



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGON

"SISTEMA DE CABLEADO ESTRUCTURADO Y CONSIDERACIONES
DE DISEÑO PARA REDES DE DATOS CORPORATIVAS"

T E S I S
QUE PARA OBTENER EL TÍTULO DE
INGENIERO MECÁNICO ELECTRICISTA
P R E S E N T A :

ADRIÁN GUZMÁN LAGARDE.

ASESOR: ING. BENITO BARRANCO CASTELLANOS



Estado de México

2009.



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradecimientos.

A mis padres, quienes siempre me han apoyado de forma incondicional y me han impulsado a seguir adelante con principios y valores; en especial a mi Padre quien siempre ha sido un ejemplo a seguir y quien me enseñó aquellas cosas que en la escuela no hubiese aprendido.

Gracias Pa.

A mi esposa, que sin excepción ha estado conmigo en las buenas y en las malas y quien hasta el día de hoy me impulsa para que me supere, con amor, confianza, lealtad y comprensión, y porque con ella tengo todo lo que puedo querer en la vida, porque es el amor de mi vida y porque seguiremos juntos luchando por nuestros sueños.

Gracias Pedacito.

Te amo.

A mis hermanos: Que en su momento me han ayudado para seguir adelante.

A la Sra. Martha Hurtado Ramírez: A quien desde que conozco me ha brindado un verdadero apoyo en mi desarrollo personal y profesional.

Índice	I
Introducción	II-III
CapituloI. Redes LAN y cableado estructurado.	1
1.1 Modelo de referencia OSI.	1
1.2 Tecnología de transmisión en redes.	8
1.3 Topologías de redes LAN.	10
1.4 Enlace de datos para internet: Slip y PPP.	13
1.5 Estándares de IEEE.802	16
1.6 Medios de comunicación.	19
1.7 Cableado estructurado: el concepto.	25
1.8 Elementos del cableado estructurado.	29
1.9 Consideraciones en el diseño de sistemas de cableado estructurado.	35
1.10 Recomendaciones para diseño de sistemas de cableado horizontal.	37
1.11 Procedimientos generales de cableado.	40
CapituloII. Routers&Switches.	41
2.1 TCP/IP.	42
2.2 Internet protocolo IP.	45
2.3 Protocolos de transporte.	49
2.4 Servicios de TCP/IP.	53
2.5 Ruteo	54
2.6 Switcheo WAN.	58
2.7 Frame Relay antecedentes.	60
2.8 Mode de Transferencia Asincrono	68
Capitulo III. Sistemas operativos, servicios& e-Business.	75
3.1 Características de los sistemas operativos.	77
3.2 Sistemas operativos por servicios.	79
3.3 Sistemas operativos de red.	81
3.4 La integración de servicios.	90
3.5 Características de las redes multiservicios.	95
3.6 Integración de redes corporativas.	97
3.7 Los ISP ´S y la industria de internet.	103
3.8 Nuevos servicios de acceso de internet.	108
3.9 Business Inteligence (BI) piedra angular del e-Business.	116
3.10 Plataformas accesibles para sus clientes.	121
Conclusiones	125
Glosario	127
Bibliografía	141





INTRODUCCIÓN.

La principal motivación de este trabajo de tesis es el conocer las diferentes tecnologías existentes en el mercado y algunas aplicaciones dentro del terreno de la convergencia, voz, datos, vídeo y sus combinaciones, se menciona la tendencia tecnológica y de mercado orientada hacia las nuevas filosofías de negocios en Internet y el ámbito de aplicación de distintas tecnologías englobadas dentro de una misma plataforma. Para ello se ha recopilado, estudiado y analizado gran cantidad de información referente a este sistema, así como la aplicación práctica de conocimientos referentes a diversas materias aprendidas a lo largo de la carrera y su puesta en práctica en un proyecto real.

Otra de las razones para llevar a cabo este proyecto de titulación es la importancia del mismo en la actualidad. Debido a la imposibilidad de determinadas empresas para crear y administrar la organización completa de una red de comunicaciones y así poder entrar al comercio virtual de gran envergadura, se ofrece la alternativa de subcontratar gran parte de estos servicios a un proveedor dedicado (operadora de telecomunicaciones), con experiencia en sistemas de comunicaciones de alto rendimiento, capaz de gestionar de una manera más eficiente la transferencia de datos y el mantenimiento posterior de la red, abaratando en gran medida los costos de la misma. De igual forma el continuo avance al que está sometida cualquier tecnología hace imprescindible el apoyo de una empresa experta en telecomunicaciones para garantizar la mejora y madurez del sistema sin estar supeditado al crecimiento de la red.

Un punto a tener en cuenta en toda instalación independientemente del tamaño de la misma es la seguridad informática, se hace énfasis en el capítulo tres sobre los sistemas operativos con los cuales actualmente podemos trabajar y que existen en el mercado, tanto a nivel de privacidad, confidencialidad, integridad y fiabilidad como a la hora de transmitir información y de su posterior almacenamiento.

Entre los objetivos principales es el de manejar el comercio electrónico y adquirir conocimientos sobre redes y cómo gestionarlas en grandes instalaciones (Se hace mención en el capítulo uno en el diseño de la red y su cableado), seguridad



informática, conocer el hardware de una operadora de telecomunicaciones de ámbito nacional y aprender a hacer un buen diseño de redes.

No se puede dejar de mencionar que el diseño de la red de datos de ámbito nacional planteado sigue los criterios técnicos más exigentes para asegurar y garantizar el correcto funcionamiento y fiabilidad de la estructura, componentes, protocolos y tecnologías (en el capítulo dos se hace referencia a las tecnologías a usar que son propiamente de ruteo y de switching, Frame Relay y ATM) utilizadas, es decir, en definitiva, de las comunicaciones.

La metodología a seguir a lo largo del desarrollo del proyecto estará basada en un estudio de necesidades tecnológicas actuales en base a unos objetivos finales garantizando siempre unos requisitos mínimos, el diseño de la mejor solución técnica y el correcto mantenimiento o gestión posterior de la red de datos a través del centro de gestión personalizado.

En el proyecto se ha detallado todo el hardware elegido de forma homogénea (que pertenezca en la medida de lo posible a un solo proveedor, de los mejores en su rango), para que sea capaz al día de hoy de ofrecer las mejores prestaciones ante las necesidades planteadas actualmente y las necesidades futuras que puedan aparecer durante el crecimiento y expansión de una red de estas dimensiones.

CAPITULO 1

REDES LAN Y CABLEADO ESTRUCTURADO.

Las redes LAN juegan un papel muy importante dentro del campo de las telecomunicaciones, de aquí la importancia de conocer las tecnologías de punta del mercado y las posibles tendencias para brindar soluciones empresariales y de negocios.

Las Redes de Área Local, generalmente llamadas LAN (Local Area Network), son redes de propiedad privada dentro de un solo edificio o campus.

Se usan ampliamente para conectar computadoras personales PC's y estaciones de trabajo en oficinas de compañías y fábricas con el objeto de compartir recursos (Por ejemplo: impresoras, capacidad de almacenamiento, dispositivos de comunicaciones) e intercambiar información entre usuarios

Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo, compartido al cual están conectadas todas las máquinas, con sistemas de difusión (Broadcasting).

Las LAN tradicionales operan a velocidades que van de los 10 a los 1000 Mbps (Mega Bits por Segundo).

1.1 Modelo de referencia OSI.

A principios de los años 80 se produjeron grandes aumentos en cantidad y tamaño de las redes, los dueños de estas enfrentaron a problemas cada vez más serios debido a su expansión caótica. Resultaba cada vez más difícil que redes con especificaciones diferentes pudieran comunicarse entre sí.

Para enfrentar este problema de incompatibilidad, la Organización Internacional para la normalización (ISO, International Organization for Standardization) estudió esquemas de redes como: DECNET, SNA, TCP/IP. A fin de encontrar un conjunto de reglas para crear un estándar que asegurara una mayor compatibilidad e interoperabilidad entre distintos tipos de tecnología de red utilizada por empresas a nivel mundial.

El modelo de referencia OSI (Open Systems Interconnections) fragmenta el problema de comunicación entre equipos en siete capas (Ver figura 1.11). Cada capa se ocupa solamente de hablar con su capa correspondiente localizada en la siguiente máquina.

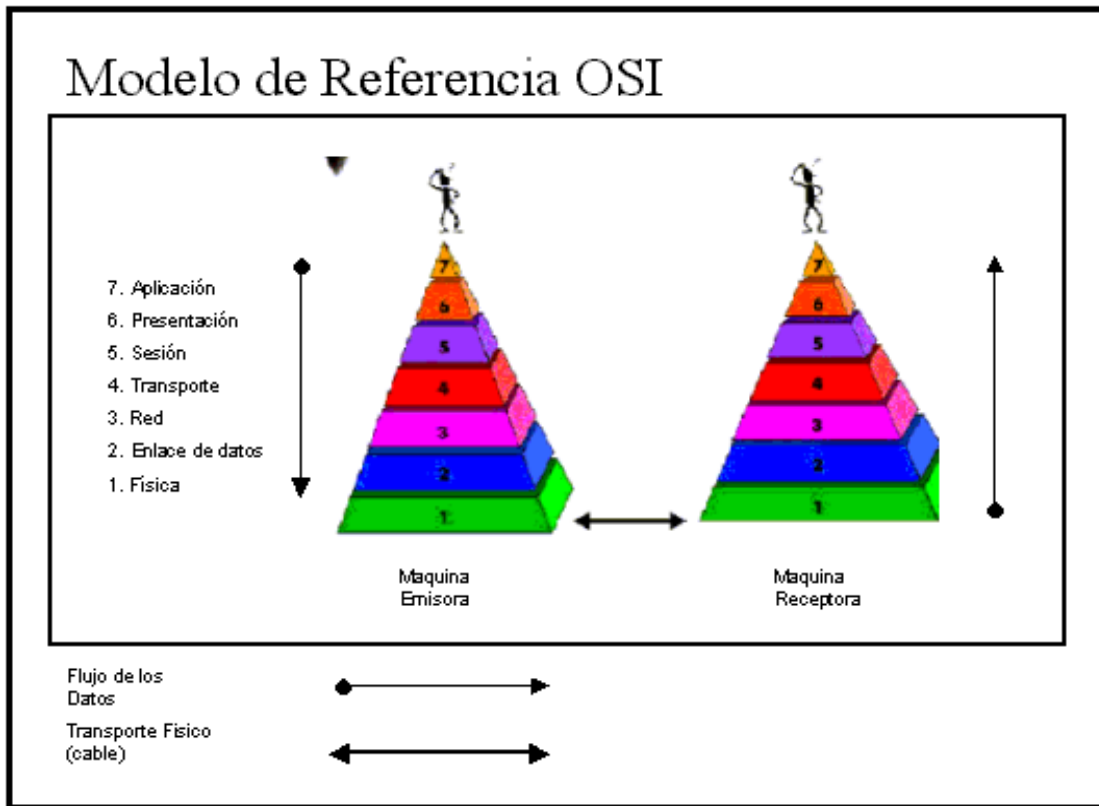


Fig. 1.1

Por ejemplo, la capa 5 sólo se ocupará de comunicarse con la capa 5 de la máquina receptora y no sobre cuál puede ser el medio físico de transmisión. Además, cada capa del modelo de referencia OSI proporciona servicios a la capa superior a ella y solicita determinados servicios a la capa inmediata inferior.

Este manejo de información por capas, permite que cada una de ellas maneje una pequeña pieza de información, le realice cualquier cambio necesario a los datos y agregue las funciones que necesita dicha capa (Figura 1.2) antes de permitir el paso de los datos.

La información deja de parecerse a datos humanos para ser cada vez más un lenguaje de máquina conforme se hace el recorrido sobre el modelo de referencia OSI y finalmente convertirse en ceros y unos (impulsos electrónicos) en la capa física.

La importancia del modelo de referencia OSI radica en que es un marco que se puede utilizar para comprender cómo viaja la información a través de la red, además se puede visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación por ejemplo hojas de cálculo, documentos, etc. a través de un entorno de red (como son los cables) hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el remitente y el receptor posean distintos tipos de red.

Las capas que conforman el modelo de referencia OSI se listan a continuación:

7. Capa de Aplicación.

6. Capa de Presentación.

5. Capa de Sesión.

4. Capa de Transporte.

3. Capa de Red.

2. Capa de Enlace de datos.

1. Capa Física.

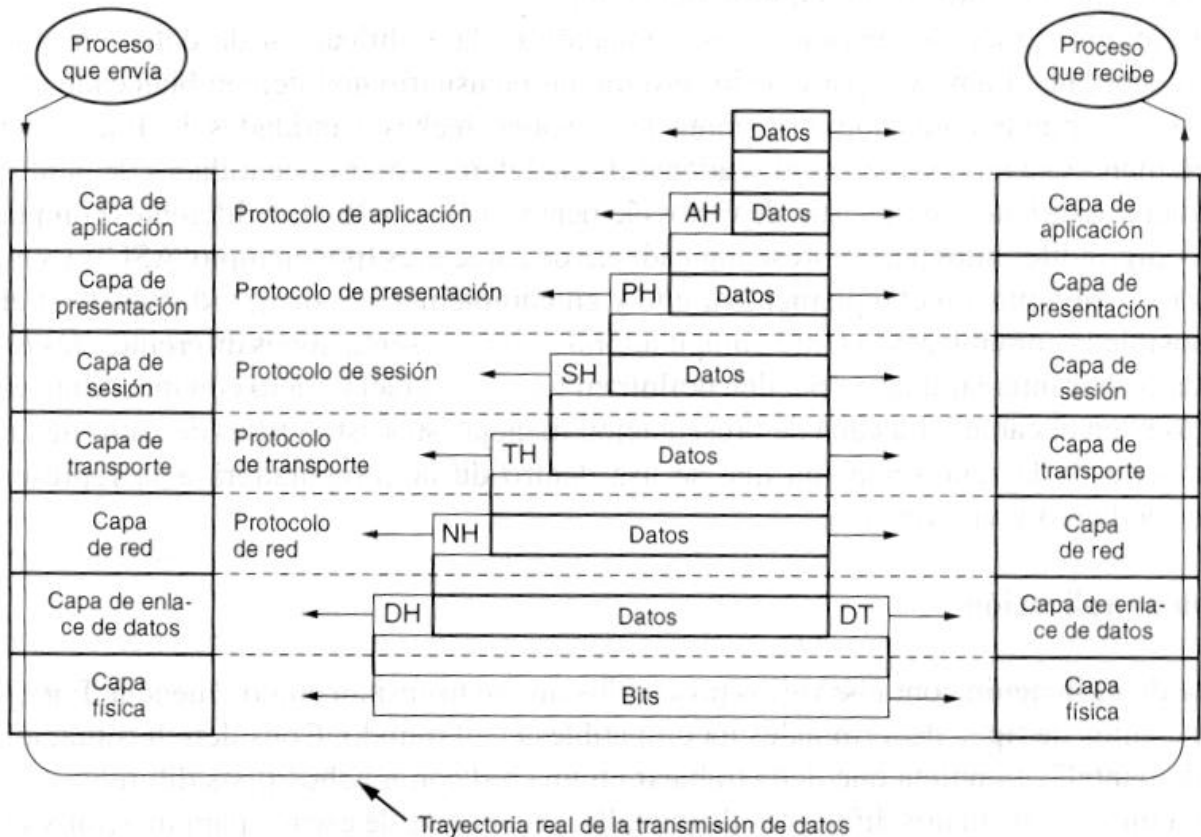


Figura 1.2. Funcionamiento del Modelo de Referencia OSI.

La capa de aplicación (7).

La capa de aplicación (Figura 1.3) es la más alta dentro del modelo de referencia OSI y está relacionada con los servicios que soportan directamente las aplicaciones de usuario, como software para la transferencia de archivos, acceso a bases de datos y correo electrónico. Este sirve como una ventana a través de la cual los procesos de las aplicaciones pueden acceder a los servicios de la red.

De esta forma, un mensaje enviado a través de la red entra por éste punto del modelo OSI, y sale por la capa de aplicación del equipo receptor.

Esta capa difiere de las demás debido a que no proporciona servicios a ninguna otra capa OSI, solamente a aplicaciones que se encuentran fuera del modelo OSI.

La mayoría de los usuarios se encuentra familiarizada con esta capa de aplicación. Pues algunas aplicaciones bien conocidas incluyen:

- Correo electrónico.
- Navegador Web.
- Procesador de textos.

La capa de presentación (6).

La capa de presentación (Figura 1.3) garantiza que la información enviada por la capa de aplicación de un sistema sea legible para la capa de aplicación del otro sistema. Si fuera necesario, la capa de presentación traduce entre múltiples formatos de datos utilizando un formato de representación de datos común.

La capa de presentación se ocupa no sólo del formato y representación de los datos de usuario, sino también de las estructuras de datos utilizados por las aplicaciones. Por tanto, además de la transformación de formatos de datos (si esto fuese necesario), la capa de presentación negocia la sintaxis de transferencia de datos para la capa de aplicación. De ésta manera, si se transmite una secuencia ASCII (conjunto codificado de caracteres con números) y el nodo que recibe los datos no dispone de ese sistema de codificación, en este nivel se realiza una conversión de datos de forma que puedan ser interpretados por el sistema receptor.

El nivel de presentación es responsable de la conversión de protocolos, la traducción de los datos, la encriptación de los datos, la modificación o conversión del conjunto de caracteres y la expansión de los comandos básicos. En esta capa se gestiona la compresión de datos para reducir el numero de bits para la transmisión.

La capa de sesión (5).

La capa de sesión (Figura 1.3) establece, administra y termina sesiones entre aplicaciones, las sesiones consisten en el diálogo entre dos o más entidades de presentación (recordemos que la capa de sesión proporciona sus servicios a la capa de presentación).

En el nivel de sesión se sincronizan las tareas de usuario colocando puntos de control en el flujo de datos. Los puntos de control dividen los datos en grupos más pequeños para la detección de errores. De ésta forma, si la red falla, sólo tienen que retransmitirse los datos posteriores al último punto de control. Este nivel

también implementa control de diálogo entre los procesos de comunicación como la regulación de que parte transmite, cómo, cuando y durante cuanto tiempo.

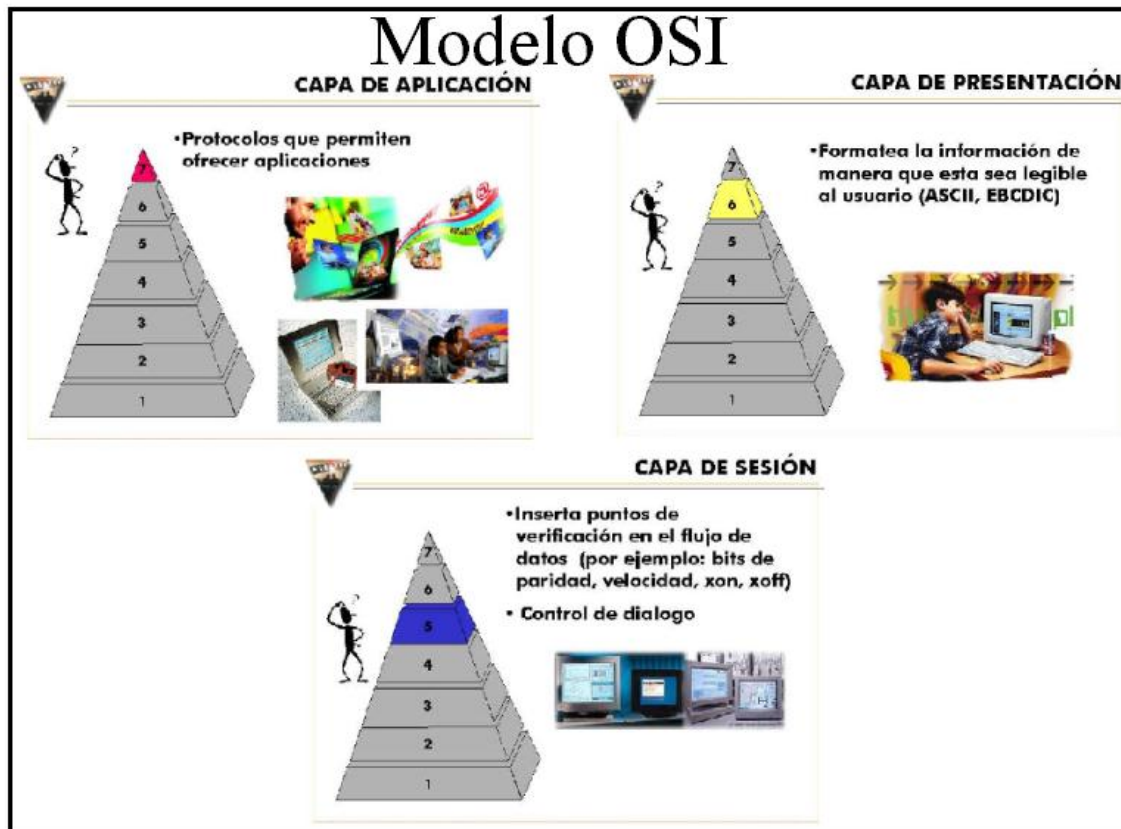


Figura 1.3 Capas 7, 6,5

Las capas siguientes se encargan de que los datos sean preparados, transportados y dirigidos desde un nodo a otro en la red.

La capa de transporte (4).

La capa de transporte (Figura 1.4) se encarga de asegurar el traslado de los datos de manera fiable. Esto se realiza mediante el control de flujo, verificación de errores, confirmación de extremo a extremo, la retransmisión y secuencia de dato. Su objetivo fundamental es la independización de los servicios ofrecidos a los usuarios (niveles superiores) de las características de los diferentes tipos de red (área local, extensa) subyacentes en los niveles inferiores.

La capa de red (3).

Esta capa (Figura 1.4) decide el camino por el cual se van a transmitir los datos, por tanto, debe ser capaz de reconocer la topología o configuración física de la red. La decisión puede ser estática, utilizando siempre la misma ruta o dinámica, adaptándose al estado de la red a partir de la información que recibe desde todos los nodos.

En éste nivel OSI la información o trama de datos recibe la denominación de paquetes, estos pueden ser de diferentes tamaños según el protocolo de red utilizado, por ejemplo el TCP/IP tiene un tamaño máximo de 64 KB.

La capa de enlace de datos (2).

