ANEXO 9

Redes de Computadoras

A. 9. 1. Constitución de las LAN, MAN y WAN

En 1964 IBM lanzó al mercado un nuevo computador denominado Sistema 360. En realidad fue una familia formada por varios modelos solo compatibles entre sí. La arquitectura Sistema 360 evoluciona hasta desembocar en los grandes mainframes y da la pauta para poner las computadoras en red (1974). De allí, para liberarse de la hegemonía de IBM y de su protocolo SNA, crear las computadoras personales y las redes de datos (1980), faltó solo un paso. Luego vino el gran auge y jaleo de Internet (1990).

El tema de redes de datos, fue tratado en el desarrollo del curso, en este anexo se encaran los sistemas de redes de computadoras, desde el punto de vista de su funcionalidad y componentes. Dada la importancia actual del mismo y considerando que continuamente se le suman nuevos contenidos, se considera necesario hacer esta nueva exploración.

Repasemos, los conceptos de las redes de computadoras LAN, MAN y WAN, para posteriormente relacionar algunas de las definiciones de sus elementos constitutivos y en general aclarar algunos de sus términos más utilizados.

Una red formada por un conjunto de computadoras personales (PC), equipadas como estaciones de trabajo, con el objeto de compartir recursos e intercambiar información, se puede calificarse según su escala de extensión. Se define así, como red de área local LAN (Local Area Network), red de área metropolitana MAN (Metropolitan Area Network) o red de área amplia o extendida WAN (Wide Area Network).

Una LAN, consiste en una red privada que vincula dos o más computadoras y/o recursos compartidos, sobre distancias cortas. Es un medio para optimizar los recursos en espacio, tiempo, ancho de banda, etc., donde se intercambian distintas aplicaciones.

Esta interconexión facilita el acceso a la información desde nodos de red. Al disponer la implementación de la información y de su procesamiento distribuido, obtendremos grandes ventajas prácticas, en definitiva económicas. Al constituirse redes distribuidas, se pone la potencialidad de la computación mas cerca de los usuarios, en oposición a las primeras redes centralizadas que empleaban enormes computadoras (mainframes).

Dado que una LAN no esta conformada como una línea dedicada, que solo envía información en la manera de un direccionamiento y almacenamiento preestablecido, no es estrictamente una red de paquetes de datos. Así también, como una LAN incorpora la detección de errores con su retransmisión y la posible confirmación extremo a extremo, no se la puede considerar como red de conmutación de circuitos.

Una LAN opera en forma similar a un bus interno de una computadora, el cual es compartido por la CPU y varios dispositivos de entrada salida I/O (Input/ Output), que lo utilizan para transferir datos, desde y a una memoria principal.

Las LAN son redes que se extienden en una habitación, un piso, edificio o varios edificios como un campus universitario o área fabril, etc., pero siempre restringidas hasta un par de kilómetros.

Al estar delimitada la longitud máxima de un segmento de LAN, según el tiempo de transmisión de la peor ocurrencia, se evitan conflictos de la información emitidas, entre las unidades intervinientes. Al limitar y conocer la extensión máxima de la red se ve facilitada su administración, lo que simplifica su operación y abarata su gestión. La extensión máxima de una LAN se podrá extender a unos 2 Km, aunque con una red óptica y el empleo de FDDI podría alcanzar los a 200 Km.

Sin embargo para cubrir áreas de hasta una ciudad, se constituyen las MAN, las que están implementadas bajo el estándar, bus dual de cola distribuido DQDB. Las MAN no disponen de elementos de conmutación. Los elementos de conmutación son computadoras especializadas que selecciona y conecta una línea de salida, entre dos o más líneas de transmisión, cuando llegan datos por una línea de entrada.

Las LAN al estar optimizadas para operar sobre distancias de unos pocos kilómetros, pierden capacidad, velocidad y confiabilidad sobre distancias mayores. Los protocolos de las MAN están diseñados para tolerar las deficiencias de los protocolos de las LAN, pudiéndose operar en ambiente expandido mas allá de 50 Km.

En cuanto una LAN o una MAN se vincula con otras, situadas en distintas ciudades, de un mismo o distinto país, la llamaremos WAN. Las WAN pueden extenderse vinculando PC, LAN o MAN, hasta formar redes mundiales. Podrán emplear diversos sistemas de transmisión, referidos éstos al tipo de red empleado como soporte.

Una LAN está restringida en términos de velocidad de transmisión respecto a una WAN, en caso contrario, una WAN está más limitada respecto al tamaño de los paquetes. Con una LAN son posibles tamaños del orden de 1500 Byte, mientras que en una WAN son típicos los paquetes de 128 Byte. Estos paquetes son los referidos, tanto en las LAN como en las WAN, a los datos enviados por los usuarios, mas la información necesaria para la gestión de la red y los que permiten la correspondencia entre dispositivos emisores y receptores.

Los cableados se realizan mediante cables multipares de cobre trenzados denominados UTP, mientras que el mejor cableado troncal (backbone) tanto de las LAN, como en las MAN y las WAN se logra utilizando cables de fibra óptica. Solo en cortos tramos, derivaciones o acometidas se utilizan, denominados UTP, mientras que los cables coaxiales por su costo comparativo se han dejado de emplear.

Las redes LAN podrán utilizar cables de fibra óptica multimodo, por ser más fáciles de empalmar, mientras que las redes MAN deberán emplear fibras ópticas monomodo, utilizando la segunda y/o tercera ventana de transmisión.

A. 9. 2. Definiciones para las Redes de Computadoras

A modo de introducción, deberemos refrescar algunos conceptos esenciales al estudio de las redes de computadoras.

Logear, bootear, linkear

Diferentes términos de uso común en informática se han tratados de esclarecer hasta aquí, como ser servidor y Host. Otros muchos se dilucidarán en el transcurso del análisis que estamos efectuando. Sin embargo, varios términos son habitualmente usados por los analistas de sistemas y que se confunden en su aplicación. Los términos más comunes son derivados del idioma inglés y que en la práctica quieren significar, respectivamente:

"loguear - autenticarse al iniciar una sección indicardo el nombre de usuario (login).

"bootear" - reiniciar la computadora, hacer efectivo algún cambio de configuración.

"linkear" - conectarse a una máquina distante.

Networking

Se denomina networking a la gestión y operación del cableado de una red de datos.

Aplicaciones

Se denomina aplicación a un programa (software), por ejemplo un procesador de texto, como ser Word de Windows.

Recurso

Se denomina recurso a una base de datos o archivo, como un documento de textos, hojas de cálculo, gráfico, correo electrónico, etc.

Periférico

Dispositivos como un mouse, una unidad de disco duro o disquetera CD-ROM externa, una impresora, un joystick, un trazador (plotter), escáner, módem, etc.

Tanto los perisféricos, como las aplicaciones podrán ser utilizadas en exclusivo por una PC o compartidas en red.

Arquitectura de la red

Se denomina arquitectura de la red de datos, a la conjunción del concepto topología de red y al acceso al medio correspondiente. En ciertos casos, significa la conjunción de un interfaz entre capas y de un protocolo de cierto nivel de capa (protocolo de la capa n).

Estación de trabajo

Se denomina estación de trabajo (workstation, WS), a una PC equipada con un microprocesador, el que se utiliza para operar las aplicaciones en la red.

Protocolo

Un protocolo, es el conjunto de reglas que gobiernan la secuencia de los sucesos entre equipos del mismo nivel de esa arquitectura.

Host

Un Host (anfitrión) puede ser una computadora preparada como estación de trabajo o como un servidor. Genera o recibe paquetes, nunca encaminan paquetes destinados o provenientes de otros nodos. A los Host, se les conoce también como nodos Terminales, DTE en la terminología X.25, o sistemas Terminales en la terminología ISO. A diferencia de los Host, los nodos de tránsito como ser un Router, encaminan paquetes entre varios Host.

Los nodos de tránsito se los conoce como Routers, conmutadores en X.25, o sistemas intermedios en ISO.

Redes de difusión

Las redes de difusión trabajan bajo el principio de propagación colectiva. Son también redes de difusión las llamadas de multiacceso y las de recepción en competencia. Las redes de difusión podrán tener el carácter de estáticas o dinámicas para la asignación del canal a transmitir.

En el método estático, se divide el tiempo en intervalos discretos y se ajusta un algoritmo de asignación cíclica que fija el turno de transmisión. En el método dinámico, el mecanismo de arbitraje podrá ser centralizado o distribuido. En el arbitraje centralizado se toma la decisión de acuerdo a un algoritmo interno, mientras que en el descentralizado cada máquina decide por si misma si transmite o no.

Como todo sistema de difusión (broadcasting), en una LAN del tipo bus o en anillo, en cualquier instante una computadora puede transmitir, luego es necesario un mecanismo de arbitraje para resolver conflictos.

Sistema operativo de red, NOS

Las computadoras en red, para su conexión y operación, deberán disponer de un sistema operativo de red, NOS (Network Operation System). El NOS, consiste esencialmente en un sistema operativo de disco DOS (Disk Operating System), mas algún programa del tipo Windows Workstation.

El sistema operativo de red NOS, constituye el administrador principal de la red. El NOS que opera en el servidor, se comunica con los sistemas operativos de disco DOS, de las estaciones de trabajo, mediante un programa redireccionador de recursos y éste, hace considerar a las estaciones, que los recursos cedidos por el servidor pertenezcan a ellas. Por ejemplo, el programa Shell es un redireccionador de recursos.

La mayoría de los sistemas operativos NOS, tienen un sistema básico de entrada salida en la memoria de acceso RAM (Random Access Memory), como ser del tipo NetBIOS (Basic Input Output System), software original de IBM. Este programa de interfaz, obra entre el NOS del servidor y la placa interfaz adaptadora de red NIC (Network Interface Card), de una PC. El mismo permite que un programa de aplicación dado, pueda establecer una conexión, con otro programa distinto, a través de la red.

Las computadoras deberán estar interconectadas, por medio de estas placas interfaz de red NIC, en cada computadora y que contengan los programas controladores (driver).

Datos, paquete, trama y mensaje

Se refiere a transmisión de datos, como la transmisión de información, mas un encabezamiento, campos de direcciones, control de sincronismo, control de errores, etc.

En las computadoras habilitadas como estaciones de trabajo (workstation) y en los nodos de enrutamiento, cada mensaje de datos a transmitir, se organiza, emite y procesa en pequeñas unidades denominadas paquetes (Capa 3). Estos se podrían envían independientemente, pero formalmente forman tramas (Capa 2), que se transite en secuencias de bit (Capa 1).

Los paquetes están constituidos por pequeñas unidades de grupos de dígitos binarios, los que disponen de una cabecera que contienen las direcciones de origen y destino, señales de control y la carga útil (payload), donde radican los datos de información. Se denomina anidamiento o encapsulado, a un mensaje dentro de un paquete y éste dentro de una trama (Fig. 1).

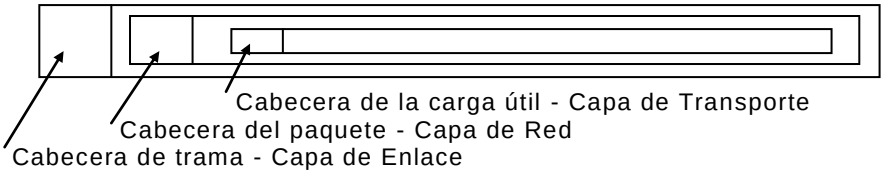


Fig. 1 - Anidamiento o encapsulado de una carga útil

Sistema de direccionamiento MAC

La dirección MAC, que posibilita en las redes LAN el direccionamiento de destino y de origen, son asignadas por el fabricante de tarjetas de red, según el registro de la OUI (Organizationally Unique Identifiers), organismo que distribuye los números de identificación de cada fabricante.

Este código del fabricante corresponde a los tres primeros Byte (24 bit) de la Dirección MAC, que consta de un total de 6 Byte (48 bit). Los últimos 3 Byte, a su vez, corresponden al número de máquina en particular, el cual el fabricante asignará por única vez a una máquina particular, grabando el número total de 6 Byte en el ROM de la tarjeta. Con este sistema, al menos en teoría, no existirían dos tarjetas de red en el mundo, con la misma Dirección MAC (existen más de 10^{14} posibilidades distintas). Esto hace que las direcciones MAC, sirvan para la identificación inequívoca de la estación a la cual se dirige una trama.

En caso de que se desee enviar tramas a varias estaciones simultáneamente (multicast), se reserva para ello una dirección MAC identificatoria del grupo, y en un caso más general, que la trama se desee difundir en forma generalizada (broadcast) se utiliza la dirección especial “todo unos” es decir, los 48 bit de la dirección de destino con valor 1. Esto hace que las estaciones recepcionen todos los mensajes cuya dirección MAC de destino sea, o bien la del receptor, o bien la dirección de Broadcast, en cuyo caso también los procesa.

Las direcciones MAC son también comúnmente llamadas *Direcciones Físicas*, en contraste con las direcciones asignadas en capas superiores, llamadas *Direcciones Lógicas*, como es el caso de las Direcciones IP.

Programas controladores (Driver)

Se denomina controlador (driver) al software que permite a un equipo funcionar con un dispositivo en particular, como ser un periférico (mouse, placa de red, micrófono, grabadora, disquetera, plotter, impresora, etc.

Los controladores de red proporcionan comunicación entre una placa de red y el redirector de red del equipo. La placa de red a su vez, proporciona un vínculo entre el equipo y el resto de la red.

Los controladores de placa de red residen en la subcapa inferior MAC, de la Capa 2, Enlaces y aseguran la comunicación entre el equipo y la placa de red. Durante la instalación los controladores se almacenan en el disco rígido del equipo, actuando en el sistema operativo. Los controladores de disco mas comunes son el de interfaz de sistema de pequeñas computadoras, SCSI (Small Computer System Interface) y el controlador con electrónica de dispositivos integrados, IDE (Integrate Dispositive Electronic).

El propósito tanto de la, especificación de interfaz de controlador de red, NDIS (Network Device Interface Specification), como del, interfaz abierta de enlace, ODI (Open Data link Interface), es estandalizar la interfaz entre drivers (controladores de red) y placas de red. De esta forma no se requiere drivers separados, para cada tipo de protocolo, que se desee ejecutar en la placa.

Redirector

El puerto de base de entrada / salida I/O (In/Out Port), especifica un canal a través del cual se transferirá la información entre el CPU de la computadora y algún elemento de su hardware como ser la placa de red. Un redirector es un software de red que admite peticiones de entrada / salida I/O (In/Out) para archivos o procesadores de mensajes a ser redirigidos a un servicio de red remoto.

La actividad de un redirector se origina en un equipo cliente, cuando emite una petición sobre un recurso o servicio de red, el redirector interpreta la petición y la reenvía hacia el propio equipo o hacia la red.

Dominio

Con dominio nos referimos a la agrupación lógica de equipos, dispuesta para simplificar su aplicación tanto en una red local, como para red mundial. Cada dominio dispone de por lo menos un servidor. Al establecer un primer servidor en un dominio se instala como, controlador principal de domino PDC (Principal Dominio Controlator). Tal PDC es responsable del mantenimiento de los usuarios, las directivas de seguridad e información general del dominio. Éste no solo contiene una copia maestra de la información del dominio y valida los usuarios, sino que actúa también como servidor de archivo, impresora, y aplicaciones.

Luego de instalar el primer controlador de dominio, los siguientes servidores a instalar en ese dominio, podrán tener el carácter simple de servidor y actuar como servidor de archivo, impresora y aplicación. Un dominio solo contendrá un PDC, sin embargo los servidores instalados subsecuentemente podrán tomar el carácter de, controlador de reserva del dominio BDC (Backup Dominio Controlator). Tal BDC recibe una copia directiva de seguridad (backup), también puede actuar como servidores de archivo, impresoras y aplicaciones. Es recomendable disponer en un dominio con por lo menos un BDC.

Los nombres de dominio se indican constituidos por sufijos después de la arroba @, de una dirección de e-mail (como ser yahoo o hotmail), luego su tipo (com u org). Por último podrá llevar la indicación del país (ar o uy), si no lleva tal indicación de país, corresponderá a USA.

Se podrán adoptar diferentes modelos básicos de configuraciones de redes LAN, utilizando cada uno distintos sistema operativo, tipo “Par a Par”, del tipo “Server Dedicado” o “Cliente–Servidor”.

Red de Par a Par

En la red del tipo Par a Par (igual a igual), los periféricos están distribuidos en todas las estaciones de trabajo. Cada equipo puede operar tanto como cliente o como server, según se requiera. Ninguno de ellos es el administrador responsable de toda la red. El modo par a par implica que, todas las computadoras poseen la misma jerarquía.

Al actuar cada estación de trabajo como cliente y servidor a la vez, cada equipo deberá disponer una parte importante de sus recursos, para actuar como servidor y a su vez soportar cada usuario remoto. Cada usuario organiza su propia seguridad, estableciendo una contraseña sobre un recurso dado. La red par a par, trabaja como un grupo pequeño de trabajo, no mayor de 10 equipos.

Es recomendable, si se prevé un cierto crecimiento, optar por una primer etapa con una red pequeña basada en un Servidor Dedicado, escenario más escalable.

Red con Servidor Dedicado

En el caso de red con Servidor Dedicado se dispone en la red de un server para el manejo exclusivo de los recursos. Mediante éste, todas las estaciones de trabajo podrán solicitar la utilización de cualquier recurso.

El server está constituido por una PC con una o más placas de red a ese fin. En un sistema operativo con Servidor Dedicado, una o más computadoras se reservan como servidor de archivo no pudiéndose utilizar estas para ninguna otra función.

Este servidor ejecuta el sistema operativo de red y brinda los servicios de gestión y protección de red a las otras máquinas, llamadas estaciones de trabajo o clientes, que podrán o no disponer de disco rígido. En esta red, un usuario se conecta desde su PC al server y accede a programas y archivos del mismo, envía el documento a su disco rígido y ejecuta estos programas en su propia memoria y con su propio procesador. El principal beneficio de una red con server dedicado, es proveer el control central de los recursos, disponer mayor seguridad y fácil mantenimiento de los programas.

Existen varios tipos de servers: de archivo e impresión, de aplicación, de correo, de fax, de comunicaciones, etc. que llamamos servers especializados. El software del server organiza los usuarios y equipos en grupos como dominios. Al iniciar un server, como ejemplo el Windows NT Server, éste crea una sesión de dominio, mantiene el plan de seguridad y una base de datos de seguridad maestra.

En muchos casos se podrá combinar ambos métodos, Red Par a Par y Red con Servidor Dedicado, manteniendo bases de datos poderosas para determinados trabajos y disponer de periféricos propios, para otras labores.

RED PAR A PAR Y RED CON SERVER DEDICADO

Red par a par	Red con server dedicado
Recursos distribuidos a bajo número de clientes	Recursos compartidos a gran número de clientes
Los usuarios verifican apropiadamente los datos	Se requiere seguridad sobre archivos distribuidos
Los usuarios poseen potentes estaciones	Se utilizan estaciones de bajos recursos

Red Cliente - Servidor

La configuración de Red Cliente-Servidor, hace referencia al concepto de compartir el trabajo en el proceso de administración y transferencias de datos, entre un equipo servidor y un equipo cliente.

En una configuración centralizada, un terminal envía una petición al sistema central, este obtiene la información y luego la presenta. Toda la base de datos puede ser transferida en fragmentos al terminal que efectuó la petición. Si la base de datos es grande ocuparía mucho tiempo la red. En el entorno de Red Cliente-Servidor, la consulta del cliente es procesada en el servidor y solo los resultados son enviados por la red al cliente. Esta filosofía se basa en un protocolo del tipo solicitud / respuesta, y en modo sin conexión.

En una configuración con respaldo distribuido BDD, se realizan fragmentaciones de las Tablas de Datos, los que se distribuyen en los servidores más utilizados. Esta última es una red de avanzada, actualmente con importante utilización. La ventaja de este sistema BDD, es disponer de mayor proximidad a los datos, mayor seguridad (se utiliza replicación) y mayor paralelismo en los procesos. Asimismo, por la propia naturaleza actual de las instituciones, los datos están cada vez más distribuidos geográficamente.

El lenguaje de consulta estructurado SQL (Structured Query Language), desarrollado por IBM en los años de 1970, es utilizado en esta configuración para consultas de bases de datos. Permite efectuar complejas operaciones sobre bases de datos, con el empleo de un número pequeño de comandos sencillos. Casi todos los sistemas de base de datos tipo cliente - servidor, están basados en SQL.

Líneas de petición de interrupciones, IRQ

En una computadora, las líneas de petición de interrupciones IRQ (Interrupt Request Line) son líneas del tipo hardware, que utilizan el teclado, discos o placas de red, para efectuar solicitudes al microprocesador del equipo. Cuando la placa de red desea una demanda a la computadora, envía una interrupción como signo electrónico del CPU.

Cada recurso de computadora debe utilizar un diferente impulso o línea de interrogación IRQ. Por ejemplo el IRQ7 para el puerto LPT1 o el IRQ13 para el procesador matemático. Estas líneas son especificadas cuando es configurado un dispositivo y tienen asignados, diferentes niveles de prioridad para cada petición.

Sistema de alimentación ininterrumpido, SAI

Se denomina, sistema de alimentación ininterrumpido (SAI), a un método externo y automático que evita al servidor y demás dispositivos que estén funcionando los efectos perjudiciales de un fallo de corriente. Proporciona a la red, una fuente de alimentación que utilizan los equipos durante un tiempo breve de seguridad para salvar los datos y un servicio seguro de administración de apagado del equipo. Los sistemas tolerantes a fallos ofrecen alternativas a la redundancia de datos, como ser:

a) Creación de bandas de disco, dividiendo los datos en bloques de 64 Kb/s y distribuyéndolos en iguales cantidades entre ellos,

b) Creación de espejo de disco, donde se duplica una partición y mueve los datos a otro disco físico que dispone de controlador ó

c) Reserva de sectores, donde se agrega automáticamente capacidades de recuperación de sectores.

Placas adaptadoras de red

La placa adaptadora de red, también llamada tarjeta adaptadora de red, es un interfaz entre el equipo y el cable o medio de enlace, que conforma la red. Toda computadora que se desee conectar a una red, necesita disponer de una placa de red. Ésta debe soportar un esquema de red específico como Ethernet, ArcNet o Token Ring.

La placa contiene el hardware y el firmware (software almacenada en una memoria de solo lectura), que implementan el, control de enlace lógico, LLC y el control de acceso al medio MAC del modelo OSI. La placa de red se instala en ranuras de zócalos denominados slots. Estos están provistos en la placa madre (motherboard), en el interior de la CPU, de una PC o servidor de red.

Las funciones de una placa de red incluyen: Preparar, enviar, recibir y controlar los datos, a y desde otro equipo. Cuando la placa de red desea una demanda de la computadora, envía una interrupción como signo electrónico del CPU. Cada recurso de computadora debe utilizar un diferente impulso o línea de interrogación IRQ, que es especificada cuando es configurado un dispositivo.

A. 9. 3. Modelos de Referencia

Los distintos modelos de las redes de datos han sido normados y publicados, por principales organismos rectores en el ámbito mundial, como ser la ITU, la ISO y el IEEE. Cada prototipo de arquitectura dispone diferentes niveles o capas, cada una con una serie de protocolos, para su intercomunicación y a la transmisión entre equipos. Las arquitecturas se definen de 3 niveles a 7 niveles, por ejemplo X.25 en 3 niveles, TCP/IP en 5 niveles y OSI en 7 niveles.

A. 9. 3. 1. Modelo ISO / ITU

En 1978 la Organización de Estandarización Internacional ISO (International Standard Organization), desarrolló el modelo de arquitectura de red, con la filosofía de aplicar los mismos protocolos y estándares, al uso de los dife-rentes fabricantes. En 1984 al publicarse una revisión del mismo se le denominó, Sistema de Interconexión Abierto OSI (Open System Interconnection).

El organismo Unión Internacional de Telecomunicaciones ITU (International Telecommunications Union) adoptó el estándar OSI, reestructurándolo y publicándolo como recomendación X.200. Esta norma considera la operatividad de los distintos elementos de red, mediante una estructura que define cada una de las distintas funciones de un sistema, constituidas en siete capas diferenciadas:

Capa 7, de Aplicación

Capa 6, de Presentación

Capa 5, de Sesión

Capa 4, de Transporte

Capa 3, de Red

Capa 2, de Enlace

Capa 1, Física

En el modelo original OSI no se especificó que servicio o protocolo exacto se debe usar en cada capa, solo se indicaba la funcionalidad de cada una de ellas, es decir lo que debe hacer cada capa. En estándares posteriores la ISO elaboró las normas respectivas para cada capa (Fig. 2).

Capa 7	Aplicación
Capa 6	Presentación
Capa 5	Sesión
Capa 4	Transporte
Capa 3	Red
Capa 2	Enlace
Capa 1	Física

Fig. 2 - Modelos de referencia OSI

La comunicación desde la máquina transmisora, comienza en el nivel superior Capa de Aplicación y llega a la capa inferior que emite el tren de bit hacia la red física. En concordancia, en la máquina receptora, comenzamos desde la capa inferior física llegando al nivel superior Capa de Aplicación. En el sistema todo sucede, como si cada capa del emisor se comunicara en forma virtual, con la capa del nivel equivalente en el receptor.

Mientras que los niveles superiores, definen como se tiene acceso a las aplicaciones a los servicios, los niveles inferiores definen el medio físico de la red y sus tareas relacionadas con ésta. Por ejemplo, como se colocan los bit de datos en la placa y cable de red. Cada capa (n) tiene como función primordial, proporcionar servicios de apoyo a la capa inmediata superior (n+1). El uso que la capa (n) haga de los servicios de su capa inferior (n-1), no afecta ni incumbe a su capa superior (n+1).

Una interfaz interactua entre dos capas adyacentes, mientras que un protocolo regla la comunicación entre las capas equivalentes de las máquinas emisoras y las capas de las máquinas transmisoras. Un interfaz pertenece al ámbito del hardware, mientras que un protocolo al ámbito del software.

Los datos pasan de un nivel de software a otro inferior. En cada nivel, el software agrega una dirección adicional al formato como cabecera del mismo, necesaria para su transmisión a través de la red. En el extremo receptor, cada nivel desglosa cada cabecera y pasa la información al nivel adyacente superior, llegando al nivel de aplicación, en su forma emitida original.

Capa 7, Capa de Aplicación - Sirve de ventana a los usuarios para que mediante sus programas de aplicación y el sistema operativo de red, tengan acceso a la misma. Soporta las aplicaciones del usuario, tales como el software para la transferencia de archivos, búsqueda de archivos en bases de datos o acceso al correo electrónico. Controla el acceso general a la red. Ejemplos de los protocolos de Capa de Aplicación son: CCITT X.400, X.420, X. 500, Telnet, FTP, HTTP y SMTP.

Capa 6, Capa de Presentación - Esta capa es responsable de la conversión de formatos de archivo, encriptado los datos, la traducción de códigos, convertir juegos de caracteres, compresión de textos, etc, presentándolos al usuario en la forma esperada. Determina el formato reconocido por la computadora para su comunicación. En el receptor, esta capa transforma este formato intermedio, en el utilizado por la correspondiente aplicación para aparecer en pantalla y/o ser impresa.

Se la reconoce con la función de redireccionador de entrada/ salida (I/ O), a efectuarse en un servidor. También provee los servicios de seguridad como encriptado de datos y la regla de transmisión de los datos, como ser la compresión de datos.

Capa 5, Capa de Sesión - Esta capa es la primera que es accesible al usuario. Permite establecer, ejecutar y finalizar una conexión, la que es llamada Sesión. Ejecuta el reconocimiento de nombres y funciones, como la de seguridad necesaria para permitir a dos aplicaciones comunicarse en red o los modos de transmisión (conmutación de paquetes, de circuitos, de área local o metropolitana, enlaces satelitales o terrestres.

Provee la sincronización entre usuarios. Efectúa el control dentro del flujo de datos, si la transmisión falla solo se tiene que retransmitir los datos posteriores a ese punto. También implementa el control del diálogo en el proceso de comunicación, regulando que extremo, cuando y por cuanto tiempo transmite. En un sistema multiusuario, esta capa se ocupa de ofrecer un punto de acceso al servicio SAP (Service Access Point) a cada usuario, para acceder al nivel de transporte.

Capa 4, Capa de Transporte - Esta capa se ocupa de comunicar directamente los nodos Terminales, extremo a extremo, gracias a los servicios obtenidos de la capa de red. Reúne varios mensajes cortos recibidos de la capa de sesión en un solo paquete o divide largos mensajes en varios paquetes, a fin de incrementar la eficiencia de la transmisión sobre la red. En el receptor, envía una señal de confirmación de la recepción del mensaje y lo ensambla a su formato original. Se proporciona también aquí el control de flujo. Además, los controles de errores para sistemas tales como ATM o Frame Relay, que lo han suprimido de sus capas inferiores.

Esta capa establece una conexión virtual, que asegura que los paquetes sean transmitidos libres de errores, en la secuencia correcta y sin pérdida o duplicación de los mismos. Por ello, este nivel trabaja normalmente orientado a la conexión como en TCP, sin embargo algunas veces se prefiere un servicio más sencillo, no orientado a la conexión y sin acuse de recibo como el UDP.

Este nivel, se encarga del tipo de conexión solicitada por la capa de sesión, sin errores manteniendo el orden de entrega o de datagrama, de broadcast, etc Para las conexiones múltiples, se encarga de multiplexarlas en la forma mas adecuada. Ejemplos de protocolos de la Capa de Transporte son: CCITT X.22 y para Internet: TCP y UDP.

Capa 3, Capa de Red - Se encarga de llevar los grupos discretos de bit, formados en paquetes, desde el origen hasta el destino, pasando por los distintos enrutadores. Los paquetes tienen tamaños variables, pudiendo llegar a ser muy elevados, sobretodo en los recientes protocolos, para poder aprovechar eficientemente la elevada velocidad de los nuevos medios de transmisión (fibra óptica, ATM, etc). Mientras que en TCP/IP el tamaño máximo de paquetes es de 64 KBytes, en el nuevo estándar IPv6 puede llegar a 4 GBytes (4 294 967 296 Bytes).

Controla y garantiza la direccionalidad lógica de paquetes, dentro del encaminamiento topológico de la red. Determina la ruta entre segmentos de red, basándose dinámicamente en la prioridad del servicio y condiciones de la red. Administra problemas de tráfico sobre la red, según el estado de conmutación de los paquetes, enrutamiento y congestión de datos. También de la contabilidad del tráfico, para la facturación de servicios según los datos recibidos. En caso de ofrecer servicio con QoS garantizado, se encarga de la reserva de los recursos necesarios

Si la estación de destino indica que no puede recibir los datos por su gran tamaño, la estación de emisión rompe los paquetes en unidades mas pequeñas. La estación de destino reensambla los datos a su tamaño original. Para las redes broadcast al no tomarse decisiones de encaminamiento, las funciones de esta capa son casi inexistentes. Ejemplos de protocolos de la Capa de Red son: el IP (Internet Protocol), CCITT: X.25 y X.75, ITU-T: Q.931, Q.933 y el OSI: CLNP (Connection Less Network Protocol).

Capa 2, Capa de Enlace - Facilita el intercambio de datos, para lograr una comunicación confiable y eficiente. En la máquina emisora, toma la información en formación de paquetes desde la Capa de Red, organizándolos en tramas (frames) que envía virtualmente a la máquina receptora. Una trama es una organización de datos con estructura lógica. En realidad, la trayectoria efectiva es hacia su capa inferior, la Capa Física y de allí al medio físico. El tamaño de una trama es desde unos pocos cientos hasta unos pocos miles de Byte. Para Ethernet tiene un tamaño desde 64 Byte a 1518 Byte, mientras que en Token Ring podrá tener de 5000 a 20 000 Byte.

Se emplean mecanismos de regulación del flujo de tráfico y define el espacio de almacenamiento temporal (buffer) necesario. Si un paquete recibido de la capa superior es mayor que el tamaño de trama permitido para esa comunicación la fragmente al tamaño conveniente.

En redes broadcast, el control de acceso al medio de transmisión compartido, se realiza por la subcapa inferior MAC (Media Access Control), mientras que la subcapa superior LLC (Logical Link Control) cumple la función de la capa de enlace para las líneas punto a punto.

Este nivel es responsable de la transferencia de las tramas de datos libre de errores. Luego del envío de la trama, se espera por la señal de reconocimiento emitida por el receptor. Esta señal será emitida al recibirse la trama y solo si no se detecta algún problema o error en la misma. Si una trama no ha sido recibida correctamente, no es confirmada, por lo que esta capa se encarga de enviarla nuevamente. También detecta las tramas recibidas duplicadas.

Ejemplos de protocolos de Capa de Enlace son, del CCITT el X.25, RDSI, LAP-D (Link Access Procedure-D); de la ISO el HDLC (Hight level Data Link Control); de la IBM el SDLC (Synchronous Data Link Control). Protocolos de la subcapa MAC son de la IEEE el 802.3 Ethernet, el 802.5 Token Ring y de la ISO el 9314 FDI. Protocolo de la subcapa LLC es el IEEE 802.2.

Capa 1, Capa Física - Es responsable del envío del flujo de bit, o sea pulsos eléctricos o de luz y su representación en ceros y unos, desde una computadora a otra. Define los bit de codificación y sincronización, voltajes permitidos, como son recibidos los bit, la formación del pulso, su duración en mseg, la velocidad adecuada para el tipo de cable de red, radio o satelital, utilizado y el tipo de transmisión empleado. Estos bit, representan los datos propiamente dichos, más los correspondientes al direccionamiento y al control.

En Capa 1, se define las características mecánicas del conector, como el cable es terminado en la placa de red, cuantos contactos (pines) tiene el conector y las funciones de cada contacto. Muchos de los protocolos de la Capa Física se refieren a la interfaz a un módem: EIA RS-232, EIA RS-449, CCITT X.21, X.21 bis y V.35.

Concepto del modelo OSI

El concepto del modelo OSI es que, en el extremo emisor, los datos pasan de un nivel de software a otro inferior, conformándolos en una unidad de información denominada paquete. En cada nivel, el software agrega una dirección adicional o formato al paquete y trama, necesaria para su transmisión a través de la red. En el extremo receptor, cada nivel desglosa la dirección y pasa la información al nivel adyacente superior, llegando los datos al nivel de aplicación en su forma emitida original.

Mientras que las tres capas inferiores establecen comunicación entre las máquinas adyacentes, es decir entre equipos vinculados directamente por algún medio físico o inalámbrico, las cuatro capas superiores ejercen el proceso administrativo interno y establecen una vinculación lógica extremo a extremo (Fig. 3).

