internetwork a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Telecomunicaciones

Término que se refiere a las comunicaciones (generalmente involucrando computadores) a través de la red telefónica.

telnet

Instrucción utilizada para verificar el software de capa de aplicación entre estaciones de origen y de destino.

Terminal

Dispositivo simple en el que se pueden introducir o recuperar datos de una red. En general, las terminales tienen un monitor y un teclado, pero no tienen procesador o unidad de disco local.

TFTP

Protocolo de transferencia de archivos trivial. Versión simplificada de FTP que permite la transferencia de archivos de un computador a otro a través de una red.

Token

Trama que contiene información de control. La posesión del token permite que un dispositivo de red transmita datos a la red.

Token Ring

LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo. Similar a IEEE 802.5.

Topología

Disposición física de nodos de red y medios dentro de una estructura de redes empresarias.

Topología de anillo

Topología de red compuesta por una serie de repetidores conectados entre sí por enlaces de transmisión unidireccionales para formar un bucle cerrado único. Cada estación de la red se conecta a la red a través de un repetidor. Aunque son anillos lógicos, las topologías de anillo a menudo se organizan en una estrella de bucle cerrado

Topología de bus

Arquitectura lineal de LAN en la que las transmisiones desde las estaciones de la red se propagan a lo largo del medio y son recibidas por todas las demás estaciones

Topología en árbol

Topología de LAN similar a una topología de bus, salvo que las redes en árbol pueden tener ramas con múltiples nodos. Las transmisiones desde una estación se propagan a lo largo del medio y todas las demás estaciones las reciben

Topología en estrella

Topología de LAN en la que los puntos finales de una red se encuentran conectados a un switch central común mediante enlaces punto a punto Una topología de anillo que se organiza en forma de estrella implementa una estrella de bucle cerrado unidireccional, en lugar de enlaces punto a punto.

TTL

Tiempo de existencia. Campo en un encabezado IP que indica el tiempo durante el cual un paquete se considera válido.

UDP

Protocolo de datagrama de usuario. Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP.

UIT-T

Sector de Normalización de la Unión Internacional de Telecomunicaciones(UIT-T) (anteriormente el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT)). Organismo internacional que desarrolla estándares de comunicación.

UNIX

Sistema operativo desarrollado en 1969 en los laboratorios Bell. UNIX ha pasado por varias iteraciones desde sus comienzos. Esto incluye UNIX 4.3 BSD (Distribución Estándar de Berkeley), desarrollado en la universidad de California en Berkeley, y UNIX System V, versión 4.0, desarrollado por AT&T.

WAN

Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por proveedores de servicio comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

WWW

World Wide Web. Red de servidores de Internet de gran tamaño que suministra hipertexto y otros servicios para terminales que ejecutan aplicaciones cliente tales como un navegador WWW.

X.25

Estándar de UIT-T que define cómo se mantienen las conexiones entre DTE y DCE para el acceso a terminales remotas y las comunicaciones entre computadores en las PDN Frame Relay ha reemplazado en cierta medida a X.25.

XNS

Sistema de red de Xerox. Conjunto de protocolo originalmente diseñado por PARC. Muchas empresas de networking para PC tales como 3Com, Banyan, Novell y UB Networks utilizaron o actualmente utilizan una variante de XNS como protocolo de transporte principal.

BIBLIOGRAFÍA

CISCO SYSTEMS
Programa de la academia de Networking de Cisco
CCNA
Semestre 1
V.2.1

CISCO SYSTEMS
Programa de la academia de Networking de Cisco
CCNA
Semestre 2
V.2.1

Diplomado de Telecomunicaciones
Redes de Datos
Alcatel University México
Tomo 1
Edición 0A
Marzo 2000

Alcatel University México
Diplomado de Telecomunicaciones
Redes de Datos
Tomo 2
Edición 0A
Abril 2000

REFERENCIAS:

www.redes.upv.es/LAR/lar2/default.htm

www.fact.cl/fact/seminarios/cursos/dc800.asp

www.informaticaintegrada.com.mx

www.cybercursos.net