En esta (Figura 1.4) capa los conjuntos de bits son encapsulados en tramas de datos, con una información adicional (origen y destino), con un control y corrección de errores en los datos que se desean transmitir, estableciendo un nivel donde se interconectan los diferentes nodos o estaciones que conforman la red.

La capa de enlace se divide en dos subcapas MAC (Media Access Control, Control de acceso a medios) y LLC (Logical Link Control, Control de enlace lógico).

La subcapa LLC: es la subcapa superior dentro de la capa de enlace y se encarga de la interconexión entre dos puntos de la red.

La subcapa MAC: controla el medio físico asegurando la comunicación entre la capa 1 y el resto.

La Capa Física (1).

La capa física (Figura 1.4) se ocupa de crear unos y ceros para su transmisión por un canal de comunicación. Se realiza una conversión de los bits de datos (unos y ceros) a pulsos eléctricos, señales ópticas, tonos de módem, etc. según sea el dispositivo que va realizar la transmisión de datos. Esta conversión de datos es requerida por la capa de enlace de datos de la maquina receptora.

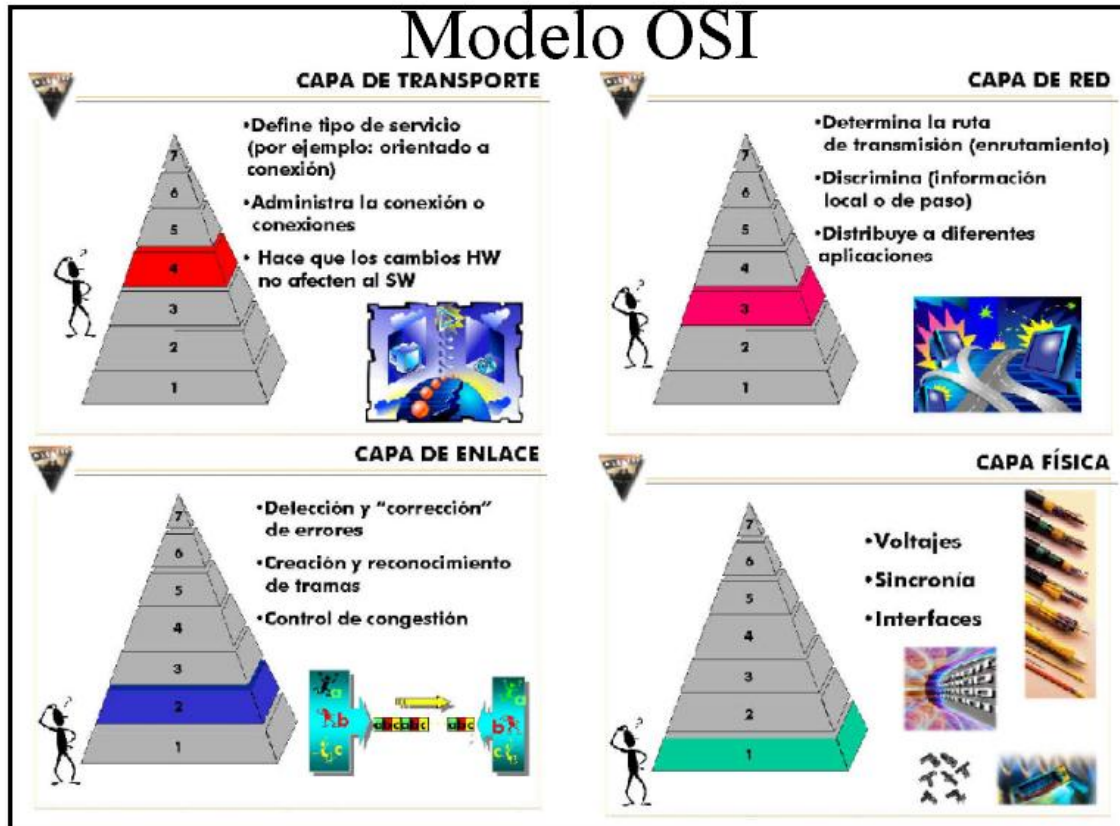


Figura 1.4 Capas 4, 3, 2 y 1

1.2 Tecnología de transmisión en redes

En términos generales, hay dos tipos de tecnologías de transmisión:

- Redes de Difusión (Broadcast).
- Redes Punto a Punto (Point to Point).

Redes de Difusión (Broadcast): Tienen un solo canal de comunicación compartido por todas las máquinas de la red.

Los mensajes o paquetes que genera una máquina son escuchados por todas las demás. Un campo de dirección dentro del mensaje o paquete especifica a quién se dirige y por lo tanto, quién debe de procesarlo.

Dentro del esquema de broadcast se puede considerar a dos divisiones:

El multicast y el Unicast.

- Multicast (Multidifusión): Una forma de Broadcast (Difusión) en el cual el paquete es liberado en base a un conjunto predefinido de posibles direcciones destino.
- Unicast (Unidifusión): En este caso un frame es enviado de una estación a otra. El Unicast contiene una dirección MAC específica de los dispositivos origen y destino.

Este tipo de redes determina la tecnología de transmisión en la conmutación de paquetes, por ejemplo Ethernet.

Las redes Punto a Punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino es posible que el paquete tenga que pasar por máquinas intermedias y que tenga que viajar por varias posibles rutas de diferente longitud, por lo que los algoritmos de ruteo desempeñan un papel importante en estos tipos de redes.

En el caso de las redes punto a punto se puede considerar que el ejemplo más común son las redes en base a la conmutación de circuitos, como lo son las redes telefónicas públicas.

Como regla general las redes pequeñas, geográficamente localizadas tienden a usar la difusión y las redes más grandes suelen ser punto a punto.

Principales características de las redes LAN

El propósito de una LAN es la de compartir recursos (HW y SW) con el fin de lograr los siguientes objetivos:

Mejorar la productividad,

Mejorar la administración de la información,

Mejorar la interacción entre el personal

Reducir y controlar costos

Estandarizar el uso de recursos HW y SW.

Podemos afirmar que una red de área local es efectiva si cumple con las siguientes características.

- Simplicidad
- Confiabilidad
- Transparencia
- Facilidad de administración.
- Por otro lado, una red de área local se caracteriza por:
- Medio de transmisión: el medio utilizado para la interconexión de los dispositivos (cable/inalámbrico)
- Topología: La apariencia física y/o la manera cómo operan los dispositivos interconectados mediante el medio de transmisión.
- Método de acceso al medio: El control de acceso al medio determina la forma en la cual los dispositivos de la red pueden acceder al medio de transmisión.
- Técnica de transmisión: La forma en la cual se envía la información sobre el medio de comunicación.

1.3 Topologías de Redes LAN

La topología de una LAN se determina por la forma como se utiliza el medio de transmisión para interconectar los diferentes dispositivos. Se debe tomar en cuenta que dentro del contexto de LAN, la palabra topología tiene dos acepciones. Las dos son importantes para el funcionamiento de la red. Estos dos significados son los siguientes:

Se refiere a la topología física de la LAN, a la apariencia física.

Topología también se refiere a cómo funciona la LAN. Esta es una topología lógica que describe cómo se transmiten los mensajes desde un dispositivo a otro.

Existen varios ejemplos en los que una LAN tiene una cierta apariencia física, pero lógicamente transmite sus mensajes en forma diferente. Por ello es necesario hacer una distinción entre la topología física y la topología lógica de una LAN.

Existen tres topologías principales:

- Estrella.
- Bus.
- Anillo.

Bus lineal

En una red en bus, en cualquier instante una computadora es la maestra y puede transmitir; se pide a las otras máquinas que se abstengan de enviar mensajes. Para esto es necesario un mecanismo de arbitraje para resolver conflictos cuando 2 o más máquinas quieren transmitir simultáneamente y se genera algo llamado Colisión. El mecanismo de arbitraje puede ser centralizado o distribuido, un ejemplo de un mecanismo centralizado es el utilizado por la IEEE 802.3, popularmente llamada Ethernet, cuando se detecta una colisión en el nodo de comunicación o conmutación, las terminales involucradas dejan de transmitir un tiempo al azar, transcurrido el cual lo intentan de nuevo.

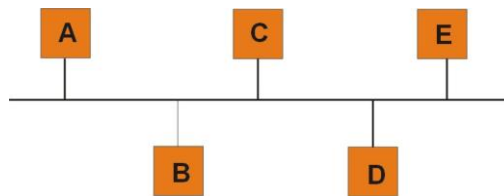
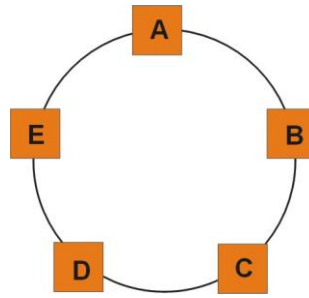


Fig.1.5

Anillo

Un segundo sistema de difusión es el anillo. En una topología de anillo, todos los dispositivos que conforman la red forman un círculo, conectándose sobre un solo canal de transmisión.

Cuando se envía un mensaje, éste viaja de dispositivo en dispositivo (alrededor del anillo) en una dirección predeterminada. Cada dispositivo entre el emisor y el receptor “escuchan” el mensaje. Si dicho dispositivo no es el receptor, retransmite el mensaje al siguiente dispositivo y así sucesivamente hasta que el mensaje llega al dispositivo destino.



Fin 1.6

Topología en estrella.

La topología en estrella es otra estructura ampliamente utilizada en sistemas de comunicación de datos. Todo el tráfico surge del centro de la estrella, como se observa en la figura 1.7

El nodo A, típicamente una computadora, controla completamente los equipos conectados a esta. Es responsable de encaminar el tráfico entre los demás componentes. También es responsable de ocuparse de los fallos. La localización de averías es relativamente simple en redes con topología tipo estrella, ya que es posible ir aislando líneas para identificar el problema.

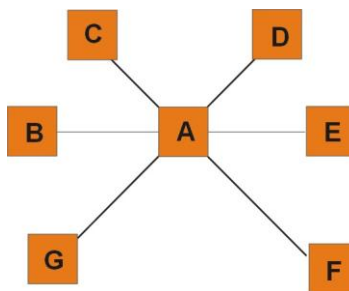


Fig. 1.7

1.4 Enlace de datos para internet: SLIP y PPP

Internet consiste en máquinas individuales (Hosts y enrutadores) y la infraestructura de comunicaciones que los conecta.

Dentro de un solo edificio las LAN se usan ampliamente para la interconexión, pero la mayor parte de la infraestructura de área amplia está construida a partir de líneas arrendadas punto a punto. Estas líneas las proporciona un proveedor de servicio de telecomunicaciones, por ejemplo Telmex.

En la Práctica, la comunicación punto a punto se utiliza principalmente en dos situaciones:

- Para interconectar LANs mediante una subred de Enrutadores que se conectan mediante líneas arrendadas punto a punto.
- La segunda situación, en Internet son los millones de usuarios que tienen conexiones caseras a Internet a través de módems y líneas telefónicas dedicadas.

Los usuarios de casa para poder establecer su conexión a Internet realizan una llamada al enrutador del proveedor de servicios de Internet (ISP) y entonces actúan como un Host de Internet con un enlace conmutado.

Tanto para la conexión por línea arrendada de enrutador a enrutador como para la conexión conmutada de Host a enrutador, se requiere de un protocolo punto a punto de enlace de datos en la línea para el manejo de tramas, control de errores y las demás funciones de la capa de enlace de datos, actualmente se manejan dos protocolos de este tipo.

SLIP

SLIP (Serial Line Internet Protocol) data de principios de los 80 y se diseñó como un método sencillo, aunque no muy potente, para conectar dos dispositivos IP a través de un cable serie. En el 84, se logró que SLIP funcionara bajo UNIX y en pocos años los usuarios empezaron a utilizar ampliamente el término SLIP por todo el mundo.

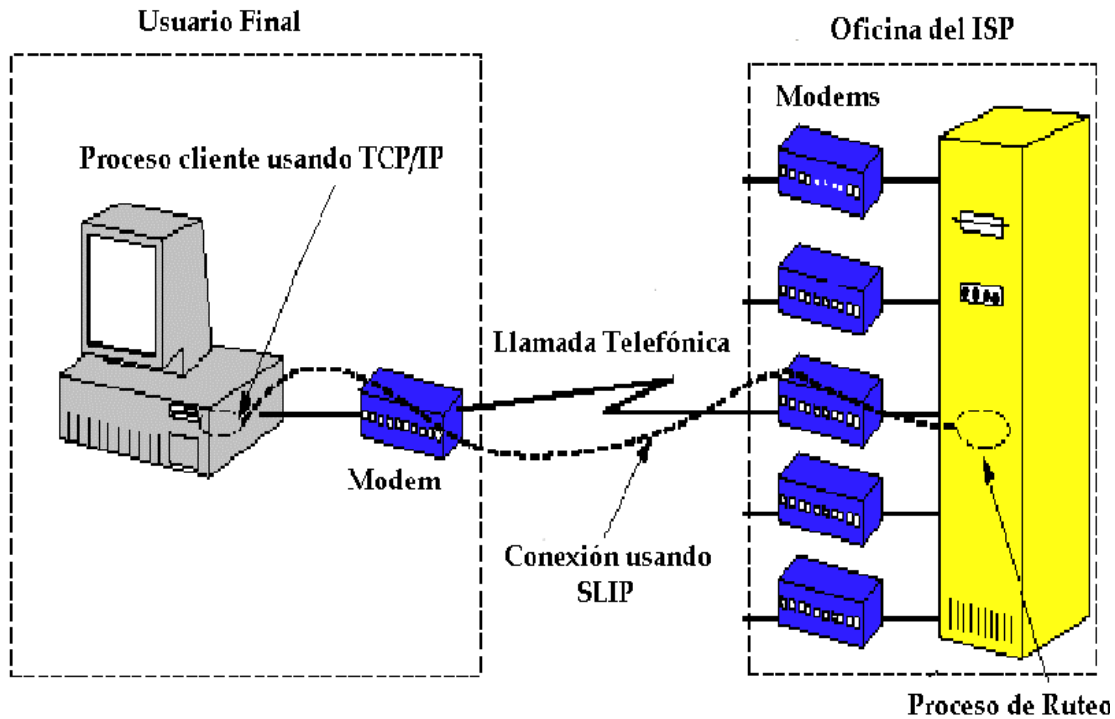


Fig.1.8 Protocolo slip.

A comienzos de los 90, cuando INTERNET empezó a crecer, muchos empezaron a utilizar SLIP para conectar computadoras a la Red, a través de una línea telefónica.

Esto suponía que se podía obtener una conexión real con Internet, incluso cuando la computadora no formara parte de una red local.

A finales de los 80, se observó que SLIP era insuficiente en algunos aspectos importantes, por lo que se creó un sustituto de **SLIP**, llamado **PPP**.

Aunque aún se utiliza ampliamente, SLIP tiene algunos problemas serios:

- SLIP no efectúa detección o corrección de errores, por lo que es responsabilidad de las capas superiores detectar y recuperar tramas perdidas.
- SLIP solo reconoce IP.
- Cada lado debe conocer por adelantado la dirección IP del otro, no hay asignación dinámica, esto es grave, pues es muy difícil darle a cada usuario una dirección IP única.

- SLIP no proporciona ninguna forma de verificación de autenticidad, por lo que ninguna parte sabe realmente con quién está hablando, si son líneas arrendadas no hay problema, pero si son de discado sí.
- SLIP no es un estándar aprobado de Internet. Para mejorar la situación han surgido varias versiones que solucionan uno u otro problema, pero actualmente se utiliza otro protocolo punto a punto.

PPP (Point to Point protocol) - protocolo punto a punto.

La siglas PPP, corresponden a Point to Point Protocol (protocolo punto a punto).

En noviembre de 1989, se propuso a PPP como estándar oficial de Internet. Aquí se describía las ventajas de PPP, sobre SLIP. PPP es mas potente (funciona con otros sistemas y no solo con TCP/IP), fiable, flexible y más fácil de configurar que SLIP a la hora de instalarlo y ponerlo a funcionar en un sistema nuevo".

Este protocolo fue generado por un grupo de estudio establecido por la IETF (Internet Engineering Task Force) subsidiaria de la IAB (Internet Activities/Architecture Board), y se define en el RFC 1661 y que se ha actualizado en las RFC 1662 y 1663.

El PPP realiza la detección de errores, reconoce múltiples protocolos, permite la negociación de direcciones en el momento de la conexión (asignación dinámica). Permite la verificación de autenticidad. PPP permite tres cosas:

- Un método de enmarcado que delinea sin ambigüedades el final de un marco y el inicio del siguiente. El formato de marco también maneja la detección de errores.
- Un protocolo de control de enlace para activar líneas, probarlas, negociar opciones y desactivarlas ordenadamente cuando ya no son necesarias. Este protocolo se llama LCP (Link Control Protocol, protocolo de control de enlace).

- Un mecanismo para negociar opciones de capa de red con independencia del protocolo de red usado. El método escogido consiste en tener un NCP (Network Control Protocol, protocolo de control de red). Distinta para cada etapa reconocida.

1.5 Estándares de IEEE.802

Estos estándares, conocidos en conjunto como el IEEE 802, incluyen las normas y reglas de operación de las redes de datos y su tecnología relacionada, tales como: CSMA/CD, token bus y token ring.

- Los diferentes estándares difieren en la capa física y en la Subcapa MAC, pero son compatibles en la capa de Enlace de datos.
- Los estándares IEEE 802 han sido adoptados por el ANSI y por la ISO (conocidos como ISO 8802).
- El estándar 802.1 es una introducción al grupo de estándares y define las primitivas de la interfaz. También es responsable de estándares de administración de LAN.
- El estándar 802.2 describe la parte superior de la capa de enlace de datos, que usa el protocolo LLC (Logical Link Control, control de enlace lógico).
- Las partes 802.3 a 802.5 describen los tres estándares para LAN, CSMA/CD, Token Bus y Token Ring, respectivamente.
- Cada estándar cubre la capa física y el protocolo de la subcapa MAC.

Ethernet /IEEE 802.3

Ethernet es el nombre de una de las redes de área local más populares hoy en día.

Inventada por Xerox a principios de los 70's. La versión a continuación descrita fue estandarizada por Xerox Corporation, Intel Corporation y Digital Equipment Corporation en 1978. IEEE sacó una versión compatible con la norma bajo el número 802.3.

La tecnología Ethernet consiste fundamentalmente en un cable coaxial llamado *ether* de aproximadamente media pulgada de diámetro y hasta 500

metros de longitud. Estos pueden ser extendidos por medio de dispositivos llamados repetidores que duplican señales eléctricas de un cable a otro.

Ethernet suele utilizarse para referirse a todas las LANs tipo "carrier sense multiple access/collision detection (CSMA/CD)" que suelen cumplir con las especificaciones Ethernet, incluyendo IEEE 802.3. Ethernet está bien adaptada a las aplicaciones en que el soporte de comunicaciones local a menudo tiene que procesar un elevado tráfico con puntas elevadas de intercambio de datos.

Sus principales características de operación son:

- Velocidad: 10Mbps
- Topología: Bus y estrella
- Método de acceso al medio: CSMA/CD
- Medios: Par trenzado, Coaxial y fibra.

Comparación Ethernet/IEEE 802.3

Las estaciones en una LAN CSMA/CD pueden acceder a la red en cualquier momento y, antes de enviar los datos, las estaciones CSMA/CD "escuchan" la red para ver si ya es operativa. Si lo está, la estación que desea transmitir espera. Si la red no está en uso, la estación transmite. Se produce una colisión cuando dos estaciones que escuchan el tráfico en la red no "oyen" nada y transmiten simultáneamente. En este caso, ambas transmisiones quedan desbaratadas y las estaciones deben transmitir de nuevo en otro momento.

Ambas LANs, Ethernet y IEEE 802.3 son redes de difusión, lo que significa que todas las estaciones ven todos los paquetes, sin tener en cuenta si representan un destino determinado. Cada estación debe examinar los paquetes recibidos para determinar si la estación es un destino.

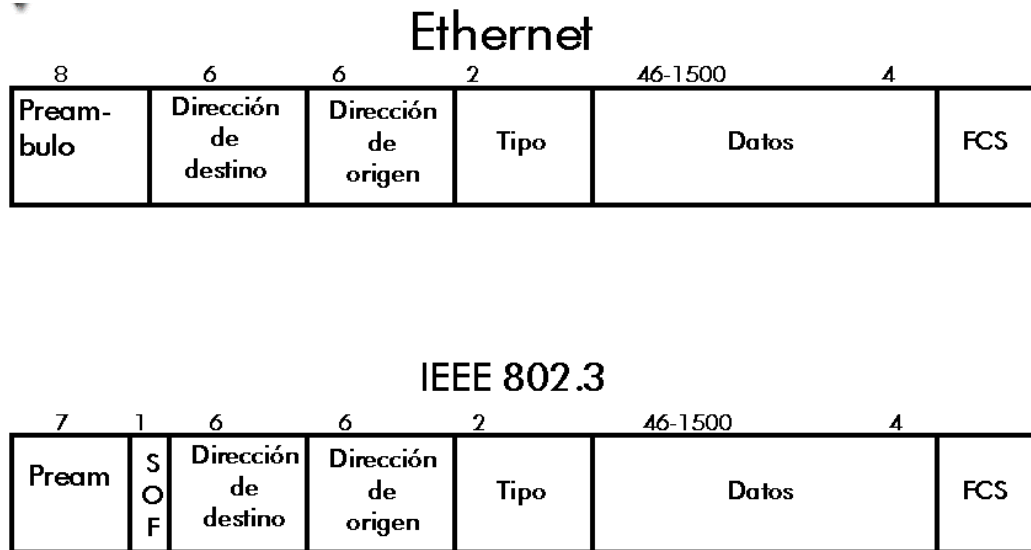
En este caso, el paquete se pasa a una capa de protocolo superior para su procesamiento adecuado. Las diferencias entre LANs Ethernet y IEEE 802.3 son sutiles. Ethernet proporciona servicios correspondientes a las capas 1 y 2 del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física (Capa 1) y la parte de acceso-canal de la capa de enlace (Capa 2), pero no define

un protocolo de control de enlace lógico. Así como el resto de funciones de las capas 1 y 2, tanto Ethernet como IEEE 802.3 están implementadas en hardware, en general a través de una tarjeta de interfaz en un ordenador o a través de una tarjeta principal en la propia computadora.