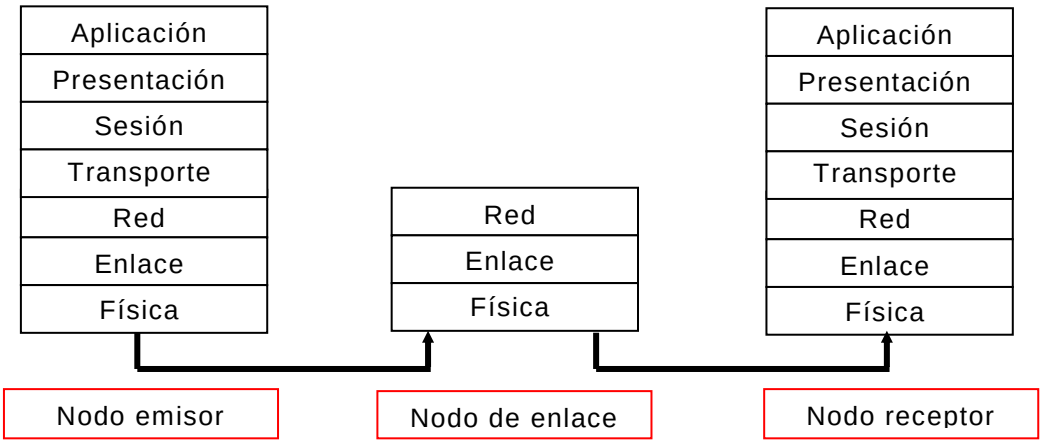


Fig. 3 - Comunicación entre las máquinas adyacentes

Símil correspondencia postal

Analicemos la funcionalidad asignada a cada capa mediante un ejemplo símil, de dos ejecutivos que hablan diferentes lenguas y viven en diferentes países. Uno es Presidente de una compañía alemana y desea mandar una nota de agradecimiento, al Director de Ventas de una firma en Japón. En primer lugar transmite su inquietud al Director de Relaciones Públicas de la empresa, acción que corresponde al Nivel de Aplicación (Capa 7). La secretaria de Relaciones Públicas, escribe en idioma japonés en formato carta, acción del Nivel Presentación (Capa 6).

El asistente de secretaría registra el documento a enviar y escribe el sobre de la carta, Nivel Sesión (Capa 5). El encargado de la correspondencia saca las copias necesarias, ensobra la carta u asigna un número de envío, Nivel Transporte (Capa 4). Luego establece el contacto con la oficina de distribución de correspondencia en Japón, con lo que queda establecido la ruta y destinos intermedios, Nivel Red (Capa 3).
En la sala de correos se pesa la correspondencia y se asigna indicativo en las bolsas de destino común, Nivel En lace (Capa 2). Por último se la despacha en camión, barco, etc., con sus destinos intermedios, Nivel Físico (Capa 1).

En el Japón se desarman las bolsas, para separar la correspondencia de cada destino y se encamina a la dirección de destino, en proceso inverso al del envío.

Trama OSI

El modelo OSI también regula como los datos son tratados por las capas, desde la emisión de la aplicación, en la red y hasta la aplicación de destino. Los datos podrán forman archivos grandes que al ser enviarlos por la red la saturarían imposibilitando la correcta comunicación de las restantes máquinas y de ella misma.

Este problema se subsana creando tramas de datos, con longitudes acordes a los requerimientos de la red.

De tal forma en este esquema las tramas transmitidas tienen ciertos componentes agrupados como encabezado, con la dirección de destino, de remitente y de control. Luego se transmiten los datos propiamente dichos y por último como cola, el protocolo de detección y corrección de errores surgidos en la transmisión, como ser el código de redundancia cíclica CRC (Cyclic Redundance Code).

Este código se corresponde a un algoritmo algebraico originado por el dispositivo transmisor y luego decodificado por el receptor, para la detección de errores, el que dispone de un buen porcentaje de efectividad (Fig. 4).

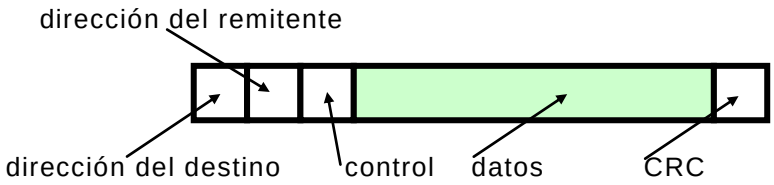


Fig. 4 - Trama OSI

La transmisión de la información virtual entre las mismas entidades (capas) de dos máquinas, se realiza transmitiendo entre capas la información como carga útil (payload, P).

En el emisor el pasaje entre las capas, implica el agregado de una información de "cabecera" (header, h), para el encaminamiento de la carga útil, y en Capa 2 de la información de "cola" (trailer, t), para el reconocimiento y corrección de errores. En el receptor, esta información extra es eliminada en el pasaje entre capas (Fig. 5).

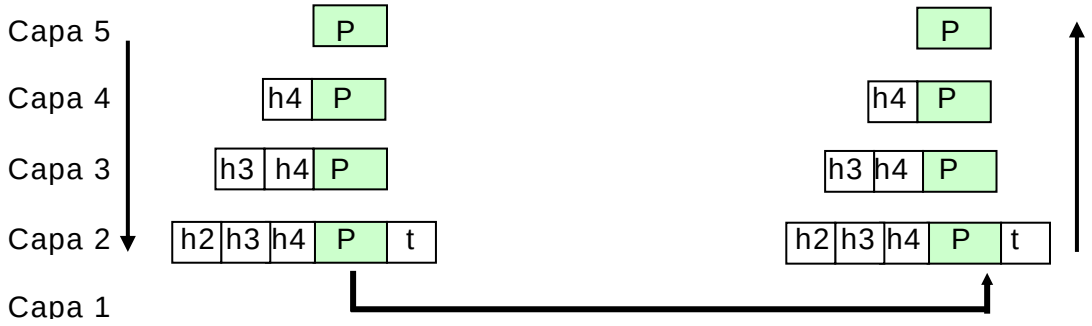


Fig. 5 - Flujo de información entre dos máquinas

A. 9. 3. 2. Modelo IEEE

El IEEE (Institute of Electrical and Electronics Engineers), ha publicado en febrero de 1980, su especificación internacional referida a las redes de datos, llevando el número 802. Este número fue establecido según su año (80) y mes de emisión (2).

Tales normas, cubren ciertas faltas de la norma ISO original, que no preveían su uso para redes del tipo broadcast. Divide la Capa 2 (Enlace) en dos subcapas, redefiniéndola según dos subcapas: el subnivel inferior, control de acceso al medio MAC (Media Acces Control) y el subnivel superior, control de enlace lógico LLC (Logical Link Control) (Fig. 6).

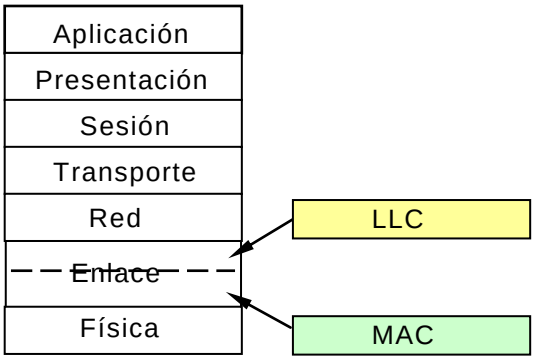


Fig. 6 - Modelo IEEE con subcapas LLC y MAC

La subcapa inferior MAC, se encarga de controlar el acceso compartido de las placas de red a los equipos de nivel físico. Este subnivel se comunica directamente con la placa de red y es la encargada que solo un dispositivo a la vez, pueda acceder al medio para la transmisión y entrega de datos. Además salva de errores a la red entre equipos.

La subcapa superior LLC, corresponde a las funciones comunes de la capa de enlace, administra el establecimiento, mantenimiento y terminación de un enlace punto a punto y define el uso de interfaz lógica llamados, puntos de acceso al servicio SAP (Service Access Point). Esta subcapa LLC, es la responsable de transferir esta información a las capas superiores. Las direcciones SAP son las direcciones del destinatario.

La subcapa LLC suministra tres tipos de servicio: de datagrama sin acuse de recibo, de datagrama con acuse de recibo y los orientados a la conexión. Este subnivel LLC, de la norma 802.2 del IEEE, incluye a su vez a las normas 802.3 (Ethernet), 802.4 (Token Bus) y 802.5 (Token Ring).

Los servicios cubiertos por LLC responden a los modos: Clase 1 (sin conexión/ sin reconocimiento), Clase 2 (orientados a la conexión) y Clase 3 (sin conexión/ con reconocimiento).

En esta norma se especifica el uso de distintos tipos de cables: pares trenzados sin blindar UTP (Unshielded Twisted Pair); pares trenzados blindados STP (Shielded Twisted Pair); tipo coaxial o cables de fibras ópticas. Así también diversos tipos de conectores, BNC, RJ-45, ó AUI. Estos componentes son tratados en detalle en los anexos correspondientes.

A. 9. 3. 3. Modelo TCP/IP

En diciembre de 1969, esta red denominada ARPANET, entró en funcionamiento con cuatro nodos ubicados en distintas universidades. El DoD creó para ese entonces, un comité con el mandato de supervisarla, al que se le denominó Consejo de Actividades de Internet IAB. Este organismo creaba los estándares que eran implementados por los recientes graduados de las universidades adheridas.

En diciembre de 1969, esta red denominada ARPANET, entró en funcionamiento con cuatro nodos ubicados en distintas universidades. El DoD creó para ese entonces, un comité con el mandato de supervisarla, al que se le denominó Consejo de Actividades de Internet IAB. Este organismo creaba los estándares que eran implementados por los recientes graduados de las universidades adheridas.

La red, ya en 1972 contaba con 34 nodos, que cubrían el territorio de USA. Pronto se estableció una red de radio terrestre y satelital. (Ver Capítulo 2 Evolución de las redes).

Este modelo se definió en 1974 y se le da una nueva perspectiva en 1985. Al igual que el modelo OSI se basa en la interación de un gran número de protocolos independientes.

El Departamento de Defensa de USA, procuró que sus comunicaciones permanecieran intactas aún cuando los nodos intermedios sufrieran un ataque y dejasen de funcionar. Estos requerimientos condujeron a la red ARPANET, una red de conmutación de paquetes.

En sus comienzos funcionaba sobre líneas directas, rentadas a la red telefónica existente. Por ello se empleaban las líneas multipares y los canales de radio terrestre y satelitales de múltiples redes. Esta interconexión a variadas redes trajo problemas para interactuar entre ellas. Se diseño entonces un conjunto de protocolos que salvasen estos problemas.

Las Capa Física y de Enlace, permiten su conexión con el empleo de varios estándares de las LAN aparte de la ARPANET. Las diferentes partes de una interred pueden tener disímiles topologías, anchos de banda, retardos, tamaños de paquetes y demás parámetros.

Al reunir diferentes estándares LAN, e incluso con diferentes estándares MAN y WAN, se forman complejas interredes. Por ello, la Capa Interred define un protocolo de interred IP (Internet Protocol). Su función es entregar los paquetes IP donde corresponda y evitar la congestión, sin importar los tipos de redes que atraviese.

El modelo TCP/IP se diferencia del modelo OSI, en la cantidad empleada de niveles y de las funciones asignadas a cada uno de ellos.

La Capa 1, de Acceso a la Red de este Modelo TCP/IP, se corresponde con la Capa Física y la Capa de Enlace del Modelo OSI, también la Capa Interredes tiene cierta relación con la Capa de Red, al igual que la Capa de Transporte con su similar del modelo OSI. Esto no significa que las funciones y delimitaciones no siempre puntualmente coincidentes (Fig. 7).

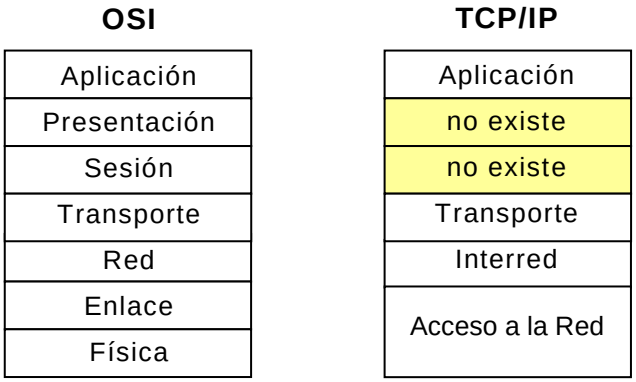


Fig. 7 - Modelos TCP/IP y ISO

En la Capa de Transporte actúa el, protocolo de control de la transmisión TCP (Transmission Control Protocol). Este protocolo orientado a la conexión, fragmenta los Bytes entrantes en mensajes discretos que entrega ala Capa de Interred. También efectúa el control de flujo ente emisor y receptor.

Esta capa dispone también del Protocolo de datagrama de usuario UDP (User Datagrama Protocol). Es un protocolo sin conexión, para aplicaciones que no requieran la asignación de secuencia, ni el control de flujo. Por ello es aplicable a transmisiones de voz o video, donde la entrega pronta es más importante que la entrega precisa.

La IEEE en sus subcomités 802.1p y 802.1Q estudia un mecanismo para etiquetar tramas de forma que pueda determinarse prioridades según la clase de servicio deseada.

En el modelo TCP/IP, no se dispuso Capa de Sesión y Capa de Presentación, pues se consideró innecesarias. La Capa de Aplicación contiene todos los protocolo de aplicación, como ser: correo electrónico (SMTP), terminal virtual (Telnet), transferencia de archivos (FTP), servicio de dominio (DNS) y recuperación de paginas Web (HTTP).

A. 9. 3. 4. Modelo Novell

La empresa Novell, previo al modelo OSI, ya había estructurado un modelo que llamó Net Ware. Este, tuvo la finalidad de posibilitar a grandes empresas emplear redes de PC en uso Cliente-Servidor, compartiendo archivos y aplicaciones, reemplazando a sus enormes mainframes.

La pila de protocolos en que se basa Net Ware es una versión modificada del XNS (Xerox Network System) y con un cierto parecido al protocolo TCP/IP (Fig. 8).

<table>
<tr><td>SAP</td><td colspan="3">Servidor de archivos</td></tr>
<tr><td colspan="2">NCP</td><td colspan="2">SPX</td></tr>
<tr><td colspan="4">IPX</td></tr>
<tr><td>Ethernet</td><td>Token Ring</td><td colspan="2">ARCnet</td></tr>
<tr><td>Ethernet</td><td>Token Ring</td><td colspan="2">ARCnet</td></tr>
</table>

Fig. 8 - Modelo Net Ware de Novell

La Capa Física y la Capa de Enlace permiten su conexión a varios estándares de la industria que incluye a Ethernet de DIX (Digital Intel Xerox), Token Ring de IBM y ARCnet de Datapoint Co.

La Capa de Red emplea el protocolo sin conexión denominado, intercambio de paquetes entre redes IPX (Internet Packet Exchange/Sequence Packet Exchange), de transferencia de paquetes. Es un protocolo no fiable, orientado a sin conexión (Fig. 9).

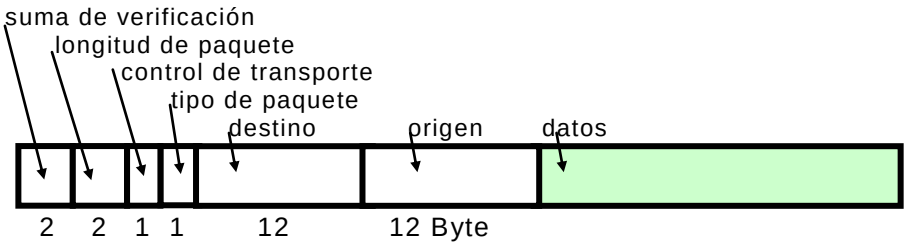


Fig. 9 - Paquetes IPX

En conjunto con el IPX de la Capa de Red, actúa en la Capa de Transporte el, protocolo central de red NCP (Network Core Protocol) orientado a la conexión, que junto al denominado, intercambio de paquetes secuenciados SPX (Sequence Packet Exchange), proporcionan servicio de transporte de datos de usuario.

El Modelo Novell no posee capas de Sesión y Presentación. La Capa de Aplicación contiene al, protocolo de publicidad de servicio SAP (Service Advertising Protocol). Éste emite cada minuto un paquete que indica los servicios que ofrece.

A. 9. 4. Topologías de las Redes de Computadoras

Se entiende por topología la conformación física de una red, considerando su tipo de conexionado. Cada topología toma en cuenta la capacidad de información a manejar y los sistemas operativos mas convenientes.

Tal configuración podrá tomar la forma: a) bus lineal, b) de estrella, c) de árbol, d) anillo o sus combinaciones. (Fig. 10).

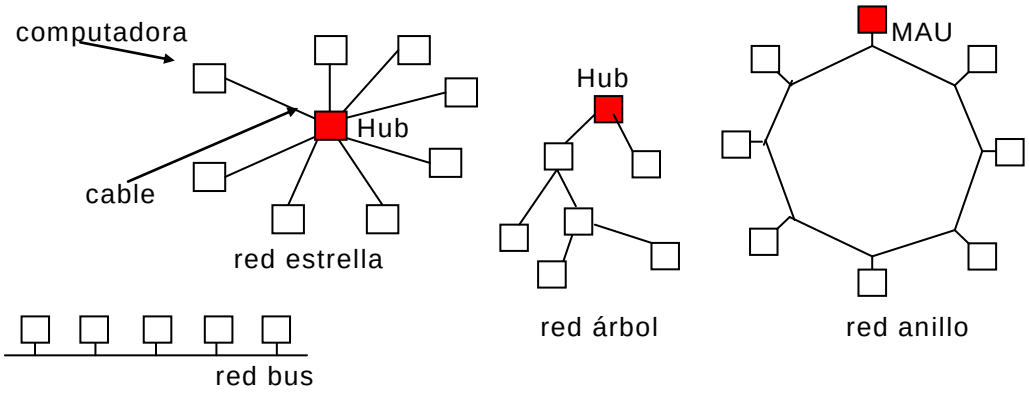


Fig. 10 - Redes de difusión de topología disímiles

Topología Bus

No se establece una mensura estándar de la influencia del número de equipos a conectar en Bus, sin embargo a mayor cantidad será más lenta la operación en la red. Su número varía de acuerdo a numerosos factores de la red:

- Capacidad de hardware de los equipos.
- Cantidad de veces que los equipos transmisión datos.
- Tipos de aplicaciones que se ejecutan.
- Tipo de cables utilizados.
- Distancia entre los equipos.

Para hacer que la transmisión de datos no se refleje en cada equipo, afectando la comunicación en red, debe adaptarse mediante el uso de terminación de red. La ampliación de este tipo de red se realiza mediante conectores apropiados a cada tipo de cable utilizado, como ser el tipo BNC. En caso de tramos extensos se emplean repetidores, los que regeneran las señales

En esta topología, para el caso de desconectarse un extremo, al producirse reflexiones, se interrumpe toda la actividad de la red.

La topología bus podrá tomar el carácter de tipo Bus Regular ó de Bus Local: En Bus Regular, las computadoras preparadas como estación de trabajo WS (workstation) son conectadas mediante transceptores y cables de derivación a un cable coaxial del tipo grueso (thicknet). Esta topología se emplea en las redes Ethernet 10Base-5.

En Bus Local, las workstation están vinculadas entre sí, mediante cables coaxiales del tipo fino (thinnet) y conectores BNC. Estas topologías se emplean en las redes Ethernet 10Base-2.

En estas redes Bus la fiabilidad depende de la continuidad del cable coaxial, sobretodo en la topología Bus Local ya que el coaxial fino se conecta directamente a cada computadora, por lo cual los usuarios pueden interrumpir accidentalmente su conexión.

Este problema se evita conectando todas las máquinas a un concentrador (Hub), conformando una topología física en estrella. No obstante este conexionado, la conformación lógica en Bus se puede mantener mediante software. El concentrador Hub dispone de relevadores de derivación (bypass) sustentados por cada workstation. Si una conexión individual falla, el relevado cortocircuita su conexión restableciendo la topología general.

Una estructura en Bus podrá tomar el carácter de topología pasiva o activa. En la pasiva, los equipos no son responsables de mover los datos de un equipo a otro. Si un equipo falla no afecta al resto de la red. En la topología activa los equipos regeneran las señales y pueden mover los datos a través de la red.

Topología Estrella

En la estructura en Estrella, todos las workstation se conectan a un equipo concentrador Hub, el que recibe las señales y las reenvía a toda la red. Esta conformación ofrece la posibilidad de tener administración y recursos centralizados. En caso de fallar el equipo central, se interrumpe toda la actividad de la red. Sin embargo al cortarse un segmento o falla un equipo, solo este tramo es afectado, el resto puede funcionar normalmente.

Se tienen los Hub pasivos y activos. Un Hub activo puede transmitir señales a cables de mayor longitud que alimenten otros Hub más pequeños, conformando así una red combinación de varias estrellas con distintas jerarquías. El sistema de arquitectura de red SNA (System Network Architecture), diseñado por IBM, dispone esta topología.

La filosofía de SNA se basa en dar acceso al usuario, desde un terminal "tonto" a una computadora central (mainframe), mediante una red de estructura fuertemente jerárquica. Una configuración típica SNA comprende cuatro niveles diferentes, entre el Terminal y el Mainframe.

También se podrá conformar una topología física en estrella, con topología lógica en anillo. Ello se aplica en las redes Token Ring. También aquí se emplean los relevadores como bypass restaurando el anillo en caso de una falla de conexión en una máquina en particular.

Topología en Anillo

En la estructura en Anillo, se conectan los equipos formando un círculo, sin necesidad de terminadores de red. En este caso cada equipos actúa como repetidor. En caso de falla en un equipos afectará a toda la red.

En las topologías tipo anillo se emplean concentradores de acceso múltiple, denominados MAU (Multistation Access Unit). Para la formación de la red anillo, se puede emplear tanto par trenzado, coaxial o fibra óptica. Estas topologías se emplean en las redes Token Ring, que veremos mas adelante.
Las redes de Token Ring de IBM, disponen concentradores /repetidores de acceso multiestación de fibras ópticas, con interfaz para datos distribuidos por fibra FDDI (Fiber Distributed Data Interface) y derivaciones en par trenzado. La topología física podrá ser del tipo estrella, aunque su topología lógica mediante software será en anillo.

Topología Bus en Estrella

En la estructura en Bus en Estrella, hay varias redes en topología en estrella conectadas en comunicación de bus lineal. Si un equipo falla no afecta al resto de la red. Si falla un concentrador se incomunican solo los equipos conectados directamente a él. En caso de un concentrador central se interrumpe todas las conexiones (Fig. 11).

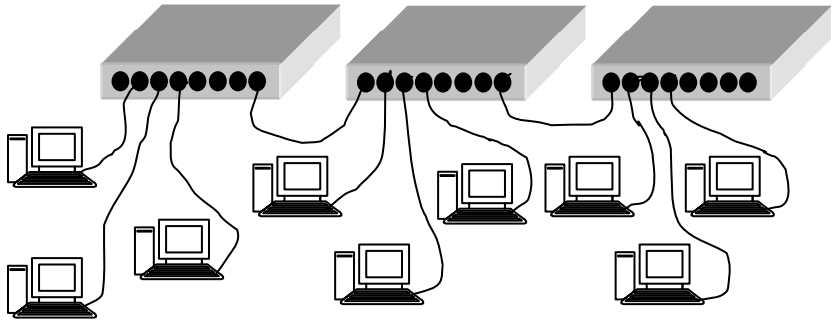


Fig. 11 - Red Bus en Estrella

Topología Anillo en Estrella

La topología Anillo en Estrella, también llamado anillo cableado en estrella, dispone un concentrador que configura un anillo (Fig. 12).

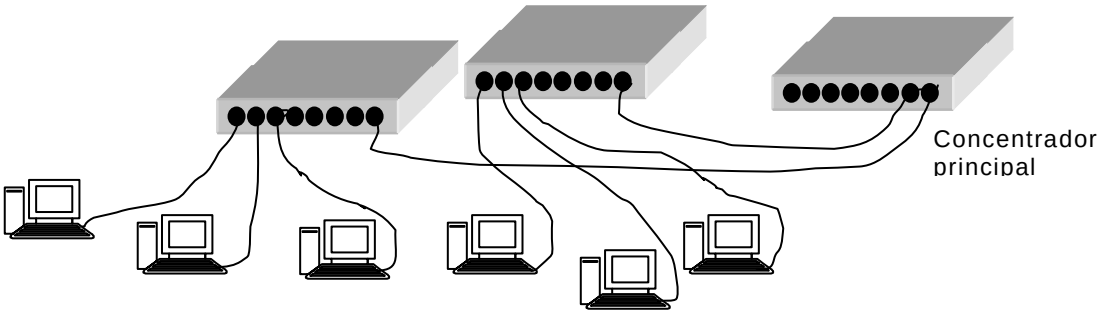


Fig. 12 - Topología de Anillo en Estrella

A. 9. 5. Sinopsis de los Protocolos

Se denomina protocolo, a la serie de reglas y procedimientos utilizados para comunicarse entre un mismo nivel de capas de distintos equipos interconectados. Cada nivel tiene su propio conjunto de reglas. Cada protocolo puede dividir los datos en paquetes, agregar información de secuencia, sincronización y comprobación de errores. Un equipo que utilice un tipo de protocolo, no será capaz de comunicarse con otro equipo que utilice otro.

Los protocolos se pueden diferenciar en enrutables o no enrutables. Se denomina protocolo enrutable, al protocolo que disponga de la habilidad de enrutar los datos fuera de una LAN.
Esta cualidad agrega complejidad al protocolo y sobrecarga al controlador (driver) del protocolo. Los driver de protocolo no enrutables son mas simples, pequeños y rápidos. Protocolos enrutables son el TCP, IP, XNS, SPX, IPX y el DDP de AppleTalk. Como no enrutable está el controlador de protocolo de Microsoft, NetBEUI y LAT de Digital.

Existe una gran de variedad de protocolos, cada uno con distinto propósito y cualidad.

Pueden funcionar en distintos niveles de un estándar dado, como por ejemplo el OSI (Open Systems Inteconnect) de la ISO (International Standard Organization) y también actuar en un conjunto a lo que se llama pila de protocolos. Una pila (stack), es un grupo coordinado de protocolos que utiliza una determinada arquitectura en todas sus capas (pila OSI, SNA, TCP/IP, etc).

Los protocolos y las placas de red se pueden combinar y asignar según se necesiten. Por ejemplo dos pilas de protocolo como IPX/SPX y TCP/IP pueden estar enlazadas en una placa o a dos placas de red. El orden de enlace determina la sucesión en que el sistema operativo ejecuta el protocolo. Si hay múltiples protocolos enlazados a una única placa, el orden de enlace indica en que secuencia se utilizarán los protocolos para intentar una conexión.

Existen pilas como modelos estándar de protocolos, tales como el ISO de OSI, el SNA de IBM, el DECnet de Digital, el Net Ware de Novell, el AppleTalk de Apple y el TCP/IP de Internet. Los protocolos se establecen para cada nivel, pudiendo definirse en grupos de niveles, como: a) de aplicaciones, b) de servicios de transporte, c) de servicios de red, d) a nivel físico.

a) Protocolos de aplicaciones

Los protocolos de aplicaciones funcionan en el nivel superior de un estándar y proporcionan la interacción entre las aplicaciones y el intercambio de datos. Por ejemplo:

X.500 - UIT-T, para servicios de archivo y de directorio sobre varios sistemas,
X.400 - UIT-T, para transmisiones internacionales de correo electrónico, MHS,
SMTP - de Internet, para transferir correo electrónico,
FTP - de Internet, para transferencia de archivos,
SNMP - de Internet, para controlar redes y componentes de redes,
Telnet - de Internet, para sesión de Host remotos y procesar datos localmente,
SMB - de Microsoft e intérpretes de comandos,
NCP - de Novell e intérpretes de comandos,
AFP - de Apple, ingreso remoto a archivos (login).
AppleTalk y Apple Share - para redes Apple,

b) Protocolos de transporte

Los protocolos de transporte proporcionan las sesiones de comunicaciones entre distintas computadoras. Por ejemplo:

TCP - entrega garantizada de datos secuenciales,
UDP - no orientado a la conexión y sin acuse de recibo.
NWLink - desarrollo de Microsoft del IPX/SPX,
IPX - parte de IPX/SPX, encaminamiento y reenvío de paquetes de Net Ware,
ATP - de sesiones de comunicaciones y transporte de Apple.
NetBEUI - servicios de transporte para las sesiones y aplicaciones NetBIOS,

c) Protocolos de red

Los protocolos de red proporcionan los servicios de vínculo. Controlan la información y encaminamiento, comprobación de errores y petición de retransmisiones. Por ejemplo:

IP - encaminamiento y reenvío de paquetes,
SPX - parte del IPX/SPX, de Novell para datos secuenciales,
NWLink - desarrollo de Microsoft del protocolo IPX/SPX,
DDP - protocolo de transporte de datagramas de AppleTalk.

d) Protocolos de enlace

X.25, RDSI y LAP-D (Link Access Procedure-D), del CCITT
HDLC (Hight level Data Link Control), de ISO
SDLC (Synchronous Data Link Control), de IBM
Ethernet 802.3 y Token Ring 802.5 en Subcapa MAC, de IEEE
Ethernet 802.2 en capa LLC, de IEEE.

e) Protocolos a nivel físico

El IEEE, ha tratado al nivel físico, los protocolos para los sistemas:

802.1 - arquitectura, puentes, VLAN,
802.2 - LLC (Logical Link Control),
802.3 - CSMA /CD (Ethernet),
802.4 - Token Bus,
802.5 - Token Ring,
802.6 - DQDB,
802.7 - redes de banda ancha,
802.8 - redes de fibra óptica,
802.9 - ISO-Ethernet,
802.11 -redes inalámbricas,
802.12 -100VG-AnyLAN,
802.14 -para CATV.
802.1D - puentes transparentes
802.1p -filtrado según clase de tráfico
802.1Q - puentes en VLAN
802.3u -Fast Ethernet
802.3x -Ethernet Full Duplex
802.3z -Giga Ethernet
802.3ab - Giga Ethernet con cable UTP-5

A. 9. 6. Control de Acceso al Medio

Las redes de difusión, también llamadas de multiacceso, al trabajar bajo el principio de competencia, deben disponer de un elemento de control que ordene el acceso al canal. El conjunto de reglas que definen, como tomar los datos de la red y como disponer una combinación de datos en una red, se denomina Control de Acceso al Medio.

La idea básica de estos métodos, es aplicable a cualquier sistema en que usuarios no coordinados, compiten por el uso de un solo canal compartido. Si se envían datos desde un usuario o desde un servidor a otro, debe haber un procedimiento para que los datos tengan acceso al cable sin interferir con otros datos. Asimismo, se debe tener el acceso a los datos con la seguridad de que no se hallan producido errores durante la transmisión.
Si distintos equipos utilizan métodos de acceso diferentes, la red fallaría por dominio de algún método sobre otro. Por ello, los métodos de acceso a utilizar, deberán ser coherentes entre sí. Los métodos de acceso aseguran que solo un equipo pueda poner los datos en el cable en un determinado momento y hacer que el envío y recepción de los datos se realice en forma ordenada.

Los protocolos empleados para establecer quien tomará primero el acceso al medio, pertenecen a la subcapa inferior de la Capa 2, de Enlace. Esta subcapa se denomina, control de acceso al medio MAC (Medium Access Control).

Si se envían datos desde un usuario a otro, o desde un servidor a un usuario, debe haber un procedimiento para que:

- Los datos tengan acceso al cable sin interferir con otros datos
- El equipo tenga acceso a los datos con la seguridad de que no se hallan producido errores por colisión durante la transmisión

Si distintos equipos utilizan métodos de acceso diferentes, la red podrá fallar por el dominio de algún método sobre otro, por ello, los métodos de acceso a utilizar, deberán ser coherentes entre sí.

Los métodos de acceso aseguran que solo un equipo pueda poner los datos en el cable en un determinado momento. Hacen que el envío y recepción de los datos se realice en forma ordenada. Varios son los métodos para impedir la toma simultánea del cable:

- Aloha
- Con detección de portadora con detección de colisiones (CSMA /CD)
- Con detección de portadora con prevención de colisiones (CSMA /CA)
- Paso de testigo (Token Passing)
- Prioridad según demanda

A. 9. 6. 1. Red Aloha

En 1970, la Universidad de Hawai desarrolló una red de datos del tipo extendida WAN que vinculaba por radio los distintos organismos distribuidos en las islas. Para esta red, llamada ALOHA, el equipo de investigación utilizó transmisores de radio viejos que empleaban los taxis. Unieron las distintas islas con una red de radio enlace, asignando solo dos canales para toda comunicación, uno el sentido descendente, de 413.475 MHz, y otro en sentido inverso ascendente, de 407.350 MHz.

Cada canal tenía un ancho de banda de 100 KHz y una capacidad de 9.6 Kb/s, de haber dividido el ancho de banda en varios canales la capacidad de cada uno habría sido mucho menor.

La solución a las colisiones se resolvió mediante el código de detección y corrección de errores CRC de la trama transmitida. Si la confirmación no llegaba en un tiempo prudencial se reenviaba el mensaje. Es decir, que el método parte del principio de transmitir, sin interesar colisión y pérdida de la trama o del mensaje. A estos sistemas que pueden originar conflictos entre usuarios, se les denominan sistemas de contención.

Un método para duplicar la capacidad del sistema fue dividir de antemano el tiempo en intervalos discretos de duración constante, denominados ranura, correspondientes cada uno a una trama.
De alguna manera las estaciones estarían sincronizadas para saber cuando empieza un mensaje. Este método se conoce como ALOHA ranurado. Este método es usado actualmente por algunas redes de satélites o en canales de acceso de las redes GSM, donde es muy baja la probabilidad de colisión.

A. 9. 6. 2. Acceso CSMA/CD

En el mecanismo apodado, acceso múltiple con detección de portadora y detección de colisiones CSMA/CD (Carrier Sense Multiple Access/ Collision Detection), cada estación en red ausculta (sensa), si existe una señal de portadora activada, ya fuese un nivel de tensión o de luz, para poder enviar su trama de datos. Hasta que los datos no lleguen a su destino la red no queda disponible para otra transmisión. En el caso que detecte que el canal está ocupado, la estación espera un determinado período y vuelve a sensar hasta que perciba que esta desocupado. Una vez enviada la trama, en cada estación es analizada su dirección de recepción, para determinar si ha sido recibida o ignorada.

Acceso múltiple significa la posibilidad de acceder al medio, compitiendo por cualquier estación. En este acceso se actúa según la idea de “primero aborda, primero opera”, por lo que se lo denomina acceso por competición, pues los equipos de la red pugnan por una oportunidad para el envío de los datos. No existe un control centralizado encargado de conceder el acceso a la red, sino que todas las estaciones compiten entre sí por el acceso. Este tipo de protocolo se utiliza para las distintas variantes de las LAN Ethernet normadas en el IEEE 802.3.

Para el acceso múltiple compitiendo con cualquier otra estación, se emite la trama de datos en ausencia de señal de portadora. En el supuesto caso que dos estaciones detectaran libre el cable de señal de portadora, enviasen los datos al mismo tiempo y se produjera una colisión, cada una deberá generar un número al azar, el mismo significa el tiempo aleatorio de espera de cada estación, para intentar una nueva transmisión. Un algoritmo, determina el instante en volver a retransmitir la trama.

En este método, el procedimiento es enviar la trama a los equipos y la recibe solo el equipo receptor deseado, mediante la dirección insertada en su sector de encabezado. Luego toma del cable la trama y la copia a un buffer de la placa. No obstante la trama continúa a los restantes equipos, que analizarán la dirección insertada en el encabezado y al detectar que no les corresponde, dejan pasar la trama. Asimismo se podrá emitir mensajes tipo difusión (broadcast), donde la trama llega a todos los equipos en general.

Al aumentar el tráfico en la red, aumenta la posibilidad de colisión, lo que hace mas lenta la red. El envío de muchas y cortas tramas, incrementan la probabilidad de colisión, que a su vez hace bajar el rendimiento (throughput) de la red. Ello indica que el mecanismo CSMA/ CD trabajará mejor al enviar muy pocas tramas y de tamaño considerable. Existe la probabilidad de que justo después que la estación comenzó a transmitir, otra estación no detecte señal, por efecto del retardo debido al tiempo de propagación, comience a enviar también y se produzca una colisión.

La atenuación en el cable, restringe los tiempos de propagación y el retardo de propagación tiene efecto importante en el desempeño de este método Cuanto mayor sea el tiempo de propagación más importante será su efecto en desmedro del desempeño del método. Al producirse una colisión se genera un voltaje anormal detectable por las estaciones. La capacidad de detectar las colisiones, se ve restringida al sobrepasar cierta distancia entre los equipos.

Llamemos latencia, al tiempo τ que tarda una trama en llegar de un extremo al otro de un segmento de red. Si en el momento que la estación A, en un extremo del segmento, envía una trama y antes que esta trama llegue a la estación B, en el otro extremo, esta estación B envía otra trama, se produce una colisión, se aborta la transmisión y se genera una ráfaga de 32 bit para avisar a las demás estaciones.

En el tiempo 2τ la estación A verá la ráfaga y aborta la transmisión, luego espera un tiempo aleatorio antes de reintentar. El tiempo mínimo para detectar una colisión 2τ, será el determinante de la longitud de ese segmento de red y según la velocidad de propagación de ese elemento. Dado que el período de incertidumbre en CSMA /CD se reduce a ese tiempo 2τ estas redes se suelen modelar como un sistema ALOHA ranurado con intervalo de tamaño 2τ.

El correcto funcionamiento de CSMA /CD requiere que el tiempo de ida y vuelta entre dos estaciones, no supere el tiempo que tarda en emitirse la trama mínima permitida. Este tiempo que depende de la velocidad de la red, fija a su vez unas distancias máximas entre estaciones. Estos cuatro parámetros (velocidad de la red, tamaño de trama mínimo, tiempo de ida y vuelta y distancia máxima) están relacionados entre sí. Ciertos sistema indican que la detección no es efectiva mas allá de los 2500 m.

Consideremos los elementos fundamentales que tienen lugar una vez que las estaciones detectan una colisión, para evitar que continúen intentando transmitir y vuelvan a colisionar. Estos elementos fundamentales son:

- *Slot Time,* tiempo máximo (de ida y vuelta) de propagación de la señal para el largo máximo de la red establecida en el estándar.

- *Jam,* trama de datos especial de 32 bit, que una estación envía a la red indicando a las demás estaciones que también "sensan" el medio, que se abstengan de transmitir.

- *Algoritmo de Retroceso Exponencial Binario REB,* algoritmo que calcula el rango en que se escogerá un tiempo para volver a transmitir. Este rango se fija entre 0 y 2^k slot times siendo k la cantidad de intentos de retransmisión realizados antes del décimo intento. Del décimo al decimosexto intento, se busca un valor aleatorio entre 0 y 2^{10} y al decimosexto intento sin éxito, se descarta la trama informándolo a la capa superior. Esto último es de una probabilidad menor al 0.1%, por lo que en condiciones normales, el algoritmo funciona adecuadamente.

Consideremos los pasos consecutivos de un proceso que incluye una colisión:

1. La estación A sensa el medio y percibe que se encuentra libre.
2. La estación A inicia su transmisión enviando una trama.
3. La estación B sensa el medio antes que la trama de la estación A llegue hasta ella, por lo que también considera al medio libre.
4. La estación B también inicia su transmisión enviando una trama.
5. Las tramas colisionan en un punto intermedio, produciendo un voltaje anormal que viaja de vuelta en ambos sentidos.
6. Como la estación B empezó a transmitir más tarde, está más cerca del punto de colisión, por lo que la detecta antes que la estación A.
7. Al detectar la colisión, la estación B detiene la transmisión de tramas de datos y envía el *Jam* a la red y espera un tiempo aleatorio para retransmitir.
8. La estación A detecta luego la colisión, por lo que análogamente detiene el envío de tramas y envía a su vez un *Jam.*
9. Ambas estaciones esperan tiempos aleatorios para retransmitir, de acuerdo al algoritmo REB, por lo que muy probablemente una de ellas, por ejemplo la estación A retransmitirá en alguna de las iteraciones sin volver a colisionar con la otra, mientras las demás esperan.
10. Una vez que la estación A retransmitió, la estación B lo hará de acuerdo a su algoritmo sin colisionar, dejando ambas finalmente libre el medio, para nuevas transmisiones.

En la práctica se depende de múltiples factores como ser el número de repetidores intermedios en la red, cables utilizados y sus longitudes reales instaladas. En la tabla adjunta se indican la correspondencia de valores óptimos,

RELACIÓN ENTRE PARÁMETROS DE UNA LAN

Velocidad (Mb/s)	Tamaño de trama mínimo (bit)	Tiempo ida y vuelta (ms)	Distancia máxima (m)
10	512	51.2	4000
100	512	51.2	412
1000	4096	4.096	330

Un mecanismo de este tipo, que tiene sus complejidades, lo que impactará negativamente sobre la performance de la red. Como veremos existen especificaciones Ethernet llamadas Full-Dúplex, en las cuales se sortea la posibilidad de colisiones pero al costo de duplicar el cableado de la red.

A. 9. 6. 3. Protocolos de acceso sin colisiones

En cualquiera de los protocolos donde pueda haber competencia entre computadoras para acceder al medio se producen colisiones con disminución del rendimiento al producirse transmisiones infructuosas.

Acceso CSMA/CA

En el llamado, acceso múltiple con detección de portadora / prevención de colisiones CSMA/CA (Carrier Sense Multiple Access /Collision Avoidance), cada equipo indica su intención de transmitir. De esta forma, los equipos detectan cuando se podrá producir una colisión, antes que realmente se produzca y pueden así variar los tiempos de transmisión. Sin embargo, difundir esta intención de transmisión crea un tráfico ficticio en la red, lo que hace mas lento el funcionamiento de la misma. En este método, se puede emitir mensajes tipo difusión (broadcast).

Protocolo Bitmap

El protocolo Bitmap cada equipo solicita turno para transmitir con un acuerdo de reglas muy estrictas. Se supone una red de n computadoras, numeradas de 0 á n-1. Para comenzar a transmitir se establece una ronda exploratoria de n intervalos donde cada una, empezando de 0 tiene la oportunidad de indicar con un 1 ó un 0 si tiene trama para transmitir. Pasados n intervalos todos saben quien tiene tramas para transmitir. Supongamos que tenemos 8 computadoras y que las máquinas 1, 3 y 7 indiquen que tienen tramas para transmitir, la computadora 1 comienza la transmisión, luego transmite la 3 y luego la 7. . Agotados los turnos comienza una nueva ronda exploratoria.

A este tipo de protocolos se le denomina, protocolo de reserva. Con este método se evitan las colisiones pero de cualquier forma se genera un tráfico dado por las continuas rondas exploratorias. Supongamos que ninguna máquina tiene trama par transmitir la ronda se generará constantemente. En él supuesto que todas tengan tramas para transmitir el protocolo Bitmap produce un reparto equitativo lo que resulta equivalente a utilizar una modulación del tipo TDM. Resumiendo, este protocolo resulta más eficiente y más homogéneo a medida que la carga de tráfico aumenta en la red.

Protocolos con Contención Limitada

Vimos que los protocolos con contención, es decir orientados a colisiones, son preferibles cuando los niveles de tráfico son bajos. En cambio, cuando el tráfico aumenta es preferible perder una parte de la capacidad del canal en habilitar mecanismos de detección y /o prevención, ya que de lo contrario no es posible utilizar el canal al máximo de sus posibilidades.

Luego, podemos concluir que un protocolo ideal sería el que englobe ambas filosofías. Debería actuar con colisiones en bajo tráfico y poner mecanismos de arbitrajes rigurosos en caso de que el tráfico aumente por encima de ciertos niveles, es decir que sería ser auto-adaptativo. Estos protocolos se denominan protocolos de contención limitada.

Paso de Testigo (Token Passing)

El método Paso de Testigo (Token Passing), es un mecanismo de acceso al medio disímil al CSMA/CD, ya que mientras dicho mecanismo es del tipo competitivo, el Token Passing es un sistema de Control Centralizado.

Se utiliza en una red de topología lógica en bus (Token Bus) o en anillo (Token Ring), aunque se emplee físicamente con concentradores en topologías tipo estrella. En el IEEE 802.5 se emplea un anillo físico, mientras que en IEEE 802.4 se especifica un bus y en ArcNet se emplea una topología estrella. El token Ring es un eficiente diseño para el movimiento de datos sobre redes medias o pequeñas, con muchas pequeñas tramas. En este caso provee mejor rendimiento que el CSMA /CD.

En el Paso de Testigo se emplea como verificación una pequeña trama testigo token (ficha) que circula por el anillo. El método consiste en el pasaje del testigo (Token Passing), de un equipo a otro alrededor del anillo, en tanto que las estaciones que deseen enviar datos, deben esperar por un token libre para poder transmitir.

Cuando un equipos desea transmitir un mensaje, debe esperar que le llegue un token libre, el equipo toma el control del mismo sacando el token del anillo. La estación incorpora los datos al token, adjuntando a él cabecera y cola con las direcciones del emisor y receptor. El token viaja alrededor del anillo hasta el receptor, sin ser analizado en ninguna estación. Cuando el destinatario ha recibido (copiado) la información del token, éste regresa a la estación de origen con el mensaje de verificación, indicando que los datos fueron recepcionados en forma correcta. Una vez liberado, el token pasa a la estación siguiente en el anillo, tal que ésta estación pueda transmitir. El token va pasando a intervalos fijos.

Al estar usando un equipo el token, los demás equipos no compiten, ni producen colisiones, con lo que se agiliza la red. Una estación puede transmitir múltiples tramas mientras tiene al token, sin embargo dispone de un tiempo máximo de transmisión.

Por la red circulan dos tipos de mensajes: los token y las tramas. Un token indica que la red está disponible. Cada estación dispone de igual acceso al cable, puesto que el token es pasado alrededor del anillo, dando a cada estación un turno. Se puede incluir información de prioridad, de forma tal que el control de la red lo pueda tomar sólo una estación, con igual o con mayor prioridad. Hay un temporizador (timer), que asegura que ninguna estación retenga el token demasiado tiempo.

Se requiere la correcta vigilancia, detección y resolución de errores en esta red. Un tipo de error se refiere a la circulación continua de la trama alrededor del anillo, sin ser reconocido por ningún equipo, llamado “error de trama persistente” (persistent frame). Otro error es el producido al tomar y retener una estación cualquiera al token, causando una condición donde no hay token en el anillo, llamado como “error de token perdido”.

Para mantener estas condiciones de vigilancia, una o mas estaciones deben ser responsables de monitorear las funciones del protocolo Token Ring. Si se produce una condición de error, la estación responsable reinicia el anillo y/o comienza un nuevo token.

Prioridad según Demanda

El método de acceso al medio denominado Prioridad según Demanda, ha sido diseñado para el estándar Ethernet de 100 Mb/s designado como 100Base-VG y publicado en la norma IEEE 802.12. Con este método de acceso al medio, las estaciones de trabajo pueden recibir información al mismo tiempo que transmitir. Esto es posible gracias a la utilización de cuatro pares de conductores, para enviar un cuarteto de señales, de 25 MHz en cada par.

Este método de acceso se basa en redes con concentradores y nodos finales, con topología bus en estrella. Un nodo final podrá ser un equipo de trabajo, un puente, un enrutador o un conmutador. En el modo puerto a puerto, también llamado Round Robin (petirrojo rondante), los concentradores administran el acceso, realizando búsquedas de peticiones desde todos los nodos de la red, con requisitos de prioridades.

El concentrador es responsable de anotar todas las direcciones, vínculos y nodos finales, y comprobar que todos estén funcionando correctamente. En el caso CSMA/CD se producían contiendas y eventuales colisiones, mientras que en el método de acceso Prioridad según Demanda, al recibir ciertos tipos de datos de prioridad, en caso de situación de contienda, el concentrador o repetidor dará preferencia a la petición de mayor prioridad.

En este método solo hay comunicación entre el equipo emisor, el concentrador y el equipo receptor. Esto resulta más eficiente que en el caso de CSMA/CD donde se difunde la transmisión en toda la red. Los concentradores solo tienen las direcciones de los equipos conectados directamente al mismo. Este método utiliza la topología bus en estrella.

COMPARACIÓN DE MÉTODOS DE ACCESO

Tipo	CDMA/CD	CSMA/CA	Paso de Testigo	Prioridad por Demanda
Comunicación	Difusión	Difusión	Testigo	Concentradores
Acceso	Competición	Competición	Sin competición	Competición
Red	Ethernet	Local Talk	Token Ring ArcNet	100VG-Any LAN

A. 9. 7. Arquitecturas de las LAN

Hemos definido como arquitectura de la red de datos, a la conjunción del concepto topología de red y al acceso al medio correspondiente. Vimos las distintas topologías que conforman las redes y sus tipos de conexionado, en las formas de bus lineal, estrella y anillo. También vimos los distintos tipos de accesos a la red a los fines de poder compartirla. Estos son ALOHA, CSMA /CD y CSMA /CA, Token Passing y Prioridad según Demanda.

Nos toca explayarnos en los detalles que engloban la arquitectura como redes de área local, para tratar posteriormente las redes de mayor extensión, MAN y WAN.

Existen diversos estándares que se han aplicado a través del tiempo para la implementación de las LAN. De estos estándares, vamos a poner énfasis en los más difundidos, en particular a los estándares Ethernet y Token Ring, que en la actualidad son las opciones que mayores ventajas presentan, por su difusión, escalabilidad, performance y bajo costo.

A. 9. 7. 1. Arquitecturas Ethernet

En el año 1970, la Universidad de Hawai, para evitar el uso de la red de datos de la AT&T, por su elevado costo y de baja calidad de transmisión, que operaba en las islas de Hawai, dispuso un equipo de investigación para solventar ese tema. Utilizando varios transmisores de radio viejos de taxis, unieron las distintas islas con una red de radio enlace, formó una red de datos del tipo extendida, como si fuese una primitiva WAN.

En el año 1972, basado en este diseño, la compañía Xerox concibe la red experimental Ethernet. Así denominada por usar el “eter”, en su transmisión por radio.

En aquellos años, la tendencia de los fabricantes era hacia arquitecturas de redes jerárquicas. La arquitectura de red SNA (System Network Architecture), diseñada por IBM, dispone esta topología. Como vimos anteriormente, la filosofía de SNA se basa en el uso de terminales “tontos” y de una mainframe, constituyendo una red jerárquica. Una configuración típica SNA comprendía cuatro niveles. La idea de Xerox fue radicalmente opuesta, cada usuario disponía de una PC, integrando en ellas todas las funciones y conectándolas en red. No existiría ningún control centralizado en la red, la comunicación se establecería par a par.

En el año 1975, Xerox concibió el producto Ethernet de 2.94 Mb/s, utilizando 100 equipos y una extensión de un kilómetro, donde emplea el control de acceso al medio con detección de portadora CSMA /CD. Con el protocolo CSMA /CD cuando una máquina quiere transmitir primero ausculta la señal de portadora, para detectar si otra máquina esta transmitiendo, si así fuese espera un tiempo aleatorio para efectuar un nuevo intento.

Seguidamente, las empresas Xerox, Intel y Digital Equipment Corporation (DEC), reunidas como la alianza DIX (DEC, Intel y Xerox), implementaron la red Ethernet para 10 Mb/s, que fue tomada luego como norma IEEE 802.3. Con esta arquitectura distribuida, se permitió el desarrollo de las redes de PC y el aumento de las velocidades en red.

La especificación Ethernet efectúa las mismas funciones que las capas de los niveles Físico y de Enlace del modelo OSI. La trama Ethernet podrá ser conformada entre 64 Byte y 1518 Byte, aunque la trama de datos en sí es de 18 Byte (Fig. 13).

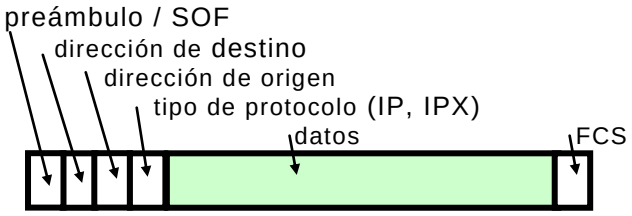


Fig. 13 - Ejemplo de trama Ethernet II

En la figura se alude a los campos constitutivos de la trama:

- *Preámbulo* (7 Byte): Indica a la estación receptora la presencia de una trama.
- *SOF - Start of Frame* (1 Byte): Comienzo real de la trama para su sincronización.
- *Dirección de Destino* (6 Byte): Puede ser Unicast, Multicast o Broadcast.
- *Dirección de Origen* (6 Byte): Siempre es Unicast.
- *Campo Length* : (2 Byte): El número de Byte del campo de datos, el cual a diferencia de los restantes es variable, dependiendo del tipo de protocolo empleado.
- *Data* (46 a 1500 Byte): Trama de Datos, que luego de los procesos de capa física y capa de enlace hayan concluido, se enviará a las capas superiores.
- *FCS Frame Check Sequence* (4 Byte): Secuencia de chequeo de la Trama, a fin de detectar y eventualmente corregir errores. En general se implementa con un procedimiento llamado Código de Redundancia Cíclica (CRC)

Al disponer el campo Datos de una variación de 46 a 1500 Byte causa a su vez una variación en la longitud de la trama total, pero siempre dentro de cierto rango. Existe un tamaño máximo de trama, que tiene como objetivo no ocupar indefinidamente la red con una transmisión “secuencial”, con lo cual bajaría el "tiempo medio de respuesta" a cada estación.

En caso de fallos, con la necesidad del reenvío de las tramas, se bajaría sensiblemente la performance de la red.

Por otra parte existe un tamaño mínimo de la trama, para que en la longitud máxima de la red, se suministre el tiempo necesario para identificar colisiones, como se vio al considerar en detalle los mecanismos de acceso al medio utilizados.

Uno de los aspectos clave para el funcionamiento de una red es definir como se codificarán los bit para la transmisión. En el caso de Ethernet, el sistema de codificación utilizado por las Redes Ethernet es el Sistema Manchester.

Según este sistema cada cierto tiempo de reloj de sincronísmo, se produce una transición de voltaje. Si la transición es hacia un valor de voltaje alto representa un 1, y si es hacia un valor más bajo, representa un 0. Asimismo, esta transición interesa al ajuste del sincronísmo del voltaje a la posición adecuada para codificar un 0 o un 1.

La red Ethernet, puede utilizar varios protocolos de comunicaciones, incluido TCP/IP. La red Ethernet es mas conocida, por la tecnología utilizada, por ejemplo: 10Base-2, 10Base-5, 10Base-T y 10Base-FL.

La red Ethernet conmutada, provee mayor velocidad en la transferencia de datos que la red Ethernet original de señal participada. La combinación Ethernet /ATM logra altas velocidades. Los estándares 100Base-VG /AnyLAN Ethernet, 100Base-X /Fast Ethernet, 1000Ethernet-SX y el 1000Ethernet-LX, han sido creados para manejar aplicaciones de gran ancho de banda.

Estos trabajar con multimedios, con diseños asistido por computadora CAD (Computer Aided Design) e implementa los sistemas de fabricación asistida por computadora CAM (Computer Aided Manufacture).

Una de las ventajas importantes del estándar Ethernet, es que permite la coexistencia de diferentes especificaciones de capa física en la misma Red. Ello permite hacer adiciones a una red existente de tecnología más antigua, como puede ser 10Base-5, anexándole un nuevo tramo de red con una tecnología actualizada, como ser Fast Ethernet, sin necesidad de cambiar la estructura de cableado existente.

La tarjetas de red Ethernet, permiten diferentes conexionados mediante diferentes tipos de conectores hembra. En particular el BNC para cableado coaxial y los AUI y RJ-45 para cables de pares trenzados no blindados UTP (Fig. 14).

Fig. 14 - Tarjeta de red Ethernet

A. 9. 7. 2. Arquitecturas Ethernet Estándar

Podremos diferenciar como normas Ethernet Estándar a las primeras especificaciones Ethernet implementas originalmente: la Ethernet DIX (10Base-5) en coaxial grueso, posteriormente la Ethernet II (10Base-2) en coaxial fino y más reciente las que emplean cable UTP (10Base-T) y la que utiliza cable de fibra óptica (10Base-F).

Como estas especificaciones logran una velocidad máxima de 10 Mb/s, no es muy adecuada para las actuales necesidades de ancho de banda. Aún así es importante conocerlas, dado que aun existe gran cantidad de este tipo de redes Ethernet en el mundo.

Ethernet 10Base-5

La especificación 802.3 del IEEE, definen la norma Ethernet 10Base-5, también llamada Ethernet DIX o de coaxial grueso. Esta construida sobre la base de una topología de Bus Regular, es decir con un cable troncal (backbone) del cual parten derivaciones. Se denomina 10Base-5, con el valor 10 que indica la velocidad de transmisión de datos a 10 Mb/s y con el valor 5 por lleva la señal hasta 5 veces la unidad de 100 m., es decir que se extiende hasta 500 m.

El cable troncal es un coaxial grueso (RG-11), de 50 Ω (thicknet de ∅ 1/2”), por ello se le llama Ethernet Thicknet. Las derivaciones se realizan con conectores tipo vampiro (Piercing Tap), para conectar mediante perforaciones al conductor central del coaxial (Fig. 15).

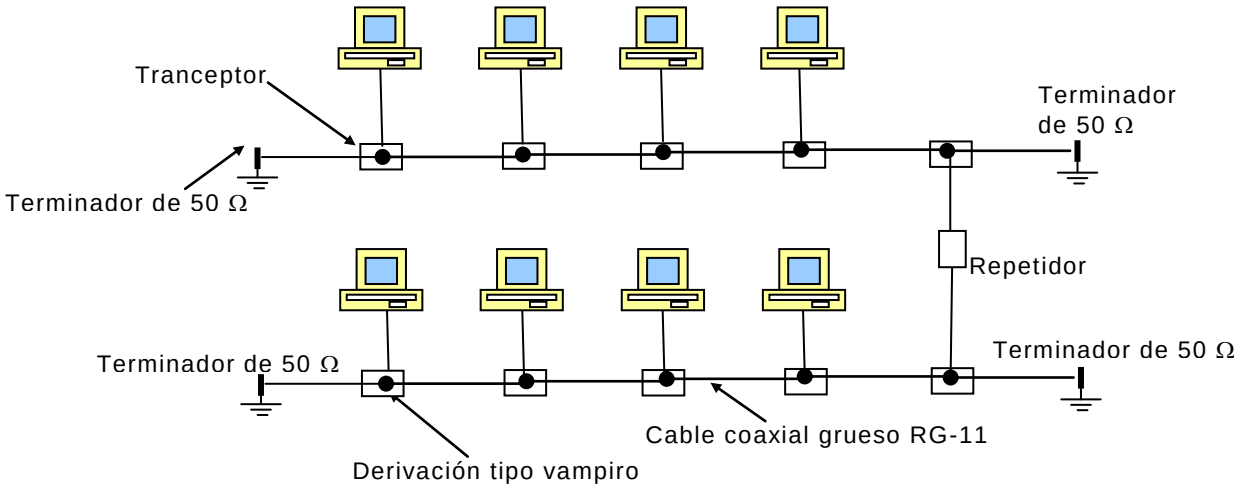


Fig. 15 - Red Ethernet 10Base-5, de cable grueso

Desde estos conectores, mediante tranceptores de 5 pares aislados, parten cables que conectan a las placas de red, mediante conectores tipo N ó AUI. El tranceptor transmite las señales de datos con 2 prs y de control con 2 prs. El mismo puede tener bajadas de derivación, de hasta 50 m. El tranceptor contiene la electrónica para manejar la detección de portadora y la detección de colisiones.

La red Ethernet 10Base-5, funciona como red pasiva, es decir que cada estación esta a la “escucha”, no siendo responsable del movimiento de los datos desde una estación a otra. En caso de falla en el cable troncal, se pierde la conectividad.

Para integrar los segmentos se podrá optar por varias alternativas:

- Utiliza un Repetidor
- Destina un Servidor con una tarjeta Ethernet por cada segmento.
- Poner en algunas estaciones dos placas y hacer que además de su tarea normal, funcionen como retransmisores (en ese caso se las llaman puente).

Se deben respetar ciertas limitaciones. Una red Thicknet, con estaciones de trabajo y repetidores, tendrá como máximo 500 m, en cada segmento de cable troncal. Esta medida no incluye los cables de derivación. El backbone puede soportar un máximo de 260 nodos, en su longitud de 500 m, o 100 nodos por segmento.

La distancia mínima, en el cable backbone, entre derivaciones debe ser de 2.50 m., para evitar reflexiones indeseables. No incluye los cables de derivación.

La red Ethernet, Thicknet puede combinar un total de 5 segmentos, conectados por hasta 4 repetidores. Pero tan solo 3 segmentos, podrán tener estaciones de trabajo conectadas. Por ello, a esta formación se denomina 5-4-3. Luego tendrá una longitud máxima teórica de 2500, limitada en la práctica a 2460 m. Cada segmento de red deberá estar terminado con un adaptador de terminación, de 50 Ω, con toma a tierra, que llamaremos terminador de 50 Ω.

En la tabla siguiente se resumen las principales características a tener en cuenta para esta especificación:

10Base-5	
Velocidad	10 Mb/s
Topología	Bus
Cableado	Coaxial grueso
Conectores	BNC
Largo máximo del segmento	500 m
Largo mínimo del segmento	2.5 m
Máximo de nodos por segmento	100
Otras limitaciones	Regla 5-4-3
Modo	Half-dúplex

Ethernet 10Base-2

La red Ethernet 10Base-2, llamada Ethernet II, es una evolución más económica que la anterior 10Base-5, por lo que se la llamó también *Cheapernet* (Ethernet más barata).

La especificación 802.3 del IEEE, define a la norma Ethernet 10Base-2, como construida con coaxial delgado (RG-58), de 50 Ω (thinnet de ∅ 1/4”), por lo que se le denomina generalmente como Ethernet Thinnet o de coaxial fino. Se le designar 10Base-2 pues trabaja con velocidad de transmisión de datos a 10 Mb/s, en banda base y lleva la señal, hasta 2 veces la unidad de 100 m, es decir se extiende hasta 200 m (su máximo real está especificado en 185 m).

Al tener el cable coaxial utilizado un menor apantallamiento, tendrá mayor atenuación y por ello permite disponer de segmentos de menor longitud. Esta red, dispone una topología de Bus Local, por ello también se la llama Local Ethernet. Vincula las computadoras, mediante cables con conectores BNC macho, que se acoplan mediante en conector T, a los conectores hembra que poseen la placa de red. (Fig. 16).

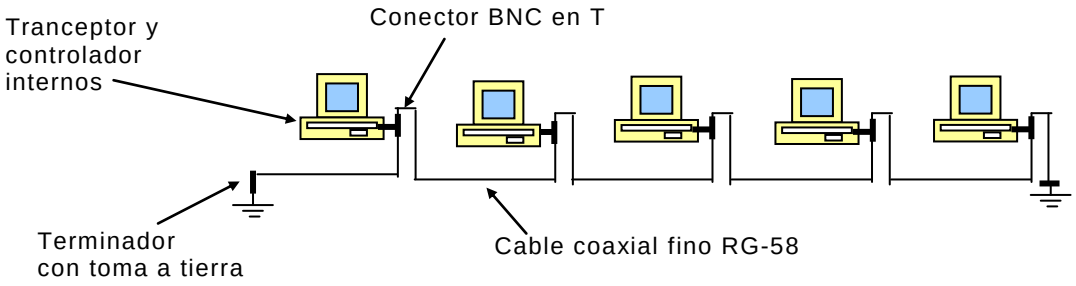


Fig. 16 - Red Ethernet 10Base-2, de coaxial fino

Se trata, al igual que la Thinnet, de una red totalmente pasiva. Solo un equipo a la vez puede enviar datos, los equipos no retransmiten la señal, los datos pasan de una computadora a otra, si le corresponden a ella los recibe sino la deja pasar. En cada extremo del segmento de cable formado, se conecta una resistencia de terminación de red con valor de 50 Ohm. Esta terminación, asegura la no reflexión de la señal. La distancia mínima de cable entre conexiones debe ser de 0.50 m (1.6 pie)., para evitar las reflexiones indeseables. Una instalación correcta debe comprender la puesta a tierra de solo uno de los terminadores.

Para integrar los segmentos esta norma posibilita varias alternativas:

- Utiliza un Repetidor.
- Destina un Servidor con una tarjeta Ethernet por cada segmento.
- Poner en algunas estaciones dos placas y hacer que, aparte de su trabajo normal, funcionen como retransmisores (en ese caso se las llaman puente).

Aún así la norma dispone ciertas limitaciones. En la red Ethernet de cable fino, podrá haber como máximo 30 equipos de trabajo, por segmento de 185 m. Una Thinnet puede combinar un total de 5 segmentos, conectados por hasta 4 repetidores. Pero tan solo 3 segmentos, podrán tener estaciones de trabajo conectadas. Por ello, a esta formación se denomina 5-4-3. En la tabla siguiente, se resumen las principales características a tener en cuenta para esta especificación:

10Base-2	
Velocidad	10 Mb/s
Topología	Bus
Cableado	Coaxial fino
Conectores	BNC
Largo máximo del segmento	185 m
Largo mínimo del segmento	0.5 m
Máximo de nodos por segmento	30
Otras limitaciones	Regla 5-4-3
Modo	Half-duplex

Ethernet 10Base-T

La especificación 802.3 del IEEE, Ethernet 10Base-T, es más moderna y más económica. Esta se definió en 1990, basándose en cables multipares trenzados (twisted pair) que se concentran en un Hub o un Switch. Tanto un Hub, concentrador /repetidor conectado en estrella, como un Switch, conmutador operan distribuyendo la señal a las diferentes ramas de la red estrella. Otra diferencia cualitativa en esta especificación, es el modo soporte como Full-Dúplex.

La red Ethernet 10Base-T, es así llamada por transmitir en 10 Mb/s, en banda base y con el carácter T que se construye con cables multipares trenzados sin blindaje UTP (Unshielded Twisted Pair) (Fig. 17).

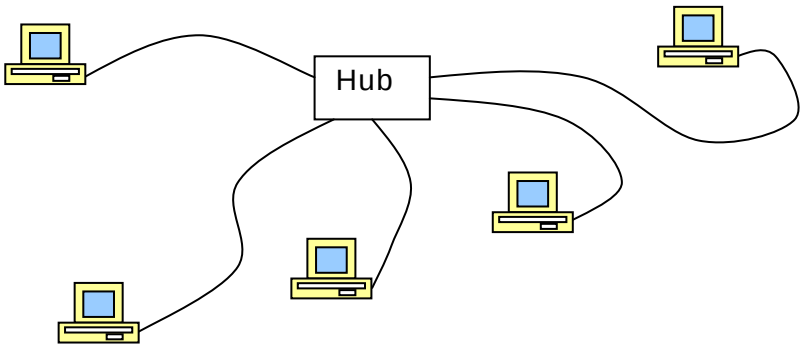


Fig. 17 - Conexionado para una red 10Base-T

Se podrá usar, en caso de interferencias un cable blindado STP (Shielded Twisted. Dos pares de conductores vinculan cada estación al Hub. Un par es utilizado como transmisor y otro par como receptor. Cuando una señal llega a un Hub, éste la difunde por todas las líneas de salida.

Se pueden conectar un Hub a otros Hub, formando una red jerárquica en esquema del tipo árbol o de doble estrella. El Hub puede tener hasta 12 puertas de salida. Es decir se pueden conectar a él hasta 12 workstation (WS) o 12 Hubs a un Hub central. Mediante esta arquitectura, se podrá dotar de servicio a 1024 equipos

La longitud máxima de un segmento es de 100 m. Si se emplean cables de categoría Clase 5 esta distancia se podría ampliar a 150 m. Se suelen utilizan repetidores para ampliar esta longitud. La longitud mínima, del cable entre computadoras es de 2.50 m.

Muchas de estas redes se configuran físicamente tipo estrella, con software de señalización interna del tipo bus. Se pueden obtener redes para velocidades superiores a 10 Mb/s, mediante concentradores repetidores multipuerto y paneles de conexiones.

10Base-T	
Velocidad	10 Mb/s
Topología	Estrella
Cableado	UTP
Conectores	RJ-45
Largo máximo del segmento	100 m
Modo	Full-Dúplex

El conexionado empleando una red existente de un edificio, podrá contar con vínculo montante vertical, backbone, de fibra óptica o cable coaxial, conectado a un concentrador o a transceptores, para efectuar la unión con otras LAN. De allí, mediante un cable de 50 pares, se llega a una regleta de conexiones, desde donde parten cables de dos pares, terminados en conectores del tipo RJ-45.

Ethernet 10Base-F

Con el advenimiento de la Fibra Óptica, emergen tres nuevos tipos de Ethernet designándolo el IEEE como 10Base-F, porque trabajan a 10 Mb/s en banda base y su red esta constituida con fibras ópticas.

Se diferencian según la especificación de capa física empleado: del tipo fibra pasiva (fiber passive FP), fibra de enlace (fiber link, FL) o fibra troncal (fiber backbone, FB).