CSMA/CD

A continuación describiremos el proceso de cómo trabaja este protocolo:

- Cuando la interfaz del servidor tiene un paquete para transmitir, escucha al ether para determinar si hay mensajes siendo transmitidos.
- Si no detecta transmisión alguna, la interfaz comienza a enviar.
- Cada transmisión está limitada en el tiempo, pues existe un tamaño máximo de paquete. Cuando un nodo comienza a transmitir, la señal no llega a cada punto de la red simultáneamente, a pesar de que viaja a casi un 80% de la velocidad de la luz.
- Por lo anterior, es posible que 2 nodos determinen que la red está ociosa y comiencen a transmitir al mismo tiempo; provocando la colisión de las dos señales.
- Detección de Colisiones (CD): Cada nodo monitorea el cable mientras está transfiriendo para verificar que una señal externa no interfiera con la suya.
- Cuando una colisión es detectada, la interfaz aborta la transmisión y espera hasta que la actividad cese antes de volver a intentar la transmisión.
- Política de retención exponencial. El emisor espera un tiempo aleatorio después de la primera colisión; un periodo de espera 2 veces más largo que el primero en caso de una segunda colisión; 4 veces más largo la próxima vez, etc., reduciendo así al máximo la probabilidad de colisión.



SOF = Delimitador del inicio de trama
 FCS = Secuencia de verificación de la trama

Fig. 1.9 Protocolo MAC del estándar IEEE 802.3 y ethernet.

1.6 Medios de comunicación

La configuración física para el cableado de interconexión de terminales es de tipo bus compartido y dependiendo del tipo de sistema serán las normas a seguir en la Implantación de la arquitectura de la red.

Como ya se mencionó anteriormente la norma 802.3 especifica una familia completa de sistemas de cableado.

Entre las cuales se encuentran:

10 base 5

- También llamado Ethernet de cable coaxial grueso (Thick Ethernet) que usa un cable especial "amarillo" de 50 ohms de impedancia en una estructura de bus. Con una desventaja, si el coaxial es interrumpido en cualquier lugar, la red entera se caerá.
- Se requiere un tranciver para la traducción de señales entre el bus y la tarjeta adaptadora de red a través de un cable AUI (Attachment Unit Interface: Interfaz de Unidad de Conexión).
- El bus debe ser terminado en ambos extremos con una resistencia de 50 ohms

- Utiliza un conector N sobre el coaxial (vampiro)
- Los segmentos de cable no deben de exceder de 500 m de longitud
- Habrá mínimo 2.5 m entre cada tranciever
- Máximo 100 usuarios por segmento
- Velocidad en el bus de 10 Mbps
- Se usa en backbone de alta velocidad

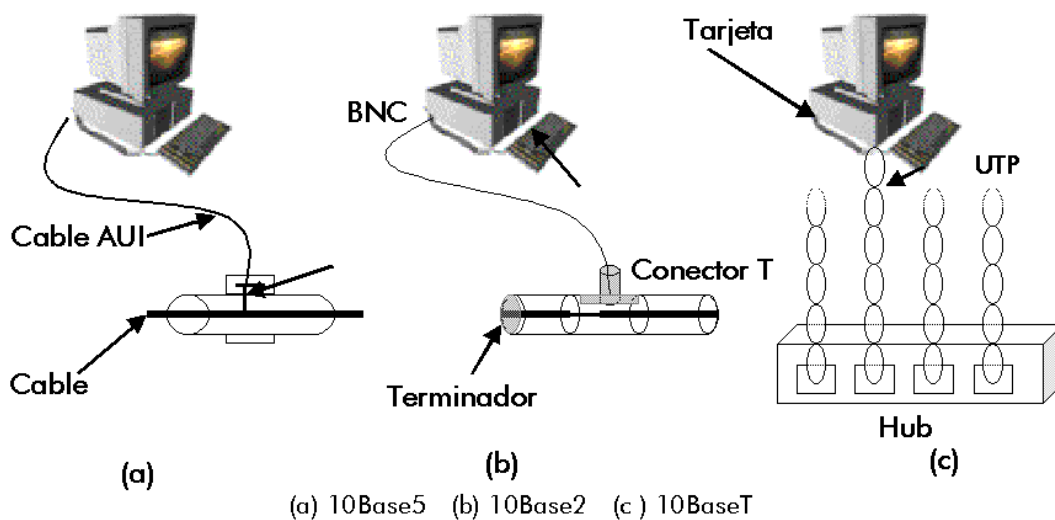


Fig. 1.10 Diferentes normas para IEEE 802.3

10 base 2

- También llamado Ethernet delgado (Thin Ethernet) usa un cable coaxial delgado (RG58) con una impedancia de 50 ohms.
- Se instala en una estructura de bus.
- El tranciever o traductor está incluido en la tarjeta adaptadora de red.
- El bus debe tener un terminador en ambos extremos con resistencia de 50 ohms.
- Usa conectores BNC.
- Segmentos de cable máximo de 185 m.

- Deberá haber al menos 0.5 m entre dos T's.
- Máximo 30 usuarios por segmentos.
- Velocidad en el bus hasta de 10 Mbps.

10 Base T

Es la versión en par trenzado de Ethernet, este puede ser UTP (Unshielded Twisted Pair), FTP (Foiled Twisted Pair) o STP (Shielded Twisted Pair). 10BaseT solo usa los pares dos y tres.

- La red se implementa en una topología en estrella en donde el Hub es el centro.
- Un Hub es un repetidor multipuerto o un concentrador de cableado. 10BaseT tiene físicamente una topología en estrella la cual es convertida a una estructura de bus Ethernet dentro del Hub.
- Usa un conector estandarizado RJ45 de 8 hilos.
- Hasta 100m entre el Hub y la terminal.
- Hasta 1,24 nodos por segmento.

10 BASE FL

- También conocido como el estándar FOIRL (Fiber Optic Inter Repeater Link) o Ethernet sobre fibra óptica.
- Normalmente usa fibras de 50/125 y 62.5/125 micrómetros de diámetro
- Es un enlace dual de fibras (transmisión y recepción)
- Es comúnmente usado para soportar Columnas Dorsales (Backbone) .
- Configuración en estrella igual que 10BaseT
- El Hub consiste de un acoplador pasivo en estrella y retransmite todas las señales recibidas de las fibras ópticas a todos los puertos, para de esta manera formar un segmento simple de fibra óptica.
- El término Base para todos los casos anteriores, viene de BaseBand que significa que una señal se transmite en su forma original y no modificada por algún proceso de modulación, es decir, que los datos de una computadora se envían en forma digital.

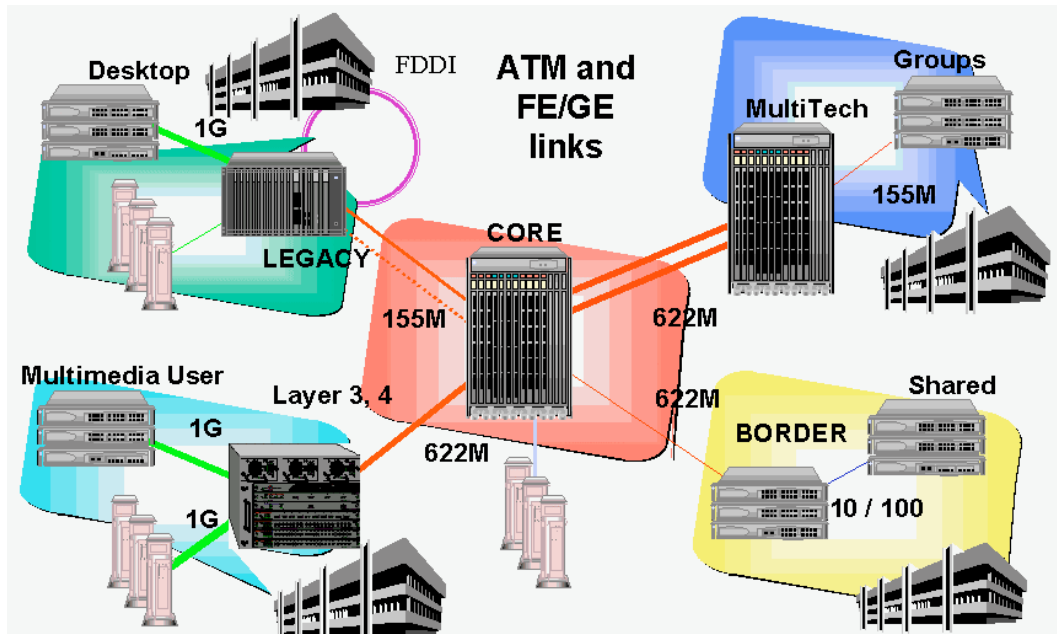


Fig. 1.11 Switches

Giga Ethernet

Una alternativa, para satisfacer este crecimiento en las redes, es usar la tecnología Gigabit Ethernet.

Avances recientes en la tecnología de semiconductores han permitido que el protocolo Ethernet proporcione un mejor desempeño. Gigabit Ethernet es un concepto bastante simple que toma como base la velocidad de 100 Mbps de Fast Ethernet y multiplica a esta por 10, obteniendo un ancho de banda de 1000 Mbps.

Existen dos principales ventajas que proporciona Gigabit Ethernet:

- Administradores de red, técnicos e ingenieros de soporte, ya conocen como trabaja Ethernet. Esto reduce los costos de capacitación y permite que una organización migre a esta nueva tecnología de forma transparente para el usuario.
- Es mucho más sencillo trasladar puertos Ethernet corriendo a diferentes velocidades en un switch, esto permite llevar a cabo una migración de tecnología más sencilla.

La capa física de Gigabit Ethernet.

Gigabit Ethernet está definido por las especificaciones del estándar IEEE 802.3z. Gigabit Ethernet define para la capa física el uso de fibra óptica y par de cobre, existe otra especificación llamada Canal de Fibra que permite aumentar la forma de transmisión en menor tiempo. Las opciones de cableado que utiliza Gigabit Ethernet son:

- Fibra óptica multimodo (1000BaseSx y 1000BaseLx). Sx utiliza una frecuencia de 850 nm y LX usa 1330 nm. Un cable de 62.5 micras cubre un máximo de 300 metros (en la especificación SX) o 500 metros (en la especificación LX). Un cable de 50 micras cubre una distancia de 550 metros (para las dos especificaciones SX y LX). La fibra óptica cuenta con ventajas como la inmunidad a interferencias eléctricas, siendo ideal para ambientes propensos a ruidos altos.
- Debido a que muchas empresas cuentan con instalaciones de cableado multimodo, este sea probablemente el estándar a usar.
- Fibra óptica monomodo (1000BaseLx). La máxima distancia que soporta Gigabit Ethernet es de 3000 metros haciendo uso de este tipo de cable. El incremento de la distancia sobre el soporte de la fibra óptica multimodo es la baja dispersión.

Gigabit ethernet y la calidad de servicio (QoS)

Existe un continuo debate en la industria de las redes sobre la calidad de servicio (QoS) y Gigabit Ethernet.

Actualmente el estándar de Gigabit Ethernet no contiene explícitamente el soporte de QoS. Algunos discuten que proporciona ancho de banda suficiente, que permite liberar paquetes a velocidades máximas. Este simple argumento tiene sus méritos; el tamaño variable de los paquetes, congestión en la red y la necesidad de controlar variaciones en el retardo. Sea o no válido este argumento el ancho de banda que soporta GE ciertamente ayuda en la liberación de la QoS.

Algunos proveedores han decidido implementar estándares que realicen priorización de colas y otros mecanismos.

Muy pronto tendremos una larga lista de técnicas que nos permitirán clarificar que

técnicas usar en cada aplicación.

Dentro del desarrollo de protocolos que permiten asignar calidad de servicio en redes transmisión de paquetes, se encuentran 802.1p, 802.1q y RSVP.

- 802.1P es un estándar de la IEEE que prioriza tráfico en tiempo crítico y filtra tráfico multicast para asegurar que este no se propagara en la capa 2 de las redes conmutadas. El encabezado del 802.1p incluye un campo de 3 bits para priorización, permitiendo establecer 8 prioridades sobre la red. La reciente ratificación de 802.1p como parte de una nueva revisión del estándar, ha proporcionado a la conmutación LAN el soporte de la convergencia en tráfico de voz, datos y vídeo. 802.1p es una especificación para dar la capacidad de priorización de tráfico y filtro dinámico multicast a switches de capa.
- 802.1q es un protocolo de etiquetado a nivel de VLANs, definido por la IEEE. Este protocolo requiere multiplexar VLANs sobre los enlaces físicos. El encabezado de 802.1q también incluye un campo para priorización, que permite establecer prioridades en la red. La especificación 802.1q define una etiqueta de cabecera de 32 bits, todos insertados después del encabezado normal del paquete (donde se encuentra la dirección origen y destino). Los bits de prioridad de 802.1q pueden establecerse vía enrutadores, servidores, estaciones de trabajo o incluso switches de capa 2. En estaciones de trabajo y servidores, 802.1p es compatible con tarjetas de red (NICs) que establecen los bits vía puerto de monitoreo e identificadores de sockets para determinar las prioridades de tráfico.
- RSVP (Resource Reservation Protocol). RSVP y sus protocolos asociados como RTP (Real Time Protocol) y
- RTCP (Real Time Control Protocol), son usados para solicitar requerimientos de Calidad de Servicio (QoS) a través de una red

basada en Frames. RSVP es un estándar de Internet y ha estado implementado en muchos dispositivos de red. Este será gradualmente aplicado en estaciones de trabajo, permitiendo a usuarios y aplicaciones hacer una solicitud de QoS en redes IP.

1.7 Cableado estructurado: el concepto.

Un sistema de cableado estructurado consiste de una infraestructura flexible de cables que puede aceptar y soportar múltiples sistemas de comunicación de voz, datos y vídeo, independientemente de quién fabricó los componentes del mismo. Esta disposición permite la comunicación virtualmente de cualquier dispositivo, en cualquier lugar y en cualquier momento. Un plan de cableado bien diseñado puede incluir distintas implantaciones de cableado interdependiente, utilizando diferentes tipos de medios que son instalados de manera tal que se cubre los requerimientos de funcionamiento del sistema.

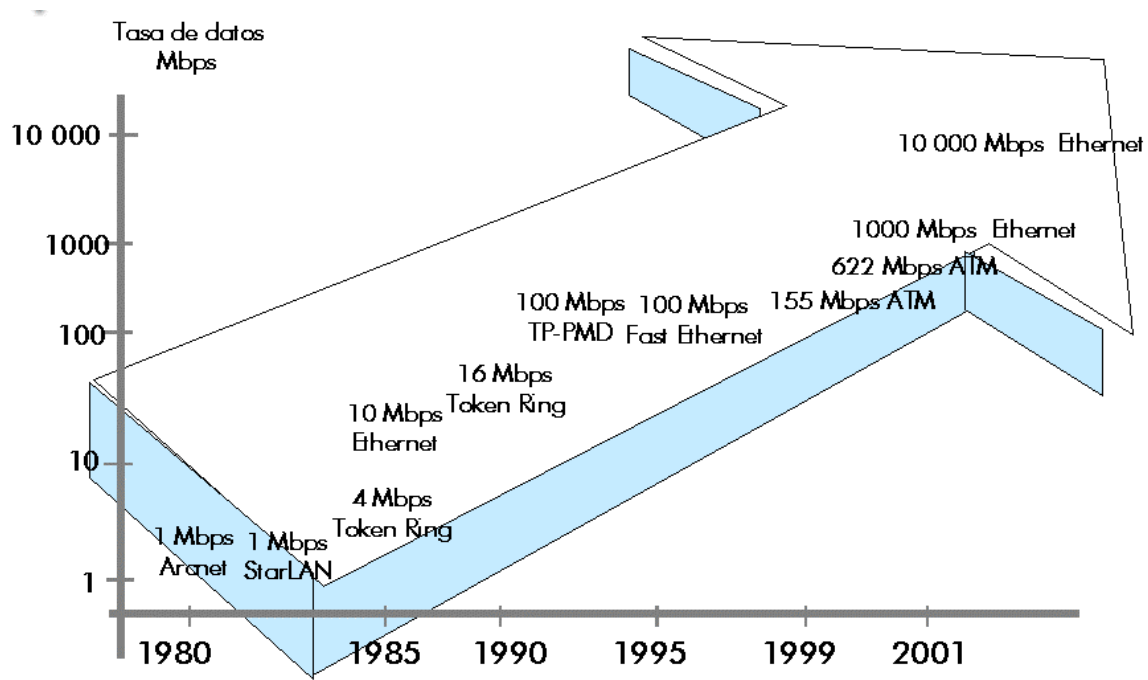


Fig. 1.12 Evolución de la tecnología

Evolución de los sistemas de cableado.

Diez años atrás, el único cable utilizado en los sistemas de cableado de edificios, era el cable tipo POTS (Plain Old Telephone System), o cable regular para teléfono, instalado por la compañía de teléfonos local. El conjunto de cables POTS era capaz de manejar comunicaciones de voz, pero para poder apoyar las comunicaciones de datos, se tenía que instalar un segundo sistema privado de cables.

Los sistemas privados independientes eran aceptables, sin embargo, el mercado actual requiere ser capaz de proveer comunicaciones de voz, vídeo y datos por medio de un sistema de cableado universal, esto origino que algunos organismos de la industria electrónica y de telecomunicaciones (EIA/TIA) tomaran cartas en el asunto.

100 Mbps x factor de conversión = ??? MHz

LA CODIFICACION ES UNA APLICACION DEPENDIENTE DE LA NECESIDAD

	Velocidad	Frecuencia	Código
Token Ring	4 Mbps	⇒ 4 MHz	(Manchester)
Ethernet	10 Mbps	⇒ 10 MHz	(Manchester)
Token Ring	16 Mbps	⇒ 16 MHz	(Manchester)
TP-PMD	100 Mbps	⇒ 62,5 MHz ⇒ 31,25 MHz	(NRZI + 4B5B) (MLT-3 + 4B5B)
ATM	155 Mbps	⇒ 78 MHz	(NRZ)
1000BASE-TX	1000 Mbps	⇒ 125 MHz	(PAM-5)

Fig.1.13 Aspectos técnicos del cableado.

Dichos organismos propusieron que los sistemas de cableado se adecuaran a una estructura para proveer la plataforma ó base sobre la que se construyese una estrategia general de los sistemas de información y voz y que evolucionara constantemente sin grandes costos de inversión.

A pesar de que estos sistemas ayudaron a definir las pautas relacionadas con el cableado, no fue sino hasta que se presento el anteproyecto de norma SP 1907B

y después la publicación de la norma sobre tendido de cables en edificios ANSI/EIA/TIA-568 en 1991, que estuvieron disponibles las especificaciones completas para guiar en la selección e instalación de los sistemas de cableado.



Fig. 1.14 Organismos reguladores internacionales.

Estándar TIA/EIA 568.

A principios de 1985, las compañías representantes de la industria de telecomunicaciones y computación se preocupaban por la falta de un estándar para sistemas de cableado de un edificio de telecomunicaciones.

La Asociación de la Industria de Comunicaciones Computacionales (CCIA) solicitó que la Asociación de Industrias Electrónicas (EIA) desarrollara este modelo necesario. En julio de 1991 se publicó la primera versión del estándar como EIA/TIA-568. En agosto del mismo año se publicó un Boletín de Sistemas Técnicos TSB-36 con especificaciones para sistemas de cableado con mayor capacidad de ancho de banda (Categoría 4 y Categoría 5) en sistemas con cable UTP.

En agosto de 1992 el Technical System Bulletin 40 (TSB-40) fue publicado, enfocándose a elementos de conectividad para cable UTP con mayor ancho de banda.

En Enero de 1994 el TSB-40 fue corregido por el TSB-40A que trataba, más detalladamente, sobre implantaciones de conexión provisional con cable UTP y esclarecía los requerimientos de prueba de los conductores hembra modulares UTP.

El estándar 568 fue corregido por el TIA/EIA 568-A. El TSB- 36 y el TSB-40A fueron absorbidos en el contenido de este estándar revisado, junto con otras modificaciones.

Propósitos del estándar TIA/EIA 568-A.

- Establecer un cableado estándar genérico de telecomunicaciones que respalde un ambiente multiproveedor.
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución técnico para varias configuraciones de sistemas de cableado.
- Actualmente ISO está desarrollando un cableado estándar sobre una base internacional, con el título: Cableado Genérico para Cableado de Establecimientos Comerciales bajo la norma ISO/IEC1. El documento equivalente para Canadá es el CSA T529

Campo del estándar TIA/EIA 568-A.

El estándar especifica:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina, campus corporativo.
- Topología y distancias recomendadas.
- Parámetros de medios de comunicación que determinan el rendimiento.
- Disposiciones de conexión y sujeción para asegurar la interconexión.
- La vida productiva de los sistemas de telecomunicaciones por cable por más de 10 años.

Categorías de Cableado

Es la especificación que se da a un elemento del sistema de cableado que ha sido probado bajo la norma dictada por la EIA/TIA a un ancho de banda y distancia determinados y los resultados han sido satisfactorios.

Categoría 3 o clase c.

Cables/conectores de equipo con parámetros de transmisión caracterizados hasta 16 MHz.

Categoría 4 o clase d.

- Todos los componentes son probados para un funcionamiento eléctrico de hasta 20 Mhz.
- Buena separación diafónica.
- Acomoda aplicaciones Token Ring/Ethernet.

Categoría 5 o clase e.

Cables/conectores de equipo con parámetros de transmisión caracterizados hasta 100 Mhz.

- Sistema UTP disponible en la actualidad.
- Acomoda aplicaciones como ATM y Fast Ethernet.

Categoría 6 o clase f.

Cables/conectores de equipo con parámetros de transmisión caracterizados hasta 200 Mhz.

- Sistema UTP de mejor rendimiento disponible en la actualidad.
- Acomoda todas las aplicaciones como ATM y Giga Ethernet.

1.8 Elementos del Cableado Estructurado.

Cable par trenzado sin blindar (UTP).

Es un cable compuesto de 8 hilos de cobre forrados individualmente por una cubierta plástica que es de un color diferente para cada cable, estos pares se encuentran forrados por una cubierta plástica que forma en si el cable, cada par esta trenzado para evitar los ruidos la emisión y recepción de interferencia electromagnética, la relación de torque de cada par es diferente, así la señal de cada par no se interfiere con la de otros pares dentro del mismo cable.