La longitud máxima del segmento, varía según el tipo especificado:

- 10Base-FP 1 Km. entre estaciones y repetidores.
- 10Base-FL 2 Km. entre estaciones y repetidores.
- 10Base-FB 2 Km. entre repetidores.

10Base-F	
Velocidad	10 Mb/s
Topología	Punto a punto
Cableado	Fibra
Conectores	Específicos p/ fibra
Largo máximo del segmento	Hasta 2000 m
Modo	Half-duplex

Este estándar se utiliza principalmente para vincular largas distancias evitando el uso de repetidores. La distancia típica se forma con segmentos de 2 Km, permitiendo usar repetidores FOIRL (Fibra Optica Inter Repeater Link).

Es una alternativa costosa debido a sus equipos terminales, pero es efectivo por su inmunidad a ruidos electromagnéticos interferentes. Se emplea por su alcance, en la vinculación entre edificios.

A. 9. 7. 3. Arquitecturas Fast Ethernet

Con la evolución de las telecomunicaciones, la demanda creciente de ancho de banda hizo insuficiente el máximo de 10 Mb/s. Además las redes Token-Ring superaban a las rede Ethernet, llegando hasta 16 Mb/s. Esto llevó al desarrollo de nuevas especificaciones Ethernet que alcanzaran velocidades de 100 Mb/s, más adecuadas a estos tiempos.

Ethernet 100Base-X

El estándar Ethernet 100Base-X, indica que trabaja a 100 Mb/s con señal en banda base, con X diferentes tipos de cables. Es también llamado Fast Ethernet (Ethernet rápido). Este estándar corresponde a la norma 802.3u del IEEE, aprobada en 1995. Tiene una topología bus en estrella, con uso de concentradores y utiliza el método de acceso a la red CSMA/ CD. No se permite el uso de conectores tipo vampiro o BNC.

Esta opción, permite que dos dispositivos conectados entre sí intercambien, no solo datos, sino también información acerca de sus capacidades de operación, tales como velocidad, soporte para Full-Dúplex, lo cual permite que los dispositivos “negocien” la mayor velocidad posible, y también se autoconfiguren, por ejemplo en el caso de un cambio de Half-Dúplex, a Full-Dúplex.

Las especificaciones 100Base-T4, 100Base-TX, 100Base-FX, indican respectivamente su implementación de uso, con conductores según:

a) T4 - 4 pares UTP, Categoría 3 (telefónico) ó de Categoría 4 / 5 (para datos),

b) TX - 2 pares UTP ó STP de Categoría 5 (datos),

c) FX - 2 fibras ópticas.

Los cables de Categoría 3 tienen la desventaja de no poder transportar señales de 200 MBaud (100 Mb/s en codificación Manchester), a distancias de 100 m,. Solo se podrá alcanzar estos 100 m, con cables de Categoría 5 y mucho mayores distancias con cables de fibra óptica.

Ethernet 100Base-T4

La norma Ethernet 100Base-T4 es un modo de lograr velocidad con uso de 4 pares UTP. Como estos 4 pares se permite en cada uno, una transmisión máxima de 33 Mb/s, en realidad, los 100 Mb/s se logran al destinar uno de ellos como fijo para un sentido de transmisión, otro fijo para el sentido contrario, y los dos restantes, de sentido variable. De esta manera, siempre se dispone de tres pares para transmisión en un sentido, con lo que se logran aproximadamente los 100 Mb/s.

100Base-T4	
Velocidad	100 Mb/s
Topología	Estrella
Cableado	UTP 3 o 5 – 4 pares
Conectores	RJ-45
Largo máximo del segmento	100 m
Diámetro máximo	200 m
Modo	Half-duplex

Ethernet 100Base-TX

La red Ethernet 100Base-TX es otra variante de la norma 802.3u, con cableado de mayor calidad y soporte para Full Dúplex.

Por ello la hace adecuada para redes en las que se requiera alta performance o bien extender la red más allá de los límites permitidos por el CSMA/CD.

En la tabla, se resumen las principales características referidas a esta especificación:

100Base-TX	
Velocidad	100 Mb/s
Topología	Estrella
Cableado	UTP 5/ STP–2 pares
Conectores	RJ-45
Largo máximo del segmento	100 m
Diámetro máximo de la Red	200 m
Otras limitaciones	Máximo 2 Hubs
Modo	Full-dúplex

Ethernet 100BaseFX

La versión Ethernet 100Base-FX, se refiere a una red Ethernet que emplea fibra multimodo, por la cual se consiguen distancias de unos 2000 m. Las ventajas de esta versión de Ethernet, se muestran ejemplificada en la siguiente tabla:

100Base-FX	
Velocidad	100 Mb/s
Topología	Estrella
Cableado	Fibra multimodo (2)
Conectores	Dúplex SC – PCM
Largo máximo del segmento	412 m / 2000 m
Modo	Full-Dúplex

Mientras que en Modo Half Dúplex el largo máximo del segmento es de 412 m, lo cual se deriva del cálculo del *slot time,* como hemos visto antes; en el modo Full Dúplex es posible llegar al límite que permite la atenuación de la señal, es decir unos 2000 m.

El fenómeno de atenuación se hace más evidente en la conducción de electricidad, debido a la resistencia del medio conductor de cobre. No obstante, aunque la señal de luz no tiene este problema al ser transmitida por medio de una fibra de alta calidad, defectos microscópicos en la misma, ocasionan pérdidas de la señal de luz, que en grandes distancias se hace presente.

Ethernet Full Duplex

El IEEE ha normalizado al Ethernet Full Duplex, en 1997, bajo el estándar 802.3x. Esta tecnología permite mediante la duplicación del cableado, que dos estaciones intercambien datos simultáneamente, proveyendo así caminos independientes para la transmisión y la recepción, obteniendo la transmisión full dúplex.

Esta diseñada exclusivamente para enlaces punto a punto, pueden por lo tanto implementarse en topologías tipo estrella. Con este sistema, se elimina la posibilidad de colisiones, aunque el mecanismo CSMA/CD continuará sensando el medio antes de transmitir, pero lo encontrará invariablemente libre.

Otra ventaja es que al no requerirse el mecanismo CSMA/CD, las distancias máximas anteriormente consideradas quedan sin efecto, si bien subsisten limitaciones debidas a la atenuación de la señal y otros factores.

A los inconvenientes de costos de cableado duplicado, deben añadirse los del mayor costo de tarjetas que soporten Full-Dúplex y fundamentalmente la necesidad de utilizar como concentradores conmutadores, en lugar de los Hub, que si bien tiene mayores posibilidades, su costo suele duplicarse. No obstante, en redes con un tráfico importante, estos costos se verán ampliamente compensados por el aumento en la performance.

Junto con la opción Full-Dúplex, en la norma 802.3x, se introduce una nueva funcionalidad llamada *Control de Flujo*, según la cual la estación receptora puede enviar en cualquier momento un comando *Pause* (esto se implementa mediante una trama especial) indicándole por cuanto tiempo deben dejar de transmitirle, a los efectos de evitar la saturación de los buffers del receptor con el consiguiente descarte inconveniente de tramas.

Ethernet 100Base-VG

La tecnología 100Base-VG es también denominada Ethernet AnyLAN o 100VG-AnyLAN. Se designa así por trabajar tanto a 100 Mb/s en banda base de estructura Ethernet o de fibras ópticas en Token Ring. La sigla VG (Voice Grade), se refiere al tipo de cableado específico que utiliza.

Esta técnica fue desarrollada por Hewlett Packard y ratificada por el IEEE en la norma 802.12. Combina elementos de Ethernet (802.3) y Token Ring (802.5). Soporta tramas Ethernet y paquetes Token Ring y capacidad para opciones de filtrado de tramas. En una red existente, es posible utilizar cualquiera de estos dos estándares pero solo uno de ellos por vez.

El protocolo MAC está basado en el principio de sondeo (polling), donde el concentrador moderador, pregunta a las estaciones en turno rotatorio si tiene tramas para enviar, terminada la ronda las estaciones están habilitadas para transmitir en ese orden. Cuando existen mas de un concentrador se crea una estructura jerárquica en cascada.

Para ello, se hace uso de un concentrador primario llamado Root Hub, ampliándose la red con el agregado de concentradores secundarios y desde donde parten otras redes estrella, hacia las workstation.
El concentrador primario es una unidad de acceso múltiple MAU que permite trabajar en anillo. Los concentradores secundarios podrán ser del tipo Hub (Fig. 18).

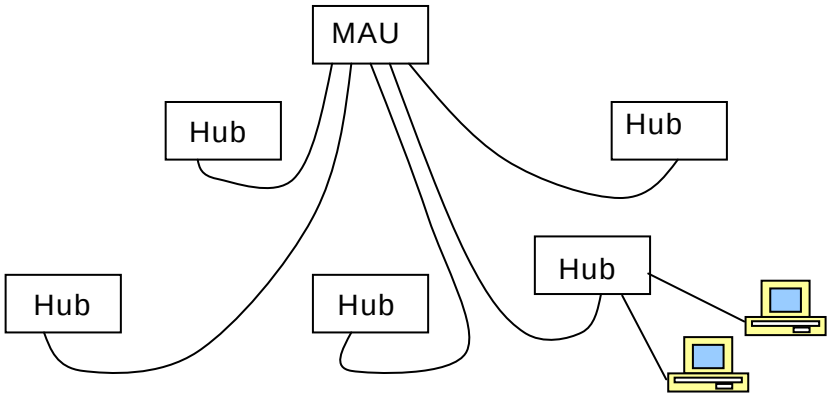


Fig. 18 - Concentrador primario con cinco secundarios

Luego, esta topología requiere sus propios concentradores y placas de red, estando sus distancias limitadas. Se obtiene la topología estrella, mediante cables UTP de categorías 3, 4, y 5 o cables de fibra óptica. Permiten los métodos de demanda con prioridad de acceso, del tipo baja y alta. Además admite tráfico isócrono como voz o video, clasificándolo como de alta prioridad.

A. 9. 7. 4. Arquitecturas Gigabit Ethernet

El ambicioso proyecto de llevar las redes Ethernet a velocidades de 1000 Mb/s, trajo consigo dificultades relacionadas con el largo de tramas, por lo que se debieron implementar mecanismos que los resolvieran adecuadamente, pero manteniendo la compatibilidad con otros sistemas Ethernet, para permitir la coexistencia de los mismos. Estos mecanismos son la *Extensión de Portadora* y el *Frameбursting.*

Extensión de Portadora

Una de las decisiones más difíciles que tuvo los comités 802.3z y 802.3ab, formados con el fin de fijar un estándar Gigabit Ethernet, fue mantener, además del mismo mecanismo de acceso al medio CSMA/CD, igual formato de trama que en el resto de los 802.3, por las razones de compatibilidad a los sistemas existentes.

Esto trajo consigo cierta complicación, ya que así como al pasar de 10 Mb/s a 100 Mb/s la longitud máxima de la red se vio acotada de 2500 m a 500 m. Con un razonamiento similar, para pasar de 100 Mb/s a 1000 Mb/s la red se reduciría a un máximo inaceptable de 50 m.

Para resolver este problema, se decidió mantener el formato de la trama de datos, pero agregarle un campo “de relleno” a continuación del FCS, que llevaría el largo máximo de la trama original de 512 bit a 4096 bit, y un nuevo Slot Time para Gigabit Ethernet, que permita mantener las distancias anteriormente utilizadas en Ethernet 10 y 100 Mb/s.

Framebursting

Si bien el mecanismo de Extensión de Portadora, resuelve el problema de las distancias manteniendo la compatibilidad, es indudable que genera ineficiencias en la red. Se estaría transmitiendo solo “relleno” la mayor parte del tiempo, sobre todo considerando que en los sistemas, estadísticamente la mayoría de las tramas que se transmiten son cortas.

De tal forma, el sistema *Framebursting* (ráfaga de tramas) se ideó como un método para mejorar la eficiencia con la transmisión de tramas cortas. Este sistema consiste en enviar una primera trama de datos en forma normal, con la Extensión de Portadora y si ésta no colisionó, a continuación enviar una ráfaga de tramas sin relleno, hasta un máximo de 65.536 Kbit.

A su vez, las tramas siguientes van separadas por un *interFrame*, como relleno específico que indica la separación entre las tramas de la ráfaga. Con esta optimización, se obtienen resultados de alta performance, con la ventaja de que al mantener la compatibilidad, permite la existencia de redes mixtas, conformadas por diferentes especificaciones dentro del estándar 802.3.

A. 9. 7. 4. 1. Ethernet 1000Base-X

Las redes Ethernet 1000Base-SX, 1000BaseLX, 1000BaseCX, de norma 802.3z y la 1000BaseT de norma 802.3ab, se les denominan genéricamente como Gigabit Ethernet, al proporcionar velocidades de 1 Gb/s, o también se les suele llamar Super Fast Ethernet. Corresponden a la tercera generación de Ethernet, subsiguiente de la primera de 10 Mb/s y la segunda de 100 Mb/s.

Los estándares IEEE 802.3z, aprobados en 1998, referidos a esta tecnología, contempla la especificación ANSI de Fiber Channel de 800 Mb/s. El Giga Ethernet es aplicable a enlaces troncales (backbone) de fibras ópticas, empleando, tanto técnicas ATM como FDDI. Provee actualmente velocidades hasta de 40 Gb/s.

Para Giga Ethernet se ensayó el método usado en Fiber Channel, donde se aprovecha para redes de cortas longitudes, el emisor Laser con fibra multimodo. Las redes con fibras ópticas multimodo son las más usadas en la práctica para las LAN, por ello se quiso usar ese método. Al querer utilizarla para redes con longitudes mayores, se presentó un nuevo fenómeno hasta entonces desconocido, al que se le denominó dispersión por retardo de modo diferencial. Tal fenómeno tiene el efecto de ensanchar el pulso luminoso, en forma proporcional a la distancia recorrida. Ello reducía la longitud máxima permisible de la red, a valores menores que los esperados.

Finalmente se estandarizaron dos sistemas el 1000Base-SX y el 1000Base-LX. El sistema 1000Base-SX, con la S se indicaba short wavelength o de primera ventana y en el sistema 1000Base-LX, con la L se indicaba long wavelength o de segunda ventana. El SX funciona solamente en con fibra multimodo (50/125 ó 62.5/125), mientras que el LX puede utilizar ambos tipos, multimodo o monomodo.

Para el desempeño en pequeñas redes, de hasta 500 m, se utilizan fibras y láser multimodo, de 770 á 860 nm y estándar 1000Ethernet-SX. Para redes mayores, de hasta 2 Km, se utilizan fibras y láser monomodo, se emplea el rango de 1270 á 1355 nm y estándar 1000Ethernet-LX que permite mayores capacidades.

Los Láser VCSEL (Vertical Cavity Surface Emitting Láser), actúan actualmente solo en primera ventana, luego, para las redes del tipo 1000Base-LX se debe emplear técnicas mucho más costosas como lo es el Láser Fabry-Perot. A cambio, permiten que 1000Base-LX en segunda ventana disponga de un mayor alcance. Se obtiene sobre fibras monomodo, distancias de 5 Km (ver anexos sobre redes ópticas y componentes ópticos.

El tamaño de trama, software y topología, es similar a las otras generaciones de Ethernet, con las diferencias en el manejo de alta resolución de gráficos y en el manejo de altas velocidades de transferencia de datos. Su uso primario apunta a los enlaces punto a punto, entre conmutadores Ethernet de 1 Gb/s, luego su uso podrá comprender conmutación full Giga Ethernet con segmentos de 10 Mb/s y 100 Mb/s. Se utiliza la codificación 4B5B.

Se diferencia con las otras Ethernet por ser su construcción en red de fibra óptica. Sin embargo, es compatible a los conductores UTP de Categoría 5. Se puede emplear conductores UTP con longitudes limitadas. Si la red esta afectada por interferencias de radiofrecuencias se emplea cable STP.

Como cualquier red Ethernet, al emplear el CSMA /CD, la detección de colisiones se realiza en un ambiente tipo broadcast, es decir de difusión masiva hacia todos los nodos. El nodo Ethernet controla la recepción de cada paquete. Esto significa, que cualquier colisión para ser detectada, debe ocurrir durante el tiempo de propagación de la señal ida y vuelta. Aún con velocidades de 1 Gb/s, y en fibra óptica, debido a la situación de colisión, la longitud de la red es restringida a una longitud de 260 m.

Una red Ethernet emplea la transmisión unidireccional, llamada también como Half Dúplex (HDX). Por ello, para poder efectuar una comunicación bidireccional o sea Full Dúplex (FDX), sin restricción de distancias, se deberá emplear dos pares, con conmutadores que indiquen el camino de emisión y el de recepción. De tal forma la restricción de distancia máxima de transmisión esta dada por la atenuación y la dispersión. La atenuación, limita el rango sobre el que la señal puede ser realmente transmitida, mientras que la dispersión limita la máxima velocidad de datos para una cierta distancia dada.

La multiplexación DWDM, permite a Gigabit Ethernet un aumento aún mayor de capacidad. Los dispositivos DWDM integrados en el conmutador permiten, multiplexar, 32 ó más canales y en ambos sentidos, sobre una única fibra óptica.

A diferencia de lo que sucede con 10Base-FL ó en 100Base-FX, donde el alcance viene dado por la atenuación de la señal, en 1000Ethernet sobre fibra multimodo está limitado fundamentalmente por el efecto antes mencionado de dispersión por retardo de modo diferencial.

Existe en el mercado el procedimiento 100Base-SX a un costo mitad que un 100Base-FX. el alcance propuesto está limitado a 500 m por su valor de atenuación. Se utiliza en cableados de edificios, tanto en distribución horizontal como vertical, con cables UTP Categoría 5.

Ethernet 1000Base-SX

La red Ethernet 1000Base-SX, trata la aplicación Ethernet con empleo de fibra multimodo para onda corta. La tabla resume y describe sus principales características:

1000Base-SX	
Velocidad	1000 Mb/s
Topología	Estrella
Cableado	Fibra multimodo (2)
Conectores	Para fibra onda corta
Largo máximo del segmento	220 m
Modo	Full-Dúplex

Ethernet 1000Base-LX

La red Ethernet 1000Base-LX, similar a la 1000BaseSX, emplea fibra multimodo para fibra de onda larga.

1000Base-LX	
Velocidad	1000 Mb/s
Topología	Estrella
Cableado	Fibra multimodo (2)
Conectores	P/fibra onda larga
Largo máximo del segmento	500 m
Modo	Full-duplex

Ethernet 1000Base-CX

La red Ethernet 1000Base-CX, es la versión más económica de la norma 802.3z. Emplea cables en pares de cobre, blindado de alta calidad. Como se puede apreciar en la tabla, el largo máximo del segmento es mucho menor, por lo que se utiliza para conexiones al nivel de la Sala de Telecomunicaciones o conexiones a nivel de escritorio.

1000Base-CX	
Velocidad	1000 Mb/s
Topología	Estrella
Cableado	Cobre blindado (2)
Conectores	RJ-45
Largo máximo del segmento	25 m
Modo	Full Dúplex

Ethernet 1000Base-T

La red 1000BaseT, de norma 802.3ab, permite también implementar Gigabit Ethernet. Emplea cable UTP de Categoría 5, pero utilizando 4 pares, en un sistema similar al 100Base-T, visto anteriormente

1000Base-T	
Velocidad	1000 Mb/s
Topología	Estrella
Cableado	UTP 5 – 4 pares
Conectores	RJ-45
Largo máximo del segmento	100 m
Modo	Full Dúplex

Como conclusión, podemos decir que el esfuerzo realizado por los distintos comités Ethernet por homologar las especificaciones, en lo que tiene que ver con el largo de tramas, y mecanismo de acceso al medio, permite no solo la coexistencia de los distintos tipos de redes Ethernet consideradas, sino también la migración gradual de un sistema a otro.

ALCANCE MÁXIMO PARA DIFERENTES REDES ETHERNET

ESTÁNDAR	VENTANA	LUZ	CONECTOR	FIBRA	DISTANCIA
10Base-FL	primera	normal	ST	62.5 /125	2 Km
100Base-FX	segunda	normal	SC	62.5 /125	2 Km
1000Base-SX	primera	Láser	SC	62.5 /125 50 /125	275 m 550 m
1000Base-LX	segunda	Láser	SC	62.5 /125 50 /125 9 /125	550 m 550 m 5 Km

En particular, en la actualidad ha tomado auge la migración a Gigabit Ethernet en muchos edificios, abordando generalmente el sustituir los cableados y switches en la línea de backbone (línea troncal o montante de distribución vertical), encarando posteriormente los diferentes grupos de estaciones, siguiendo la prioridad en lo referente a las necesidades de ancho de banda, jerarquía de la organización; etc.

A. 9. 7. 4. 2. Ethernet Isócrona

El método de acceso múltiple CSMA /CD no permite asegurar un reparto equitativo del ancho de banda. Una computadora con gran poder de generación de tramas podrá monopolizar la red. Por ello Ethernet no es una red apropiada para la transmisión de tráfico isócrono como lo es voz o video en tiempo real. Por ello se creó la variante denominada Ethernet Isócrona, también llamada ISO Ethernet, cuya estandarización corresponde al IEEE 802.9, del año 1995. Se utiliza la codificación 4B5B.

A. 9. 8. Otras Arquitecturas LAN

Existen otros estándares de Redes LAN, aparte de las Redes Ethernet. De algunas de ellas existen implementaciones pertenecientes a épocas preliminares del mundo de las redes, tales como las redes Token-Bus, normalizadas en el estándar 802.4 de IEEE.

En un tiempo también tuvo cierto desarrollo las redes AnyLan (802.12), en un intento por mejorar las aptitudes de las redes Ethernet de 10 Mb/s, pero con el advenimiento de 100 Mb/s y las Gigabit Ethernet y los bajos costos de Ethernet, la popularidad de AnyLan cayó bruscamente. Algo similar ocurre con las redes AppleTalk, que si bien tienen sus campos de aplicación, pertenecen a un medio ambiente específico restringido.

Se debe considerar que otro estándar, el 802.11 correspondiente a Redes Inalámbricas, es un tipo de redes que tendrá amplio desarrollo en los próximos años, debido a la gran difusión que están teniendo los dispositivos portátiles, handhelds, palms y teléfonos inteligentes (smart phones). Sin perjuicio de esto, hemos incluido esta variedad de estándares menos adoptados en la actualidad y otras que si completan el mercado Ethernet, como ser por ejemplo el Token Ring.

A. 9. 8. 1. Arquitectura Token Passing Ring

El protocolo de las redes Token Passing Ring, es base de la arquitectura de redes del sistema SNA de IBM, creada como objetivo de disponer una estructura de cableado simple. Esta versión IBM fue introducida en 1984 y en 1985 el IEEE /ANSI la convirtió en el estándar 802.5.

El método llamado Token Ring es utilizado tanto para las LAN como para las MAN. Su deferencia radica en que realmente no es un método de difusión, sino un conjunto de enlaces punto a punto que coincidentemente forman un círculo. En Token Ring, el control es totalmente centralizado. Para mantener las condiciones de vigilancia, una o más estaciones deben ser responsables de monitorear las funciones del protocolo Token Ring. Si se produce una condición de error, la estación responsable reinicia el anillo y/o comienza un nuevo token.

Las redes Token Ring deben su nombre a una pequeña trama de datos llamada “token” que cumple un papel esencial en este tipo de red, y a su característica topología en forma de anillo (ring).
Sin embargo la red Token Ring podrá tomar configuraciones físicas en anillo o en estrella. La configuración en estrella permite el alambrado centralizado con par trenzado que es más económico, además podrá disponer fácilmente del control centralizado. El Token Ring es un eficiente diseño para el movimiento de datos sobre redes medias o pequeñas. Como permite emplear muchas pequeñas tramas, provee mejor rendimiento que el CSMA/ CD.

Por definición Token-Ring consiste en un conjunto de estaciones conectadas en cascada formando un anillo virtual en el que la información es transferida de una estación activa a la siguiente. En la conformación Token Ring cuando se conecta un equipo a la red, se genera una pequeña trama de datos como señal testigo, denominada token. Este token es pasado (passing) de una estación a la siguiente, formando un anillo (ring) virtual. Una estación debe esperar por un token libre para poder transmitir los datos del mensaje. Cada estación recibe y regenera los bit que recibe, de forma tal que actúa como repetidor cuando está activa. Una vez recibido (copiado) los datos por el destinatario, éste envía mediante una marca una señal de confirmación de la recepción correcta. El token entonces es liberado y pasa a la estación siguiente, para el envío de un nuevo mensaje. Cuando la información vuelve a la estación que originó la transmisión, el mensaje es retirado de circulación.

Este método provee igual acceso a cualquier estación. Una de las estaciones actúa como monitor del token, resolviendo posibles accidentes. Los bit y cada trama transmitida datos la vuelta completa al anillo, en un determinado momento solo una computadora esta en modo transmisión, mientras que el resto han de estar en el modo a la escucha. Si no hay tráfico en la red, todas las computadoras están a la escucha. Se puede decir por ello que a los efectos prácticos, la red funciona como un medio broadcast.

Existen tiempos máximos de procedimiento, esto establece un tamaño máximo de trama, por ejemplo para un Token Ring de 4 Mb/s, tiene un tiempo máximo permitido para el envío de las tramas por máquina (Token Holding Time) de 10 mseg no podrá ser superior a 5000 Byte, mientras que para un Token Ring de 16 Mb/s, podrá ser de 20 000 Byte.

Cada estación de la red añade una cierta cantidad de jitter en la transmisión, lo cual limita la cantidad de máquinas para una red de este tipo. En las redes de 4 Mb/s con cable UTP el máximo es de 72 estaciones, mientras que para las redes de 16 Mb/s con cable STP el máximo es de 250 estaciones.

Aunque el Token Passing Ring presente un software virtual en anillo, se conforma físicamente con un concentrador central en estructura estrella. En este tipo de red, las estaciones de trabajo (WS) y el servidor, están conectadas por medio de cables UTP /STP a un concentrador central, del tipo unidad de acceso múltiple MAU (Multistation Access Unit). IBM ha implementado un modelo de red, con nombres específicos llamando unidad de acceso multiestación MSAU (Multistation Access Unit) o unidad inteligente de acceso multiestación SMAU (Smart Multistation Access Unit). El MSAU se encarga de realizar las vinculaciones (enganches) correspondientes y lograr la conformación virtual en anillo.

Cada MSAU, podrá soportar un máximo de 72 estaciones de trabajo con UTP ó mas de 260 WS con STP. Cada red podrá disponer de un máximo de 33 MSAU (Fig. 19).

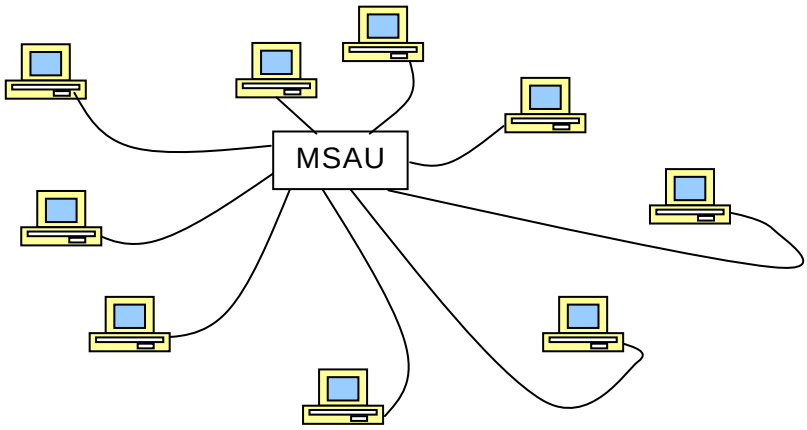


Fig. 19 - Cableado Token Ring

La velocidad de transmisión original era de 4 Mb/s, pero hay versiones de 16 Mb/s.

La codificación es Manchester diferencial. Las máquinas se conectan a las bocas 1 a 8 del MSAU mediante cables llamados adaptadores ó lobe pair (par de lóbulo), este nombre surge de considerar a cada vértice de la estrella como un lóbulo de ella.

Si la red tiene más de 8 puestos, se forma un anillo de MSAU conectando la salida de una MSAU llamada Ring Output (RO), con la entrada de la siguiente MSAU, llamada Ring Input (RI).

Los MSAU poseen un relevador por cada boca; la estación que se conecta, debe activar el relevador (relay), para insertarse en el anillo. Así se podrán conectar varias MSAU formando una conformación en anillo (Fig. 20).

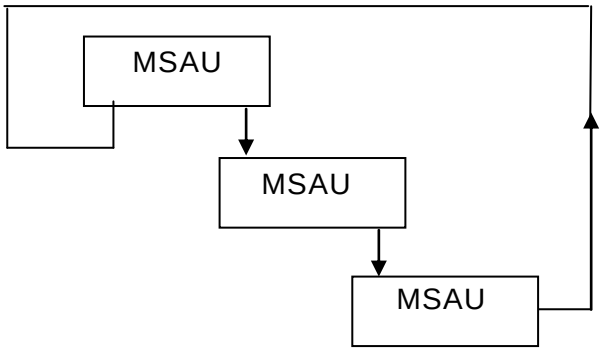


Fig. 20 - Configuración de una topología en anillo

La distancia entre dos MSAU tiene un límite de 15 m. Las vinculaciones entre las MSAU y las estaciones de trabajo, podrán tener como máximo hasta 100 m con STP, ó 45 m con UTP.

La menor longitud entre estaciones con STP ó UTP, deberá ser de 2.50 m. Las MSAU poseen un dispositivo que permite reconformar el anillo en sentido contrario, si se produjese una falla en uno de los segmentos utilizando los conductores redundantes del cable.

Hay dos formas de cablear el sistema, el llamado, sistema de cableado pequeño movible (small movable cabling system) y el, sistema de cableado grande no movible (large non-movable cabling system).

En ambos casos, se tienen los siguientes límites:

Small movable cabling system

- Se pueden conectar hasta 96 estaciones.
- Hasta 12 unidades MSAU 8228
- Distancia máxima entre el MSAU 8228 y una estación: 45,7 m (150 pies), al que hay que sumarle 2,4 m (8 pies) del adaptador.
- Distancia máxima entre dos MSAU 8228: 45, 7 m (150 pies).
- No franquear el cable por exteriores ni por conductos de ventilación, ni exponerlos a más de 75º Celsius, ni a interferencia eléctrica.

Large nonmovable cabling system

- Se pueden conectar hasta 260 estaciones y 33 MSAU 8228, pero se usa un montaje físico diferente (Fig. 21).

Formato de tramas Token Ring

El formato de una trama de datos Token Ring se esquematiza en la figura, aunque en realidad, el sector de datos ocupa casi el total de la trama.

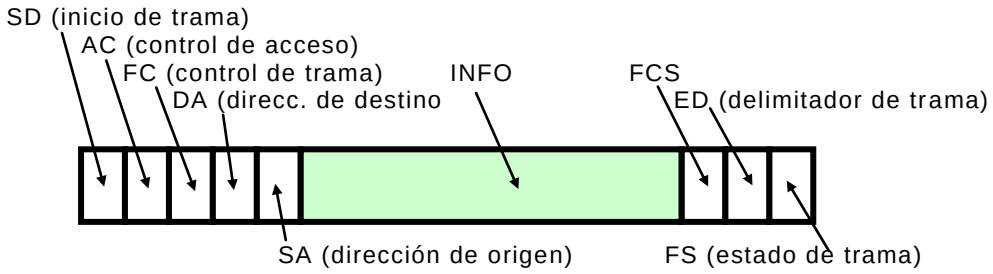


Fig. 21 - Ejemplo de trama Token Ring

Los campos de la trama Token Ring tiene los siguientes formatos:

1. SD, Starting Delimiter (1 Byte) Indica el comienzo de la trama.
2. AC, Acess Control (1 Byte) Permite identificar si es una trama común o es un token.
3. FC, Frame Control (1 Byte) Indica si la trama es de datos LLC o es una trama de control MAC
4. DATOS, Destination Adress (6 Bytes) Dirección de destino.
5. SA, Source Adress (6 Bytes) Dirección de origen.
6. RIF, Routing Information Field (2 a 18 Bytes) Campo Opcional de ruteo.
7. INFO Campo dedicado a los datos de información.
8. FCS, Frame Check Séquense (4 Bytes) Secuencia de chequeo de formato, es implementado con un CRC como en Ethernet.
9. ED, Ending Delimiter (1 Byte) Indica el fin de la trama.
10. FS, Frame Status (1 Byte) Estatus de formato, contiene los bit J y K que marcan si una dirección fue reconocida y si la trama fue o no recibida. Práctica común en Token-Ring, de utilizar bit dentro de los campos con fines específicos.

Los campos SD, AC y ED son los que componen la pequeña trama llamada Token.

Conexionado Token Ring

Diversas clases de conexionado han sido definidos por IBM, según una tipología de cables de pares trenzados de conductores de cobre:

- El Tipo 1 posee 2 pares AWG 22 con blindaje. Se usa principalmente para conectar los MSAU.
- El Tipo 2 ofrece 2 pares AWG 22 blindados y 4 pares AWG 26 sin blindaje; los pares extras son para conectar el teléfono con el mismo cable.
- El Tipo 3 tiene 2 pares telefónicos sin blindar. Es una alternativa barata al Tipo 1. La ventaja de usar este cable Tipo 3 es que en muchas empresas donde hay centrales telefónicas internas, quedan pares disponibles, por lo que no hay que hacer un nuevo tendido; la desventaja es que se limitan el alcance y la cantidad de dispositivos que se pueden soportar (72 en vez de 255).
- El Tipo 6 consta de 2 pares de cables de AWG 26 sin blindaje; es flexible y se usa para los alargues entre el cable adaptador y el MSAU 8228.
- El Tipo 9 consta de dos pares de AWG 26 blindados. Tiene menor alcance que el Tipo 1 (aprox. 66%), pero es más barato.
- Los cables mencionados soportan 16 Mb/s, excepto el Tipo 3 con sólo 4 Mb/s.

También se incluyen los cables de fibra óptica, de 140 micrones, que podrán sustentar 250 Mb/s o mayores velocidades digitales según sistema empleado.

Para ampliar el anillo, se puede usar el MSAU 8218, repetidor Token-Ring para cobre (Token Ring Copper Repeater), pudiéndose extender hasta 775 m. Otra alternativa es emplear el MSAU 8219 para fibras ópticas (Token - Ring Network Optical Fiber Repeater), que posibilita enlaces de hasta 2 Km.

Hay dos modelos básicos de placas: la Token Ring PC Adapter , para PC, XT, AT, y compatibles y la Token Ring Adapter/A (TRN/A), para PS/2 Modelo 50 y superiores. La diferencia entre ambas es, fundamentalmente, que la primera se conecta en una placa mainboard con bus tipo XT, mientras que la segunda es para un bus MCA (MicroChannel).

La dirección de base en el mapa de I/O es A20h (default); se puede escoger IRQ 2, 3 ó 7 (la IRQ 7 se superpone con la primera impresora). Se debe tener en cuenta que la Token Ring PC Adapter, decodifica 12 bit en I/O y no 10 (como es usual en una PC). Por lo cual se debe tener cuidado con las direcciones fantasmas, por ejemplo A20h se puede superponer con 220h (Fig. 22).

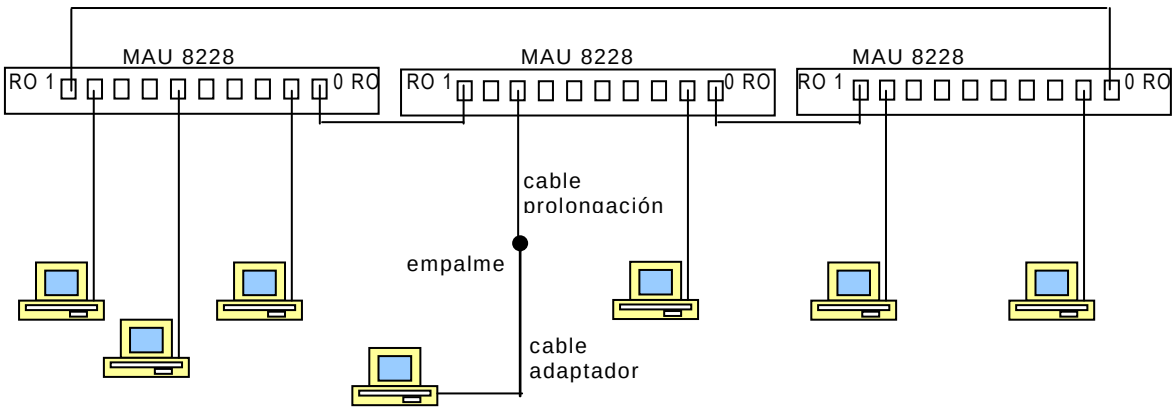


Fig. 22 - Conexionado Token Ring

Mantenimiento del Token Ring (Monitor activo)

En Token-Ring una de las estaciones tiene el importante papel de *Monitor Activo.*

Este tiene diversas funciones, que debe cumplir y eventuales problemas que debe solucionar, entre los que se cuentan:

- **Token perdido**

  Es el caso de que una estación tuviese retenido al token, quedase fuera de circulación antes de insertar un nuevo token.

- **Token corrupto**

  En su viaje a través de la red el token haya incorporado errores propios de la transmisión.

- **Token duplicado**

  Por falla en una estación que no capturase el token antes de trasmitir, con lo cual al recibir la trama insertará otro, duplicándolo.

- **Trama circulando indefinidamente**

  Una vez recibida una trama por la estación receptora y devuelta en el ínterin, la estación transmisora quedase fuera de servicio, con lo cual la trama seguiría circulando indefinidamente sin que ninguna estación la capture.

Estos y otros problemas deben ser resueltos para el normal desempeño de la red, por lo cual, el *Monitor Activo,* como su nombre lo indica monitorea constantemente la situación, detectando y corrigiendo las diversas anormalidades.

Manejo de Prioridades

A pesar de su alto costo, existen algunas ventajas en las redes Token-Ring. Una de ellas es la posibilidad de asignar diferentes prioridades a las distintas estaciones, algo que el Token Ring puede registrar, como vimos en el formato de trama del token, y por tanto se dispone de un mecanismo centralizado de asignación del derecho a transmisión, basado por ejemplo, en prioridades que reflejen la estructura de la organización en cuestión.

Token Ring	
Velocidad	4,16 o 100 Mb/s
Topología lógica	Anillo
Topología física	Estrella
Cableado	UTP / STP / Fibra
Concentradores	MSAU 8228

A. 9. 8. 2. Arquitectura Token Bus

El estándar Token fue creado por la empresa General Motor en 1985 y luego normalizado como IEEE 802.4. Describe una LAN llamada Token Bus, que cuenta con una disposición física en bus lineal, aunque dispone de una conformación lógica en anillo. La arquitectura Token Bus es empleada en el protocolo ArcNet.

En fábricas de automotores, la operación de montaje es lineal, luego su control y el curso de la información requieren que sea también lineal.

En el método Token Bus las estaciones están organizadas en forma de anillo al igual que en la red Token Ring, aunque físicamente se conforman sobre un cable lineal o en esquema de forma árbol. Emplea cables coaxiales de 75 Ohm, con velocidades de 1, 5 ó 10 Mb/s. Su trama puede tener un tamaño máximo de 8190 Bytes (Fig. 23).

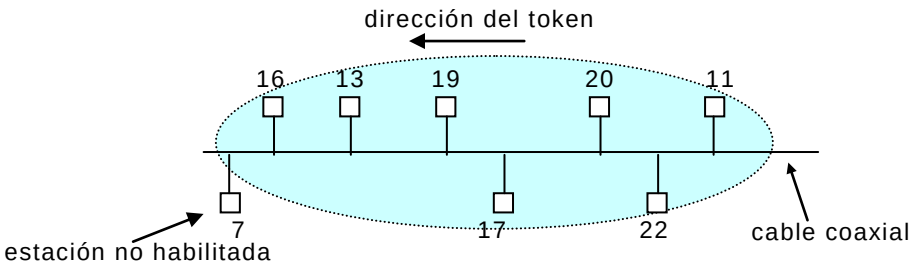


Fig. 23 - Token Bus

Cada máquina conoce a posición de cada una de las otras máquinas. Cuando se inicia el anillo lógico, se numeran las máquinas habilitadas en ese momento y la estación de número mas alto puede enviar la primera trama.

El orden es descendente. En Token Bus cada estación dispone de igual acceso al cable, puesto que el token es pasado alrededor del anillo, dando a cada estación un turno. En Token Bus, el control es totalmente descentralizado.

Además, este modo permite proveer prioridad de asignación al acceso sobre el anillo. Se podrá asignar alta prioridad o baja prioridad de transmisión, a cualquier estación. El Token Bus tiene cuatro niveles de prioridades para tráfico, de 0, 2, 4 a 6, con 6 el valor de mayor prioridad.

El Token busca la máquina de valor 6, si tiene datos los transmite, luego de expirar el temporizador busca la máquina de prioridad 4, continuando en esa secuencia.

A. 9. 8. 3. Arquitectura Apple Talk

La arquitectura AppleTalk (comúnmente llamadas LocalTalk), fue introducida por Apple Computer Inc. en 1983, para un pequeño grupo de investigadores. Esta diseñada como red económica para el hardware Macintosh.

AppleTalk Opera conforme a:

- Cuando se conecta un equipo a una red AppleTalk, el dispositivo se asigna aleatoriamente a si mismo una dirección, desde un conjunto de direcciones permitidas,

- El dispositivo difunde la dirección a la red para determinar si cualquier otro dispositivo la esta utilizando,

- Si ningún otro dispositivo la está utilizando, almacena esta dirección para ser utilizada en su próxima conexión.

Utiliza el método de acceso al medio CSMA /CA una topología de bus o árbol que conforme una topología lógica estrella bus. Puede utilizar cables UTP, STP o fibra óptica.

Aunque los sistemas Apple proveen sus productos, módulos de conexión, amplificadores, etc. están abiertos al desarrollo de productos de terceros. Apple Share es el servidor de archivos o servidor de impresora para la red AppleTalk.

La placa EtherTalk permite ejecutar redes AppleTalk en conexión a redes Ethernet con cable coaxial. Estas redes son sencillas y se pueden unir formando redes más grandes, creando “zonas de subredes” (Fig. 24).

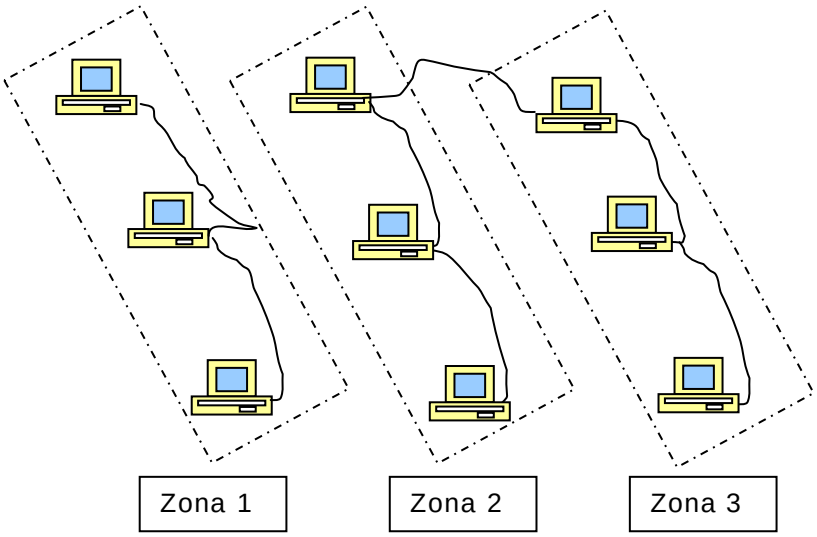


Fig. 24 - Red AppleTalk con zonas de subredes

A. 9. 8. 4. Arquitectura ArcNet

La arquitectura ArcNet fue diseñada por Datapoint Co en 1977, bajo la técnica Token Passing Bus, transmitiendo a una velocidad de 2.5 Mb/s. Posteriormente se creó la ArcNet Plus, que puede soportar una velocidad de 20 Mb/s. La norma IEEE 802.4 especifica su estándar, Token Passing Bus para banda ancha.

Esta técnica utiliza transmisión en banda base. Se trata de una red económica, que utiliza cables coaxiales, con un Hub pasivo, activo o inteligente. Un concentrador pasivo distribuye la señal, mientras que un concentrador activo regenera los pulsos y un concentrador inteligente, además de regenerar los pulsos, diagnostica cambios de configuración y permite conexiones a puertos de control.

Esta arquitectura puede tener una topología tanto tipo bus, como estrella. Los paquetes contienen un campo de datos y las direcciones de origen y destino, según el esquema de la Fig. 25.

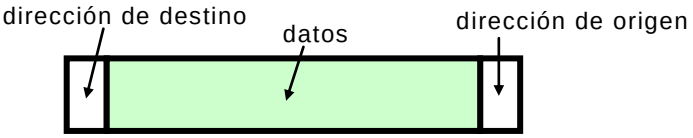


Fig. 25 - Paquete ArcNet

En esta red, el cableado estándar se realiza con cable coaxial de 93 Ohm. Se pueden obtener distancias de 600 m en topología estrella, ó 305 m en topología de Bus. La distancia entre Hub activo y Hub pasivo será de 30 m. Utilizando cableado UTP, la distancia máxima es de 244 m entre dispositivos, para la topología de bus o estrella. También admite cableados en fibra óptica.

A. 9. 8. 5. Arquitecturas LAN ATM

La tecnología ATM para conectar varias LAN esta llevando a disponer de redes ATM que funcionan como una LAN. El problema principal a resolver es como proporcionar servicio de LAN que se realizan sin conexión a través de una red ATM orientada a la conexión. Una posible solución es introducir un servidor sin conexiones.

Cada Host se comunica con este servidor y envía a este todos los paquetes para que los reenvíe. Esta solución tiene el inconveniente de no aprovechar todo al ancho de banda de la red ATM.

Otra alternativa propuesta por el Foro ATM, es que cada Host disponga de circuitos virtuales ATM potenciales a todos los otros Host. Estos circuitos virtuales pueden establecerse dinámicamente según se necesiten o podrán ser circuitos virtuales permanentes. Para enviar una trama el Host de origen encapsula un paquete en el campo de carga útil de un mensaje AAL ATM y lo envía a destino, de la misma forma que en cualquier red LAN Ethernet o de otro tipo.

En este último caso, el inconveniente reside en como determinar los circuitos virtuales a los que pertenecen las direcciones IP. Como las LAN ATM no operan el modo difusión se introduce un servidor que sí lo maneje. Puede ser el Servidor de simulación de LAN, denominado LES (LAN Emulation Server) que encapsula el mensaje deseado enviándolo a destino o el Servidor de difusión /desconocido BUS (Broadcast /Unkown Server) que tiene conexión a todos los Host y puede simular difusión enviando los paquetes a todos ellos.

Un modelo semejante ha sido adoptado por las Fuerza de Tareas de Ingeniería de Internet IETF (Internet Engineering Task Force), como la manera oficial en que Internet utiliza una red ATM, para enviar paquetes IP. En este modelo, al servidor LES se le denomina server ATMARP. Con el mismo, se puede agrupar un conjunto de Host ATM para formar una subred, a la que se le denomina IP Lógica ó LIS (Logical IP subnet).

Otra solución es crear redes ATM con conmutadores en diferentes topologías. En ese caso las placas de red ATM, trabajan a velocidad de 25 ó 155 Mb/s. Se crea un backbone con unos pocos conmutadores ATM interconectados y estos a otros conmutadores denominados de acceso LAN-ATM,. Estos conmutadores LAN-ATM, permiten conectar ATM a Host de redes locales, del tipo Ethernet, Token Ring ó FDDI. La solución del ATM Forum, denominada ATM LANE (LAN Emulation) consiste en encapsular en celdas ATM las tramas MAC de la LAN que emula (Ethernet, Token Ring ó FDDI).

El tamaño máximo recomendado para estas redes es de 200 estaciones en Apple Talk, 500 en Novell Net Ware y 100 en IP.

A. 9. 9. Fiabilidad y códigos LAN

El estándar 802.3 estableció inicialmente una tasa de error máxima o BER (Bit Error Rate) de 10^{-8}, mientras que los nuevos medios físicos fijaron requerimientos superiores, por ejemplo el FDDI fija una tasa no superior a 4×10^{-11}. y el Fibre Channel no superior a 10^{-12}. Debido a ello la subcapa MAC no efectúa ninguna verificación.

En Ethernet la transmisión se realiza asíncrona es decir que no hay reloj maestro, por ello se emplea el sincronismo embebido en la misma trama de datos, mediante ciertos códigos. Por ejemplo a 10 Mb/s Ethernet emplea el código Manchester. En este caso, el emisor debe enviar el doble de pulsos de lo que haría falta con un código como el NRZ (Non Return to Zero). Se transmiten 20 MBaud (megasímbolos) para enviar 10 Mb/s de información útil. Como consecuencia, por el cable viaja el doble de los pulsos.

Se dice que este código tiene poca eficiencia, con una sobrecarga del 100% (overhead 100%). Pero se implemento cuando se diseño Ethernet originalmente, con cables coaxiales (10Base-2 y 10Base-5), al ser sencillo de ejecutar y por ello económico. En cuanto se quiso utilizar cable UTP, surgió el problema. En Fast Ethernet el uso del código Manchester habría requerido transmitir 200 MBaud con cables de Categoría 5 lo cual excede las normativas de cables estructurados.

Los estándares 100Base-FX, con dos fibras ópticas y 100Base-TX, con dos pares trenzados, UTP ó STP de Categoría 5 requirieron utilizar el código 4B5B. Este código se creó para el sistema FDI y emplea 5 símbolos para enviar 4 bit. La señalización es de 125 MBad para 100 Mb/s. Esto permite cable Categoría 5, aunque este especificado hasta 100 Mb/s.

El estándar 100Base-T4 es un caso más complejo ya que utiliza cable de Categoría 3 telefónico, el protocolo CSMA /CD requiere que en todo momento haya un par disponible para notificar la presencia de colisiones. Por ello se emplean cuatro pares. La codificación que se emplea es la 8B6T, 8 bit/ 6 trits, llamado trit a una señal que puede tomar tres valores o sea tres valores en Volt distintos.

En el caso de GigaEthernet para los distintos 1000Base-X se emplea el código 8B10B (8 bit en 10 Baud que también se utiliza en Fibre Channel. Este código tiene una sobrecarga del 25% (overhead 25%), igual que en 4B5B, pero al agrupar mas símbolos tiene una mayor redundancia. Para conseguir transmitir 1 Gb/s full dúplex en GigaEthernet, por un cable UTP Categoría 5 se ha adoptado:

- Utilizar PAM 5x5,
- Repartir la señal entre cuatro pares, Cada par con 250 Mb/s y 125 MBaud,
- Usar cada par simultáneamente en ambos sentidos.

Se dice que, podrá lograr cualquier caudal de datos, por cualquier categoría de cable UTP, si se utiliza un número adecuados de pares y un código suficientemente rico, lógicamente para ello se requiere una relación señal /ruido mayor en los transceivers (transmisor y receptor) y por ello mayor costo.

A. 9. 10. Comparación entre sistemas LAN

Ambos tipos de protocolos, el CSMA/CD y el Token Passing tienen uso generalizado, aunque el CSMA/CD se ha estado imponiendo en los últimos años. La ventaja de éste es permitir mayor performance, especialmente cuando hay pocas colisiones.

Esto ocurre si la mayoría de las transmisiones se originan en la misma máquina o si hay relativamente poco tráfico en la red. Una ventaja del segundo es que puede asegurarse que, independientemente del tráfico en la red, una máquina va a poder transmitir antes de un tiempo predeterminado.

Ello tiene dos efectos positivos. Uno es que la performance de la red no disminuye tanto al aumentar el tráfico; otro efecto (aunque su uso es menor) es constituir un sistema de control, donde es importante asegurar que un mensaje llegue a destino, antes que pase cierto tiempo, como sucede en el caso de aplicaciones críticas. Otra ventaja posible para el segundo efecto es que soporta un esquema de prioridades para el uso de la red.

Por estas razones, el CSMA/CD ha sido durante mucho tiempo el preferido para oficinas, mientras que el Token Passing, se ha antepuesto para su empleo en fábricas. Con el advenimiento de las últimas tecnologías Fast-Ethernet y Gigabit Ethernet, la balanza se ha ido volcando paulatinamente a favor de Ethernet para los diversos usos, especialmente considerando que en Full Dúplex no subsiste la desventaja de las colisiones.

El Token Ring tuvo auge cuando alcanzó los 16 Mb/s, se llegó a desarrollar para 100 Mb/s aunque a costos elevados. En su momento se formó un comité para un eventual Gigabit Token-Ring, pero con poco éxito, en vista del desarrollo masivo de Ethernet y el hecho de ser éste un estándar independiente del fabricante.

Con todo, existen muchas redes implementadas con este sistema, en las cuales incluso es posible añadirles nuevas redes Ethernet (mediante un tipo de Bridges llamados “traductores”).

A. 9. 11. Planificación de una LAN

Vemos sucintamente los pasos a seguir para una correcta planificación de una LAN, lo cual incluye la elección de los diferentes sistemas expuestos.

Podríamos describir ocho pasos básicos:

1. **Relevamiento de necesidades**

   Considerar sobre la base de los eventuales usuarios de la red, sus necesidades de comunicación, tanto internas como externas. A partir de esto, generar un Documento de Especificación de Requerimientos, como se acostumbra en el caso de la producción de software, para tener en claro los objetivos a seguir, y que servicios brindará o no la red propuesta.

2. **Elección de la topología**

   En un principio es necesario determinar la estructura física de la red. Para ello es de utilidad obtener un plano del lugar, edificio o edificios en los que se realizará el tendido. Luego, analizando de lo más general a lo menos significativo, definir la ubicación de Servidores, Centro de Telecomunicaciones y ubicación de los diferentes Puestos de Trabajo.

   Una vez que está especificada la ubicación de los puestos, se puede definir como se realizará el cableado necesario para llegar hacia ellos. Es posible colocar ductos adosados a la pared, bandejas en el cielorraso o bien un sobrepiso para realizar todas las conexiones por debajo de los puestos. Su elección dependerá de las necesidades de flexibilidad, seguridad y también, obviamente del presupuesto disponible.

   Por otra parte, es importante prever los eventuales crecimientos, para que la red no fuera insuficiente al poco tiempo de su instalación; por ejemplo, colocando más terminales en salas de reuniones; etc. Una vez definido, por lo general la tarea del cableado en sí, se contrata con compañías de cableado estructurado, especializadas para ello y que suelen dar garantía por las instalaciones.

3. **Elección de elementos activos**

   En esta etapa se seleccionan los Switch, Hub y las velocidades de los mismos, así como los Bridge, en caso de que se requirieran. Las velocidades se pueden definir sobre la base del tráfico esperado, cantidad de puestos, necesidad de ancho de banda, posibilidades de crecimiento; etc. Se debe tenerse en cuenta que, para cada especificación, deberán también adquirirse las tarjetas de red para las estaciones y servidores, como parte de la infraestructura.

4. **Sistemas operativos**

   Una elección clave, que depende de varios factores, pero básicamente de que software va a correr encima, corresponde a los distintos Sistemas Operativos. Estos permiten ofrecer diferentes servicios, niveles de seguridad, soporte plug & play; etc. Un factor a tener en cuenta es el de las licencias, dado que se requieren licencias para el Servidor o Servidores, licencias de usuarios en las estaciones, pero también Licencias de Acceso de Cliente (LAC) para las mismas, a fin de cumplir los requisitos legales (sí bien es común que varias de éstas últimas estén incluidas con la licencia del Servidor).

5. **Estructura de dominios**

   Aquí se definen el o los dominios a utilizar, Directorio Activo; etc., es decir la estructura lógica de la organización reflejada en la red.

6. **Seguridad**

   Los Sistemas Operativos ofrecen diferentes niveles de seguridad disponibles, sobre los cuales se deberá decidir en esta etapa para diseñar un sistema seguro y sustentable.

7. **Documentación**

   Preparar y legalizar (llegado el caso) la respectiva documentación, un paso muy importante que a veces se obvia en organizaciones pequeñas, con las consiguientes complicaciones a la hora de realizar ampliaciones o reparaciones.

8. **Capacitación de usuarios**

   Si bien no es parte específica de la planificación de la red, lo incluimos, para enfatizar la importancia de no obviarlo, ya que sin él, la mejor planificación fracasará. Al dar debida atención a la capacitación de os usuarios, cerramos el último eslabón en la cadena de comunicación, a los efectos de que la organización funcione eficientemente en lo que tiene que ver con el uso de la red y sus servicios.

A. 9. 12. Redes de áreas amplias, MAN y WAN

En el amplio escenario de las WAN, con la interconexión de varias LAN distantes y formando así una Red Corporativa, muchos de los protocolos y categorías de redes empleados, se refieren a la implementación de Redes Privadas, como ser de Intranet.

Un objetivo de las redes WAN, es el acceso e integración del usuario doméstico y de una pequeña empresa a la Red Mundial, como el caso de Internet.

Las WAN se constituyen en subredes que vincula dos o más LAN. En esta subred, un Host es un usuario final y un nodo un medio de conmutación. Las grandes redes para transporte de datos, utilizan en su arquitectura para la transferencia de datos ciertas técnicas y protocolos exclusivos creados a ese fin.

Con estos enlaces entre LAN, se pueden formar considerables redes, las redes de áreas metropolitanas MAN (Metropolitan Area Network) cuando se desarrollan en el ámbito de una ciudad, o las redes de área extendida WAN (Wide Area Network) cuando se amplían en el ámbito nacional o internacional. Las LAN usan un canal multiacceso como base de su comunicación, en cambio las WAN usan enlaces punto a punto.

Muchos medios de transmisión o dispositivos de redes, no permiten aportar todas sus posibilidades. Para tener una idea de los volúmenes de información que manejan los medios físicos de transmisión y las limitaciones que ofrecen los Terminales, podremos dar un ejemplo. Si un enlace de fibras ópticas transmite a 622 Mb/s, representará la cantidad de información de todo el contenido de la Enciclopedia Británica, incluyendo los gráficos, transmitido todo en tan solo un segundo. Si el mismo volumen de información se transmite con un módem de 2400 Baud la operación llevaría a tardar más de dos días. Estas velocidades hicieron a la expansión de los enlaces con fibra óptica y creación de las técnicas propias de las MAN y las WAN.

A. 9. 12. 1. Capa física WAN

Puede considerarse que existen semejanzas en algunos aspectos entre LAN y WAN, particularmente en la aplicabilidad del modelo de separación en capas de OSI, útil también al caso de las WAN.

Sin embargo, una diferencia clave existe entre ambos tipos de redes, mientras en las LAN vimos que en general estas redes no superan áreas de 2 Km de extensión, en las MAN y WAN el objetivo es superar esta restricción. Asimismo en las LAN se interconectan muchas estaciones compartiendo un medio común, en las WAN tendremos siempre un enlace *punto a punto*, por lo que para vincular entre sí muchos sitios se recurre a la utilización de conmutadores, por lo que se les suele llamar redes conmutadas.

En la Capa Física (Capa 1), existen como ya se consideró anteriormente, dos DTE conectados a sus correspondientes DCE, mediante interfases, y entre ambos DCE un medio de transmisión, que puede ser conductores metálicos, de fibra óptica o sistema inalámbrico, este último de enlace terrestre o a través de un satélite de comunicaciones.

Las red de telecomunicaciones es una combinación de topologías tipo estrella, anillo, árbol y malla, mientras que las redes satelitales son de difusión (broadcasting), por lo tanto es imprescindible la conformación, dentro de estar redes y sistema, de redes privadas mediante la creación de canales virtuales.

En el caso de las LAN, se posibilitaban velocidades de hasta los Gb/s, sin embargo para el caso de las WAN, por las distancias a cubrir y el uso de las redes públicas sus velocidades se verán acotadas a menos de 1 Mb/s. Aunque las redes de transporte que enlazan centrales son implementadas actualmente en fibra óptica, la red de acceso al cliente lo son en pares trenzados de cobre. Ello, impacta sobre el tipo de servicios que puede brindarse, e incluso en el diseño del software a utilizar. Para subsanar esta restricción de la red de acceso, se deberán emplear en la misma módems tipo xDSL.

Por otra parte, también hay un obstáculo en cuanto a su confiabilidad. Si bien en las LAN, la seguridad e integridad de los datos se conseguía, con una baja tasa de error, en el caso de las WAN, debido a la diferente naturaleza de los enlaces y su mayor extensión, se debe considerar y proveer, los mecanismos que permitan un enlace confiable.

En la formación de las MAN, se emplea el estándar denominado, sistema bus dual de cola distribuida DQDB (Distributed Queue Dual Bus), mientras que para la formación de las WAN varias podrán ser las técnicas utilizadas, tales como X 25, Frame Relay, FDDI y ATM o las dedicados a redes ópticas SONET/ SDH, vistas en el anexo respectivo. Los equipos que permiten la formación de estas grandes redes, pueden ser, repetidores, Bridges, Routers y gateway, cada uno con sus respectivas características de aplicación.

A. 9. 12. 1. 1. Interfases

Las interfaces empleadas en las WAN, como en el caso de otras conexiones físicas, implican la utilización de ciertos conectores, cableado, protocolos de hardware y ciertos valores eléctricos u ópticos específicos para cada caso. Veamos las diferentes especificaciones de las interfaces mayormente difundidas.

Interfase Serial RS-232

La interfase Serial RS-232, se emplea considerablemente, ello se debe a que con él, se pueden alcanzar velocidades digitales de hasta 64 Kb/s, con un cableado de longitud máxima de 30 m.

Esta interfase se denomina "Serial", debido a que su conector es el propio puerto serial.

Dicho conector, es un conector del tipo “D” (norma ISO 2110), pudiendo contener 9 ó 25 pines. En forma convencional, los conectores de puerto serial tipo macho, se utilizan para los DTE y los de tipo hembra para el DCE. Por ejemplo se puede observar que el puerto serial de una PC es de tipo macho.

Las funciones de cada una de estas conexiones se pueden resumir en

1. Tierra de Protección
2. Transmisión de Datos (Permanece activo en la transmisión)
3. Recepción de Datos (Permanece activo en la transmisión)
4. Request to Send (Control de flujo, indicando petición de transmisión)
5. Clear to Send (Control de flujo, indicando señal de estar listo "Ready", una vez que se desocupa el buffer. No son muy utilizadas, debido a que provocan un corte abrupto en caso de llenarse el buffer, mientras que mediante control desde software se puede lograr un corte más llano)
6. Data Set Ready (Indica sí el DCE está listo para la transmisión. Una vez que se establece, esta línea permanece en 1 durante toda la transmisión)
7. Tierra de Señal (Línea de retorno para cerrar el circuito de la señal)
8. Data Carrier Detect (Informa respecto a la disponibilidad del medio entre DCE)
9. TXC y RXC (Para las transmisiones sincrónicas, estas líneas sincronizan respectivamente la transmisión y la recepción, entre el DTE y el DCE, a fin de permitir la identificación de los bit de las mismas. No siempre son utilizados en la actualidad, debido a que en muchos casos se utilizan relojes proporcionados por las propias redes)
10. Data Terminal Ready (Análogo a la señal Data Set Ready, pero para el DTE, indicando sí está listo para la transmisión. Permanece fijo en 1, durante toda la transmisión).

En algunos casos se realiza una Conexión Balanceada, sin utilizar el retorno común del Pin 7 (que era tanto para el transmisor TXC, como para el receptor RXC). Al independizarlo, se logra llevar el límite de velocidad hasta los 2 Mb/s.

CORRESPONDENCIA ENTRE PINES DTE y DCE

DTE	FUNCIÓN	SENTIDO	DCE
1	Tierra protección		1
2	Transmisión de datos	→	2
3	Recepción de datos	←	3
4	RTS (Request To Send)	→	4
5	CTS (Clear To Send)	←	5
6	Data Set Ready	←	6
7	Tierra de señal		7
9	DCD (Data Carrier Detect)	←	9
15	TXC	←	15
17	RXC	←	17
20	DTR (Data Terminal Ready)	→	20

Interfase V.35

La Interface V.35 funciona con datos y relojes balanceados pero con control no balanceado, pudiendo lograrse de esta manera velocidades mucho mayor. Se alcanza velocidades digitales de hasta 2 Mb/s. Se trata de la interfase más utilizada, para los casos de emplear Routers.

Con respecto a los conectores, se utiliza una tecnología un tanto obsoleta y costosa, como lo son los Conectores Winchester, americanos. Por su compatibilidad a las redes existentes, continúa siendo el estándar ventajoso a esta interfaz.

Interfase X.21

La Interfase X.21 es de origen europeo. Utiliza datos y relojes balanceados, y para el control. Se utilizan solamente dos Pin. El ahorro en Pin, se traduce en una dificultad mayor a la hora de codificar /decodificar, ya que los mensajes son enviados como una combinación de caracteres, por lo que son necesarios algoritmos de codificación /decodificación. No obstante ello, el efecto negativo en las competitividades es mínimo.

El conector en la interfase X.21 es el “D”, muy parecido al de ISO 2110, aunque no compatible con este. Las diferencias entre las interfases, para los distintos estándares no son de todos modos insalvables, existen en el mercado adaptador entre unos y otros, tanto al nivel de la conexión mecánica como de la señal eléctrica.

Interfase G.703

La Interfase G.703, ha sido diseñada para velocidades altas, pudiéndose lograr en su versión estándar con cable coaxial, velocidades digitales de hasta 2 Mb/s. Para el caso de utilizar fibra óptica, existen normas de 155 Mb/s y hasta 622 Mb/s.

A. 9. 12. 1. 2. Nodo conmutador o enrutador

Las redes MAN se caracterizan por no contener elementos de conmutación, mientras que las grandes redes WAN si utilizan redes de transporte con arquitectura que involucran nodos de conmutación para la transferencia de los datos. Estos nodos, son constituidos por computadoras especializadas que disponen de varias líneas de entrada y varias de salida. Oficiando como conmutadores, escogen la línea de salida correspondiente a la dirección solicitada y la vinculan a la línea de entrada.

Según las diferentes tecnologías empleadas, se podrá hablar de nodos conmutadores o de nodos enrutadores, aun cuando sus procedimientos son similares. Se emplean ciertas técnicas y protocolos para el enrutamiento de los paquetes de datos y en particular para la conmutación de las líneas de entrada/ salida. Estas técnicas ofrecen una mayor categoría de ancho de banda, al que requieren los accesos al medio y enlaces de las redes LAN.

Mediante un conmutador LAN se divide una red en partes, obteniendo mayor capacidad (velocidad de transmisión) en cada una de ellas. Al acomodar un segmento de red por equipo, disponemos de todo el ancho de banda para él.

Los Routers trabajan al nivel de Capa 3, mientras que un conmutador podrá trabajar a nivel de Capa 2 o de Capa 3. Por ello, se lo distingue, indicando como Conmutador de Nivel 2, ó Conmutador de Nivel 3.

A. 9. 12. 1. 3. Proceso de tunelado

El logro de la interacción de dos redes diferentes es extremadamente difícil. Sin embargo hay un caso especial que puede manejarse relativamente fácil. Este es cuando el Host de origen y el Host de destino están en la misma clase de red, pero hay una o más redes distintas intermedias. Los paquetes deben viajar a través de una red de otro tipo.

Por ejemplo, fuese una casa central de una manufacturera situada en Lima, con una red Ethernet transmitiendo en TCP/IP, a una de sus sucursales situada en Caracas con una red también Ethernet, pero a través de una red WAN de un operador particular con protocolo SNA. La solución es una técnica denominada de tunelado (tunneling).

Para enviar un paquete IP al Host 2, el Host 1 construye un paquete que tiene la dirección del Host 2, lo inserta en una trama Ethernet dirigido al enrutador multiprotocolo y lo pone en Ethernet.

Cuando el enrutador multiprotocolo recibe la trama, retira el paquete IP, lo inserta en el campo de carga útil del paquete de Capa de Red de la WAN y dirige el paquete WAN a la dirección de la WAN del enrutador multiprotocolo de Caracas. Al llegar allí, el enrutador de Caracas retira el paquete IP, del paquete WAN y lo envía al Host 2, en una trama Ethernet.

La WAN puede entenderse como un túnel que se extiende desde un enrutador hasta otro, el paquete IP simplemente viaja de un extremo al otro, sin preocuparse que esta transitando por una WAN.

El tunelado supone un encapsulado con pérdida de rendimiento ya que los paquetes viajan con doble cantidad de cabeceras, sin embargo es una solución cuando se trata de enviar poco tráfico. En Internet se han definido estándares de este tipo de encapsulado.

A. 9. 12. 1. 4. Proceso de sincronismo

El modo de Transmisión Sincrónica, implica la utilización de dos líneas o dos canales, uno para enviar los datos y otra para enviar la señal correspondiente de reloj, al fin de sincronizar la transmisión y la recepción (Fig. 26).