FTP (Foil Screen Twisted Pair).

Par trenzado con doble forro metálico para una eficiencia de protección electromagnética mejorada Forro externo de PVC, impedancia de 100 Ohms.

Todos los componentes son probados para un funcionamiento eléctrico de hasta 300Mhz. Adecuado para aplicaciones de multimedia (simultáneamente vídeo y datos) y aplicaciones para datos superiores a 100 Mbps o ambientes industriales ruidosos.

STP (Shielded Twisted Pair).

Par trenzado con forro metálico por cada par separado, forro externo de PVC, impedancia de 150 Ohms, sus componentes son probados para un funcionamiento eléctrico de hasta 350Mhz. Adecuado para aplicaciones de multimedia (simultáneamente vídeo y datos) y aplicaciones para datos superiores a 100 Mbps o ambientes industriales ruidosos.

Cable multipar.

Cable compuesto de múltiples hilos forrados individualmente dentro un tubo plástico, cada par viene trenzado individualmente y existen cables desde 25 pares de capacidad hasta 4000 pares. Es ampliamente usado en enlaces principales de redes de voz para interconexión de cuartos de comunicaciones donde las relaciones costo/beneficio son adecuadas con respecto a otros tipos de cable u otro tipo de soluciones.

Cable De Fibra Óptica.

La fibra óptica es un filamento de vidrio de alta pureza y diámetro microscópico (8, 50 y 62.5 micras), está cubierto por un material de diferente densidad (con

diámetro estándar de 125 micras) para fines de operación, y tiene un forro plástico que le da protección física, las fibras no se arman en cables por separado, se constituyen en cables 6, 12, 24 y 48 fibras, cada cable cumple con especificaciones de protección mecánica para interiores o exteriores dependiendo de la aplicación, las hay Unimodo y Multimodo, esa última especificación es en base a la forma en que transportan la señal óptica.

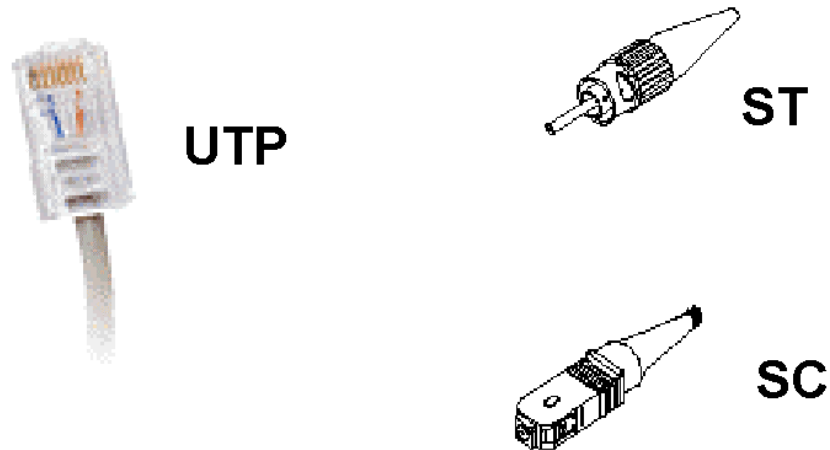


Fig. 1.15 Conectores para cobre y fibra.

Conectores RJ45.

Son dispositivos plásticos de forma rectangular que cuentan con 8 dientes en la parte superior, por la parte posterior tienen una lengüeta plástica que funciona como seguro mecánico al introducirlos en una roseta que es su elemento complementario, su uso está muy extendido en el terminado de cables para diversos sistemas de comunicaciones.

Conectores ST.

Son elementos de conectorización para fibras ópticas, son los primeros conectores que se usaron en sistemas de fibra óptica, conducen la fibra por el centro del cuerpo del conector a través de la férula que está hecha de un material llamado zirconia, sus especificaciones físicas le dan cierta resistencia mecánica y firmeza en la conexión

Conectores SC

Surgieron después de los ST, su principio de operación es el mismo, sin embargo

las características físicas del conector en si le dan más resistencia mecánica y permiten el fácil reconocimiento de las líneas de TX y RX dado que solo encajan en su complemento en una sola posición, a diferencia de los ST. Son ampliamente usados.

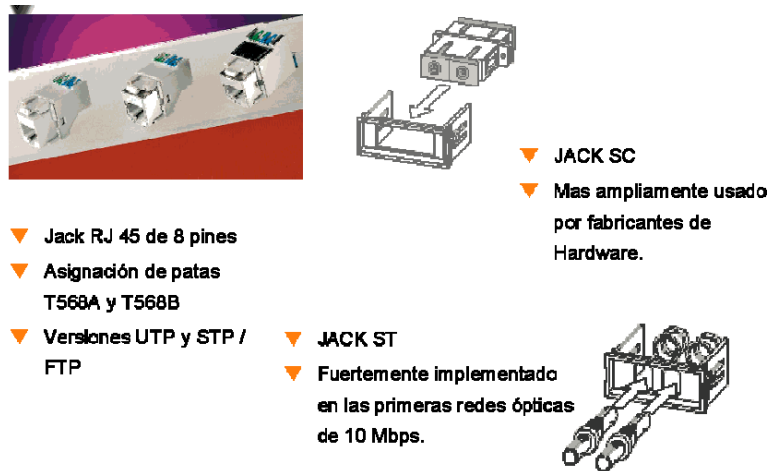


Fig. 1. 16 Jacks para cobre y fibra óptica.



Fig. 1. 17 Cables de parcheo.

Cables de parcheo UTP

Son segmentos de cable con conectores RJ45 en ambos extremos.

Se usan para conectar los equipos y servidores a las rosetas que se instalan en los lugares del usuario, así también se usa para interconectar los equipos activos de la red a los servicios del sistema de cableado.

Los hay en versiones UTP / STP / FTP.

Cables de parcheo de fibra óptica.

Se usan para interconectar los equipos activos a los servicios de cableado de fibra óptica, también se usan para hacer puentes entre los servicios de fibra con la finalidad de hacer configuraciones de conexión especiales, también se usan para interconectar servidores o estaciones de trabajo de alta capacidad que dispongan de un puerto de red de fibra óptica hacia el sistema de cableado.



Fig. 1.18 Panel de parcheo de F.O

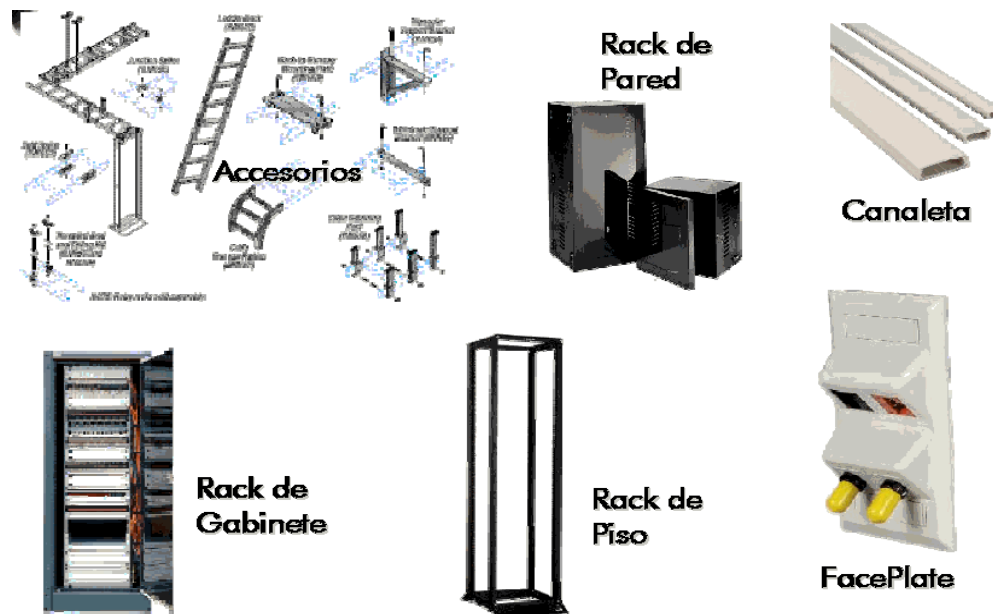


Fig. 1.19 Elementos de cableado estructurado.

Racks o bastidores.

Son estructuras metálicas que se usan para la fijación de los sistemas de cableado en los sitios donde existe equipo de comunicaciones o elementos de conexión de cableado, existen para montura en piso de altura completa (7 pies), de media altura (4 pies) tipo gabinete, para montura en pared etc. Su ancho es de 19 pulgadas como estándar aunque existen versiones de algunos fabricantes en 24 pulgadas. Están hechos de aluminio o de acero de alta resistencia.

Canaletas.

Son elementos plásticos que se usan para llevar líneas de cableado por lugares donde el cable no puede ocultarse, hay de diversas medidas y acabados estéticos, también existen diferentes elementos para su acoplamiento como son esquinas cruces y elementos "T" para adaptarse a todas los escenarios posibles, se fijan a pisos techos y paredes a través de adhesivos o tornillos.

Escalerillas.

Son elementos metálicos (aluminio o acero inoxidable) que se usan para transportar cantidades de cables hacia sus destinos por las diferentes trayectorias

del sistema de cableado, se fijan a pisos techos y paredes por medio de birlos que se atornillan anclas incrustadas en barrenos, se usan en lugares no visibles como plafones y pisos falsos.

Face Plates.

Son elementos plásticos que se usan para fijar las terminaciones de los cables en las áreas de trabajo del usuario, permiten una apariencia estética y pueden soportar múltiples combinaciones de diversos tipos de cable según se requiera, algunos modelos permiten etiquetación para su administración posterior.

1.9 Consideraciones en el Diseño de Sistemas de Cableado Estructurado

Identificación de necesidades.

- Requerimientos de funcionamiento y de ancho de banda.
- Aplicaciones en redes respaldadas.
- Costo durante la vida útil.
- Características del producto.

Estos puntos son importantes porque contemplan varios aspectos relacionados con la especificación, compra, y mantenimiento de un sistema de cableado.

Recuerde estas preguntas ANTES de iniciar un proyecto de cableado:

- ¿Cuánto tiempo va a permanecer el sistema en uso?
- ¿Qué demandas de funcionamiento y de aplicación se le impondrán al sistema?
- ¿Migrará el sistema hacia aplicaciones más exigentes tales como CAD/CAM, ATM (Asynchronous Transfer Mode), Gigabit Ethernet, reproducción de imágenes o multimedia?
- ¿Existen requerimientos físicos especiales en el proyecto que deberán ser considerados?
- ¿Qué tipo de apoyo es necesario para el producto y el diseño?

Los Seis Subsistemas del Sistema de Cableado Estructurado.

Acometida de edificio

La instalación de entrada del edificio da el punto en donde el cableado exterior entra en contacto con el cableado central interior del edificio. Los requerimientos físicos del contacto de la red son definidos en el Estándar EIA/TIA-569.

Sala de equipo

Los aspectos de diseño de la sala de equipo se especifican en el estándar EIA/TIA-569. Las salas de equipo, generalmente alojan componentes de mayor complejidad que los gabinetes de telecomunicación. Cualquiera o todas las funciones de un cuarto de telecomunicaciones pueden estar disponibles en una sala de equipo.

Cableado backbone

El cableado central provee la interconexión de telecomunicaciones, salas de equipo e instalaciones de entrada. Consiste en los cables centrales, interconexiones intermedias y principales, terminaciones mecánicas y cables de parcheo o puentes, utilizados para interconexiones de central a central.

Cuarto de telecomunicaciones

Un armario de telecomunicaciones es el área de un edificio que aloja el equipo del sistema de cableado de telecomunicaciones. Este incluye las terminaciones mecánicas y/o interconexiones para el sistema de cableado central y horizontal. El estándar EIA/TIA-569 indica las especificaciones de diseño del armario de telecomunicaciones

Cableado horizontal

El sistema de cableado horizontal se extiende desde la toma de corriente de telecomunicaciones (información) del área de trabajo hasta el armario de telecomunicaciones y consiste en lo siguiente:

Área de trabajo

Los componentes del área de trabajo se extienden desde la salida de información hasta el equipo de estación. El cableado del área de trabajo está diseñado de manera que sea sencillo el interconectarse, para que los cambios, aumentos y movimientos se puedan manejar fácilmente.

Ambientes de cableado.

Para un diseño eficiente, se consideran 3 ambientes de aplicación, aunque la norma aplica para oficinas comerciales, las consideraciones presentadas en estos escenarios aplican para ambientes domésticos, hoteles etc... Los ambientes de aplicación son:

- Cableado de Oficina.
- Cableado de Edificio Corporativo.
- Cableado de Campus.

1.10 Recomendaciones para diseño de sistemas de cableado horizontal.**Topología:**

- La distribución topológica del cableado horizontal siempre será en estrella o en estrella de estrellas.
- Solo se permite un nivel jerárquico por debajo del Backbone de fibra óptica.
- Las corridas de cable deben ser completas hasta el área de trabajo desde el closet de telecomunicaciones los empalmes en cable de cobre no están contemplados dentro de la norma.
- No está permitido derivar un closet de otro closet a menos que se trate de un punto de interconexión de paso, en el caso de cobre el cable no debe seccionarse.
- En caso de manejar zonas abiertas se permite el uso de puntos de consolidación para menos de 8 nodos.

Evitando interferencias electromagnéticas (EMI)

Evitar orígenes potenciales de EMI debe ser una consideración primaria cuando se instalan las guías para las corridas horizontales, para evitar EMI, todas las guías deberán tener un margen de por lo menos:

- 1.2m de motores o transformadores
- 0.3m de cable sin protección usada para electricidad.
- 1.2m de luces fluorescentes.
- Los cruces con cables de energía solo se permite en forma perpendicular a 90 grados.

Longitud del cableado.

Las longitudes máximas para la distribución de cables en oficina son:

- En cableado horizontal hasta el faceplate: 90m.
- Cables de parcheo en el closet horizontal: 6m.
- Cables de parcheo en área de trabajo: 3m

Para los límites establecidos en la longitud de cable horizontal, unos 10m son permitidos para que se haga la combinación de longitud y cables de parcheo, estos cables son usados para conectar el equipo en el área de trabajo y el gabinete de telecomunicaciones.

Cuando las corridas de cable se están instalando, hay que considerar dejar un poco de extensión en ambas puntas para poder hacer futuros cambios en el sistema de cableado. La cantidad mínima recomendada para estas extensiones es de:

- En gabinete de telecomunicaciones 3m
- En rosetas 1m para cables de fibra óptica
- rosetas 30cm para cables de par trenzado.
- Incluya dicha extensión en todos los cálculos de
- longitud para asegurarse de que el cable horizontal no exceda a 90m.
-

Consideraciones para sistemas heredados.

- Sistemas de datos de menor velocidad tales como el sistema IBM36, 38, AS400 y sincrónicos (RS232, 422, 423, etc.) pueden operar en UTP (o STP).
- No Exceda los 90 metros en este tipo de conexiones a menos que los equipos no vayan a cambiar la tecnología de transmisión que usan para conectarse al sistema principal, en caso de que se vislumbre un cambio de dicha tecnología a futuro, proponga un enlace a un panel de parcheo en esa zona de tal forma que pueda generarse otra ramificación de la estrella y atender a los servicios cercanos en esos puntos dentro de la cobertura de 90 metros.

Otros requerimientos:

- Las trayectorias deben partir desde el Rack de comunicaciones en grupos de cables que lleguen a las diversas áreas de trabajo esto varia dependiendo de la forma y tamaño de la oficina. Evite las trayectorias diagonales. Los grupos de cables deben ir soportados bajo piso falso o por encima de plafón con escalerilla.
- Las derivaciones hacia las áreas de trabajo deben de ir protegidas por seguridad y por estética, sobre todo cuando se bajan líneas de cable del techo hacia mamparas de trabajo.
- Los grupos de distribución de cables deben llegar a las zonas que serán atendidas de manera tal que los servicios estén a una distancia equitativa del punto de separación de las líneas de cable.
- El equipo activo no se considera dentro de un sistema de cableado estructurado, sin embargo el tipo de tecnología, topología y distancias siempre son parte de las consideraciones de diseño.

Consideraciones para salas de equipo.

- Las salas de equipo deben de ser de un área mínima de 150 pies cuadrados, los sites o peceras deben de ser de un área de 24 pies cuadrados mínimo, deben contar con iluminación, sistemas contra incendio, sistemas de respaldo de energía, sistemas de tierras físicas, salidas de emergencia y condiciones reguladas de ambiente.
- La cantidad recomendada de partículas de polvo es de 100 microgramos por metro cubico medido en un periodo de 24 horas, la humedad debe estar controlada al 80% sin condensar, la temperatura debe ser de 20 grados centígrados controlada, las áreas para operadores debe considerarse aisladas y por separado.
- Las conexiones eléctricas para servicio deben ir separadas de las conexiones eléctricas para equipo de telecomunicaciones. Se recomienda la instalación de contactos a distancias de 2 metros, dichos contactos deben ser dobles polarizados y aterrizados con identificación que permita diferenciarlos.

- Considere un espacio de 0.07 metros cuadrados de espacio para cada equipo, Racks y/o accesorios de telecomunicaciones por cada 100 metros cuadrados de áreas de trabajo.
- Los Racks deben ir al menos a 60 cm de distancia de la pared a partir del equipo con mas profundidad que se instale. Deben ir fijos al piso, y a la pared en caso de que el piso sea falso.
- El diseño del sistema de cableado debe incluir la cantidad de nodos necesaria en el cuarto de equipo y la sala de sistemas.
- Debe controlarse el flujo de polvo y la fuga de temperatura entre las acometidas externas, las trayectorias para el Backbone del edificio y la sala, así también el anegado de humedad y salitrado de las paredes.

1.11 Procedimientos Generales de Cableado.

Precauciones para el manejo de los cables.

- Asegúrese que los radios de curvatura de los cables no sea menor a cinco veces el diámetro del cable para: utp y stp-a.
- asegúrese de que el radio de dobles del cable horizontal no sea menor a diez veces el diámetro del cable para 25 pares y cables compuestos que contengan fibra.
- Las fijaciones no deberán dañar la cubierta del cable o presionar excesivamente, se usa hilo de seda o cinchos plásticos. Evite usar grapas.
- Jale el cable cuidadosamente para evitar que se provoquen torceduras y nudos en el cable. Deslice con cuidado los cables durante la instalación.
- En la instalación de cables de fibra óptica, antes de fijar las conexiones en el rack, deje una holgura de dos vueltas dentro del cuerpo del rack cuidando la forma natural a la que tiende el cable y el lado por el cual entra la fibra al rack de manera que quede suficiente fibra para operaciones de sujeción y conectorización.
- Controle la tensión en la instalación del cable suspendido. El límite máximo es 1.5m o menos.

- Identifique y etiquete los cables en ambos extremos antes de introducirlos por el ducto o pasarlos por la escalerilla.
- Reduzca torceduras de los pares de cobre soltando hacia atrás únicamente la cubierta del cable como se vaya requiriendo.

CAPITULO 2. ROUTERS&SWITCHES.

El continuo crecimiento de las redes de voz y datos ha propiciado el nacimiento de tecnologías que permitan brindar rapidez, flexibilidad, administración y sobre todo la integración de estos diferentes tipos de tráfico. Dentro de las tecnologías más importantes y actuales que hoy en día proporcionan todas estas características se encuentran Frame Relay, ATM y recientemente Gigabit Ethernet.

Todas estas tecnologías se basan en la conmutación (tanto de paquetes como de celdas), por lo que en el presente modulo se analizarán las características y ventajas de las nuevas tecnologías de conmutación que nos permiten conformar una nueva generación de redes. Por otra parte el Protocolo TCP/IP, en realidad es un conjunto de protocolos diseñados para permitir la conexión de computadoras y dispositivos de conectividad de las redes, TCP/IP es el protocolo más ampliamente utilizado en las redes y con acceso a Internet.

2.1TCP/ IP

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde aquellas de más bajo nivel ejemplo: La transmisión de flujos de bits a un medio físico hasta aquellas de más alto nivel, ejemplo: El compartir o transferir información desde una computadora a otra en la red. En 1973, la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA), de los Estados Unidos, inició un programa para la investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El proyecto tenía por objetivo la interconexión de redes, por lo que se le denominó "Interneting", y a la familia de redes de computadoras que surgieron de esta investigación se le denominó "Internet". Los protocolos desarrollados se denominaron como el Conjunto de Protocolos TCP/IP, que surgieron de dos conjuntos previamente

desarrollados; los Protocolos de Control de Transmisión (Transmission Control Protocol) e Internet (Internet Protocol).

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales destaca el protocolo IP. Bajo este nombre (TCP/IP) se esconde uno de los protocolos más usados del mundo, debido a que es el más usado por Internet y está muy extendido en el sistema operativo UNIX entre otros sistemas operativos como: Linux, Windows NT, Novell, etc.

TCP/IP significa Transmission Control Protocol e Internet Protocol, o Protocolo para el control de transmisiones y Protocolo para Internet.

Características de TCP/IP

Algunos de los motivos de su popularidad son:

- Independencia del fabricante.
- Soporta múltiples tecnologías.
- Es Ruteable.
- Puede funcionar en máquinas de cualquier tamaño.
- Estándar de EEUU desde 1983.
- Otorga acceso a Internet.
- La arquitectura de un sistema en TCP/IP tiene una serie de metas:
- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura de la computadora.
- Conectividad Universal a través de la red.
- Reconocimientos de extremo a extremo.
- Protocolos estandarizados.

El modelo básico en Internet es el modelo Cliente/Servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet está basada en capas. Esto hace más fácil implementar nuevos protocolos.

El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (International Standard Organization) para la interconexión de sistemas abiertos (OSI).