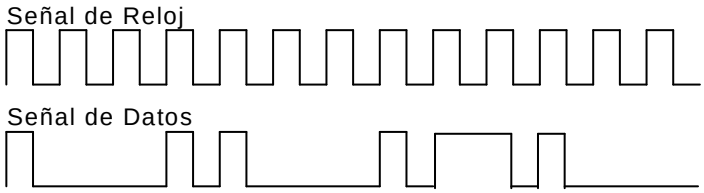


Fig. 26 - Correlación de las señales de datos y de reloj

En el caso de la Transmisión Asincrónica, al no utilizar sincronización por reloj, se requiere para el envío de la trama de información, adicionarle dos bit relativos al arranque y parada (Fig. 27).

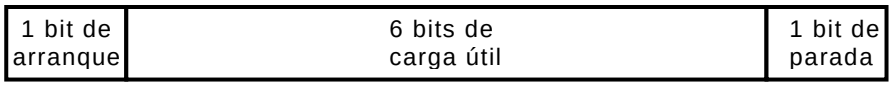


Fig. 27 - Estructura de trama para una transmisión asincrónica

En este formato, el bit de arranque estará en 0 para el reposo y en 1 cuando arranca, mientras que el bit de parada se marca con 0 al arranque y con 1 al reposo, después del final de la transmisión de la trama. Al ser utilizados por cada uno de los Byte transmitidos dos de sus ocho bit como campos de control, se introduce un 20% de ineficiencia.

A. 9. 12. 1. 5. Redes TDM

Las redes TDM (Time Division Multiplexer) son redes de enlace punto a punto y exclusivamente para ancho de banda reservado. Este tipo de multiplexación ha tenido amplia aplicación a los enlaces WAN. En Latinoamérica ha sido común que las empresas de telefonía brindasen este servicio como una opción para red de datos (ver Anexo I y Anexo II).

Las estaciones o los DTE, son conectadas mediante un, terminal de red NT (Network Terminal), punto de ingreso a la Red TDM. Se monitorea su funcionamiento, desde el Centro de Supervisión del Proveedor de Servicios de Red TDM (Fig. 28).

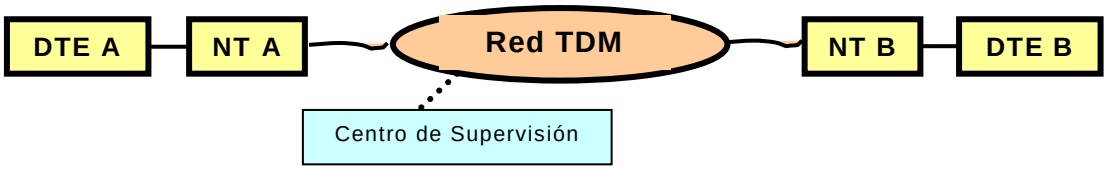


Fig. 28 - Estructura de trama en transmisión asincrónica

El sistema de TDM es de Capa Física (no un protocolos de red), por lo cual se trata de un servicio transparente que podría pensarse, como un enlace punto a punto. Debido a esto, no existen Switches en las redes TDM, sino sólo Repetidores que son dispositivos de capa Física que no trabajan sobre protocolos.

Esto resulta conveniente desde el punto de vista de la disponibilidad permanente del enlace, y la seguridad del ancho de banda que puede garantizarse.
El principal inconveniente radica en que, de esta forma se reserva un ancho de banda determinado, el que no siempre estará en uso con el consiguiente desperdicio de recursos.

Las redes TDM, por tanto, son enlaces dedicados de alto costo, muy adecuados para organizaciones grandes y medianas con alto tráfico en un enlace particular y necesidad de ancho de banda asegurado. Otras redes, de recursos compartidos resultan ser opciones más adecuadas para organizaciones medianas o empresas pequeñas, como en el caso de las PYMES.

A. 9. 12. 2. Capa de Enlace WAN

De acuerdo al modelo OSI, la Capa 2 como Enlace, es un nivel que ya no considera la transmisión de datos como una secuencia de bit como lo realiza la Capa Física, sino que la unidad de transmisión es la trama.

Entendemos por trama, de aquí en más, a un conjunto de bit delimitado de una manera predeterminada conocida. Las tramas cumplen una doble finalidad: Control del Flujo de Transmisión y Control de Errores. En redes WAN, la estructura básica de la trama ha sido normalizada según ISO, en la estructura, control de enlace de datos de alto nivel HDLC (High level Data Link Control).

Se trata de un esquema originado en los años de 1970, a partir del SDLC (Synchronous Data Link Control) de IBM (Fig. 29).

Fig. 29 - Trama HDLC de la ISO

- Los campos F (Flag), significan banderas delimitadoras de la extensión de la trama.
- El campo A (Address), donde se ubica la dirección.
- El campo C (Control), de control que identifica el tipo de trama.
- El campo INFO (Information), que contiene los datos de información.
- Campo FCS (Frame Check Sequence), para el control de errores en la trama.

Esta estructura básica HLDC es la definición a partir de la cual se derivan los diferentes protocolos de Capa 2 de Enlace, que operan sobre las WAN.

Los protocolos más utilizados en esta capa son:

- LLC (Logical Link Control)
- LAP-B
- LAP-D
- Frame-Relay
- PPP

El primero, control de enlace lógico LLC, ya lo hemos considerado en el caso de las LAN como subcapa inmediata superior a la Subcapa MAC de la Capa 2. Es el protocolo adoptado por IEEE para las LAN. Los cuatro restantes son los más utilizados en cuestión de las WAN, por lo que efectuaremos su análisis en particular.

Protocolo LAP-B

El protocolo denominado, procedimiento de acceso a enlace - balanceado LAP-B (Link Access Procedure - Balanced), es un protocolo de amplia difusión, usado en general por los Routers (Fig. 30).

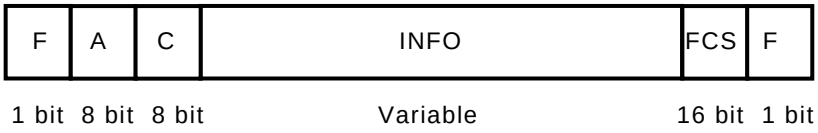


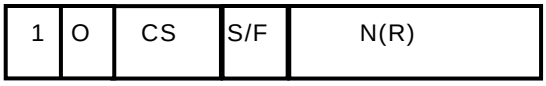
Fig. 30 - Trama LAP-B

1) Los **Campos de Bandera** (F) delimitan la extensión de la trama. En el caso del protocolo LAP-B, los 8 bit del Campo de Dirección (A), en realidad no son necesarios, ya que solo se codifica estación de origen (01) o estación de destino (03). Por ello, solo bastaría con solo 1 bit, pero se mantiene la extensión del campo por compatibilidad dentro del formato HDLC. Su finalidad es simplemente permitir identificar lo que es Comando de lo que es Respuesta.

2) El **Campo de Control** (C), puede tener tres tipos de formatos: a) de Información, b) de Supervisión, c) no Numerado.

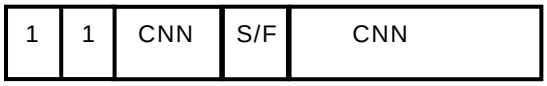
a) El Formato de Información se identifica mediante el primer bit en cero, y corresponde a las tramas que transportan tramas de información. El campo N(S) es de secuencia para la numeración de las tramas (3 bit). El campo S/F (Sondeo/Final), con S una computadora o un concentrador invitar a enviar datos; salvo con F que indica final (1 bit). El campo N(R), identifica la trama siguiente (3 bit).

b) El Formato de Supervisión se identifica con los 2 primeros bit en el valor 10. El campo CS, corresponde al tipo de códigos de supervisión, que pueden tomar cuatro posibilidades:



- 00 : RR (Receptor Ready) receptor preparado
- 01 : REJ (Rejected) rechazado
- 10 : RNR (Receptor Non-Ready) receptor no preparado
- 11 : SREJ (Selected Reject) rechazo selectivo

d) El Formato No Numerado se identifica con los dos primeros bit en 11. Estas tramas no numeradas, tienen las funciones pertinentes a las Primitivas de Servicio, que veremos más adelante.



Las tramas entrañan diferentes significados, de acuerdo a la codificación provista por el estándar.

A modo de ejemplo, mencionamos las más importantes:

- 00-010: DISC - Desconectar
- 00-110: UA - Asentimiento no numerado
- 11-000: DM - Desconectar Modo
- 11-100: SABM - Establecer ABM (Asyncronic Balanced Mode)

3) El **Campo INFO** corresponde a los datos de información. Según la estructura del modelo OSI, este campo contiene la trama completa de la Capa 3, de Red.

4) El **Campo FCS**, incluye un código CRC para verificación de errores en las tramas.

El protocolo LAP-B se implementa, para conformar una WAN mediante la interconexión de varias LAN. Para ello se emplean equipos adaptadores de red (EA), como ejemplo para interconectar dos LAN (Fig. 31).

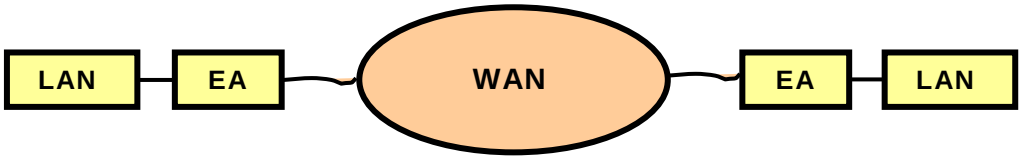


Fig. 31 - Interconexión LAP-B

Supongamos que un equipo de la LAN de la izquierda envía un mensaje, existirán dos posibilidades: que la trama corresponda a un destino local, o fuese para transmitir a través del enlace WAN. Esta verificación se hace mediante la dirección MAC, ya que el equipo adaptador de la red contiene las direcciones MAC de las estaciones de la otra LAN. Es decir que, si reconoce la trama como de destino a otra red, se preparará para transmitirla a través del enlace WAN.

Una de las dificultades que se presenta para la transmisión tiene que ver con la longitud de las tramas. Mientras que la máxima trama Ethernet posible, es como hemos visto de 1500 bit, lo habitual en el protocolo LAP-B, es que las tramas tendrán menos de 1024 bit, por lo que la WAN requerirá partir las tramas de datos Ethernet, y en el otro extremo del enlace WAN, deberá rearmarlas.

Primitivas de Servicio

Como ocurre habitualmente en el modelo OSI, cada capa solicita servicios a la capa inmediata inferior, y brinda servicios a la capa inmediata superior. Esto se hace a través de las llamadas Primitivas de Servicio, funciones normalizadas propias de cada protocolo.

En el protocolo LAP-B, existen diversas funciones, tales como:

- L_Connect
- L_Disconnect
- L_T_Data

Las cuales a su vez pueden realizar una de cuatro acciones:

- Request (interrogación)
- Indication (indicación)
- Confirmation (confirmación)
- Response (respuesta)

Se podrá establecer Primitivas de Servicio, entre dos estaciones A y B, donde se solicita establecer su conexión, su reconocimiento y enviar respuesta, correspondientes a las tramas de control.

Protocolo LAP-D

El protocolo, procedimiento de acceso a enlace- D (LAP-D), a sido desarrollado en los años 1980. Su principal característica es permitir el manejo de prioridades, mediante un sistema de direccionamiento vertical, con el cual es posible identificar las aplicaciones que corren en la capa superior. La estructura de la trama del protocolo LAP-D, tiene el siguiente formato (Fig. 32).

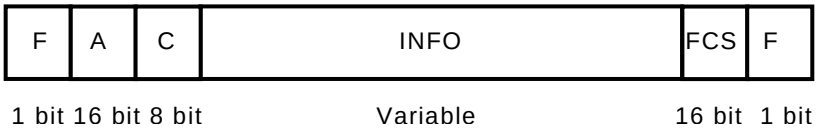


Fig. 32 - Trama LAP-D

Los campos son los establecidos según el estándar HDLC, con diferencia respecto a LAP-B, que en este caso el Campo de Dirección (A), es de longitud doble en 16 bit.

Esto se debe a que dicho campo se utiliza para direccionamiento, tanto vertical como horizontal. La estructura del Campo de Dirección, tiene el formato: (Fig. 33).

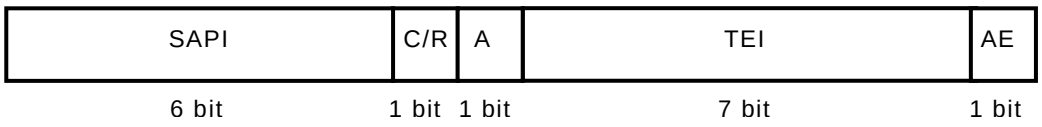


Fig. 33 - Campo de Dirección del LAP-D

SAPI (Service Adress Pointer Identifier)

El campo, indicador de identificación de direcciones de servicio SAPI, reconoce las aplicaciones con lo que se permite asignar prioridades entre ellas. Es una forma de “direccionamiento vertical”, es decir, identificando las tramas según a que aplicación le pertenece en la capa superior.

C/R (Command /Response)

Se distingue con 1 bit entre trama de Comandos o de Respuestas.

EA (End Adress)

Delimitador del Campo de Dirección, con bit en 0 se indica que termina, y con bit en 1 que continúa.

TEI (Terminal End Point Identifier)

El identificador de punto terminal TEI, permite identificar la estación de destino, como una forma de “direccionamiento horizontal”. Es un conexionado lógico que establece varios enlaces WAN, uno para cada estación

Direccionamiento horizontal y vertical

Una característica fundamental del protocolo LAP-D, es permitir tanto direccionamiento horizontal como vertical.

En el caso del direccionamiento horizontal, el campo TEI considerado, identifica la dirección de destino, de manera que aunque todas las tramas corren por la misma conexión física, se establece una “conexión lógica”. Es como si existiesen varios enlaces WAN, punto a punto, uno para cada estación. Esta abstracción, de Conexiones Lógicas de Direccionamiento Horizontal, como un grupo de enlaces virtuales a partir de una Conexión Física, es un enfoque típico en las WAN (Fig. 34).

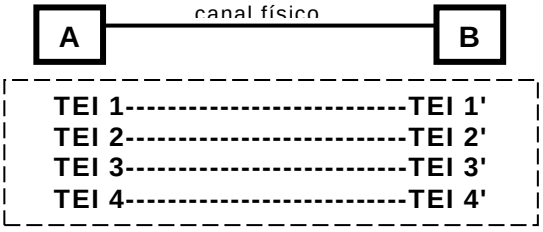


Fig. 34 - Conexiones Lógicas de Direccionamiento Horizontal

En el caso del direccionamiento vertical, el Campo SAPI considerado, identifica las diferentes aplicaciones que corren en la capa superior. El Campo SAPI, identifica las aplicaciones asignando prioridades entre ellas, en la forma del direccionamiento vertical, identificando las tramas según a que aplicación pertenece en la capa superior (Fig. 35).

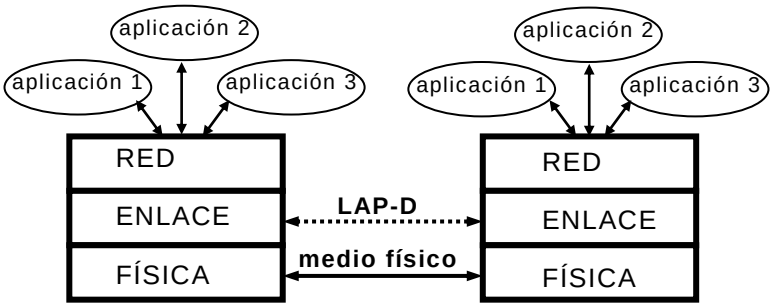


Fig. 35 - Identificación de las diferentes aplicaciones

De esta manera, se logra con la conexión física, un medio compartido con un sistema de direccionamiento horizontal que identifica las estaciones, el que se complementa con el direccionamiento vertical, y en el que se identifican las aplicaciones, las que pueden estar corriendo en forma concurrente en cada estación.

A. 9. 7. 7. Protocolo PPP

El protocolo punto a punto PPP (Point to Point Protocol), es otro protocolo de enlaces WAN, que ha sido el adoptado para Internet al nivel de Capa de Enlace. El mismo por su alta aplicación, lo hace de importancia fundamental.

El PPP, realiza la detección de errores, permite la negociación de direcciones IP en el momento de la conexión y la verificación de autenticidad. En el PPP la longitud de la trama debe ser un número entero de Byte.

De acuerdo al RFC-1547 emitido por el IETF (Internet Engineering Task Force), mediante el PPP se persiguieron ocho objetivos básicos:

1) Protocolo destinado a dos entidades, en enlace punto a punto.
2) Protocolo simple, pero que no pierda la eficiencia de los HDLC.
3) Que realice la detección de errores, pero no retransmisión de tramas.
4) Modo balanceado, donde cualquiera de las dos entidades pueda transmitir o recibir.
5) Sin control de flujo.
6) Posibilidad de definir que protocolo va en la capa superior, para trabajar con aplicaciones que requieran distintos protocolos de red.
7) Extensible (se prevén mecanismos para agregar funciones en el futuro).
8) Provea un enlace que pueda manejarse de acuerdo con varias opciones, no en un modo único.

En el Campo de Dirección, no se utiliza direccionamiento horizontal, por lo que este campo es de valor fijo. Se pone siempre FF.

En el Campo de Control existe un único tipo de tramas: UI (Unnumbered information), por lo que se deja fijo, por convención en 13. Estos valores, tanto de este campo como en el de dirección, indican que no se están usando por el momento, pero que quedan reservados para su uso posterior (Objetivo 7).

El Campo Protocolo permite definir que protocolo se utilizará en la capa superior, por lo que el valor de este campo indicará si en la Capa de Red operará el protocolo IP, IPX; etc.(Objetivo 6).

A su vez, de acuerdo al Objetivo 8, se permiten diferentes opciones, que se manejan mediante codificaciones en este campo. Por ejemplo:

- Tratamiento de Errores. Envío de notificación que se descartó una trama.
- Códigos de Autenticación. Implementa seguridad a nivel de capa de enlace.

El mecanismo de establecimiento de conexión y sus diferentes alternativas, se pueden esquematizan en un diagrama de secuencias (Fig. 36).

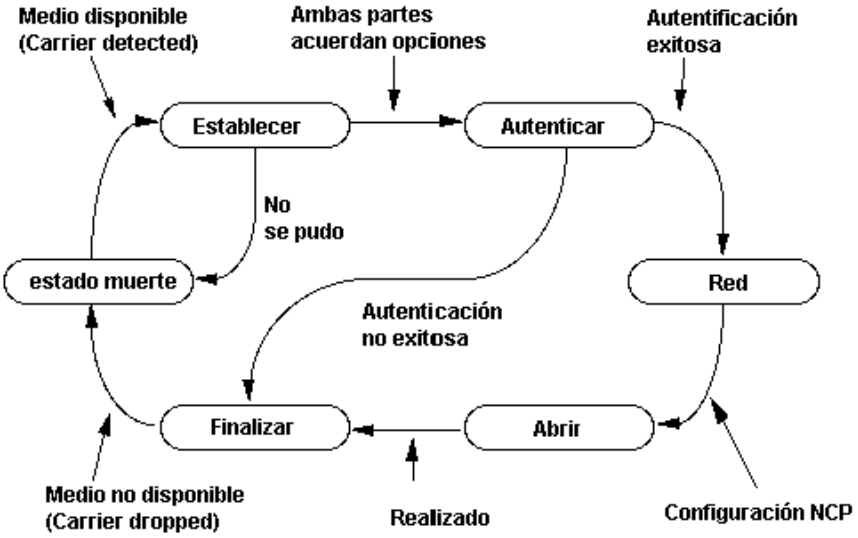


Fig. 36 - Mecanismo del establecimiento de la conexión

Como puede observarse en el esquema, originalmente se comprueba la disponibilidad del medio, hasta que esta logra establecerse, luego se acuerdan las opciones que permite el protocolo entre ambas estaciones, una vez hecho esto, se procede a su autenticación.

Si ésta no es exitosa, la sesión finaliza, y en caso contrario, se establece la conexión de red, con su correspondiente configuración. Una vez realizada la transmisión, ésta finaliza , liberándose el medio.

El PPP trabaja en conjunto con el protocolo SLIP (Serial Line IP), diseñado en 1984 para conectar estaciones de trabajo a Internet a través de líneas telefónicas usando un módem. A su vez PPP hace uso de los protocolos LCP (Link Control Protocol) y NCP (Network Control Protocol). El LCP se ocupa de negociar una serie de parámetros y de validar al conmutador que llama, en el momento de establecer una conexión. El NCP se encarga de negociar los parámetros específicos para cada protocolo utilizado.

Estos protocolos intervienen para la conexión de una PC a Internet y convertirla temporalmente en un Host de Internet:

Luego de llamar la PC al enrutador del proveedor de Internet, a través de su módem, el módem del proveedor contesta al llamado y establece la conexión física telefónica, la PC manda entonces al enrutador una serie de paquetes LCP en el campo de la carga útil de alguna de las tramas PPP, se configura la Capa de Enlace. Una vez que se han acordado que paquetes PPP usar, se envía una serie de paquetes NCP para configurar la Capa de Red. Se requiere luego, la dirección IP del protocolo TCP/IP, el proveedor provee una dirección IP mediante NCP. En ese momento ya la PC es un Host de Internet y puede enviar y recibir paquetes de IP.

Cuando el usuario ha terminado, se usa NCP para desmantelar la conexión a la Capa de Red y liberar la dirección IP. Luego se usa LCP para cancelar la conexión de la Capa de Enlace. Finalmente la PC indica al módem que cuelgue el teléfono, liberando la conexión a la Capa Física.

A. 9. 7. 8. Redes Frame Relay

Las redes Frame Relay representan un sistema de interconexión en Capa de Enlace, con recursos compartidos, lo que la hace una opción más económica que las TDM.

Para compartir los recursos y aún así asegurar ciertos niveles de performance a los usuarios, es necesario introducir nuevos controles. Consideremos como se imple-mentan estos controles, al observar la estructura de la trama Frame-Relay (Fig. 37).

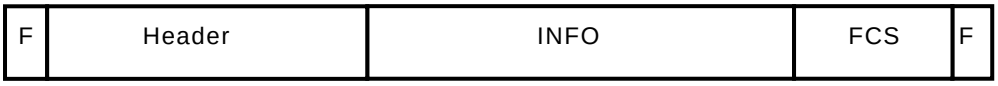


Fig. 37 - Estructura de trama Frame Relay

Los campos de esta estructura se corresponden con el HDLC genérico, a excepción del campo Header (cabezal), que se representa en el siguiente esquema (Fig. 38).

Fig. 38 - Estructura del cabezal Frame Relay (Header)

DLCI (Data Link Connection Identifier), campo de identificación de la estación (direccionamiento horizontal).

C/R, Distingue trama Comando / Respuesta.

E/A (End Adress), avisa si la dirección termina o si no corresponde.

FECN (Forward Explicit Congestion Notification), notifica cogestión hacia delante.

BECN (Backward Explicit Congestion Notification), notifica cogestión hacia atrás.

DE (Discard Elegibility), indica que la trama es elegible para descarte.

En Frame Relay (Relevo de Tramas), como primera simplificación, tenemos un solo tipo de tramas, por lo cual no hay campo de control. Otra simplificación es que no tenemos confirmación de tramas, por lo que no es necesario considerar una ventana de recepción de tramas vinculada a la confirmación progresiva de las mismas.

Si bien las redes Frame Relay dejan de lado los mecanismos de control y confirmación de enlace, han tenido amplia difusión debido al adelanto de las redes de telecomunicaciones, que ha hecho que la tasa de errores de los enlaces en la actualidad sea mucho más redu-cida que años atrás. Por ello, es posible resolver esto fuera del nivel de la Capa de Enlace, logrando así mayor performance de la red, y pasando los errores que aún se presenten a las capas superiores. Aunque esto resulte en elaborar descartes y solicitudes de reenvío de tramas en capas superiores, tendrá un impacto menor que confirmaciones redundantes en Capa 2.

Los últimos tres campos del cabezal, tienen que ver con el manejo de los niveles de congestión en Frame-Relay. La congestión tiene lugar cuando se ocupan los buffer de los Switch Frame-Relay, de modo que no pueden recibirse momentáneamente nuevas tramas.

El Switch que no puede recibir tramas envía una notificación hacia adelante de la situación (FECN), mientras que el que no puede transmitir, envía una notificación hacia atrás en tal sentido (BECN)

La existencia de este sistema de descarte de tramas y de diferentes niveles de congestión, lleva a la necesidad de asegurar niveles mínimos de cualidades dentro de un medio compartido. Esto se regula mediante ciertos parámetros que se estipulan según contrato.

Como parámetros importantes se incluye la velocidad digital nominal, la velocidad digital entregada CIR y la velocidad excedida EIR, cada una con sus particulares características.

La velocidad nominal representa la velocidad física de transmisión en el enlace, expresada en bit por segundo Esta velocidad dependerá de la cantidad de canales disponibles. Como se puede establecer hasta 30 canales, se puede obtener una velocidad digital de hasta 2048 Kb/s.

La velocidad digital entregada CIR (Commited Information Rate) es una medida estadística, consistente en promediar en intervalos cortos llamados Burst Time, la velocidad de transmisión real. Esta velocidad promedio así obtenida, no es garantizada para intervalos más largos. Los intervalos Burst Time son tiempos de ráfaga aproximados de 1 segundo.

El CIR puede tener, en un caso extremo el valor cero. En ese caso, se realizará la transmisión en la condición de “best effort”, del mejor esfuerzo de parte del sistema, es decir haciendola, pero no garantizando resultados. Como otro caso extremo, el CIR podría alcanzar un valor de 64 b/s. Ello no es práctico, ya que fijando el CIR en el máximo, se desperdiciarán recursos, dado que el promedio real va a ser necesariamente menor, debido a los silencios en la transmisión. Esto nos llevará a un gasto inútil, como ocurre en las redes TDM.

Fijar el CIR en alguno de los valores intermedios es lo usual, dependiendo del tamaño de la organización y del tráfico del enlace WAN a implementar en Frame Relay el nivel que se contrata. En general, los proveedores garantizan mediante contrato el CIR, con cláusulas específicas de resarcimiento en caso de no cumplirse.

Un aspecto importante para entender el CIR, es que se trata de un mero cálculo estadís-tico. Debe entenderse que la red nunca transmitirá a la velocidad que indica el CIR, sino que lo hará a la velocidad nominal, ya que realmente existen sólo dos velocidades posi-bles en la transmisión: la nominal o cero. A su vez, el valor estadístico del CIR, se complementa con el Burst Excess.

El CIR asegura un espacio en que la función de transmisión puede desarrollarse (entre el CIR y el eje de las abscisas). En un cierto momento t_0, la ordenada indicará el BC (Burst Commited) que revela las ráfagas de datos garantizadas, que pueden enviarse. En cambio el BE (Burst Excess) indica un excedente que podrá utilizarse si la red lo permite en ese momento, pero que no se garantiza (Fig. 39).

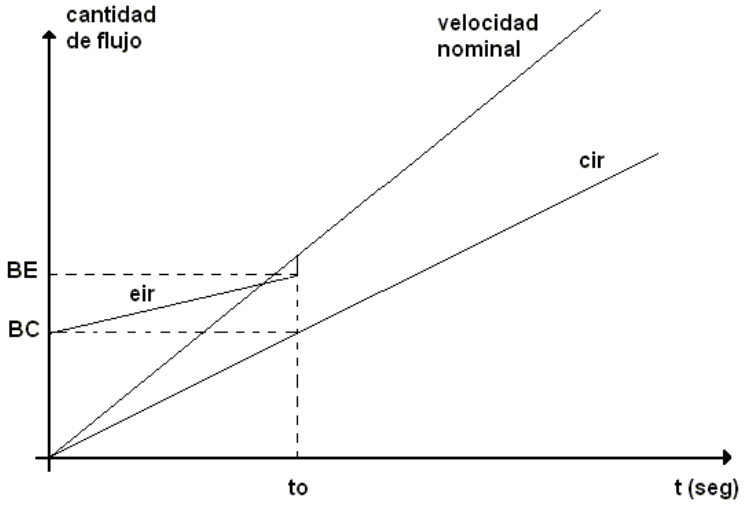


Fig. 39 - Valor de CIR y Burst Excess

En general, estimando correctamente los valores de BC y BE, fijando un CIR adecuado a cada organización, puede lograrse en el caso de empresas pequeñas y medianas y que no se requiera garantizar disponibilidad permanente del ancho de banda máximo, un resulta-do aproximadamente igual a las redes transparentes (TDM).

Se obtiene un costo sensible-mente menor, al estar usando un esquema de recursos compartidos.

Otro parámetro de uso común es el indicado como, velocidad de información excedida EIR (Excess Information Rate), como valor promedio según un BE, estimado para la transmi-sión.

Interconexión Frame-Relay

En Frame-Relay, el enlace WAN punto a punto, por ejemplo entre dos redes LAN, se ofrece en un medio compartido, por lo que se habla de un enlace lógico o circuito virtual permanente PVC. Como se muestra en la Fig. 40.

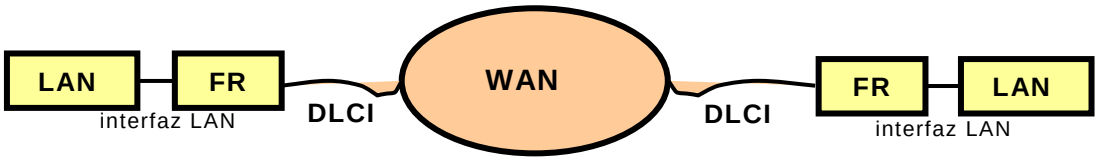


Fig. 40 - Circuito virtual permanente PVC

Según el esquema de la figura, desde la LAN de la izquierda se envía una trama al Switch FR correspondiente, mediante la interfase LAN, luego desde dicho dispositivo a la red WAN, con su propio campo de identificación de estación DLCI (Data Link Connection Identifier), para cada canal, en direccionamiento horizontal. Con este DLCI, dentro de la WAN, se crea un enlace lógico PVC y se transmite la trama hacia el otro extremo. Desde donde, la trama será entregada en la LAN de la derecha.

A diferencia de las Redes TDM, en Frame-Relay se dispone de conmutadores, por lo que habrá un cierto retardo (delay) mayor que en las TDM y dependiente tanto de la cantidad de dispositivos a atravesar, como de las condiciones de congestión de la red. Por ello, deben limitarse a un cierto número la cantidad los dispositivos empleados en la red.

Un punto importante a considerar, es que si bien en Frame-Relay existe un PVC contratado, que funciona según lo descripto anteriormente, en la realidad este PVC está integrado por una serie de enlaces WAN punto a punto entre los dispositivos, en los cuales incluso los DLCI no tienen por que ser los mismos. Por lo tanto, la capa de enlace tiene sólo validez local para cada enlace punto a punto.

En el caso de varios enlaces WAN obliga a que la trama tenga que ser desarmada y rearmada modificando los DLCI pero manteniendo el mismo campo INFO. Ello explica el delay que se introduce a medida que el número de dispositivos aumenta. Este delay implica un Retardo de Serialización, que ocurre cuando se saturan las colas de espera de tramas para ser transmitidas en los Switches.

Este Retardo de Serialización, se intenta disminuir frecuentemente no enviando todas las tramas a un destino en forma secuencial, sino distribuyendo las trasmisiones entre diferentes nodos (Traffic Shaping).

A. 9. 7. 9. Arquitecturas HIPPI

La Interfaz paralela de alto desempeño HIPPI (Hight Performance Parallel Interfaz), tiene su origen en Los Álamos, en los laboratorios de armamento nuclear de USA.

Su diseño, de 1987, estuvo dirigido a conformar redes que contuviesen a super computadoras. Se diseñó originalmente como Canal de Datos, operando punto a punto desde una supercomputadora maestra a un periférico subordinado, con uso de líneas dedicadas.

No existe red broadcast ni medio compartido. Luego al incluir un conmutador de barras cruzadas (crossbar) tomó la conformación de una LAN que permitía interconectar varios dispositivos entre sí. Los periféricos estaban constituidos por dispositivos de almacenamiento de datos o de gráficos.

La señalización se realiza a 25 MBaud transmitiendo por varios cables STP de 50 pares, en paralelo. La velocidad nominal es de 800 Mb/s o de 1600 Mb/s en transmisión simple, por lo que para cubrir los dos sentidos es necesario emplear dos vías de transmisión.

La distancia máxima en cables es de 25 m, mediante un conmutador será luego de 50 m y con varios conmutadores en cascada se posibilita una distancia máxima de 200 m..

Con fibra óptica multimodo se puede alcanzar 300 m y con fibra monomodo hasta 10 Km. Es posible utilizar SONET /SDH como medio de transporte de las tramas HIPPI para largas distancias. Las tramas HIPPI son de 1024 Bytes

Se ha definido un sistema denominado GSN (GigaByte System Network también conocido como super HIPPI, que contempla enlaces a 6.4 Gb/s. Emplea una señalización de 10 GBaud que con señalización 4B5B resulta 8 Gb/s. Mediante cables STP se logran distancias de 40 m, Se emplea 50 pares con 20 pares en cada sentido.

Con fibra óptica multimodo en primera ventana se alcanzan 220 m y en segunda ventana 300 m. Con fibra monomodo en segunda ventana se obtienen enlaces de 1 Km. En ambos casos la señal se reparte en 10 fibras en cada sentido, enviando 1 GBaud en cada una. También se considera enviar 2 GBaud por fibra con 12 enlaces.

A. 9. 7. 10. Arquitecturas Fiber Channel

La arquitectura del Fiber Channel es una evolución del HIPPI, surgida en 1988.

Fibre Channel se utiliza al igual que HIPPI, tanto para las LAN, como para los enlaces conectando a potentes perisféricos de grandes computadoras, o servir de transporte a tramas 802.2, celdas ATM, paquetes IP, tramas HIPPI o tramas Fibre Channel. Una red Fibre Channel se constituye utilizando conmutadores crossbar o concentradores. Con los conmutadores cada estación tiene un ancho de banda dedicado, con un concentrador la capacidad es compartida entre todas las estaciones. Puede haber hasta 127 estaciones en conformación anillo.

Emplea velocidades de 100, 200, 400 u 800 Mb/s, 1.062 y 2.125 Gb/s, con codificación 810 diseñada originalmente para IBM y utilizada también en Giga Ethernet. Las velocidades de señalización son 133, 266, 531, 1062 MBaud y 2.12, 4.25 GBaud. El medio de transmisión puede ser cable STP, coaxial o fibra óptica multimodo o monomodo.

DISTANCIA MÁXIMA EN FIBRE CHANNEL

Tipo de cable	800 Mb/s	400 Mb/s	200 Mb/s	100 Mb/s
Fibra monomodo	10 Km	10 Km	10 Km	-
Fibra multimodo	500 m	1000 m	2000 m	10 Km
Fibra multimodo	175 m	350 m	1500 m	1500 m
Cable coaxial de video	25 m	50 m	75 m	100 m
Cable coaxial miniatura	10 m	15 m	25 m	35 m
Cable STP	-	-	50 m	100 m

Fibre Channel suministra las tres clases de servicios a la Subcapa LLC, de Tipo 3 de conmutación de circuitos, del Tipo 2 de paquetes con entrega garantida y de Tipo 1 de paquetes sin entrega garantida. La carga útil de la trama es de hasta 2048 Bytes con 32 en el CRC. Tiene una tasa de error menor a 1 en 10^{12}.

A. 9. 8. Protocolos de Internet

Si bien Internet y sus protocolos básicos TCP/IP existen desde 1974, no fue hasta 1993 que estuvo disponible al público en general. El advenimiento masivo a Internet se produjo con la introducción del sistema de comunicaciones World Wide Web, por ser éste muy sencillo de operar. Internet es una "interred" mundial que comunica a millones de personas mediante las computadoras. Virtualmente no tiene dueño y no es necesario permiso alguno para conectarse a ella.

La idea de la tecnología Internet es conectar diversas redes con distintos equipos, sistemas y medios de transmisión, en forma eficiente libre de errores y fundamentalmente sin depender de fabricante o vendedor en particular.

Cualquier usuario, se conectan a la red de larga distancia realizando solo llamadas telefónicas de tarifa local, mediante un proveedor de esa ciudad o barrio. Las universidades, gobiernos y empresas de servicio brindan todo tipo de información a través de ella.

La conexión a la red telefónica se realiza empleando un módem, generalmente de 56 Kb/s, (57 600 Kb/s) del tipo Dial Up IP, que modula los pulsos digitales en ondas analógicas. La atenuación en el par telefónico, en los equipos de conmutación y al debido por tráfico en línea, realmente restringe comúnmente esta velocidad a alrededor de 28 000 bit/s.

Las compañías de CATV, también brindan el servicio de Internet, pero a mayor ancho de banda, pues emplean una red del tipo coaxial /fibra óptica. Utilizan para la transmisión también un módem apropiado a esta conexión. Se conoce comúnmente a esta transmisión como cable módem.

Los servicios de comunicaciones más importantes proporcionados por Internet son, el correo electrónico (e-mail) bajo la norma X.400, X.500, el protocolo transferencia de correo SMTP, la transferencia de archivos FTP, foros de discusión News, transferencias de noticias NNTP y el W.W.W. (World Wide Web) con el, lenguaje de marcación de hipertexto HTML (Hypertext Markup Language). Estos sistemas utilizan a la red Internet como medio de transporte, para que usuarios se comuniquen con programas comunes.

Internet actúa en el modelo cliente-servidor. Un usuario con un programa FTP-cliente, accede al servidor remoto que dispone de un programa FTP-servidor. Transfiere una copia del archivo, bajo TCP/IP, por ejemplo de un e-mail y se queda con el original.

La transmisión de datos se realiza mediante paquetes, a diferencia de las comunicaciones de circuitos telefónicas. Estas comunicaciones por paquetes no requieren un canal de comunicaciones dedicado, sino que muchas computadoras comparten el canal troncal y reduce así los tiempos y costos de transmisión.

A. 9. 8. 1. Protocolos de la Web

La denominada "telaraña ancha mundial Word Wide Web, o simplemente Página Web, es un servicios multimedia de Internet, como interred, que contiene un fabuloso almacén de documentos escritos como hipertextos.

El protocolo con el que se comunica entre clientes y servido Web se denomina, protocolo de trasferencia de hipertexto HTTP (Hyper Text Transfer Protocol). El lenguaje Java hace posible preparar páginas Web altamente interactivas.

El Web presenta Internet al usuario, como un sinnúmero de páginas de hipermedia (textos, imágenes, video y audio), conectados entre si por medio de un hipervínculo (hyperlinks). Una hyperlink es una conexión lógicas a saltos hacia otras páginas. Las páginas vinculadas "linkeadas", son distribuidas por todo el mundo. La combinación de páginas de hipertexto, con otros medios como ser videos, audio o ambas, se denomina hipermedia.

Es posible acceder a el Web a través de una interfaz gráfica amigable para el usuario, llamada navegador gráfico (Browser). Los Browser empleados son Internet Explorer de Microsoft y el Netscape Communicator, operando sobre sistemas operativos tales como Windows.

Los Browser son muy fáciles de operar, con solo introducir la dirección electrónica de la página deseada se puede acceder a la misma, luego con solo "clickear2 con un ratón (mouse) al, localizador uniforme de recursos URL (Universal Resouse Locator), o a una determinada referencia de hipervínculo, se puede acceder a otra cualquier página en el mundo Web.

El URL identifica mundialmente cada página Web. El URL consta de tres segmentos, el protocolo HTTP (http), el nombre del dominio DNS del Host (www.clarin.com) y el nombre del archivo (/suplementos/informática/html).

Cada computadora en red se identifica con un número denominado dirección IP. Las direcciones IP están compuestas por números de 32 bit, por ello se los reconoce por su equivalente en nombres mnemónicos. El método que traduce estas direcciones se le denomina, sistema de nombre de dominio DNS (Domain Name System).

Los nombres están organizados en jerarquías: Jerarquía de país, que se indican en último término y en letra minúscula, por ejemplo: pe: Perú, py: Paraguay, ar: Argentina, uk: Reino Unido, jp: Japón. USA no requiere asignación alguna.

Otra jerarquía esta dada por el tipo de entidad, que se indica antecediendo al de país: com: comercial, org: organización no gubernamental, edu: educación, gov: gobierno, mil: militar, net: servicio de Internet, int: organismo internacional.

Antecediendo a estas asignaciones se indica por ejemplo la Facultad y el Departamento, si es que existiesen, por ejemplo: lab por Laboratorio de Electrónica , frba por Facultad Regional de Buenos Aires y luego utn por Universidad Tecnológica Nacional. Por último se identifica cada máquina.

El DNS mediante un procedimiento de biblioteca llamado "resolvedor", relaciona un nombre con una dirección IP. Con la dirección IP, el programa puede establecer una conexión TCP con el destino, o envío UDP sin conexión.

Los buscadores o motores de búsqueda (Search Engines) hacen posible encontrar rápidamente, páginas de las cuales desconocemos el nombre exacto o lo hemos olvidado. Varios son los entes comerciales que ofrecen estos servicios, por ejemplo Yahoo.

A. 9. 8. 2. Niveles del Modelo TCP/IP

La arquitectura en capas del Modelo TCP/IP sigue la estructura del Modelo OSI, aunque con ciertas diferencias (Fig. 41).

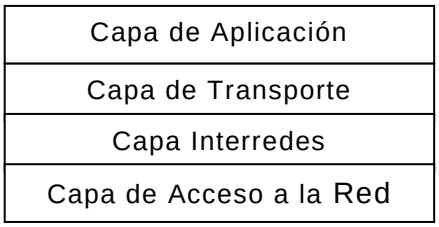


Fig. 41 - Modelo en capas TCP/IP

Podemos apreciar que en el Modelo TCP/IP en comparación al Modelo OSI, la Capa Acceso a la Red se corresponde con la Capa Física y la Capa de Enlace, también la Capa Interredes tiene cierta relación con la Capa de Red, mientras que la Capa de Transporte con su similar del modelo OSI. No obstante esta relaciones las fronteras exactas no siempre son coincidentes. Seguidamente vemos que desde la Capa Transporte se pasa directamente a la Capa de Aplicación.

Esta estructura TCP/IP es más realista que la de OSI, donde aparecen las capas de Sesión y de Presentación, actualmente prácticamente nulas de funcionalidad. La principal objeción que se le ha hecho al modelo de referencia TCP/IP, es no ser adecuado para modelar arquitecturas de red en sentido amplio, como el caso del modelo OSI, sino que sólo es adecuado a su modelado propiamente dicho.

La combinación de los protocolos de control de transmisiones e Internet, TCP/IP (Transmission Control Protocol / Internet Protocol), ha sido desarrollada por el Departamento de Defensa de USA, en combinación con universidades e industria. Provee la comunicación entre redes y sistemas disímiles, lo cual representa su mayor ventaja.

Permite dar acceso a Internet y son enrutables. La mayor desventaja es su tamaño y velocidad, ya que tiene el doble de tamaño que el protocolo NetBEUI.

Mientras TCP provee la comunicación confiable entre computadoras una vez establecido el enlace, el IP provee los servicios necesarios para el movimiento de los datos, dirección, enrutado y conmutación. Corresponde TCP a la Capa 4, de Transporte, mientras que IP atañer a la Capa 3, de Interred del Modelo TCP/IP.

Con TCP/IP los datos se transmiten en datagramas, donde los datos son reensamblados cuando llegan a su destino, para formar el mensaje original. Una conexión TCP es una corriente de Byte. Todas las conexiones TCP son dúplex, punto a punto.

A. 9. 8. 3. Capa de Acceso a Red

En la Capa de Acceso a Red del Modelo TCP/IP actúan dos protocolos el, protocolo de resolución de direcciones ARP (Addresses Resolution Protocol) y el ARP en reversa, RARP (Reverse ARP).

Protocolo ARP

Para poder enviar datos a un Host de destino, el Host de origen debe armar la trama de datos correspondiente. A su vez, para hacerlo, debe conocer la dirección MAC del Host de destino.

Para acceder a dicha información lo efectúa a través del protocolo de Capa de Acceso el, protocolo de resolución de direcciones ARP, que se encarga de obtener direcciones físicas (MAC) a partir de direcciones lógicas (IP).

Para tal operación, el ARP efectúa el siguiente procedimiento:

a) El ARP dispone de una tabla que contiene las direcciones físicas conocidas y las respectivas direcciones IP que les corresponden en el ARP-Caché.

b) Si la dirección MAC buscada no se encuentra en el ARP-Caché, envía un mensaje de ARP-Request, a la red. Dicho mensaje indica la dirección IP.

c) El host que reconoce la dirección IP que está en la solicitud, responde con un mensaje ARP-Answer. Este mensaje contiene la dirección MAC requerida.

d) Una vez recibido, el Host solicitante guarda en el ARP-Caché, la dupla compuesta por la dirección IP y la dirección MAC para ulteriores envíos.

Protocolo RARP

El protocolo inverso al ARP es el, protocolo resolución de direcciones en reversa RARP, que tiene la función de obtener la dirección IP, a partir de su dirección MAC. Aunque esta operación es menos requerida, puede ser de gran utilidad en el caso de las LAN.

A. 9. 8. 4. Capa Interredes

Al reunir diferentes estándares LAN en una WAN, e incluso con diferentes estándares MAN y WAN, se forman complejas interredes.

La Capa Interred del Modelo TCP/IP, comprende al, protocolo Internet, IP. Su función es entregar los paquetes IP donde corresponda y evitar la congestión, sin importar los tipos de redes que atraviese.

Protocolo de Internet, IP

El protocolo Internet (IP), es el más difundido en la actualidad, muchos dispositivos más allá de las computadoras, tales como equipos de microondas, refrigeradores, teléfonos, alarmas; etc., podrán disponen de direcciones IP y por tanto se podrá lograr comportan como un Host en la red.

El protocolo IP requiere para funcionar de:

1. Un plan de direccionamiento
2. Una trama IP
3. Un plan de encaminamiento

Direccionamiento IP

El Direccionamiento IP es un sistema de identificación de Host, para Capa 3, Red.

El motivo de porque es necesario un sistema de direccionamiento en la Capa 3, si está disponible el direccionamiento MAC, al nivel de Capa 2, es que si bien, no sería necesario en el entorno de una LAN, la operación se complica al nivel de los enlaces WAN. En estos casos no siempre sería posible conocer la dirección MAC de los Host remotos.

Si bien algunos protocolos de Capa de Enlace como Frame Relay permiten identificar las direcciones de destino, en la mayoría de los casos esto no es posible.

Por otra parte, un direccionamiento fijo en la Placa de Red, como es el MAC, sería impráctico para comunicaciones a escala mundial, al no tener una estructura jerárquicamente ordenada. Por ejemplo, para las transmisiones multicast o para una traducción de direcciones en forma jerárquica, como es el caso de los protocolos DNS en la Capa 7, de Aplicación.

Para solucionar esta cuestión, se establece un nuevo sistema de direccionamiento particularmente útil para las WAN, como es el de Internet con el direccionamiento IP.

La dirección IP consta de 32 bits, dividiéndose éstos en partes, las correspondientes a indicar la Clase de la dirección, a los de la Red y a las del Host. Esta división no es igual para todas las direcciones IP, sino que sigue uno de los siguientes esquemas, definidos por clases, de acuerdo al estándar estipulado en la RFC 1166 del IETF - Internet Engineering Task Force (Fig. 42):

1) Clase A

2) Clase B

3) Clase C

4) Clase D

5) Clase E

11110	Uso futuro

Fig. 42 - División del direccionamiento IP según RFC 1166

Veamos a que aplica cada uno de estos formatos de dirección IP:

a) Las direcciones de Clase A se identifican porque empiezan con “0”. Se componen de 8 bits correspondientes a la Red y 24 al Host, máquina que opera. Fueron asignadas a las primeras redes que participaron de ARPANet y posteriormente de Internet, tales como el Departamento. de Defensa de USA, IBM y algunas Universidades. Así, permiten una amplia capacidad de direccionamiento para los Host que integran estas redes.
b) Las direcciones de Clase B se identifican porque empiezan con “10”. Se componen de 16 bits de Red y 16 bits de Host. Con amplia capacidad para Host, fueron asignadas masivamente durante los últimos años. Actualmente, se han agotado.
c) Las direcciones de Clase C se identifican porque empiezan con “110”. Se componen de 24 bits de Red y 8 bits para Hosts. Son las que se asignan actualmente, y para evitar su agotamiento como ocurrió con las direcciones Clase B, se utilizan las máscaras de Sub-Red (SubNetting).
d) Las direcciones de Clase D se identifican porque empiezan con “1110”. No están divididas en bits de Red y de Host. Se utilizan para direcciones de Multi-Casting.
e) Las direcciones de Clase E se identifican porque empiezan con “11110” y están reservadas para uso futuro, o usos experimentales.

Máscaras de Sub-Red

Una máscara de subred es una dirección que enmascarando la dirección IP para indicar si otra dirección IP pertenece a la misma subred o no. Una subred en una WAN es la que vincula dos o más LAN. Se indica en la tabla siguiente las máscaras de subred correspondientes a cada clase:

CLASE	MASCARA DE SUBRED
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si expresamos la máscara de subred de Clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los 1 indican los bits de la dirección correspondientes a la red y los 0, los correspondientes al Host. Según la máscara anterior, el primer Byte (8 bits) corresponde a la red y los tres siguientes (24 bits), al Host. Por ejemplo, en la dirección 35.120.73.5 de Clase A, 35.0.0.0 pertenece a la red.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110.

Si expresamos esta dirección y la de la máscara de subred en numeración binaria, tenemos:

148.120.33.110 10010100.01111000.00100001.01101110 (dirección de una máquina).

255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red).

148.120.0.0 10010100.01111000.00000000.00000000 (dirección de su subred).

Al hacer el producto binario de las dos primeras direcciones (obrando donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario un 0), obtenemos la tercera.

Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

148.120.33.89 10010100.01111000.00100001.01011001, dirección de una máquina.

255.255.0.0 11111111.11111111.00000000.00000000, dirección de su máscara de red.

148.120.0.0 10010100.01111000.00000000.00000000, dirección de su subred.
En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

148.115.89.3 10010100.01110011.01011001.00000011, dirección de una máquina.

255.255.0.0 11111111.11111111.00000000.00000000, dirección de su máscara de red.

148.115.0.0 10010100.01110011.00000000.00000000, dirección de su subred.

En una red de redes TCP/IP no puede haber Host aislados, todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un ordenador sabe si otro ordenador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente.

En cambio, si los Host están configurados en redes distintas, el mensaje se enviará a la puerta de salida o Router de la red del Host origen. Este Router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del Host destino y se complete la entrega del mensaje.

Cálculo de la dirección de broadcast

Ya hemos visto que el producto lógico binario (AND) de una IP y su máscara devuelven su dirección de red. Para calcular su dirección de difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara.

El paquete IP

Así como en Capa de Enlace, la estructura básica era la trama, en la Capa Interredes la estructura básica de intercambio es el paquete IP, también llamado PDU (Protocol Data Unit). El paquete IP, por trabajar en forma independiente en el tipo sin conexión se considera como un datagrama. Tal datagrama IP se compone de una parte como cabecera y una parte que lleva los datos de la información.

La cabecera es fija de 20 Byte, formada por 4 palabras (filas) de 4 By (32 bit) cada una. Se dispone luego, otra fila opcional que podrá tener 0 o más palabras y a continuación los datos, como se muestra en el esquema siguiente (Fig. 43):

Versión	IHL	Tipo de servicio	Largo Total			
Identificación			-	DF	MF	Fragment Offset
Tiempo de vida		Protocolo	Header Checksum			
Dirección IP de Origen						
Dirección IP de Destino						
OPCIONAL						
DATOS						

Fig. 43 - Estructura PDU (Protocol Data Unit)

La versión que se ejemplifica es la IPv4, que funciona actualmente para Internet, si bien existe una versión IPv6, que se encuentra en etapa experimental.

El campo Versión indica 4 si es IPv4 ó 6 si es IPv6 (4 bit) lo que permite su ejecución indiferente en la red, el campo IHL indica la longitud de las palabras en la cabecera (Header) por ejemplo de 32 bits (4 bit). El campo Tipo de servicio indica esta categoría al Host para definir la velocidad y confiabilidad y prioridad (8 bit). El campo Largo Total podrá indicar hasta un máximo de 65 535 Byte (16 bit). Luego en la fila siguiente el campo Identificación (16 bit) y tres campos pequeños, el primero no se usa en la versión IP4 (1 bit), el segundo (1 bit) corresponde a DF (Don't Fragment) e indica que el paquete no debe ser fragmentado y el tercero (1 bit) MF (More Fragments), indica que hay más fragmentos que le siguen.

El campo Fragment Offset, desplazamiento del fragmento, significa en que parte del datagrama corresponde este fragmento (13 bit). El campo Tiempo de Vida, es un contador que limita el tiempo en segundos, con una vida máxima de 255 seg. (8 bit). El campo Protocolo indica la Capa de Transporte a la que debe entregarse, TCP ó UDP (8 bit). El campo Header Cheksum, es la suma de comprobación de la cabecera (16 bit). La dirección de origen la dirección de destino indican el número de red y de Host de cada uno de estas (16 bit).

Finalmente, viene la parte de datos del texto, que es en realidad el datagrama entero de la Capa de Transporte.

La versión IPv6 tiene varias mejoras, direcciones más grandes, que incrementa la cantidad de direcciones Internet. La cabecera se simplifica a 7 campos, lo que permite mayor velocidad de procesamiento en los Routers con su mejor rendimiento. Los campos son opcionales y entrega una mayor seguridad de la información, en confiabilidad y autencabilidad. Su esquema de cabecera toma la forma de la Fig. 44:

Versión (4 bit)	Prioridad (4 bit)	Etiqueta de Flujo (3 Byte)	
Longitud de Carga Útil (2 Byte)		Siguiente Cabecera (1 Byte)	Límite de Saltos (1 Byte)
Dirección IP de Origen (16 Byte)			
Dirección IP de Destino (16 Byte)			

Fig. 44 - Cabecera fija del IPv6

El campo Prioridad distingue entre paquetes con control de flujo, el campo Etiqueta de Flujo indica requisitos especiales, el campo Siguiente Cabecera se refiere a la las 6 cabeceras opcionales de esta versión, el campo Límite de Saltos tiene funcionalidad similar al campo Tiempo de Vida del IPv4 evitando que los paquetes vivan eternamente.

Encaminamiento IP

Uno de los objetivos de diseño de TCP/IP es posibilitar la interconexión de redes físicas diferentes, de modo que, desde el punto de vista del usuario, aparezca como una sola red, permitiendo un manejo transparente para el usuario.

Para hacer posible esta interconexión, por ejemplo de dos redes, se requiere, o bien una computadora con dos Placas de Red (Multihomed), o bien un dispositivo específico, como un Router.

El protocolo Internet IP, al ser del tipo sin conexión define datagramas tratados en forma independiente a los demás. Al tratarse de un datagrama, no se garantiza que sea entregado al destino indicado, por lo que se pudiera crear algunos problemas en los casos tales como:

- Errores en los bit durante la transmisión.
- Un Router congestionado lo eliminó por falta de espacio en el buffer.
- Temporalmente no hay un camino posible hacia el destino solicitado.

El protocolo IP no resuelve estos problemas, sino que simplemente realiza el mejor esfuerzo (Best Effort) para entregar el datagrama, el mismo puede resultar faltante. Pueden también acaecer paquetes repetidos (como en el caso de las llamadas “transmisiones por inundación” donde se genera redundancia para asegurar el envío) o bien ocurrir paquetes en desorden. Por lo tanto, tales fallos se deberán solventar mediante un protocolo de capa superior.

A. 9. 8. 4. 2. Protocolo ICMP

El protocolo de control de mensaje de Internet, ICMP (Internet Control Message Protocol), es complementario del IP, trabaja para el mantenimiento de la red. Una característica principal que tiene, es manejar el tiempo de vida, mediante una cuenta regresiva, que se inicializa en determinado valor cuando la trama comienza su itinerario, y va decrementando a medida que pasa por los diferentes dispositivos, de modo que si llega a cero, sería descartada.

De esta forma se evita ocupar recursos en despachar una trama que no llegará de todos modos en un tiempo razonable. Es interesante indicar que implementaciones de línea de comandos, como el *ping*, o en ambiente Windows el *tracert*, utilizan el protocolo ICMP, para comprobar la conectividad y medir los retardos.

A. 9. 8. 5. Capa de Transporte

La Capa 4 de Transporte, del Modelo TCP/IP, se corresponde al modelo OSI. En esta capa actúa el protocolo de control de la transmisión TCP, también el, protocolo de datagrama de usuario UDP.

A. 9. 8. 5. 1. Protocolo TCP

El protocolo de control de transmisión TCP (Transmission Control Protocol), esta orientado a la conexión. Cumple las funciones de conectividad, con control de tramas, las que no se incluyen en el protocolo IP, en la capa inmediata inferior. Efectúa el control de flujo ente emisor y receptor.

Ha sido implementado originalmente, como forma nativa en el Sistema Operativo UNIX. Debido a su rápida difusión, particularmente desde que se implementó Internet sobre la combinación de los protocolos TCP e IP, respectivamente en Capas 4 y Capa 3, hoy en día es el más utilizado.

El protocolo TCP, a diferencia del UDP, es un protocolo confiable ya que permite verificar la recepción de datos, así como numerar los puertos para identificar las diferentes aplicaciones.

Si bien existen otros modos de transmisión de datos sin la sobrecarga (overhead) que ocasiona un protocolo con conexión en la capa de Transporte (como es el caso en NetWare) que suelen ser adecuados para redes con baja tasa de error (como las LAN Ethernet), el protocolo TCP es mucho más robusto, y por tanto adecuado para redes de múltiples configuraciones, como los enlaces WAN e Internet.

Por otra parte, el protocolo TCP es mucho más potente, y por tanto adecuado para redes de múltiples configuraciones, como lo son los enlaces WAN e Internet.

Los servicios disponibles a través del protocolo TCP, pueden resumirse en:

- Transferencia básica de datos
- Confiabilidad
- Control de flujo
- Multiplexación
- Conectividad
- Precedencia y Seguridad.

En TCP, se utilizan números de secuencia para numerar los paquetes, de modo que puedan identificarse paquetes faltantes, y lo que es muy importante reconstruir en el receptor el orden de los mismos.

Las entidades TCP transmisora y receptora intercambian datos en forma de segmentos. Un segmento consiste en una cabecera TCP fija de 20 Byte (más una parte opcional), más los Byte de datos. Cada uno de estos segmentos, está limitado al tamaño de los 65 535 Byte de carga útil del IP (Fig. 45).

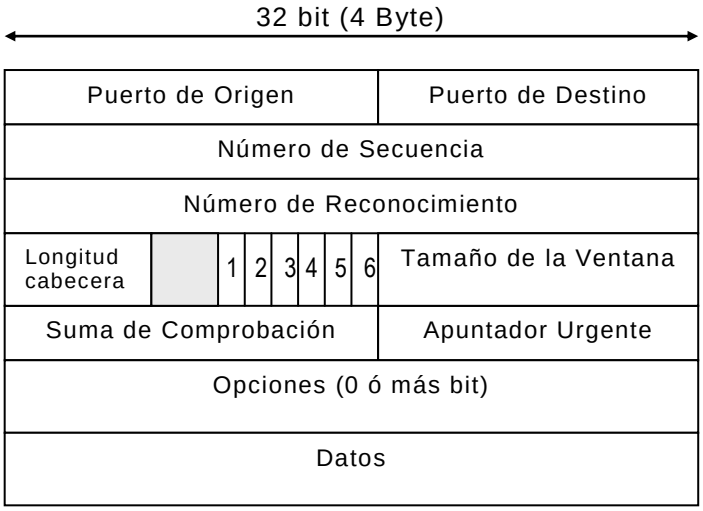


Fig. 45 - Cabecera TCP

Los campos de Puerto de Origen (2 By) y Puerto de Destino (2 By), identifican los terminales locales de conexión. Los campos Número de Secuencia (4 By) y Número de Reconocimiento (4 By) de acuse de recibo. La Longitud de Cabecera (2 bit) indica la cantidad total de palabras de 32 bit contenida en la cabecera TCP. El siguiente campo es de 6 bit que no se usan actualmente, luego 6 banderas de 1 bit cada uno.

El primero de estos es URG que indica urgente, el segundo ACK indica se dispone de acuse de recibo, el tercero PSH indica push, o sea que los segmentos sean empujado sin ponerlo en buffer. El cuarto es el bit bandera RST que sirve para restablecer o rechazar una conexión. el quinto es SYN para sincronizar conexiones y el sexto es FIN que se usa para liberar una conexión.

El campo Tamaño de Ventana, indica el número de paquetes. El campo Suma de Comprobación agrega confiabilidad. El Apuntador Urgente, permite que se reciba el paquete aunque la ventana de recepción esté cerrada en el receptor. El campo Opciones es variable y se introdujo para agregar características extras no cubiertas por la cabecera normal.

Para transitar por una red, un segmento demasiado grande puede ser dividido en varios segmentos por un Router. Cada segmento nuevo recibe su propia cabecera TCP e IP, por lo que esta fragmentación aumenta la carga total.

A. 9. 8. 5. 2. Protocolo UDP

El protocolo datagrama de usuario, UDP (User Datagrama Protocol), es esencialmente diferente al TCP, ya que es un protocolo del tipo sin conexión. No involucra control de flujo, ni asignación de secuencia con confirmación de tramas, por lo que su seguridad es muy inferior para aplicaciones donde ésta se requiera.

Su ventaja radica en brindar mayor desempeño que el TCP. Por ello, es particularmente adecuado para transmisiones en tiempo real, como es el caso del voz o video, donde la entrega pronta es más importante que la entrega precisa y con alto desempeño, donde el cambio de algún bit no tendrá la gravedad que pudiera tener en la transmisión de datos.

La IEEE en sus subcomités 802.1p y 802.1Q estudian un mecanismo, para etiquetar tramas de forma que pueda determinarse prioridades según la clase de servicio deseada.

A. 9. 8. 6. Capa de Aplicación

Debido al particular amplio desarrollo del Internet, existe una amplia gama de protocolos disponibles en la Capa de Aplicación del Modelo TCP/IP. Describimos algunos de los más conocidos y ampliamente utilizados.

Protocolo TelNet

El protocolo Telnet permite establecer una sesión con Host remotos y procesar datos localmente. Para conectarse remotamente (login), es necesario tener configurado el programa de Telnet Helper y disponer de la conexión PPP /SLIP, en Capa de Enlace WAN.

El protocolo TelNet, habilita a una Terminal conectada a una red TCP/IP a trabajar como si estuviese conectada directamente. Es decir, como si fuera un enlace punto a punto.

El servicio TelNet, uno de los más antiguos del Internet, permite de esta manera conectar dos computadoras cualesquiera de la red en forma directa desde el punto de vista del usuario. No es necesario el uso de exploradores como en el caso de la Web, sino que desde la línea de comandos se ejecuta el comando”Telnet” seguido de la dirección IP del Host al que se desea conectar.

Una de las características de este tipo de conexión, es que permite emular diferentes tipos de terminales, DEC, IBM etc. La ventaja de este servicio, es que una Terminal no queda limitada a la conexión a un Servidor Local de su ISP, sino que puede hacer login a cualquier Host de la red. Se proveen funciones tales como el uso de contraseña (password), para controlar la seguridad.

Debido al avance de otros servicios del Internet, Telnet no es tan ampliamente utilizado como en los comienzos, cuando tuvo gran difusión especialmente al nivel de universidades.

Como en otros servicios del Internet, el protocolo Telnet fue desarrollado para proveer servicios multiplataforma a través de la red. Para ello es necesario “negociar” previamente entre los terminales, para sincronizar la comunicación. Esto se hace mediante ciertas opciones y comandos especiales. Estos comandos son:

WILL/WON’T <opcion> y DO/DON’T <opcion>

Los dos primeros, solicitan que se permita determinada opción (Will) o que no se permita (Won't). Mientras que los dos últimos, permiten autorizarla o desautorizarla, por parte del otro terminal. Permiten disponer de varias opciones:

1. Capacidad de cambiar de texto de 7 bits a 8 bits
2. Permitir a una Terminal o la otra volcar caracteres
3. Especificar un tipo de Terminal
4. Solicitar el status de una opción determinada
5. Poner una marca de tiempo para sincronizar los dos finales de conexión
6. La posibilidad de terminar un registro con EOR (End of Record)
7. Configurar el Modo "Line", mediante el cual se pueden enviar cadenas de caracteres en lugar de caracteres uno por uno.

Protocolo FTP

El protocolo de transferencia de archivos FTP (File Transfer Protocol), permite la transferencia de archivos binarios o ARCII, entre equipos locales o remoto. Opera con programas distribuidos (shareware). El protocolo trabaja en el entorno TCP/IP, en el nivel de Capa 7, de Aplicación, del Modelo OSI.

Desde un Browser, mediante el tipeado de ftp://ftp.cdcom.com/pub/cica/, se puede comunicar con su servidor y solicitar la página /pub/cica/, luego seleccionar el archivo deseado. También se puede transferir (upload) archivos al FTP del servidor del proveedor. Utiliza el método "anonymous login", que permite aceptar la conexión, sin indicar nuestra identificación, y permite bajar (download) archivos disponibles al público en general.

El FTP, es un protocolo robusto diseñado para transferencia confiable de archivos entre dos terminales. Se realizan dos conexiones, una de transmisión de datos y el otra de control. Al igual que TELNET, el FTP puede ser llamado directamente desde el Sistema Operativo sin necesidad de software adicional.

Mediante FTP <dirección ip> se establece la conexión de control y luego, mediante PUT <nombre de archivo> se establece la conexión de datos que enviará el archivo indicado, permaneciendo esta segunda conexión únicamente durante el tiempo de transferencia del archivo. El correspondiente comando GET <nombre de archivo> de la otra parte permitirá recibirlo. Además de los comandos PUT/GET mencionado podremos nombrar a:

1. OPEN, abre la conexión entre dos Terminales.
2. CLOSE, cierra la misma.
3. BYE, finaliza una sesión FTP.
4. BINARY, indica que el archivo a ser transferido es un archivo binario.
5. MGET, permite uso de wildcards para enviar en un paso múltiples archivos.
6. MPUT, similar a MGET permite múltiples archivos.
7. CD, faculta cambio de directorio en el dispositivo remoto.
8. DIR, listado de directorio en el dispositivo remoto.
9. LDIR, accede obtener el directorio local.
10. HASH, indica el archivo que está siendo transferido.

Como puede verse a través de FTP, mediante ciertos comandos se permite ejecutar algunos comandos de Sistema Operativo (semejante a DOS) en el Terminal Remoto, para ubicar los Directorios a los cuales la información debe ser transferida o desde los que debe ser recibida.

Con el advenimiento de Windows y también de interfaces visuales para UNIX, se ha hecho popular el uso de aplicaciones sencillas, que ejecutan dichos comandos proveyendo una interfaz más amigable para el usuario y selección de archivos más rápida mediante uso de ListBoxes; etc. De éstas WS_TP y CuteFTP son algunas de las más difundidas.

El protocolo FTP fue el medio casi exclusivo de transferencia de archivos y aún sigue siendo ampliamente utilizado, si bien los usuarios del Internet no están concientes de ello, ya que en general estas conexiones se establecen a través de hipervínculos en la Web, de manera que el usuario cree que es mediante la Web que se realiza la transferencia.

En los últimos años se ha hecho más común la transferencia mediante otro protocolo, el HTTP, ya que muchos software para administración de Sitios Web, que es donde se realiza mucha de la transferencia de archivos, tales como Microsoft FrontPage trae integrada la transferencia automática de archivos al Servidor Web, vía HTTP.

Protocolo SMTP

El protocolo de transferencia de correo simple SMTP (Simple Mail Transfer Protocol), documentado en RFC 821,822 y 974. El SMTP, se ha diseñado para transferir mensajes y archivos, de correo electrónico (e-mail), entre equipos remotos en red de computadoras.

Para la operación de e-mail son necesarios tres protocolos, los que toman parte del proceso SMTP, POP y DNS. El SMTP es el protocolo que se encarga del envío y recepción de e-mail. Es una de las más extendidas aplicaciones del conjunto de protocolos TCP/IP.

Como en algunos de los casos anteriores, el protocolo en sí es simple. Por una parte, la sección transmisora crea un mensaje, le adosa la Dirección de Destino y lo envía desde una Aplicación Local, a la Aplicación del Servidor SMTP, donde se guarda. Luego, el Servidor, chequea a intervalos prefijados si hay nuevos e-mail pendientes de envío. Si los hay, el Servidor intentará enviarlos; de hecho, en caso de no estar operativo en ese momento el receptor, hará varios intentos. De no tener éxito en ninguno de ellos, finalmente descartará el e-mail y enviará al transmisor del mismo un mensaje de error.

El formato de dirección e-mail es del tipo: identificador local@nombre de dominio. Provee la funcionalidad mínima necesaria para la transmisión y recepción de los e-mail. El sistema consta de dos entidades, SMTP-transmisor y SMTP-receptor. Dado el concepto de simplicidad del protocolo SMTP, no están previstas en él, las funcionalidades como ser de attachments, lo que se logra mediante otros protocolos.

Se utiliza para la red de Internet, en sistema UNIX y forma parte de la pila de protocolos TCP/ IP. El SMTP es un protocolo ACHII sencillo. Proporciona, para el envío y recepción de los mensajes las funciones de cliente y servidor. En este protocolo se utiliza el POP Server, servidor de punto de presencia POP (Point of Presence) que almacena los e-mail hasta se recuperados por el cliente. También se emplea el nombre del cliente POP (User Name POP).