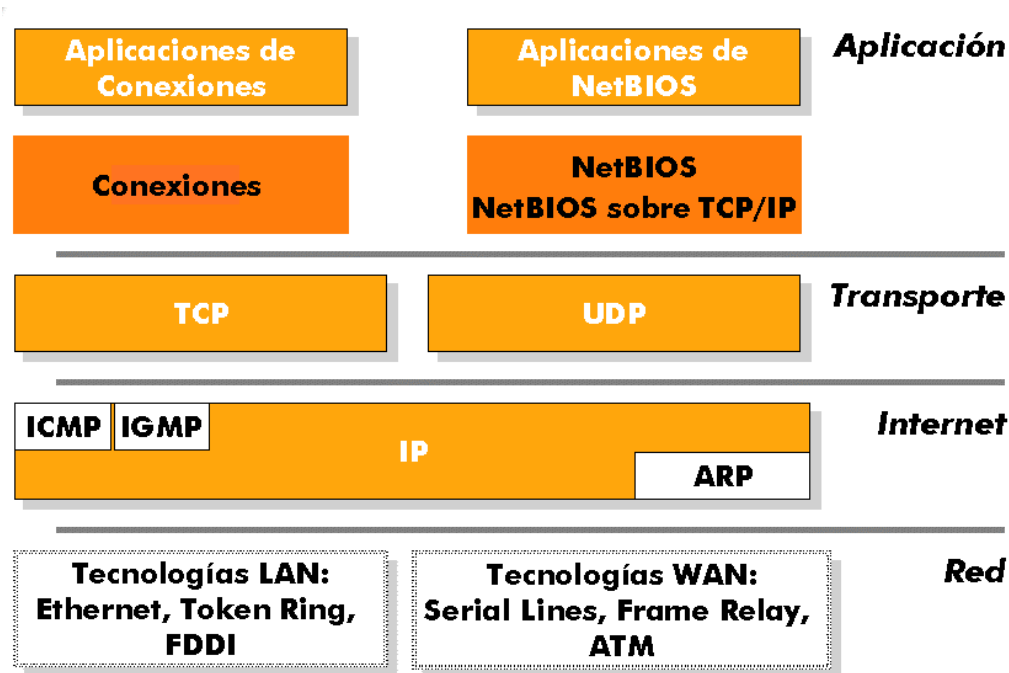


Fig. 2.1 Suite de protocolos TCP/IP

“Suite” de protocolos

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implementación real de una arquitectura puede diferir de este modelo. La arquitectura basada en TCP/IP propone cuatro capas en las que las funciones de las capas de Sesión y Presentación son responsabilidad de la capa de Aplicación y las capas de Liga de Datos y Física son vistas como la capa de Interfaz a la Red. Como puede verse TCP/IP presupone independencia del medio físico de comunicación, sin embargo existen estándares bien definidos al nivel de

Liga de Datos y Físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo TCP/IP deben considerarse la capa de Interfaz de Red; siendo los más usuales el proyecto IEEE 802: Ethernet, Token Ring y FDDI.

2.2 Internet Protocolo IP

El protocolo IP es un protocolo que trabaja a través de una sola Dirección IP, para cada host, donde cada hosts puede ser: una impresora, una computadora, un ruteador, un servidor, etc. cada uno de ellos tienen una sola Dirección IP, para que de esta manera puedan compartir o conectarse a los recursos de la red, en caso de existir más de dos dispositivo con una misma Dirección IP, se dice que entran en conflicto y no es posible realizar la conexión.

Características:

- No orientado a conexión.
- Transmisión en unidades denominadas datagramas.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

El IP no contiene suma de verificación para el contenido de datos de los datagramas, solamente para la información del encabezado. La entrega del datagramas en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensambla los fragmentos del mensaje.

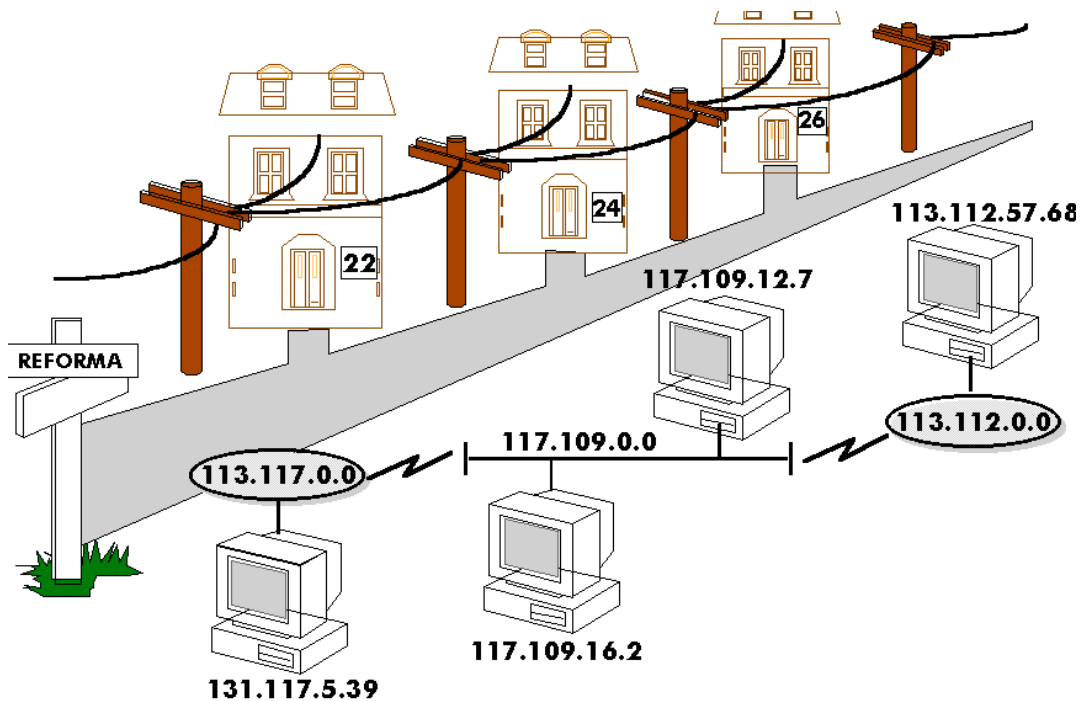


Fig. 2.2 ¿Qué es una dirección IP?

Dirección IP

La Dirección IP es una dirección de 32 bits dividida en 4 octetos que sirve para identificar a un equipo o dispositivo que esté trabajando con TCP/IP, esta dirección debe ser única y no puede estar repetida. Cada uno de los octetos tiene un posible valor en decimal que va de 0 a 255 (2^8). Esta dirección se encuentra dividida en una parte de red y otra parte de host. Como resultado de esto, solo es posible una Dirección IP por cada Host de la red, es decir solo puede existir una Dirección IP por Host en Internet.

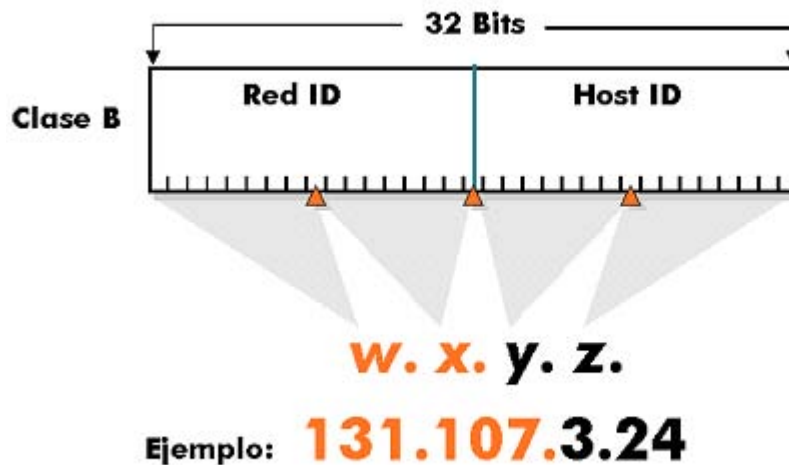


Fig. 2.3 Net ID y Host ID

Net ID Y Host ID.

Conceptualmente, cada Dirección IP está compuesta por un par Net ID y Host ID en donde se identifica la red y el Host dentro de la red. La clase se identifica mediante las primeras secuencias de bits, a partir de los tres primeros bits (de orden más alto). Las direcciones de Clase A corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.2.0.0 hasta la 126.0.0.0 (lo que permite hasta 2.6 millones de Hosts). Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 192.255.0.0. Esto permite tener 16,320 redes con 65,024 Host en cada una. Las direcciones de Clase C tienen sólo 8 bits para la dirección local o de Host y 21 bits para la red. Las direcciones de esta clase están comprendidas entre 192.0.2.0 y 223.255.255.0, lo que permite cerca de Dos millones de redes con 254 Hosts cada una. Por último, las direcciones de Clase D se usan con fines de multibroadcast, cuando se quiere un broadcast general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255. Cabe decir que, las direcciones de Clase E (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

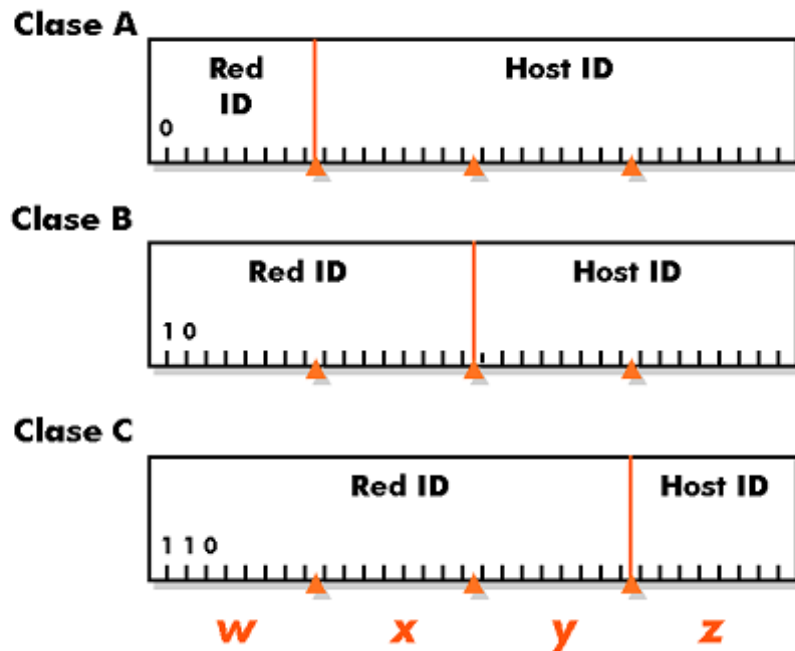


Fig. 2.4 Clases de direcciones IP

Guía de direcciones

Otra de las ventajas que ofrece el direccionamiento IP es el uso de direcciones de anuncio de direcciones (broadcast addresses), que hacen referencia a todos los Host de la misma red. Según el estándar, cualquier dirección local (Host ID) compuesta toda por 1s está reservada para broadcast. Por ejemplo, una dirección que contenga 32 1s se considera un mensaje difundido a todas las redes y a todos los dispositivos. Es posible difundir en todas las máquinas de una red alterando a 1s toda la dirección local o de Host (Host ID), de manera que la dirección 147.10.255.255 para una red de Clase B se recibiría en todos los dispositivos de dicha red; pero los datos no saldrían de dicha red.

- El Net ID no puede ser 127 en el 1er octeto.
 - 127 esta reservado para funciones de *loopback*.
- El Net ID y Host ID no pueden ser 255 (Todos los bit 1's).
 - 255 es una dirección de *broadcast*.
- El Net ID y Host ID no pueden ser 0 (Todos los bit 0's).
 - 0 indica "solo esta red".
 - El Host ID debe de ser único en toda la red.

Fig. 2.5 Guía de Direcciones IP

2.3 Protocolos de Transporte.

La Capa de Transporte es responsable de proveer comunicación entre dos Hosts, mediante la definición de Puntos Terminales (End Points) denominados Puertos, a donde las aplicaciones están escuchando a la red en espera de información cuando son activados. Hay dos protocolos en la Capa de Transporte: El TCP (Transmission Control Protocol). El UDP (Datagram User Protocol). A continuación se explican a detalle cada uno de estos protocolos de transporte.

TCP

TCP asegura una confiabilidad en la correcta entrega de los mensajes mediante números de secuencia y reconocimientos de mensajes recibidos. Los números de secuencia permiten que un mensaje muy grande pueda ser segmentado y reensamblado en el origen y el destino respectivamente, cuando la red así lo requiera. El reconocimiento verifica que la información haya sido recibida. TCP usa comunicaciones en flujos de byte, lo que significa que la información es tratada como una secuencia de bytes sin límites en los mensajes. La capa de Transporte al igual que las otras se define por los protocolos que maneja y

por los servicios que dan dichos protocolos a la capa inmediata superior en la arquitectura, en este caso a la capa de Servicios de Aplicación del Modelo TCP/IP. En el caso de TCP atiende a los Servicios de Aplicación orientados a conexión.

Envíos de TCP

En las sesiones anteriores hemos visto el servicio de entrega de paquetes sin conexión y no confiable, que forma la base para toda comunicación en InterNet, así como el protocolo IP. Ahora veremos el segundo servicio más importante y mejor conocido a nivel de red, la entrega de flujo confiable (Reliable Stream Transport), así como el Protocolo de Control de Transmisión (TCP) que lo define. En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir debido a errores (falla el hardware, sobrecarga de la red, etc.). Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega de conexión y no confiable para transferencias de grandes volúmenes de información resulta ser la peor opción. Debido a esto, el TCP se ha vuelto un protocolo de propósito general para estos casos. La interfaz entre los programas de aplicación y la entrega confiable es decir, las características del TCP son por cinco funciones:

- 1.-Servicio Orientado a Conexión: El servicio de entrega de flujo en la máquina destino pasa al receptor exactamente la misma secuencia de bytes que le pasa el transmisor en la máquina origen.
- 2.- Conexión de Circuito Virtual: Durante la transferencia, el software de protocolo en las dos máquinas continúa comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo ej. Falla el hardware, de red, etc., ambas máquinas detectarán la falla y la reportarán a los programas apropiados de aplicación, la confiabilidad que se proporciona depende del servicio de entrega de flujo.
- 3.-Transferencia con Memoria Intermedia: Los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente bytes de datos al software de protocolo. Cuando se

transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado, que pueden ser tan pequeñas como un byte. En el extremo receptor, el software de protocolo entrega bytes del flujo de datos en el mismo orden en que se enviaron, poniéndolos a disposición del programa de aplicación receptor tan pronto como se reciben y se verifican. Para hacer eficiente la transferencia y minimizar el tráfico de red, las implantaciones por lo general recolectan datos suficientes de un flujo para llenar un datagrama razonablemente largo antes de enviarlo. 4.- Flujo no estructurado: Posibilidad de enviar información de control junto a datos. 5.- Conexión Full Duplex: Se permite la transferencia concurrente en ambas direcciones. Desde el punto de vista de un proceso de aplicación, una conexión full duplex permite la existencia de dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción aparente. Esto ofrece una ventaja: el software subyacente de protocolo puede enviar datagramas de información de control de flujo al origen, llevando datos en la dirección opuesta. Este procedimiento de carga, transporte y descarga reduce el tráfico en la red.

UDP

El UDP es el otro protocolo de transporte dentro de esta suite, proporciona un servicio de entrega orientado sin conexión y no garantiza la entrega del paquete puesto que no tiene el CRC con el acknowledgement, utilizando el Protocolo Internet (IP) para transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de los dispositivos Host. El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto en número de puerto de destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta. El UDP utiliza el IP subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan

mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar.

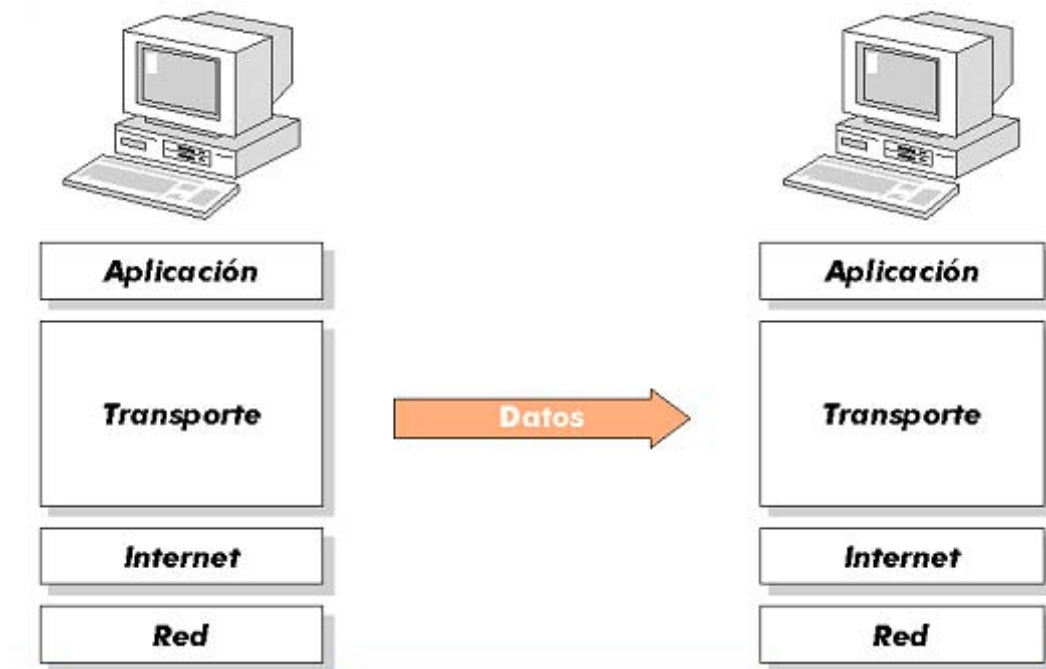


Fig. 2.6 Envíos de UDP

Envíos de UDP

Cada mensaje UDP se conoce como datagrama de usuario. Conceptualmente, un datagrama de usuario consiste en dos partes: un encabezado UDP y un área de datos UDP. El encabezado se divide en cuatro campos de 16 bits, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP. Para comunicarse con un puerto externo, un transmisor necesita saber tanto la Dirección IP de la máquina de destino, así como el número de puerto de protocolo del destino dentro de la máquina.

2.4 Servicios de TCP/ IP

En la tabla siguiente se muestran los principales protocolos o utilerías de TCP/IP con referencia al modelo OSI y con referencia a otros protocolos de transporte, así como los estándares de la IEEE 802.3:

Utilerías de TCP/IP

Se dice que estos protocolos de TCP/IP están dentro de la capa de Aplicación del modelo OSI, algunas de estas aplicaciones son tan comunes que se decidió estandarizarlas.

Trasferencia de Archivos:

- FTP: File Transfer Protocol.
- RCP: Remote Control Protocol.
- TFTP: Trivial FTP.
- Protocolos de Internet
- HTTP
- SNMP
- SMTP
- RPC
- DHCP
- RAS
- Ejecución Remota:
- Telnet.
- RSH: Remote Shell.
- REXEC: Remote Executation.
- Impresión:
- LPR: Line Printer Remote.
- LPD: Line Printer Daemon.
- LPQ: Line Printer Queue.
- Diagnóstico:
- Finger: Recupera información desde un Host remoto.
- Route: Modifica las tablas de ruteo.
- Tracert: Verifica las rutas entre los Hosts.

- Hostname: Alias coloquial de un Host.
- ARP: Mapea un IP con una dirección MAC.
- NBTSTAT: Registra el NetBios.
- NETSTAT: Registra el estado actual de conexiones.
- Ping: Verifica los protocolos y los medios físicos.
- NSLOOKUP: Examina las bases de datos del DNS.

2.5 Ruteo

Se le llama así a la función de encaminar paquetes de información hasta una estación destino utilizando el nivel de red (3) del modelo OSI. Estas funciones son realizadas por equipos ruteadores. Los ruteadores deben de ser direccionados explícitamente; las estaciones deben de conocer la dirección de los mismos para poder acceder a nodos remotos. Esta es una característica que los diferencia de los puentes, cuyas estaciones conectadas no necesitan conocer las direcciones de los mismos, lo único importante es la dirección de la estación remota con la que quieren hablar. Los ruteadores proporcionan servicios más sofisticados que los puentes: pueden seleccionar una ruta basándose en parámetros tales como la latencia de los enlaces, el estado de congestión en la red, la distancia entre nodos, etc., de modo que pueden aplicar diferentes políticas según los requerimientos específicos de cada aplicación permitiendo unas topologías más complejas y descentralizadas ya que pueden manejar diversos esquemas de direccionamiento, diferentes velocidades y tamaños de trama. No obstante todos ejecutan funciones similares: Eligen el camino más adecuado: Mantienen tablas internas que proporcionan información de los enlaces de la red. Estas tablas son fundamentales, pues en ellas basan la decisión para realizar el enrutamiento. Disponen de mecanismos para el control de Flujo: La congestión es algo común cuando redes de diferente velocidad están interconectadas, pues la más rápida excede la capacidad de la más lenta. Cuando esto ocurre y es detectado, el ruteador envía una señal a la estación fuente, indicando congestión e invitándole a reducir la velocidad de transmisión. Unen redes heterogéneas: Los ruteadores pueden conectar redes de diferente nivel MAC (Token Ring, Ethernet, etc.). Su

tarea es la de mapear las direcciones del protocolo de comunicaciones (por ejemplo, IPX) en las direcciones destino de la red utilizada (por ejemplo, Frame Relay), siendo esta una de las razones que dificultan las funciones Multicasting pues las WAN suelen ser orientadas a conexión. En la mayoría de los casos un Host determina que tiene que enviar un paquete a otro Host. Habiendo adquirido una dirección física de un ruteador por medios que después analizaremos, el Host origen envía un paquete direccionado hacia una dirección física MAC de un ruteador, pero también la dirección del protocolo a usar en el Host destino. Examinando la dirección de destino del paquete, el ruteador determina si puede o no enviar el paquete al siguiente punto de conmutación o salto (Hop), esto mediante la comparación de la dirección obtenida con las direcciones contenidas en una tabla de enrutamiento. Si el ruteador no sabe como reenviar el paquete simplemente lo desecha, si lo sabe y tiene una dirección de salida, cambia la dirección física del paquete por la del siguiente Hop y transmite el paquete. Es posible que el siguiente Hop no sea el último para llegar al otro Host, por lo tanto la dirección física de destino en el paquete irá cambiando conforme se vaya adentrando en la red y pasando de ruteador a ruteador hasta llegar al final de su trayectoria.

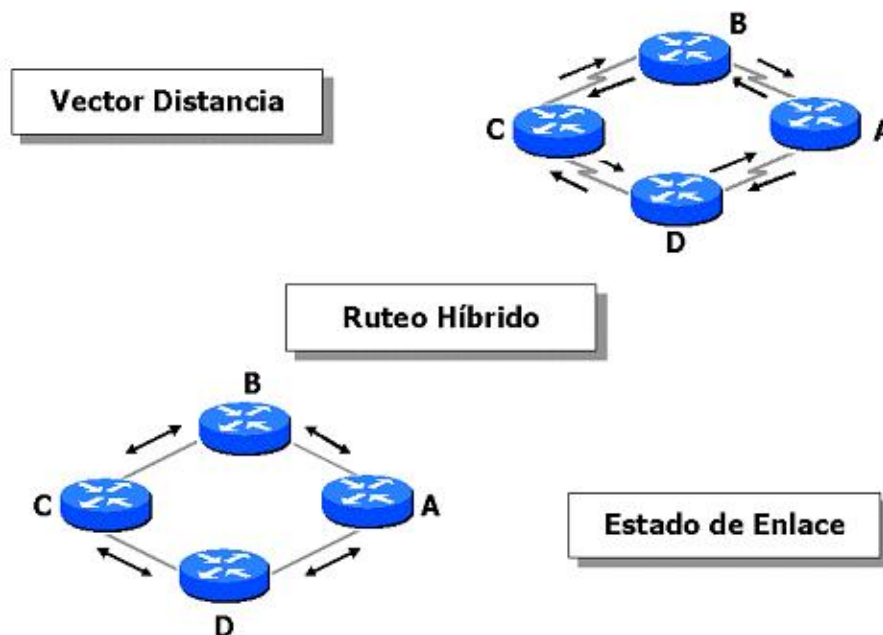


Fig. 2.7 Clases de protocolos de Ruteo

Internetworking

El mecanismo básico explicado anteriormente requiere de varias definiciones: Mecanismo/Proceso de Enrutamiento (Usando la Tabla de Enrutamiento). Son las actividades realizadas por un nodo o Host para determinar como se manejará un paquete en base a una dirección de red destino. Protocolo de Enrutamiento (Crea la Tabla de Enrutamiento). Es el conjunto de reglas (en realidad el lenguaje) usadas entre ruteadores para compartir información de la red y tomar decisiones.

Tabla de Enrutamiento.

Una tabla que contiene información acerca de los posibles destinos sobre la base de direcciones de red específicas. Las tablas de enrutamiento sobre las que se basan las decisiones de enrutamiento pueden ser configuradas de dos modos:

1.-Estáticamente: definidas en el momento de la instalación y manejables por los administradores de la red. Los ruteadores que las utilizan son eficientes, aunque obligan a un procedimiento de configuración largo y tedioso.

2.- Dinámicamente: utilizando algoritmos automáticos. Los ruteadores son más fáciles de configurar, pero pueden llegar a incrementar el “overhead” de la red por los continuos intercambios de información de control entre los ruteadores instalados.

Actividades de enrutamiento.

Encontrar información concerniente al destino de un paquete el cual tiene que ser transmitido. La dirección del paquete es comparada con los registros de la tabla de enrutamiento para decidir por cual interfaz será transmitida. Usando la tabla, si la dirección destino es 138.203.22.210, ¿por cual interfaz será enviada? Actualización de la Tabla de Enrutamiento Puede ser hecha manualmente directamente sobre las áreas de configuración de redes en el sistema operativo utilizado por un operador o administrador de la red, Por ejemplo, la configuración del Gateway por omisión para TCP/IP en Windows 95. O automáticamente por medio de protocolos de enrutamiento.

Protocolos de Enrutamiento

En general un Router Path esta compuesto de dos partes: 2.-La comunicación con sus ruteadores y Hosts vecinos para investigar que estaciones están conectadas a que parte de la red. 2.-Después de recolectar esta información, filtrarla y correr un algoritmo para decidir cuales partes de esta información son usadas para cambiar o actualizar la tabla de enrutamiento. Los algoritmos más usados en los actuales protocolos de ruteo son:

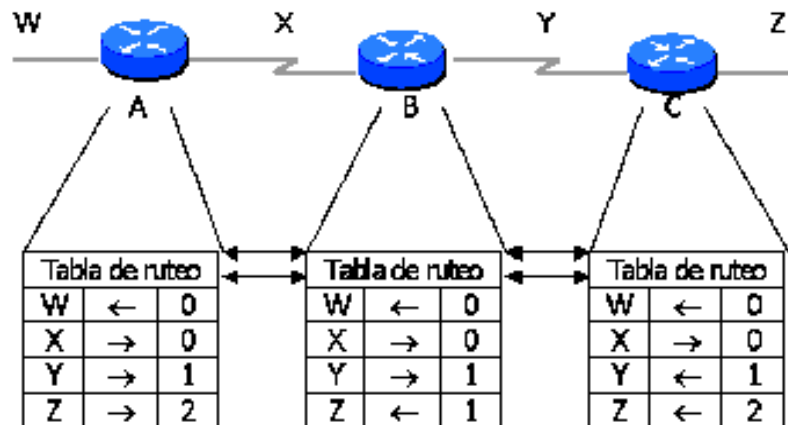
- Algoritmo por Vector Distancia.
- Algoritmo de Estado de Enlace.

Este último es el mejor en términos de estabilidad, velocidad de actualización, manejo de overhead, etc., y por lo tanto el más comúnmente usado, de hecho, salvo casos muy especiales se utiliza el protocolo por vector distancia (DV).

RIP (Routing Information Protocol)

Está basado en el protocolo de vector de distancia (Bellman-Ford). El principio es como sigue: Un ruteador llama a cada ruteador vecino para enviar toda o una porción de su tabla de ruteo. Dicha tabla contiene un vector de distancias (conteo de hops) y cada ruteador actualiza su tabla basándose en estos vectores de distancia que recibe de sus vecinos. El envío de esta información se hace por Broadcasting y esto continuo mientras el ruteador esté en línea en la red. El objetivo de su algoritmo es, una vez que llega un paquete, se analiza su dirección destino y se asigna la trayectoria más óptima basándose en la distancia más corta (menor Hop Count) que se tenga en las posibles interfaces de salida. Describe la red en términos de hops que indican el número de ruteadores que un paquete debe de atravesar antes de llegar a su destino. Una versión modificada fue la adoptada por el TCP/IP. No es apropiada para redes muy grandes pues

sobrecarga en exceso el enlace por el intercambio frecuente de tablas de enrutamiento.



• Los routers descubren el mejor camino a sus destinos a través de cada vecino.

Fig. 2.8 Vector-Distancia: descubrimiento de la red

2.6 Switcheo WAN

Conmutación

En la actualidad, las redes se encuentran en una etapa de transición. La mayoría de las redes tradicionales están conformadas por hubs para la conexión de usuarios a nivel de la LAN y por enrutadores para conexión a la WAN. Sin embargo, una gran mayoría de estaciones de trabajo se están conectando a LAN Switches (Switches/Conmutadores de LAN) y muchos de estos equipos se conectan a backbone con tecnologías como ATM o Gigabit Ethernet. Este crecimiento rápido en las redes se debe principalmente a:

- Evolución de Ethernet 10, 100 (Fast Ethernet) y 1000 Mbps (Gigabit Ethernet).
- La tendencia hacia integrar diferente tipo de tráfico (voz, datos, vídeo) en las redes corporativas basadas en tecnología ATM.
- El concepto de conmutación a nivel capa 3 en los switches, la cual permite realizar funciones de enrutamiento tradicional basado en software.

- El primer uso de los switches/conmutadores de datos fue como una alternativa de enrutadores para interconectar hubs. Los enrutadores tienden a ser muy complejos de configurar y administrar a diferencia de los equipos de conmutación LAN que permiten realizar el proceso de enrutamiento de una forma más sencilla y rápida.

- ▼ Tendencia a integrar diferentes tipos de tráfico: voz, datos y vídeo
- ▼ Conmutación en capa 3: soporte de enrutamiento a nivel de hardware
- ▼ Switcheo WAN

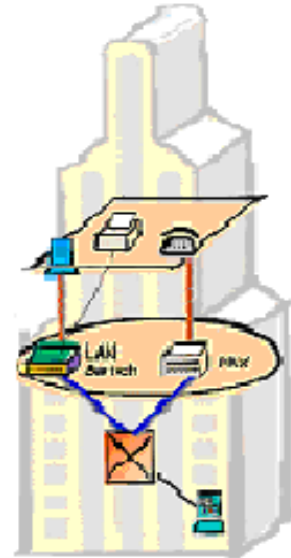


Fig. 2.9 Switcheo WAN

Tipos de conmutación

Existen dos tipos de conmutación, la conmutación de circuitos (aplicada a tráfico de voz) y la conmutación de paquetes (aplicada a tráfico de datos).

Conmutación de circuitos

En esta técnica una trayectoria o circuito físico entre el equipo fuente y el equipo destino debe ser establecida antes de que los datos puedan ser transmitidos.

Después de que la conexión es establecida, el uso del circuito es exclusivo y continuo durante el intercambio de información. Cuando este intercambio es completado, el circuito es desconectado y los enlaces físicos entre los nodos están listos para ser usados en otras conexiones. El principal uso de

esta técnica es en la red telefónica pública. Sus características principales son las siguientes:

- Tiempo de establecimiento elevado, del orden de los segundos.
- Utilización de recursos ineficiente (transmisión de datos por ráfaga).
- Retardos pequeños y constantes.
- Comunicación en tiempo real.

Tecnologías basadas en conmutación de paquetes La conmutación de paquetes las facilidades que proporciona origino el nacimiento de tecnologías como X.25 y Frame Relay. Sin embargo, gracias a la continua evolución en las comunicaciones, actualmente ya contamos no solo con tecnologías que realizan la conmutación de paquetes sino también de celdas como lo es ATM.

Frame Relay

Esta tecnología nace como evolución de X.25, también se encuentra basada en la conmutación de paquetes, pero es mucho más rápida. Frame Relay hace uso de enlaces digitales y permite integrar tráfico de voz, datos y video. En el capítulo 2 se tratará esta tecnología.

ATM

El modo de transferencia asíncrono ATM nace como predecesor de ISDN. Debido a su función de proporcionar Calidad de Servicio (QoS) y soportar tráfico de voz, datos y video, integra un nuevo concepto en conmutación: la conmutación de celdas. Su tecnología se encuentra basada en la administración de ancho de banda, altas velocidades, integración de tráfico variado y QoS.

2.7 Frame Relay Antecedentes

Las técnicas actuales de conmutación de paquetes llamadas Conmutación Rápida de Paquetes (Fast Packet Switching), toman ventaja de los medios de transmisión confiables como la fibra óptica y de la alta velocidad de procesamiento de los conmutadores para eliminar algunos procesos de control de flujo y detección/corrección de errores como en X.25. Dentro de las técnicas de conmutación rápida de paquetes se encuentra Frame Relay. Frame Relay fue aceptado con entusiasmo desde el principio, porque dio respuesta a necesidades concretas del mercado, tales como: la necesidad de mayor velocidad en las

comunicaciones, mayor rendimiento y seguridad en la transmisión. Dentro de los principales factores que impulsaron el desarrollo de Frame Relay, tenemos:

- El cambio en el contenido de la información, de texto a gráficas.
- Incremento en aplicaciones de datos de tráfico tipo ráfaga.
- Dispositivos de usuario más inteligentes y más demandantes de ancho de banda.
- Alta proliferación de redes de área local

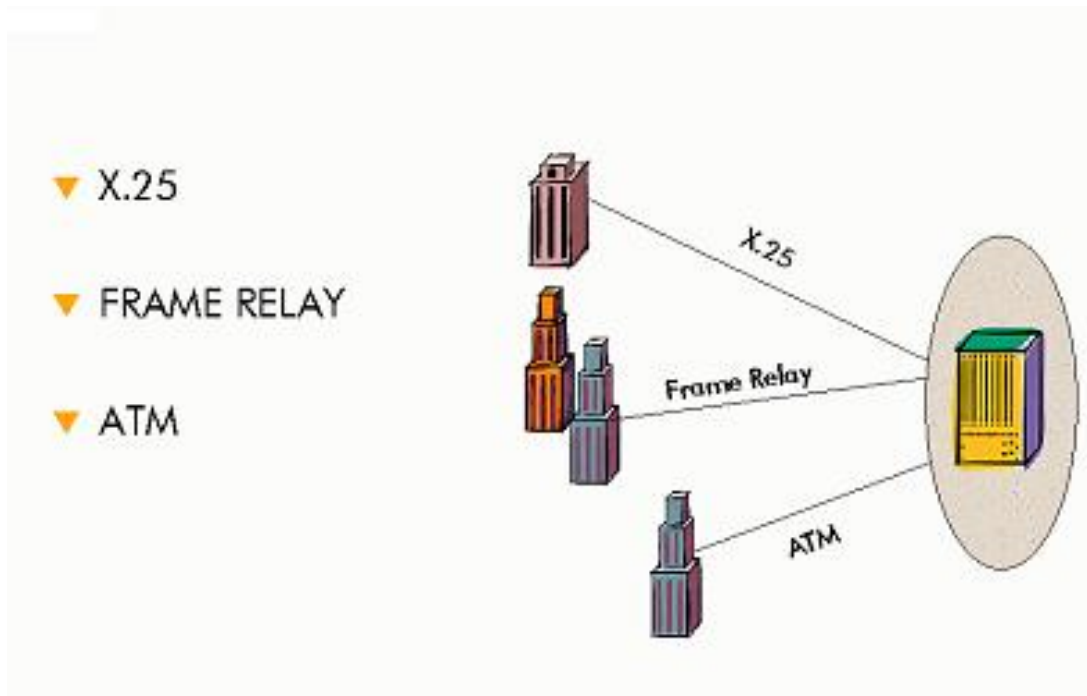


Fig. 2.10 Tecnologías basadas en conmutación

La tecnología Frame Relay optimiza la transferencia de información sobre las facilidades actuales de transmisión digital y opera en las dos primeras capas del modelo OSI. El protocolo que utiliza Frame Relay en la capa 2 está definido en la Recomendación I.441* (un subconjunto de la I.441) y se basa en el protocolo LAPD (Link Access Protocol by Channel D: Protocolo de acceso al Enlace por canal D). Su función es delimitar tramas, cálculo y verificación de los códigos de redundancia, así como controlar la congestión para proporcionar un servicio de transmisión de tramas confiable. Frame Relay combina el multiplexaje estadístico de X.25 con las características de alta velocidad y bajo retardo de TDM. Es decir,

organiza los datos en unidades individuales conocidas como tramas, a las cuales agrega direccionamiento, en lugar de usar ranuras de tiempo como en TDM. Frame Relay es una tecnología en base a tramas que usan circuitos virtuales para transportar datos desde una localidad de usuario hasta las instalaciones de otro, proporcionando múltiples conexiones lógicas sobre un solo circuito físico, además delimita y entrega las tramas en el orden correcto, enruta y multiplexa y deja a los protocolos de capas superiores, como TCP/IP, las funciones de corrección de errores, acuse de recibo, y retransmisión de tramas, así como la secuencia numerada. Las capas superiores son las responsables de la transmisión de datos extremo a extremo libres de error. El CRC (Código de verificación de redundancia cíclica) es la única verificación de error que realiza la red. Las tramas que contienen un CRC equivocado se descartan.

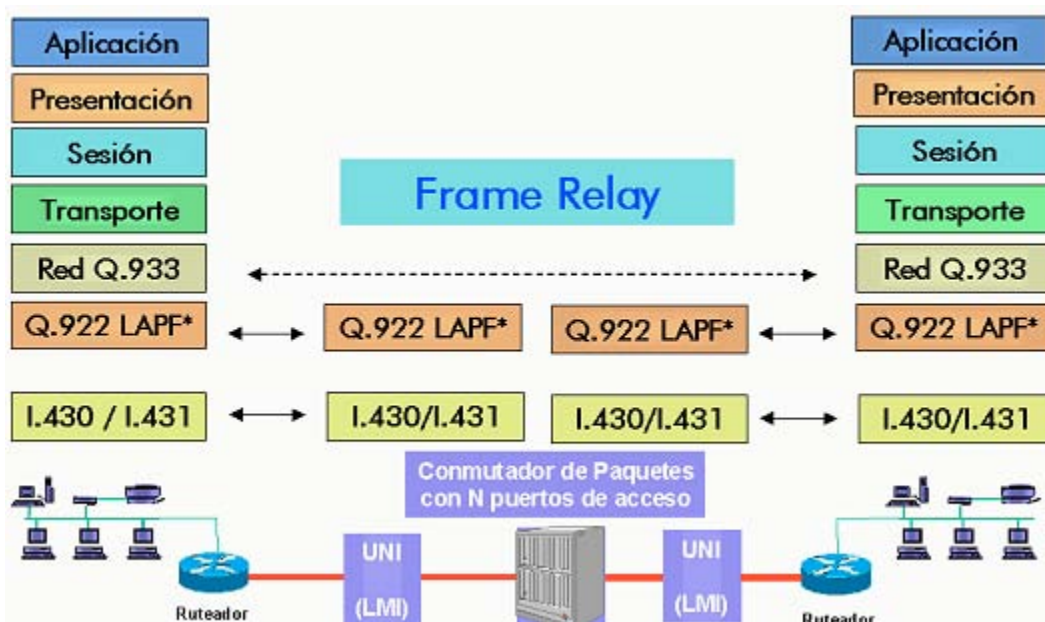


Fig. 2.11 frame Relay y el modelo OSI

Operación de Frame Relay

La Tecnología Frame Relay se basa en el concepto de circuitos virtuales o VC's. Los VC's son trayectorias entre dos puertos de datos, definidas por software, que

actúan como una línea privada. Estos circuitos virtuales pueden ser permanentes (Permanent Virtual Circuit/PVC's) o conmutados (Switched Virtual Circuit/SVC's).

- Circuitos Virtuales Permanentes / PVC's. Los PVC's se establecen manualmente por el operador de la red, mediante un sistema de administración, y permiten el establecimiento de una conexión entre dos sitios en forma permanente. Estos enlaces se pueden modificar posteriormente. Dentro de la red la trayectoria del enlace puede variar debido a re-enrutamientos que puedan ocurrir por fallas o alguna otra causa, pero los puntos extremos de la conexión siempre son los mismos. En este sentido el PVC es como una línea dedicada.
- Circuitos Virtuales Conmutados / SVC's. Los circuitos virtuales conmutados, se establecen en base a una solicitud de conexión, utilizando un protocolo de conexión definido (Q.933). El usuario especifica una dirección destino, así como los requerimientos de ancho de banda. El manejo de SVC's es más complicado que el de los PVC's, sin embargo este proceso debe ser transparente para el usuario. La red Frame Relay debe atender la solicitud y establecer la conexión en base a la solicitud.

Frame Relay opera en el Modo Orientado a Conexión (Connection oriented),

Para este modo existen dos tipos de conexiones:

- Circuitos Virtuales Permanentes, PVC: Se establecen al momento de la contratación.
- Circuitos Virtuales Conmutados, SVC: Se establecen por medio de una llamada

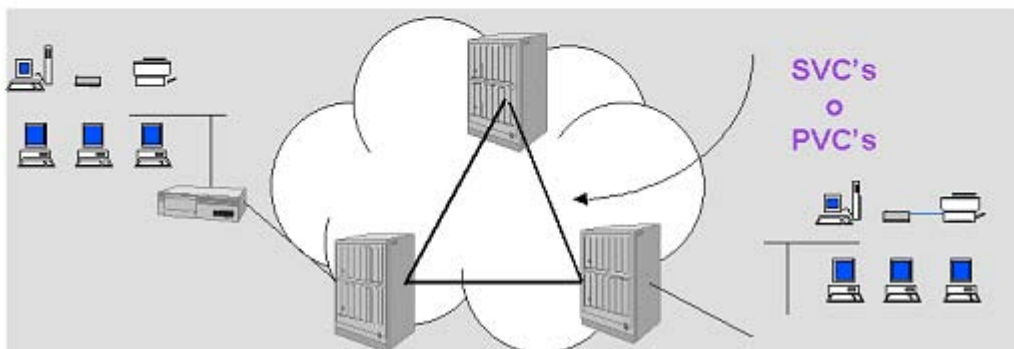


Fig. 2.12 modo de operación

Foro Frame Relay

El foro Frame Relay es una Organización de normalización iniciada por el Grupo de los Cuatro:

- DEC (Digital Equipment Corporation)
- Northern Telecom
- Cisco
- Stratacom

Este foro generó 2 interfaces basándose en los estándares que en ese momento estaba desarrollando la ANSI para Frame Relay, los estándares que definió el foro Frame Relay fueron:

- Interfaz UNI (User to Network Interface) Es un protocolo que permite a los usuarios acceder a una red Frame Relay pública o privada y establecer una trayectoria de comunicaciones hacia otro usuario dentro de la red.
- Interfaz NNI (Network to Network Interface) La interfaz de Red a Red en FR está diseñada para proporcionar una interfaz eficiente entre redes FR y permitir que los usuarios de dichas redes se puedan comunicar entre ellos.

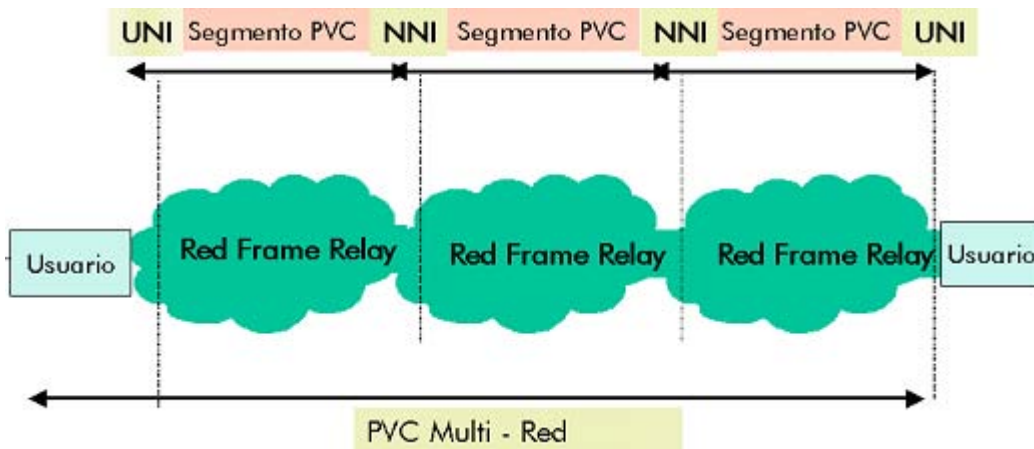


Fig. 2.13 Interfaces UNI y NNI

Elementos de una Red Frame Relay.