Protocolo POP

El protocolo de oficina postal POP (Post Office Protocol), cubre ciertas limitaciones del protocolo SMTP, especialmente con relación a hacer utilizable el sistema de e-mail, no ya a nivel de Servidores o Terminales de Red, sino de PC, e incluso de dispositivos de telecomunicaciones móviles tales como Laptops, HandHelds o SmartPhones.

El protocolo SMTP requiere que el receptor esté activo para que sea posible poder recibir un e-mail. Sin embargo, en el caso de las PC, y de los dispositivos móviles, es claro que esto no siempre será posible. De ahí la idea de un protocolo complementario POP que actúe como una Oficina Postal que esté abierta continuamente, reciba los e-mail y luego localice al receptor del mensaje cuando este esté disponible.

El protocolo POP (POP3), no cumple ninguna función de envío de e-mail, para lo que se emplea el SMTP, si el transmisor estará activo, sino que tiene que ver con las tareas de mejor recepción. El sistema consiste en que el ISP, a través de este protocolo simula para nuestra PC ser un Host en la red. De esta manera, el Servidor POP recibe habitualmente los e-mail, fuera que la PC esté conectada o no a la red y los envía cuando esta esté conectada.

No está especificado en la, petición de comentarios RFC, del Consejo de Actividades de Internet IAB, que sistema de seguridad debe utilizarse, pero por lo general al establecerse la conexión con el Servidor POP, éste solicitara un password al usuario para darle acceso.

Una vez que el usuario ingresó una casilla, el protocolo establece bloqueos para evitar problemas de concurrencia, mientras se realiza la transacción. Una vez leído el mensaje puede o no borrarse, como una de otras opciones disponibles en este protocolo a nivel del Servidor.

A. 9. 8. 6. 5. Protocolo DNS

El protocolo, sistema de nombre del dominio DNS (Domain Name System), cumple básicamente la función de hacer más amigable el sistema de direccionamiento en redes TCP/IP, tales como el servicio Internet. Si bien desde el punto de vista de la máquina, los números son mucho más fáciles de procesar, nuestra memoria que funciona de otra manera, le resultan difíciles de recordar las secuencias largas de números, y en cambio resulta fácil recordar secuencias de letras, si éstas tienen sentido.

De ahí que el DNS, cumple la función de traducir direcciones IP del tipo 232.144.155.965 en direcciones más recordables del tipo por ejemplo: www.dominio.com/usuario.

El protocolo DNS se compone de sistema de traducción y de direccionamiento.

El sistema de traducción consta de las siguientes partes: Un Servidor DNS, una base de datos y programas en las estaciones de trabajo “Name Resolvers”. El Servidor DNS contiene la base de datos que mapea (configura) direcciones IP a nombres de dominio, y los Name Resolver realizan las consultas (Query) a dicho Servidor. Los Name Resolver usualmente aparecen embebidos en aplicaciones TCP/IP o FTP. De tal manera, el manejo se hace transparente para el usuario, que puede muchas veces ingresar por la dirección IP, o bien por el nombre del DNS.

La traducción se hará en forma automática. En ese sentido, es común haber visto en los Navegadores de Internet, que mientras nos conectamos con una dirección DNS, suele aparecer la dirección IP, correspondiente en la barra de status, la que ha sido traducida por el Servidor DNS.

El sistema de direccionamiento DNS es esencialmente jerárquico y sigue una estructura similar a DOS o UNIX en el formato de las mismas. El sistema DNS, puede ser muy útil, no solo para comunicaciones a través del Internet, sino para nombrar Host dentro de una Internet privada (Intranet).

Existen aplicaciones similares para otros protocolos, tales como WINS en el caso de NetBEUI para redes Windows, pero el trabajar con TCP/IP junto con el sistema DNS, facilitará los eventuales enlaces WAN, ya que trabaja con un protocolo “routeable”.

Asimismo, dentro de la propia LAN, el sistema puede ser muy eficaz, si algunas de las máquinas funcionan bajo un sistema no-Windows, por ejemplo el UNIX /Linux, donde TCP/IP puede ser utilizado sin inconvenientes.

Se debe tener en cuenta que si bien los usuarios del sistema Name Resolver, pueden residir en las PC con direccionamiento dinámico, por lo cual pueden ser reconocidos por el Servidor DNS, dicho Servidor DNS, no admite para sí este tipo de direccionamiento, sino que debe serle asignada previamente una dirección IP fija, para poder funcionar como Servidor DNS.

Protocolo DHCP

El protocolo de configuración de Host dinámico DHCP (Dinamic Host Configuration Protocol) es un servicio ampliamente difundido. Se trata de una aplicación que funciona bajo la arquitectura Cliente-Servidor, permitiendo asignar direcciones IP a los Host de la red en forma automática. Tienen lugar los siguiente pasos:

1. Solicitud: El Cliente envía una comunicación de tipo broadcast buscando un Servidor DHCP disponible.
2. Ofrecimiento: El Servidor DHCP selecciona una dirección IP que tiene libre y se la envía al Cliente.
3. Selección: El Cliente informa al Servidor que ha seleccionado la dirección que se le ofreció. Esto para la ocurrencia de que más de un Servidor DHCP conteste la solicitud Broadcast, en cuyo caso el Cliente aceptará el primer ofrecimiento.
4. Confirmación: El Servidor DHCP marca como ocupada la dirección IP seleccionada por el Cliente, registra a su vez la dirección MAC de la máquina y envía la confirmación al Cliente, con lo que se completa la operación.

Si bien el Servidor DHCP está facultado para asignar direcciones a los Host, su propia dirección debe ser fija, y no puede haber sido asignada por otro DHCP.

El Servidor DHCP entrega las direcciones IP en carácter transitorio. El objetivo de esto es que una vez que un Host se desconecta, dado el que Servidor DHCP no se entera de ello, seguiría manteniendo ocupada su dirección IP, sin ningún propósito. Dado que estadísticamente, los Host solo estarán conectados una fracción del tiempo, el Servidor DHCP puede dar servicio a muchas más máquinas que el número de direcciones IP que dispone, por lo que son asignadas por un período determinado.

El período configurable por el Administrador de Red, suele ser entre los 3 y 8 días. El Host, próximo al vencimiento puede enviar al Servidor una Solicitud de Renovación, por otra parte, cada vez que se enciende, puede enviar una Solicitud de Confirmación para comprobar si su dirección IP sigue vigente. En caso negativo, dará paso a los cuatro pasos anteriormente descritos, para obtener una nueva dirección IP de parte de algún Servidor DHCP disponible.

El Sistema DHCP tiene múltiples aplicaciones. Es muy conveniente para los ISP, a fin de optimizar su gestión de las direcciones IP que disponen, pero también es de gran utilidad en las LAN, ya que permite ahorrar el esfuerzo de constante asignación de las IP para nuevos Host.

El sistema funciona tanto en redes Windows como UNIX o Linux. Puede observarse en los directorios del sistema winip.cfg o ipconfig/all, que allí aparecen tanto la dirección IP asignada al Host, como la dirección IP fija del Servidor DHCP.

Servicio de Acceso Remoto (RAS)

La aplicación, registro de admisión y estatus RAS (Registration Admission and Status), como servicio de acceso remoto, funciona bajo la arquitectura Cliente-Servidor. Cumple con la función de conectarse a una determinada red, a través de una conexión telefónica.

Para hacerlo, tiene lugar la colaboración entre el Servidor RAS y un Servidor DHCP de la misma red. Se cumplen los siguientes pasos:

1. El Cliente RAS solicita el acceso remoto a la red (Dial-In).
2. El Servidor RAS solicita a un Servidor DHCP una dirección IP disponible.
3. El Servidor DHCP confirma una dirección por el mecanismo anteriormente comentado.
4. El Servidor RAS asigna esta dirección IP al Cliente sólo durante el tiempo de conexión, con lo que éste queda habilitado a utilizar los servicios de red que se le hayan hecho disponibles de acuerdo a los sistemas de seguridad de la red.

Los Servidores RAS pueden admitir hasta 256 conexiones telefónicas simultáneas, y el acceso en la práctica se efectúa en forma sencilla, por ejemplo en los Sistemas Operativos Windows, mediante configurar el Acceso Telefónico de Redes.

Con respecto a la seguridad, existen disponibles sistemas de Autenticación de la Llamada y también se puede configurar que servicios de la red se harán disponibles al Cliente RAS, como ocurre con otros Host fijos de la red. También existen sistemas que permiten determinar donde debe realizarse el cargo de la llamada, como ser al teléfono del usuario o a un número definido por el usuario.

Es posible disponer de más de un Servidor RAS si la demanda lo amerita. En muchos casos, el sistema RAS es también utilizado como enlace WAN para envío de información, por ejemplo, entre sucursales de una organización y la casa central, como podría ser, envío nocturno de actualizaciones, en cuyo caso un Servidor haría de Cliente-RAS, ante el Servidor-RAS disponible en la central.

Aunque tales sistemas tuvieron amplio uso hace algunos años, en la actualidad han sido en parte sustituidos por los servicios Web. Aún puede mencionarse como una ventaja del enlace RAS, ser más seguro al ser un enlace exclusivo que funciona por fuera de la Web.

Protocolo NNTP

El protocolo de transferencia de noticias de red NNTP (Network News Transfer Protocol), permite la transferencia de noticias de red. Ofrece la consulta y envío de noticias, boletines de foros, debates. Las conversaciones tienen lugar en un foro público y al cual hay que estar asociado.

"Usenet" es una red de computadoras que acordaron propagar información como foro de discusión (newsgroup) sobre temas específicos. Los newsgroup están organizados en los "World Newsgroup", que usan libremente la red Usenet y en los "alternative newsgroup" que propagan los mensajes solo a quienes lo soliciten.

Los World Newsgroup se subdividen en las subcategorías, comp: computadoras, news. sistemas de noticias, misc. misceláneas, sci: científicos, rec: recreación. Los alternative newsgroup se subdividen en las subcategorías, bionet: biología y medio ambiente, biz: negocios y anuncios, K12: educación primaria y secundaria.

Estándares X.400

El CCITT, actual ITU-T, ha desarrollado un conjunto de estándares de tratamiento de mensajes, con independencia del hardware y el software, llamados de la Serie X, como el X.25, X.200, X.400, X.500 y el X.700. Esta serie cubre los estándares de interconexión de sistemas abiertos OSI.

El X.400 dentro de este conjunto, define al sistema de tratamiento de mensajes MHS (Message Handled System). El estándar MHS ha sido popularizado por la firma Novell. Se emplea para correo electrónico. Los usuarios podrán ser tanto máquinas o personas, y podrán ser usuarios directos o indirectos a través de otros sistemas. Los estándares X.400 establecen:

- La información de encaminamiento, identificadores de mensajes, reglas de presentación, descripción de direcciones de destino e instrucciones de entrega y confirmación de recepción.
- Identificación de usuarios autorizados, notificación de y al receptor, indicación de asuntos de los mensajes.
- Las modificaciones de los parámetros de encaminamiento y entrega, contraseñas, tamaño de mensaje y comprobación de entrega de mensajes.

Varias son las características de desempeño a proporcionar al usuario:

- Diferentes niveles de prioridad de los mensajes,
- Indicación de hora y fecha,
- Comprobante de entrega,
- Recepción múltiple y alternativo.

Las principales partes constitutivas de un sistema X.400 son:

- El agente de usuario UA (User Agent). Se ejecuta en el equipo del usuario y sirve de conexión con el servicio de tratamiento de mensaje MHS. Realiza funciones de creación, lectura y examen de mensaje.
- El agente de transferencia de mensaje MTA (Message Transfer Agent). Acepta mensajes, convierte formatos, y reenvía a otro MTA o UA de destino.
- El sistema de transferencia de mensajes MTS (Message Transfer System). Es responsable de transferir mensajes desde el UA, que crea el mensaje al destino. En un MTS existen grupos MTA, para almacenar y reenviar mensajes (Fig. 46).

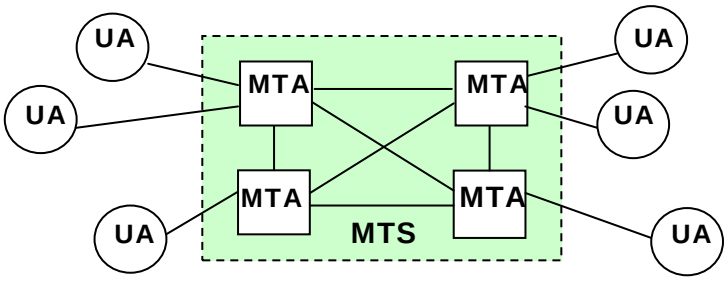


Fig. 46 - Componentes de un sistema X.400

Estándar X.500

El estándar X.500 define al conjunto de directorios de la ITU-T desarrollados para auxiliar a los usuarios de redes distribuidas, en la ubicación de usuarios de las distintas redes. Para ello, proporciona un directorio global de usuarios, con estructura jerárquica.

Servicio Chat

El servicio Chat presta comunicación en tiempo real (on-line), vía texto, aunque actualmente se puede utilizar sonido, video y compartir aplicaciones. El usuario se conecta mediante un programa de Chat a un servidor IRC (Internet Relay Chat) donde se pueden reunir cientos de personas, con el fin de intercambiar impresiones o informaciones de cualquier tipo.

Los programas más usados son, el MIRC, interfaz gráfica, de textos, comandos remotos etc, el ICQ ó el Pirch, ambos de similar utilidad.

A. 9. 9. Otros protocolos típicos

Exploremos algunos de los protocolos que se han comúnmente utilizado.

a) XNS

El protocolo XNS (Xerox Network System), ha sido desarrollado por Xerox para su red LAN Ethernet. Su mayor ventaja radica en ser un protocolo enrutable.

Es un protocolo extendido y por ello lento, similar al TCP/IP, además produce mayor cantidad de emisiones tipo broadcast, lo que crea un mayor tráfico ficticio.

b) NetBEUI

El protocolo NetBEUI ha sido desarrollado por Microsoft, en 1980. Es un protocolo del nivel de transporte, pequeño, rápido y eficiente, importante para redes medianas. Su mayor desventaja es no ser enrutable y limitada a redes basadas en Microsoft.

Originalmente estaba relacionado con el protocolo NetBIOS, sistema básico de entrada salida de red de IBM, luego fue separado como protocolo de sesión a fin de poder ser utilizado con otros enrutables de transporte.

c) DECnet

La pila de protocolos DECnet, ha sido desarrollado por Digital Equipment Co. Se trata de un protocolo enrutable, como un conjunto hardware y software, que implementan la arquitectura de las redes DAN (Digital Architecture Network), de la firma Digital.

Define las comunicaciones sobre LAN Ethernet, MAN con interfaz de datos por fibra óptica y WAN con FDDI o con protocolos TCP/IP.

d) VINES

El protocolo VINES, ha sido desarrollado por Banyan Co, como enrutable.

e) X.25

El conjunto de protocolos X.25 de la UIT, es dirigido a un servicio de redes de conmutación de paquetes. Originalmente conectaba Terminales Remotos a Host centrales (Ver su desarrollo en Anexo II).

f) APPC

El protocolo, Comunicación avanzada programa a programa APPC (Advanced Program to Program Communication), es un protocolo de transporte, desarrollado por IBM como parte de su arquitectura de red de sistemas SNA.

g) SNMP

El Protocolo sencillo de administración de redes SNMP (Simple Network Management Protocol), se definió en 1990 para controlar redes y componentes de redes Internet.

Los nodos administradores pueden ser los Host, enrutadores, puentes o las mismas impresoras, tales que sean capaces de comunica r información y que ejecuten el proceso de administración SNMP.

A. 9. 10. Valor operativo de los equipos de la Red

La vinculación entre segmentos de las LAN o entre LAN para formar MAN o WAN se realiza mediante determinados equipos y tipos de arquitecturas de red. Cada uno de estos equipos delimitará su estructura máxima, los mismos se emplearán de acuerdo al caso y requerimiento deseado.

Estos equipos componentes, utilizados para formar redes mayores, ampliando, combinando o separando redes son los repetidores, Bridge, Router, bRouter y gateways.

REPETIDOR

Para redes LAN extensas, las distancias a alcanzar son limitadas por la atenuación dada por el cableado utilizado y por el protocolo empleado. Luego se emplean repetidores que regeneran las señales a su estado original, sin traducir ni filtran los bit.

Los repetidores, son dispositivos que operan en la Capa 1, Física, es decir en el ámbito físico. Retransmiten la señal de bit en bit. Para utilizar un repetidor, los paquetes y protocolos, deben ser iguales en ambos extremos. Tampoco podrán conectar dos segmentos que usen dos técnicas de transmisión y métodos de acceso diferentes, por ejemplo CSMA /CD y Token Passing Ring. Sin embargo, los repetidores son capaces de vincular distintos medios físicos, coaxial fino con coaxial grueso o estos con fibra óptica.

Su mayor desventaja reside en que, a través de los repetidores pasan las colisiones y transmisiones tipo broadcast. Al no filtrar información, los paquetes mal formados o el alto tráfico en un segmento es transmitido al resto de la red.

Para utilizar un repetidor, los paquetes y protocolos de la subcapa LLC deben ser iguales en ambos extremos. No se podrá conectar dos segmentos que empleen técnicas de transmisión o métodos de acceso diferentes, por ejemplo CSMA /CD y Paso de Testigo. Es decir que no traducen un paquete Ethernet a un paquete Token Ring. Los repetidores multipuerto pueden actuar como concentradores.

BRIDGE

Un Bridge (puente), utiliza el nivel de subcapa MAC de la Capa 2, de Enlace, que contiene la dirección de la estación de destino, lo que le permite analizan las tramas en el ámbito de enlace. Opera monitoreando el tráfico entre las subredes que vincula, leyendo solo las direcciones de fuente y destino, de esa capa MAC. Conectan dispositivos del subnivel MAC, a través del subnivel LLC.

Luego pueden interconectar segmentos de igual o de disímil técnica de acceso al medio, tales como Ethernet, X.25, Token Ring. Reconocen las direcciones dentro de su segmento y retransmiten todas las que no reconocen a todos los equipos de todos sus puertos. Pasan las transmisiones tipo broadcast, pero no las colisiones.

Un Bridge, permite expandir el área de una LAN o permitir que dos redes LAN geográficamente separadas, por ejemplo a distancias mayores a 2.5 Km, sean tratadas como una simple red. Además, podrá dividir la red para aislar los problemas o exceso de tráfico. Una red muy extensa se puede dividir en dos segmentos mediante un Bridge y cada uno de estos serán considerados como una red independiente con mayor eficiencia por tener menos colisiones.

Similar a un repetidor, puede aumentar la distancia de un segmento o unir distintos segmentos de trabajo. Vincula distintos segmentos de redes que utilice la misma o diferente topología, como Ethernet y Token Ring de distintos cableados como cables UTP y coaxiales.

Los Bridge tienen un cierto grado de inteligencia. En la técnica de encaminamiento desde el origen, al conectarse los puentes las tablas de ruteo están vacías y se usa un algoritmo de "inundación". Desde el origen se difunde una trama preguntando a todas las LAN que esta conectado el puente, donde esta el destino buscado. Basándose en las direcciones de destino, a medida que transmite los paquetes y mediante su memoria, llena una tabla de ruteo. Posteriormente determina, la red desde la cual el paquete está llegando y a la que va dirigido, si el destino se encuentra en la tabla de ruteo envía el paquete a ese segmento de red mediante un algoritmo de ruteo.

Con este procedimiento de aprendizaje, se filtra y reduce el tráfico entre segmentos. Cada segmento transportará menos paquetes, luego se producirán menos colisiones y con ello se obtendrá mayor velocidad y más eficiencia en la red. Tal método se conoce como segmentación del tráfico. En el diseño del mejor camino de enrutamiento, una "trama de descubrimiento", es reenviada por cada puente de modo que llegue a todas las LANs de la interred. Cuando llega la respuesta los puentes registran las rutas que siguió y escoger la mejor.

Si en la topología de la red existen bucles, podrán generarse paquetes duplicados. Para limitarlos se fija un número máximo de saltos para cada paquete. Otro método es numerando los paquetes y mantener cada Router una lista de comprobación.

También, puede usarse la inundación selectiva, donde los paquetes se envían solo por los trayectos adecuados, encaminamiento por flujo menos congestionado, por menor distancia, estado del enlace, en multicast o broadcast. A medida que crece la extensión de la red, la información de enrutamiento (routing), aumenta exponencialmente luego se deberán crear encaminamientos jerárquicos, dividiendo la red en regiones.

Un algoritmo interesante es el que construye un trayecto en topología árbol, sin bucles denominado Spanning Tree. Otros métodos con complejos algoritmos son utilizados.

Un algoritmo de ruteo es el software de Capa de Red que decide la línea de salida para cada paquete de entrada. Se pueden utilizar varios Bridges para formar una red mayor.

La característica más importante de un Bridge frente a otro dispositivo de enlace inteligente, es su velocidad de conexión. Se podrá superar los 30 000 paquetes por segundo (PPS).

Para la vinculación de dos LAN muy alejada una de otra, se podrán utilizar líneas telefónicas dedicadas. Para ello se requerirá el uso de Bridges remotos y módems síncronos. Estos puentes remotos permiten formar así una única LAN, trabajando en cada LAN remota como medio puente. Cada línea dedicada, puede tener una velocidad típica de 64 ó 2.048 Mb/s. También se pueden unir los puentes remotos con sistemas X.25, Frame Relay o técnicas de radioenlaces.

Los Bridge al trabajar al nivel de Enlace son transparentes a los protocolos de niveles superiores, por lo tanto pueden manejar tráficos de distintos protocolos. Al operar los puentes, en la Capa de Enlace implica que no examinan la cabecera de trama de Capa de Red, luego puede manejar igualmente paquetes IP ó IPX, en contraste a un enrutador IP ó IPX puro, que puede manejar solo sus propios paquetes. Tales puentes que interconectan dos redes con diferente estructura de trama MAC, por ejemplo Ethernet y Token Ring, se les denominan puentes traductores o puentes de traslación.

ROUTER

Los enrutadores o Router trabajan en Capa 3, de Red. Pueden leer tanto la dirección de la estación fuente, la de destino en esa LAN, como la estación destino de otras LAN, lo que le permiten la interconexión en el ámbito de red.

Un Router, diferente a un Bridge en que puede encaminar rutas entre varios segmentos de LAN. Analizan el contenido de los paquetes (dirección de destino, dirección de origen) y toman decisiones de encaminamiento. Encaminan protocolos particulares a direcciones particulares, filtrando el resto. Determinan la dirección adonde enviar el paquete y a que Router pertenece.

Permite el filtrado de los datos, decidiendo la mejor ruta, con menor tráfico y más corta disponible en ese momento, es decir la ruta de menor costo de envío. La selección de la ruta más corta lo efectúa, determinando la cantidad de saltos a ejecutar entre segmentos.

Al trabajar en un nivel superior al de los Bridge, se tiene acceso a mayor información en la lectura de los paquetes, permitiendo conmutarlos y encaminarlos entre múltiples redes LAN y WAN.

Un Router multiprotocolo conecta redes separadas de diferentes topologías con distintos protocolos, como TCP/IP con DECnet de Digital. Pero solo utiliza los protocolos tipo enrutadores. A través de los Routers, no pasan las colisiones ni las transmisiones tipo broadcast. Suelen utilizarse para vincular varias LAN con WAN, también WAN con WAN. Se crean segmentaciones de una LAN, por ello se dice que crean LAN virtuales (VLAN). También se pueden implementar las VLAN, mediante ATM LAN.

Se refiere a un Router local, cuando trabaja dentro de las longitudes límites dadas por el controlador de esa LAN. Se dice Router remoto, cuando trabaja fuera de esos límites, generalmente utilizando un módem. Un Router permite conectar dos redes LAN, administrarlas en forma independiente, hacerlas más gestionarbles y accesibles unas a otras. Se requerirá un protocolo del tipo enrutable: DECnet, IP, IPX, XNS ó DDP, o del tipo no enrutable como el NetBEUI.

El diseño de un Router es el de un conmutador de paquetes. Los Routers ofrecen el mas alto grado de redundancia y tolerancia a fallas. Por ejemplo en una WAN formada por varias LAN, si se cortase una conexión entre dos de ellas, un Router inteligente podrá unirlas mediante un camino alternativo.

Desde el punto de vista de la arquitectura, una red que está interconectada por Bridges se asimila a una sola red, mientras que una red interconectada usando Routers se sigue correspondiendo a grupos de redes separadas, conectadas entre sí. Un Bridge y un Router se componen de hardware y software similares, pero los Routers enlazan redes al nivel de Capa de Red, ofreciendo un procesamiento más intensivo. Sin embargo al tener que realizar funciones mas complejas con cada paquete, tiene una movilidad mas lenta que un Bridge.

Los Routers dedicados trabajan solo como enrutador, mientras que Router no dedicado puede funcionar simultáneamente, tanto como enrutador o como workstation.

La tabla de enrutamiento contiene todas las direcciones de esa red, como conectarse a otras redes y las posibles rutas entre Routers. Se puede guardar direcciones de Host, dependiendo de los protocolos que se estén ejecutando. Cuando los paquetes pasan de un Router a otro, se crean nuevas direcciones. Al comunicar Routers remotos permite segmentar grandes redes en mas pequeñas, actuar como barrera de seguridad y evitar saturaciones, ya que las difusiones (broadcast) no se enrutan.

Si se requiere, los Routers pueden operar en forma de multipunto (multicast), también llamado multiprotocolo, o en forma de difusión (broadcasting). Existen enrutamiento del tipo: estático, dinámico e inteligente. En el enrutamiento estático se requiere que un administrador configure manualmente la tabla de enrutamiento y una vez establecida, los trayectos en la red nunca cambian.

El enrutamiento dinámico descubre la ruta en forma automática, tomando la decisión de paquete en paquete. Un Router inteligente, podrá mantener un mapa de la red completa y además determinar el mejor camino a un destino dado.

La función de rebalanceo del tráfico en la red, se completa con la limitación de los mensajes, evitando la congestión de los enlaces en las WAN. Si el paquete enviado es demasiado largo para que acepte la red de destino el Router la segmenta en varios paquetes mas pequeños. En la terminología TCP/IP a esta operación se la denomina fragmentación.

BROUTER

Un Brouter, es un implemento que combina las funciones de un Bridge y un Router. Un Brouter puede actuar como Router para un cierto protocolo y como Bridge para el resto de los protocolos. Podrá enrutar uno o mas protocolos enrutables tal como TCP/IP y XNS, como dejar pasar todos los otros tráficos no enrutables.

Al trabajar los Brouter en la subcapa MAC, se podrán en su fabricación asignar un esquema de direccionamiento permanente tipo tabla Bridge / Router. Ésta almacena la dirección completa de bit de cada estación. Al incorporar un Brouter a una LAN, éste leerá las direcciones de las tramas, almacenándolas en la tabla de enrutamiento y direccionándolas a solo el dispositivo asignado. Así aprender la dirección del dispositivo Terminal en la LAN. Al conocer la dirección de los dispositivos en una LAN local, podrá aprender la ruta entre las LAN, utilizando algoritmos de enrutamiento.

PUENTES TRANSPARENTES

Los repetidores filtradores de paquetes, llamados puentes transparentes, fueron desarrollados por Digital en 1984, como alternativa económica respecto a los Routers. El IEEE los estandarizó en 1990 como norma 802.1D.

CONMUTADORES LAN

Las WAN podrán emplear equipos enrutadores (Router) y/o conmutadores (Switch), ambos que trabajan a nivel de Capa 3.

En 1991 se comercializó un puente Ethernet, con un número elevado de interfaces y de alto rendimiento, capaces de soportar 10 Mb/s en cada una de sus interfaces. Al mismo se le denominó conmutador LAN o conmutadores de Capa 2, en el ámbito de enlace a nivel MAC. Así se diferencian de los conmutadores tradicionales que trabajan en Capa 3 del Nivel de Red. Los conmutadores LAN permiten el crecimiento de las redes Ethernet en capacidad.

Llevado a un extremo la filosofía de los conmutadores LAN, con un conmutador por puerto, cada usuario puede disponer de 10 Mb/s y sus mensajes no pueden ser visto por ninguna otra computadora salvo aquella a la que van dirigidos. El uso de redes conmutadas lleva de medios compartidos a medios dedicados, es decir no sería necesario el uso del protocolo CSMA /CD.

Aprovechando esta característica, se implementó la norma denominada Ethernet Full Duplex. En esencia, consiste en establecer dos canales dedicados de 10 Mb/s, uno en cada sentido tal como si se tratase de una línea punto a punto.

GATEWAY

Los gateway trabajan en Capa 6 en el ámbito del usuario. Une dos sistemas LAN que no utilicen los mismos, protocolos de comunicación, estructura de formato de datos, lenguajes y arquitecturas. Emplean para ello distintas pilas de protocolos

Convierte cada nivel de protocolos, de modo que el equipo de un usuario pueda acceder al sistema operativo de un equipo huésped que use un protocolo diferente.

El gateway toma los datos de un entorno, elimina su pila de protocolos y reempaqueta la información adaptándola a los requisitos de su destino. Al pasar de una red LAN, MAN, WAN a otra, cambia el formato de un mensaje.

Los gateways en cada capa pueden emplear distintos protocolos. Permiten enviar tráfico, desde una red usando un juego de protocolos, para ser recibido en otra red que emplea otro protocolo. Los gateways son específicos para cada tipo particular de transferencia, por ejemplo, desde Windows NT Server a una arquitectura SNA de IBM. Se utilizan en general, para conectar una mainframe (Host central) con varias PC, aprovechando redes de comunicaciones existentes.

Cada LAN tiene usualmente un equipo que actúa como un punto de entrada a la subred. Esta máquina puede ser una computadora dedicada como Router, Bridge o Gateway y trabaja como parte del sistema intermediario de enlace. De estos dispositivos, el Gateway es el mas indicado para enlazar distintos tipos de computadoras y permitir el mejor manejo de las aplicaciones compartidas. Examina la dirección, para determinar si es una computadora de esa red. Siendo así, es directamente conectada, en caso contrario toma la decisión de adelantar la trama a otro sistema intermediario de la subred.

Un gateway utiliza todas las capas del modelo OSI, para poder suministrar la vía de comunicación y traducir entre varias aplicaciones. Permite comparar los juegos de protocolos propietarios suministrados por los fabricantes, mediante procesos de translación. Esta mayor funcionalidad, se contrarresta con el incremento del encabezado, resultando en un mayor retardo de transmisión.

El gateway hace que discos e impresoras remotas en la red aparezcan como locales para el cliente, lo que significa una extensión del sistema operativo. Las conexiones podrán ser efectuadas en redes conmutadas públicas, en líneas dedicadas o red privada.

Con frecuencia los Gateway consisten en un software que reside en una workstation, corriendo en el background de otras aplicaciones. Pero, por la división de los recursos de procesamiento, podrían degradar el rendimiento de las aplicaciones, entonces es conveniente que el Gateway resida en servidores dedicados. Luego tiene como desventajas, ser específico para una tarea, ser frecuentemente lento y además costoso.

A. 9. 11. Seguridad en las Redes

En sus inicios las redes de computadoras fueron utilizadas por investigadores universitarios para el envío de correo electrónico y por grandes empresas para compartir impresoras. Al popularizarse su uso y significativamente con el empleo en compras, transacciones financieras y bancarias, sobre todo con el uso intensivo de Internet, la seguridad de las redes se ha transformado en un problema fundamental a tener en cuenta y resolver:

- Las computadoras tienen información confidencial vital de salvaguardar,
- Del exterior pueden llegar programas o virus que perjudiquen a la empresa,
- Se podrá salir al exterior para conexiones no útiles a la organización.

Los problemas de seguridad en las redes se pueden dividir en cuatro áreas interrelacionadas:

1) Secreto de la información,
2) Validación de identidad,
3) No repudio y
4) Control de integridad.

El secreto se refiere a mantener la información fuera de usuarios no autorizados. La validación de identidad se encarga de determinar con quien se está comunicando. No repudio se refiere a la comprobación de firmas y el control de integridad se encarga de asegurar que el mensaje recibido fue realmente el enviado.

El caso de las firmas digitales corresponde fundamentalmente a la validación de identificación. Se deberá asegurar que:

1) El receptor pueda verificar la identidad proclamada por el transmisor.
2) El transmisor no pueda repudiar después el contenido.
3) El receptor no haya podido confeccionar el mensaje el mismo.

El encriptado es también un tema sobre como preservar el secreto de la información. El arte de diseñar cifradores se llama criptografía y el de descifrar mensajes se denomina criptanálisis. La eficacia de una clave es su código y su longitud.
Los mensajes originales (plain text), para ser encriptados son transformados por una función clave (key), luego transmitidos como texto cifrado (ciphertext), de forma que un intruso no pueda conseguir descifrarlo. El receptor al conocer la clave puede descifrar el mensaje.

Como eventualmente la clave podrá ser conocida por el "enemigo", se emplea un método que utiliza la combinación de dos claves una pública (conocida por un grupo de usuarios) y otra privada (conocida solo por el emisor y el receptor del mensaje). Para el personal administrador de seguridad de las grandes redes, la ventaja de que cualquiera se conecte con cualquiera, significa una maldición. En las grandes corporaciones subyace el peligro de virus, inundación premeditada de información y además la pérdida de tiempo del personal en juegos o material pornográfico.

El espionaje, robo o fuga de información por medio de personas como hackers o cracker, se podrá realizar instalando programas espías (sniffer) que capturen información.

Los muros de seguridad o cortafuegos (firewalls) son filtros informáticos, que bloquean al interior o hacia el exterior paquetes de información seleccionada previamente por un método dado. En caso de máxima seguridad se utilizan servers auditor, equipos sin disco rígido, codificación de datos y /o protección centralizada contra virus. El enemigo podrá estar afuera de la red o dentro, se deben estudiar todos los puntos y caminos susceptibles o débiles de atacar. Un primer nivel del firewall podrá estar constituido por Routers, donde se han configurado distintos programas filtros, otra segunda línea la podrá constituir Host preparados en similar forma.

Los permisos de acceso, en forma de contraseñas (password), podrán tener distintos niveles de restricción. Por ejemplo de solo lectura o solo ejecución, y / o denegar el efectuar copia o modificar un archivo, directorio o recurso (programa) dado. La seguridad a nivel de usuario involucra un password a cada uno de ellos. La restricción de permisos podrá referirse a solo lectura, solo escritura, crear archivo, borrar archivo, ejecutar archivo, cambiar atributos, no acceso, etc.

---ooo0ooo---