Una red Frame Relay se encuentra compuesta por elementos físicos y lógicos.

- **Elementos Físicos:** Incluyen todos los elementos de hardware que permiten llevar a cabo la comunicación en una red Frame Relay. Dentro de estos elementos se encuentran: el equipo de usuario (servidores, estaciones de trabajo, etc.), el equipo de acceso a la red Frame Relay (enrutadores, FRAD's), conmutadores/switches Frame Relay) y por supuesto los enlaces digitales (E3, E1, DS0) que proporciona la red pública.
- **Elementos Lógicos:** Son circuitos y trayectorias virtuales, los cuales permiten llevar a cabo las conexiones a través de elementos físicos, entre los diferentes nodos que conforman la red.

SWITCHES FRAME RELAY

Los conmutadores o switches Frame Relay son los que componen a la "nube" o red Frame Relay y son los encargados de conmutar o enrutar las tramas a través de la red hasta el dispositivo destino. Esto lo hacen mediante el establecimiento de conexiones virtuales, permitiendo el transporte a alta velocidad en forma segura y confiable. Los conmutadores Frame Relay cuentan con las siguientes características:

- Permiten la conexión a enlaces desde 64Kbps hasta 34Mbps
- Soportan Interfaces seriales V.35 para conexión a la WAN (DS0) y RS232.

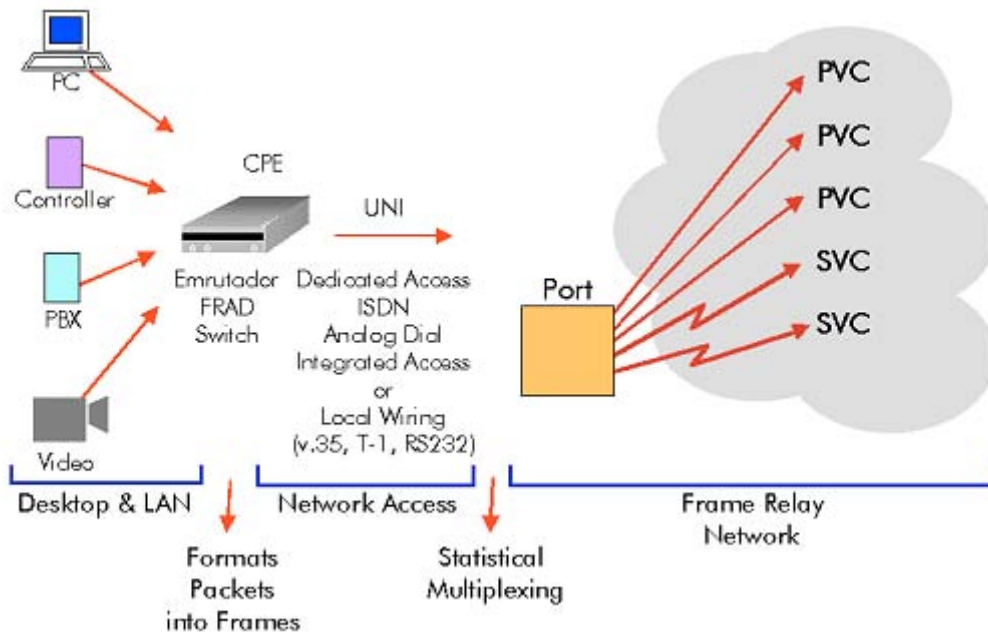


Fig. 2.14 Elementos de una Red FRAME RELAY

Soportan conexiones la WAN mediante enlaces digitales E1, interfaces G.703/G.704.

Permiten la conexión a equipos voz PBX, mediante enlaces E1 de voz (G.703).

Permite la conexión a FRAD's y enrutadores.

Permite la conexión a dispositivos de vídeo.

Equipos de acceso a una red Frame Relay

Los equipos de acceso a la red Frame Relay tienen la responsabilidad de entregar las tramas a la red en un formato pre-establecido. Dentro de los equipos de acceso a una red Frame Relay se encuentran los equipos de acceso FRAD's y los enrutadores.

- FRAD. Un FRAD recibe información de voz/datos a través de diferentes interfaces y la integra en tramas de Frame Relay para su transporte a través de la red pública o privada. Comúnmente un Frad cuenta con las siguientes interfaces:
- Puertos WAN. Interfaces RS232-C, V.35 (DS0).
- Puertos LAN. Puertos Ethernet (10 y 100 Mbps).

- para conexión a la red LAN, comúnmente integran uno o dos puertos.
- Puertos de Voz. Interfaces Analógicas que permiten la conexión a extensiones telefónicas o equipos multilínea de voz.
- Enrutador. Un enrutador tiene la función específica de enrutar la información de una LAN a la WAN. Por lo tanto estos dispositivos pueden soportar el mismo tipo de puertos de datos que un FRAD.
- Algunos enrutadores soportan puertos analógicos de voz.
- Soportan conexiones la WAN mediante enlaces digitales E1, interfaces G.703/G.704.
- Permiten la conexión a equipos voz PBX, mediante enlaces E1 de voz (G.703).
- Permite la conexión a FRAD's y enrutadores
- Permite la conexión a dispositivos de vídeo.

Equipos de acceso a una red Frame Relay

Los equipos de acceso a la red Frame Relay tienen la responsabilidad de entregar las tramas a la red en un formato pre-establecido. Dentro de los equipos de acceso a una red Frame Relay se encuentran los equipos de acceso FRAD's y los enrutadores.

- FRAD. Un FRAD recibe información de voz/datos a través de diferentes interfaces y la integra en tramas de Frame Relay para su transporte a través de la red pública o privada. Comúnmente un Frad cuenta con las siguientes interfaces:
 - Puertos WAN. Interfaces RS232-C, V.35 (DS0).
 - Puertos LAN. Puertos Ethernet (10 y 100 Mbps) para conexión a la red LAN, comúnmente integran uno o dos puertos.
 - Puertos de Voz. Interfaces Analógicas que permiten la conexión a extensiones telefónicas o equipos multilínea de voz.
- Enrutador. Un enrutador tiene la función específica de enrutar la información de una LAN a la WAN. Por lo tanto estos dispositivos pueden

soportar el mismo tipo de puertos de datos que un FRAD. Algunos enrutadores soportan puertos analógicos de voz.

•

2.8 Modo de Transferencia Asíncrono (ATM)

Antecedentes

La primera referencia de ATM (Asynchronous Transfer Mode) tiene lugar en los años 60's en los laboratorios Bell. Sin embargo, el ATM no se hizo popular hasta 1988 cuando el CCITT decidió que sería la tecnología de conmutación de la futura red ISDN en banda ancha (BISDN), una vez definido esto, se empezó a discutir sobre el tamaño de las celdas que se usarían en la transmisión, por un lado los organismos de EUA proponían un tamaño de celda grande, de unos 128 bytes, pensando en transmisión de datos, sin embargo los europeos señalaron que una celda tan grande introduciría retardos muy grandes inaceptables para transmisión de voz y en un futuro, de audio y vídeo, por lo que propusieron un tamaño de no más de 16 bytes, después de varios análisis ambos cedieron y los tamaños quedaron en 64 y 32 respectivamente pero aún no había un acuerdo. Por lo que en 1989, el CCITT decidió que el tamaño de la celda ATM sería de 48 bytes $((64+32)/2 = 48)$, para los encabezados se siguió un proceso similar y quedó en 5 bytes dando un total de 53 Bytes, el cual cumple con los requerimientos en cuanto a capacidad de transporte y retardos tanto para redes de datos como de voz y ahora las denominadas redes multimedia.

Características de ATM

ATM es un protocolo de transporte que realiza conmutación de celdas, orientado a conexión y con transmisión dúplex, que asigna ancho de banda a cada estación. Utilizando multiplexación asíncrona por división en el tiempo para controlar el flujo de información a través de la red. ATM trabaja con anchos de banda que van desde los 25 Mbps hasta los 622 Mbps. Actualmente se han diseñado nuevas tecnologías para trabajar bajo otras velocidades como lo que es IMA (Multiplexaje Inverso de ATM), el cual permite manejar hasta 8 E1's (2.048 Mbps) de ancho de banda en ATM. Sin embargo, hoy día la velocidad más usada de ATM es 155 Mbps. Dentro de los principales beneficios que contempla ATM se encuentran:

- Integración fácil de redes clásicas (ethernet).
- Manejo de ancho de banda bajo demanda.
- Capacidad para manejar la totalidad de tipos de tráfico por la red (voz, imágenes, vídeo, gráficos y multimedia).
- Adaptabilidad tanto en entorno LAN como el WAN.
- Manejo de altas velocidades de transmisión.
- Soporte de Calidad de Servicio (QoS).

Funcionamiento de ATM

Un conmutador/switch ATM establece una conexión virtual entre el nodo transmisor y el nodo receptor. Dicha conexión se lleva a cabo basándose en la dirección destino de cada celda, y dura justo lo que se tarda en transferir cada celda. La transferencia de datos puede realizarse en paralelo y con plena velocidad de la red. Ya que cada celda solo se transmite al puerto asociado con su dirección destino específico, ningún otro puerto recibe la celda, y por ello, se propicia que el tráfico sea reducido y con una seguridad elevada. Para comunicarse a través de la red ATM es necesario que las aplicaciones establezcan de antemano una conexión virtual (VC) entre conmutadores. Una VC constituye una ruta de transmisión para una celda ATM. Una conexión virtual se puede establecer entre uno o más conmutadores, de tal forma que se defina una conexión punto a punto para la transmisión de datos de la aplicación a través de las celdas ATM. Las conexiones virtuales o circuitos virtuales (CV) pueden establecerse de dos maneras:

- Circuitos Virtuales Permanentes (PVC): Estas conexiones pueden ser configuradas manualmente y como su nombre lo indica son rutas virtuales estáticas o permanentes. A cada PVC se le asigna un ancho de banda que garantiza la calidad de servicio. Dentro de las principales aplicaciones de los PVC's se encuentran la conexiones permanentes entre diferentes dispositivos de red como enrutadores y puentes (bridges).

Desde un punto de vista de transmisión, el ATM se puede dividir en tres niveles de jerarquías:

- Canal Virtual (Virtual Channel VC)
- Ruta Virtual (Virtual Path VP)
- Sección Física (Physical Section PS) Medio de transmisión

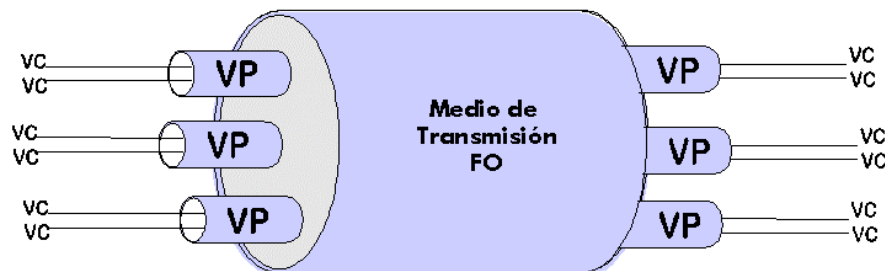


Fig. 2.15 Arquitectura de un nodo ATM (Vpi/Vci)

Modelo de Referencia ATM

El ATM llega bastante más allá en el modelo OSI que la mayoría de los protocolos de transporte. Por ello, para que pueda interactuar con protocolos de la capa de red, deben desarrollarse aplicaciones que tengan en cuenta las aplicaciones de alto nivel del modo de transferencia asíncrono.

ATM consiste de tres niveles o capas básicas.

Capa física

La primera capa llamada capa física (Physical Layer), define las interfaces físicas con los medios de transmisión y el protocolo de trama para la red. ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. A diferencia de muchas tecnologías LAN como Ethernet, que especifica ciertos medios de transmisión (10 base T, 10 base 5, etc.), ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), T3/E3 y TI/EI. En base a la tecnología de transporte se han establecido las equivalencias de las velocidades que maneja ATM, tanto para SONET como para SDH.



Fig. 2.16 La capa física

La capa de ATM

La segunda capa es la capa ATM. En ella se define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del servicio. El formato de una celda ATM es muy simple. Consiste de 5 bytes de cabecera y 48 bytes para información. Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una celda grande, que es muy eficiente para transmitir largas tramas de datos y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, vídeo y protocolos sensibles al retardo. Las celdas de longitud fija representan numerosas ventajas sobre los paquetes de longitud variable:

- Capacidad de conmutación hardware: La conmutación ATM, al consistir en el proceso de conmutación de celdas de longitud fija, puede realizarse a nivel de hardware, en lugar de utilizar software costoso que realice el

cálculo para la gestión de control de flujo, buffers y otros esquemas de gestión.

- Niveles de servicio Garantizado: Los retrasos de interconexión y de las colas de conmutación son más predecibles en el caso de celdas de datos de longitud fija. Por esta razón pueden diseñarse equipos que proporcionen niveles de servicio garantizado para todo tipo de tráfico, incluyendo servicios sensibles a retrasos, tales como la voz y el vídeo.

ATM	SONET	SDH
155 Mbps	OC3	STM-1
622 Mbps	OC12	STM-4
2.5 Gbps	OC48	STM-16

Fig. 2.17 Equivalencias de SONET y SDH para velocidades ATM

- Sus funciones :
 - Construcción / Extracción de encabezados
 - Mantiene los identificadores de las conexiones y realiza el enrutamiento (Routing) entre nodos
 - Multiplexa y Demultiplexa las celdas por los medios físicos de transmisión y controla la entrega secuencial dentro de una conexión virtual

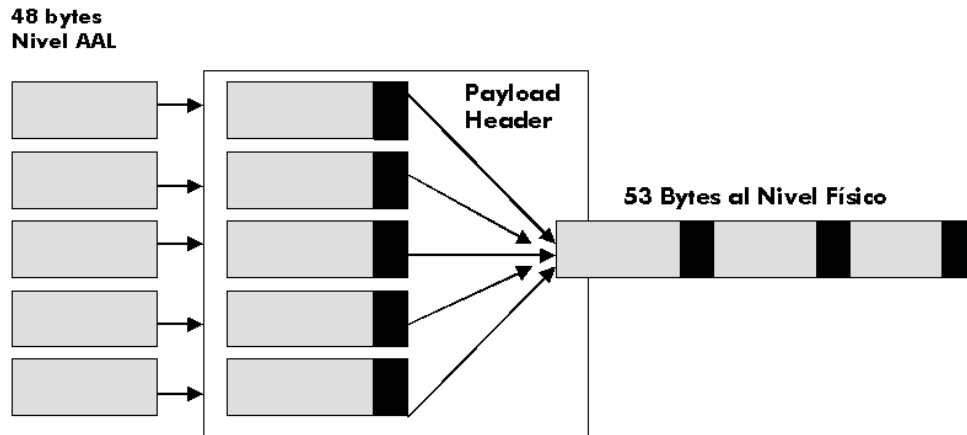


Fig. 2.18 El nivel ATM

- Procesamiento Paralelo: Las celdas de longitud fija permiten que los conmutadores de retransmisión de celdas funcionen en paralelo, para velocidades que exceden en gran medida la capacidad de la arquitectura de conmutación de tipo bus.
- Capacidad de procesamiento de voz: Aunque las celdas ATM sólo necesitan ancho de banda cuando hay tráfico que cursar, también pueden proporcionar el equivalente a las divisiones temporales de un multiplexor por división en el tiempo, para tráfico continuo. Como resultado, ATM puede manejar igual de bien tráfico continuo en tiempo real, como voz digitalizada, y tráfico en ráfagas, como en transmisiones a nivel LAN. Los comités de estándares han definido dos tipos de cabeceras ATM: los User-to-Network Interface (UNI) y la Network to Network Interface (UNI).
- La UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente (Customer Premises Equipment), tal como hubs o enrutadores ATM y la red de área ancha ATM (ATM WAN).

- La NNI define la interfaz entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interfaz entre una red ATM de un usuario privado y la red ATM de un proveedor público (carrier). Específicamente, la función principal de ambos tipos de cabeceras de UNI y la NNI, es identificar los "Virtual paths identifiers" (VPI) y los "virtual circuits" o conexiones virtuales (VC) como identificadores para el enrutamiento y la conmutación de las celdas ATM.



Fig. 2.19 Capa de adaptación ATM (AAL)

CAPITULO 3. SISTEMAS OPERATIVOS, SERVICIOS& e-BUSINESS.

La importancia de la administración de recursos de red y la optimización de está, dependen en gran medida de la correcta operación de los servidores y Sus sistemas operativos involucrados en este capítulo se hace referencia los de los más usados y su importancia para lograr nuestro objetivo en la operación del comercio electrónico. Así como del uso adecuado de Herramientas y aplicaciones, En particular los sistemas abiertos se han convertido en punta de Lanza para las nuevas soluciones ofrecidas para un entorno de trabajo cliente servidor orientado hacia el enfoque de los negocios.

Desde hace mucho tiempo el sistema operativo UNIX ha ocupado un importante lugar en el área de desarrollo de sistemas, en el área de redes y en ambientes cliente/servidor. Desde sus inicios y hasta la fecha sigue siendo uno de los principales sistemas operativos instalados en computadoras de alto, intermedio y bajo rendimiento a nivel mundial.

La importancia de los sistemas operativos nace históricamente desde los 50's, cuando se hizo evidente que el operar una computadora por medio de tableros enchufables en la primera generación y luego por medio del trabajo en lote en la segunda generación se podía mejorar notoriamente, pues el operador realizaba siempre una secuencia de pasos repetitivos, lo cual es una de las características contempladas en la definición de lo que es un programa. Es decir, se comenzó a ver que las tareas mismas del operador podían plasmarse en un programa, el cual a través del tiempo y por su enorme complejidad se le llamó "Sistema Operativo".

Así, tenemos entre los primeros sistemas operativos al Fortran

Monitor System (FMS) e IBSYS [Tan92]. Posteriormente, en la tercera generación de computadoras nace uno de los primeros sistemas operativos con la filosofía de administrar una familia de computadoras: el OS/360 de IBM. Fue este un proyecto tan novedoso y ambicioso que enfrentó por primera vez una serie de problemas debido a que anteriormente las computadoras eran creadas para dos propósitos en general: el comercial y el científico.

Así, al tratar de crear un solo sistema operativo para computadoras que podían

dedicarse a un propósito, al otro o ambos, puso en evidencia la problemática del trabajo en equipos de análisis, diseño e implantación de sistemas grandes.

El resultado fue un sistema del cual uno de sus mismos diseñadores patentizó su opinión en la portada de un libro: una horda de bestias prehistóricas atascadas en un foso de brea.

Surge también en la tercera generación de computadoras el concepto de la multiprogramación, porque debido al alto costo de las computadoras era necesario idear un esquema de trabajo que mantuviese a la unidad central de procesamiento más tiempo ocupada, así como el encolado (spooling) de trabajos para su lectura hacia los lugares libres de memoria o la escritura de resultados.

Sin embargo, se puede afirmar que los sistemas durante la tercera generación siguieron siendo básicamente sistemas de lote.

En la cuarta generación la electrónica avanza hacia la integración a gran escala, pudiendo crear circuitos con miles de transistores en un centímetro cuadrado de silicón y ya es posible hablar de las computadoras personales y las estaciones de trabajo. Surgen los conceptos de interfaces amigables intentando así atraer al público en general al uso de las computadoras como herramientas cotidianas. Se hacen populares el MS-DOS y UNIX en estas máquinas. También es común encontrar clones de computadoras personales y una multitud de empresas pequeñas ensamblándolas por todo el mundo.

Para mediados de los 80's, comienza el auge de las redes de computadoras y la necesidad de sistemas operativos en red y sistemas operativos distribuidos. La red mundial

Internet se va haciendo accesible a toda clase de instituciones y se comienzan a dar muchas soluciones (y problemas) al querer hacer convivir recursos residentes en computadoras con sistemas operativos diferentes.

Para los 90's el paradigma de la programación orientada a objetos cobra auge, así como el manejo de objetos desde los sistemas operativos. Las aplicaciones intentan crearse para ser ejecutadas en una plataforma específica y poder ver sus resultados en la pantalla o monitor de otra diferente (por ejemplo, ejecutar una simulación en una máquina con UNIX y ver los resultados en otra con DOS).

Los niveles de interacción se van haciendo cada vez más profundos.

3.1 Características de los Sistemas Operativos.

En general, se puede decir que un Sistema Operativo tiene las siguientes características:

- Conveniencia. Un Sistema Operativo hace más conveniente el uso de una computadora.
- Eficiencia. Un Sistema Operativo permite que los recursos de la computadora se usen de la manera más eficiente posible.
- Habilidad para evolucionar. Un Sistema Operativo deberá construirse de manera que permita el desarrollo, prueba o introducción efectiva de nuevas funciones del sistema sin interferir con el servicio.
- Encargado de administrar el hardware. El Sistema Operativo se encarga de manejar de una mejor manera los recursos de la computadora en cuanto a hardware se refiere, esto es, asignar a cada proceso una parte del procesador para poder compartir los recursos.
- Relacionar dispositivos (gestionar a través del kernel). El Sistema Operativo se debe encargar de comunicar a los dispositivos periféricos, cuando el usuario así lo requiera.

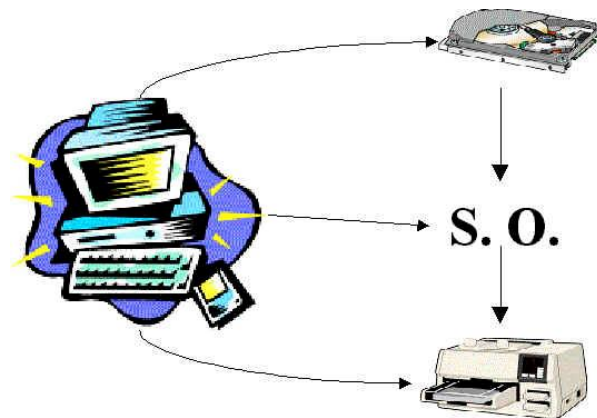


Fig. 3.1 Sistema Operativo.

- Organizar datos para acceso rápido y seguro.
- Manejar las comunicaciones en red. El Sistema Operativo permite al usuario manejar con alta facilidad todo lo referente a la instalación y uso de las redes de computadoras.

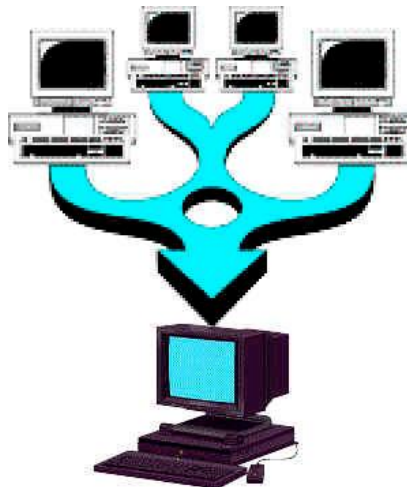


Fig. 3.2 Manejo de re red con un solo sistema operativo.

- Procesamiento por bytes de flujo a través del bus de datos.
- Facilitar las entradas y salidas. Un Sistema Operativo debe hacerle fácil al usuario el acceso y manejo de los dispositivos de Entrada/Salida de la computadora.
- Técnicas de recuperación de errores.
- Evita que otros usuarios interfieran. El Sistema Operativo evita que los usuarios se bloqueen entre ellos, informándoles si esa aplicación está siendo ocupada por otro usuario.
- Generación de estadísticas.
- Permite que se puedan compartir el hardware y los datos entre los usuarios.
- El software de aplicación son programas que se utilizan para diseñar, tal como el procesador de palabras, lenguajes de programación, hojas de cálculo, etc.
- El software de base sirve para interactuar el usuario con la máquina, son un conjunto de programas que facilitan el ambiente plataforma, y permite el diseño del mismo.
- El Software de base está compuesto por:
 - Cargadores.

- Compiladores.
- Ensambladores.
- Macros.

3.2 Sistemas operativos por servicios.

Esta clasificación es la más comúnmente usada y conocida desde el punto de vista del usuario final. Esta clasificación se comprende fácilmente con el cuadro sinóptico que se muestra en la Figura.

Monousuario.

Los sistemas operativos mono usuarios son aquéllos que soportan a un usuario a la vez, sin importar el número de procesadores que tenga la computadora o el número de procesos o tareas que el usuario pueda ejecutar en un mismo instante de tiempo. Las computadoras personales típicamente se han clasificado en este renglón.

Multiusuarios.

Los sistemas operativos multiusuarios son capaces de dar servicio a más de un usuario a la vez, ya sea por medio de varias terminales conectadas a la computadora o por medio de sesiones remotas en una red de comunicaciones. No importa el número de procesadores en la máquina ni el número de procesos que cada usuario puede ejecutar simultáneamente.

Monotareas.

Los sistemas mono tarea son aquellos que sólo permiten una tarea a la vez por usuario. Puede darse el caso de un sistema multiusuario y mono tarea, en el cual se admiten varios usuarios al mismo tiempo pero cada uno de ellos puede estar haciendo solo una tarea a la vez.

Multitareas

Un sistema operativo multitarea es aquél que le permite al usuario estar realizando varias labores al mismo tiempo. Por ejemplo, puede estar editando el código fuente de un programa durante su depuración mientras compila otro programa, a la vez que está recibiendo correo electrónico en un proceso en background. Es común encontrar en ellos interfaces gráficas orientadas al uso de menús y el ratón, lo cual permite un rápido intercambio entre las tareas para el usuario,

mejorando su productividad.

Uniproceto.

Un sistema operativo Uniproceto es aquél que es capaz de manejar solamente un procesador de la computadora, de manera que si la computadora tuviese más de uno le sería inútil. El ejemplo más típico de este tipo de sistemas es el DOS y MacOS.

Multiproceto.

Un sistema operativo multiproceto se refiere al número de procesadores del sistema, que es más de uno y éste es capaz de usarlos todos para distribuir su carga de trabajo. Generalmente estos sistemas trabajan de dos formas: simétrica o asimétricamente. Cuando se trabaja de manera asimétrica, el sistema operativo selecciona a uno de los procesadores el cual jugará el papel de procesador maestro y servirá como pivote para distribuir la carga a los demás procesadores, que reciben el nombre de esclavos. Cuando se trabaja de manera simétrica, los procesos o partes de ellos (threads) son enviados indistintamente a cualesquiera de los procesadores disponibles, teniendo, teóricamente, una mejor distribución y equilibrio en la carga de trabajo bajo este esquema.

Se dice que un "thread" es la parte activa en memoria y corriendo de un proceso, lo cual puede consistir de un área de memoria, un conjunto de registros con valores específicos, la pila y otros valores de contexto. Un aspecto importante a considerar en estos sistemas es la forma de crear aplicaciones para aprovechar los varios procesadores. Existen aplicaciones que fueron hechas para correr en sistemas monoproceso que no toman ninguna ventaja a menos que el sistema operativo o el compilador detecte secciones de código paralelizable, los cuales son ejecutados al mismo tiempo en procesadores diferentes. Por otro lado, el programador puede modificar sus algoritmos y aprovechar por sí mismo esta facilidad, pero esta última opción las más de las veces es costosa en horas hombre y muy tediosa, obligando al programador a ocupar tanto o más tiempo a la paralelización que a elaborar el algoritmo inicial.

Clasificación de los sistemas Operativos

Esta clasificación también se refiere a una visión externa, que en este caso se refiere a la del usuario, el cómo acceder los servicios. Bajo esta clasificación se pueden detectar dos tipos principales: sistemas operativos de red y sistemas operativos distribuidos.

3.3 sistemas operativos de red.

Los sistemas operativos de red se definen como aquellos que tiene la capacidad de interactuar con sistemas operativos en otras computadoras por medio de un medio de transmisión con el objeto de intercambiar información, transferir archivos, ejecutar comandos remotos y un sin fin de otras actividades. El punto crucial de estos sistemas es que el usuario debe saber la sintaxis de un conjunto de comandos o llamadas al sistema para ejecutar estas operaciones, además de la ubicación de los recursos que desee acceder.

Por ejemplo, si un usuario en la computadora hidalgo necesita el archivo matriz.pas que se localiza en el directorio /software/código en la computadora Morelos bajo el sistema operativo UNIX, dicho usuario podría copiarlo a través de la red con los comandos siguientes: hidalgo% hidalgo% rcp morelos:/software/código/matriz.pas . Hidalgo% En este caso, el comando rcp que significa "remote copy" trae el archivo indicado de la computadora Morelos y lo coloca en el directorio donde se ejecutó el mencionado comando. Lo importante es hacer ver que el usuario puede acceder y compartir muchos recursos.

Sistemas operativos distribuidos

Los sistemas operativos distribuidos abarcan los servicios de los de red, logrando integrar recursos (impresoras, unidades de respaldo, memoria, procesos, unidades centrales de proceso) en una sola máquina virtual que el usuario acceder en forma transparente. Es decir, ahora el usuario ya no necesita saber la ubicación de los recursos, sino que los conoce por nombre y simplemente los usa como si todos ellos fuesen locales a su lugar de trabajo habitual.

Todo lo anterior es el marco teórico de lo que se desearía tener como sistema operativo distribuido, pero en la realidad no se ha conseguido crear uno del todo, por la complejidad que suponen: distribuir los procesos en las varias unidades de

procesamiento, reintegrar subresultados, resolver problemas de concurrencia y paralelismo, recuperarse de fallas de algunos recursos distribuidos y consolidar la protección y seguridad entre los diferentes componentes del sistema y los usuarios.

Los avances tecnológicos en las redes de área local y la creación de microprocesadores de 32 y 64 bits lograron que computadoras mas o menos baratas tuvieran el suficiente poder en forma autónoma para desafiar en cierto grado a los mainframes, y a la vez se dio la posibilidad de intercomunicarlas, sugiriendo la oportunidad de partir procesos muy pesados en cálculo en unidades más pequeñas y distribuir las en los varios microprocesadores para luego reunir los sub-resultados, creando así una máquina virtual en la red que exceda en poder a un mainframe.

El sistema integrador de los microprocesadores que hace ver a las varias memorias, procesadores, y todos los demás recursos como una sola entidad en forma transparente se le llama sistema operativo distribuido. Las razones para crear o adoptar sistemas distribuidos se dan por dos razones principales: por necesidad (debido a que los problemas a resolver son inherentemente distribuidos) o porque se desea tener más confiabilidad y disponibilidad de recursos.

En el primer caso tenemos, por ejemplo, el control de los cajeros automáticos en diferentes estados de la república.

Ahí no es posible ni eficiente mantener un control centralizado, es más, no existe capacidad de cómputo y de entrada/salida para dar servicio a los millones de operaciones por minuto. En el segundo caso, supóngase que se tienen en una gran empresa varios grupos de trabajo, cada uno necesita almacenar grandes cantidades de información en disco duro con una alta confiabilidad y disponibilidad.

La solución puede ser que para cada grupo de trabajo se asigne una partición de disco duro en servidores diferentes, de manera que si uno de los servidores falla, no se deje dar el servicio a todos, sino sólo a unos cuantos y, más aún, se podría tener un sistema con discos en espejo (mirror) a través de la red, de manera que si un servidor se cae, el servidor en espejo continúa trabajando y el usuario ni

cuenta se da de estas fallas, es decir, obtiene acceso a recursos en forma transparente.

Ventajas de los sistemas distribuidos.

En general, los sistemas distribuidos (no solamente los sistemas operativos) exhiben algunas ventajas sobre los sistemas centralizados que se describen enseguida.

- **Economía:** El cociente precio/desempeño de la suma del poder de los procesadores separados contra el poder de uno solo centralizado es mejor cuando están distribuidos.
- **Velocidad:** Relacionado con el punto anterior, la velocidad sumada es muy superior.
- **Confiabilidad:** Si una sola máquina falla, el sistema total sigue funcionando.
- **Crecimiento:** El poder total del sistema puede irse incrementando al añadir pequeños sistemas, lo cual es mucho más difícil en un sistema centralizado y caro.
- **Distribución:** Algunas aplicaciones requieren de por sí una distribución física.
- Por otro lado, los sistemas distribuidos también exhiben algunas ventajas sobre sistemas aislados.
- Estas ventajas son:
- **Compartir datos:** Un sistema distribuido permite compartir datos más fácilmente que los sistemas aislados, que tendrían que duplicarlos en cada nodo para lograrlo.
- **Compartir dispositivos:** Un sistema distribuido permite acceder dispositivos desde cualquier nodo en forma transparente, lo cual es imposible con los sistemas aislados. El sistema distribuido logra un efecto sinérgico.
- **Comunicaciones:** La comunicación persona a persona es factible en los sistemas distribuidos, en los sistemas aislados no. _ **Flexibilidad:** La distribución de las cargas de trabajo es factible en los sistemas distribuidos, se puede incrementar el poder de cómputo.

Desventajas de los sistemas distribuidos.

Así como los sistemas distribuidos exhiben grandes ventajas, también se pueden identificar algunas desventajas, algunas de ellas tan serias que han frenado la producción comercial de sistemas operativos en la actualidad. El problema más importante en la creación de sistemas distribuidos es el software: los problemas de compartición de datos y recursos es tan complejo que los mecanismos de solución generan mucha sobrecarga al sistema haciéndolo ineficiente.

El verificar, por ejemplo, quiénes tienen acceso a algunos recursos y quiénes no, el aplicar los mecanismos de protección y registro de permisos consume demasiados recursos. En general, las soluciones presentes para estos problemas están aún en pañales.

Otros problemas de los sistemas operativos distribuidos surgen debido a la concurrencia y al paralelismo.

Tradicionalmente las aplicaciones son creadas para computadoras que ejecutan secuencialmente, de manera que el identificar secciones de código 'paralelizables' es un trabajo arduo, pero necesario para dividir un proceso grande en subprocesos y enviarlos a diferentes unidades de procesamiento para lograr la distribución.

Con la concurrencia se deben implantar mecanismos para evitar las condiciones de competencia, las postergaciones indefinidas, el ocupar un recurso y estar esperando otro, las condiciones de espera circulares y, finalmente, los "abrazos mortales" (deadlocks). Estos problemas de por sí se presentan en los sistemas operativos multiusuarios o multitareas, y su tratamiento en los sistemas distribuidos es aún más complejo, y por lo tanto, necesitará de algoritmos más complejos con la inherente sobrecarga esperada.

Por otro lado, en el tema de sistemas distribuidos existen varios conceptos importantes referentes al hardware que no se ven en este trabajo: multi computadoras, multiprocesadores, sistemas acoplados débil y fuertemente, etc.

Principales sistemas operativos en el mercado.

Los sistemas operativos empleados normalmente son UNIX, Macintosh OS, MS-DOS, OS/2, Windows y Windows NT.

MS-DOS.

El significado de estas letras es el de Microsoft Disk Operating System. Microsoft es el nombre de la compañía que diseñó este sistema operativo, e IBM la compañía que lo hizo estándar al adoptarlo en sus microordenadores. Fue el primer sistema operativo de las Pc's y está orientado a modo texto y comandos.

Los nombres de los ficheros en MS-DOS, para los que se emplean tanto letras como números, se componen de dos partes: el nombre del fichero y la extensión, estando ambos datos separados por un punto. Las diferentes unidades de disco son identificadas por el MS-DOS a través de una letra seguida de dos puntos. Los tipos de extensión más habituales son como aparecería la memoria cargada con ellos; es decir, que pueden cargar directamente a memoria sin el auxilio del sistema operativo

Los de extensión .EXE precisan que el cargador del DOS los coloque en memoria, lo que significa que el sistema operativo debe estar en memoria. Los del tipo .BAT son los compuestos de comandos que se ejecutan secuencialmente.

MS-DOS está lejos de ser el sistema operativo ideal, ya que, de momento, se trata de un sistema monotarea, pero aunque esto se resolviera, seguiría presentando problemas de diseño que provocan que el comportamiento de la máquina sea poco fiable. A pesar de estas desventajas y de que existen otros sistemas operativos en el mundo de la microinformática, hay que tener siempre presente la enorme cantidad de software que se ha desarrollado para DOS y que conviene aprovechar en lo posible.

OS/2.

Desarrollado inicialmente por Microsoft Corporation e International Business Machines (IBM), después de que Intel introdujera al mercado su procesador 80286. Pero la sociedad no duró mucho ya que IBM veía a Windows como una amenaza para el OS/2. Pero IBM continuó desarrollando este sistema operativo. El OS/2 al principio fue muy parecido al MS-DOS, tiene una línea de comando, pero la diferencia que existe con el DOS es el intérprete de comandos, el cual es

un programa separado del kernel del sistema operativo y aparece únicamente cuando se hace clic en uno de los iconos "OS/2 prompt" dentro del Workplace Shell. Otra diferencia es que este sí es un sistema operativo multitarea.

En el OS/2 muchos de los comandos son idénticos a los de su contra parte pero tiene más comandos debido a que es más grande, completo y moderno.

El ambiente gráfico es el Workplace Shell (WS), es el equivalente a un administrador del área de trabajo para el WS.

MACINTOSH OS.

El sistema operativo constituye la interfaz entre las aplicaciones y el hardware del Macintosh. El administrador de memoria obtiene y libera memoria en forma automática para las aplicaciones y el sistema operativo. Esta memoria se encuentra normalmente en un área llamada cúmulo. El código de procedimientos de una aplicación también ocupa espacio en el cúmulo.

Ahora se presenta una lista de los principales componentes del sistema operativo.

- El cargador de segmentos carga los programas por ejecutar. Una aplicación se puede cargar completa o bien puede dividirse en segmentos individuales que se pueden cargar de manera dinámica conforme se necesiten.
- El administrador de eventos del sistema operativo informa de la ocurrencia de diversos eventos de bajo nivel, como la presión de un botón del mouse o el tecleo. En condiciones normales, el administrador de eventos de la caja de herramientas transfiere estos eventos a las aplicaciones.
- El administrador de archivos se encarga de la entrada / salida de archivos; el administrador de dispositivos se encarga de la entrada / salida de dispositivos.
- Con el manejador de impresoras las aplicaciones pueden imprimir datos en diversas impresoras.
- Con el administrador de AppleTalk las aplicaciones pueden transmitir y recibir información en una red de comunicaciones AppleTalk.
- El manejador de errores del sistema toma el control cuando ocurre un error fatal del sistema y exhibe un cuadro de error apropiado.
- Los manejadores de dispositivos son programas con los cuales los diversos

tipos de dispositivos pueden presentar interfaces uniformes de entrada / salida a las aplicaciones. Tres manejadores de dispositivo están integrados al sistema operativo en ROM: el manejador de disco se encarga del acceso a la información en discos, el manejador de sonido controla los generadores de sonido, y el manejador en serie envía y recibe datos a través de los puertos seriales (estableciendo así la comunicación con dispositivos periféricos en serie como impresoras y módems).

- El Administrador de retrasado vertical programa las actividades por realizar durante las interrupciones de retrasado vertical que ocurren 60 veces cada segundo cuando se refresca la pantalla de vídeo.
- Los programas de utilidad general del sistema operativo ofrecen diversas funciones útiles como la obtención de la fecha y la hora, la comparación de cadenas de caracteres y muchas más.
- El paquete de iniciación es llamado por el paquete de archivos estándar para iniciar y nombrar discos; se aplica con más frecuencia cuando el usuario inserta un disco al que no se le han asignado valores iniciales.
- El paquete de aritmética de punto flotante ofrece aritmética de doble precisión. El paquete defunciones trascendentales ofrece un generador de números aleatorios, así como funciones trigonométricas, logarítmicas, exponenciales y financieras. Los compiladores de Macintosh generan en forma automática llamadas a estos paquetes para realizar manipulaciones numéricas.

UNIX.

Es un sistema operativo multiusuario que incorpora multitarea. Fue desarrollado originalmente por Ken Thompson y Dennis Ritchie en los laboratorios de AT&T Bell en 1969 para su uso en minicomputadoras. El sistema operativo UNIX tiene diversas variantes y se considera potente, más transportable e independiente de equipos concretos que otros sistemas operativos porque esta escrito en lenguaje C.

El UNIX está disponible en varias formas, entre las que se cuenta AIX, una versión de UNIX adaptada por IBM (para su uso en estaciones de trabajo basadas en

RISC), A/ux (versión gráfica para equipos Apple Macintosh) y Mach (un sistema operativo reescrito, pero esencialmente compatible con UNIX, para las computadoras NeXT).

El UNIX y sus clones permiten múltiples tareas y múltiples usuarios. Su sistema de archivos proporciona un método sencillo de organizar archivos y permite la protección de archivos. Sin embargo, las instrucciones del UNIX no son intuitivas. Este sistema ofrece una serie de utilidades muy interesantes, como las siguientes:

- Inclusión de compiladores e intérpretes de lenguaje.
- Existencia de programas de interfaz con el usuario, como ventanas, menús, etc.
- Muchas facilidades a la hora de organización de ficheros.
- Inclusión de lenguajes de interrogación.
- Facilidades gráficas.
- Programas de edición de textos.

MICROSOFT WINDOWS NT.

Microsoft no solo se ha dedicado a escribir software para PCs de escritorio sino también para poderosas estaciones de trabajo y servidores de red y bases de datos. El sistema operativo Windows NT de Microsoft, lanzado al mercado el 24 de Mayo de 1993, es un SO para redes que brinda poder, velocidad y nuevas características; además de las características tradicionales. Es un SO de 32 bits, y que puede trabajar en procesadores 386, 486 y Pentium.

Además de ser multitarea, multilectura y multiprocesador ofrece una interfaz gráfica. Y trae todo el software necesario para trabajar en redes, permitiendo ser un cliente de la red o un servidor.

MICROSOFT WINDOWS.

Este SO está basado en menús desplegados, ventanas en pantalla y un dispositivo señalador llamado mouse. Una de las características principales de Windows 95 y posteriores es que los nombres de los archivos no están restringidos a ocho caracteres y tres de la extensión, pueden tener hasta 256 caracteres para tener una descripción completa del contenido del archivo.

Además posee Plug and Play, una tecnología conjuntamente desarrollada por los

fabricantes de PCs, con la cual un usuario puede fácilmente instalar o conectar dispositivos permitiendo al sistema automáticamente alojar los recursos del hardware sin la intervención de usuario.

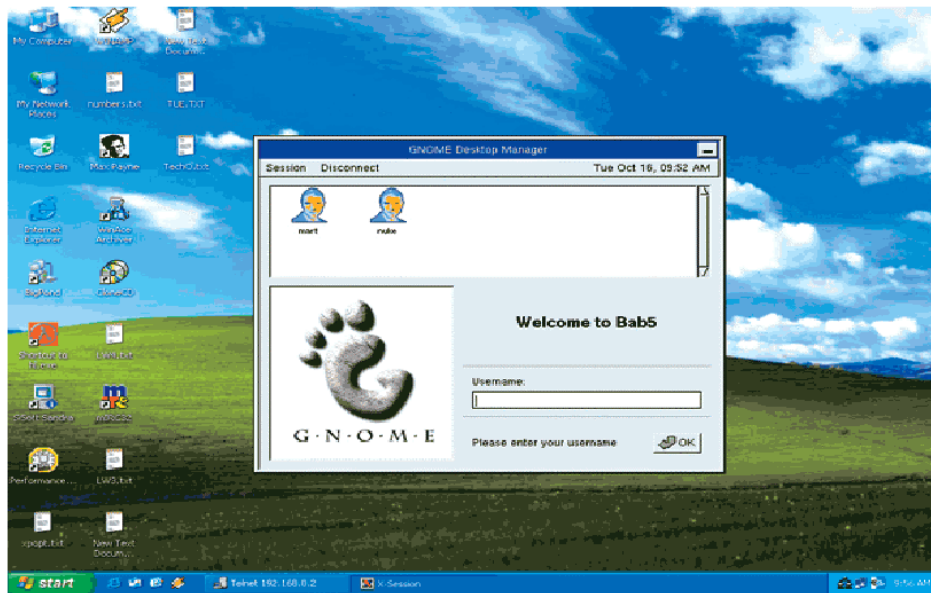


Fig. 3.3 Sistema operativo abierto.

Características de los sistemas abiertos.

Los sistemas abiertos se han caracterizado por tener la disponibilidad del código de programación, para que esté pueda ser modificado y personalizado de acuerdo a las necesidades particulares de un usuario ó inclusive para mejorar su potencialidad. Esta facilidad ha resultado muy atractiva para personas aficionadas a la informática y programación, ya que les permite poner en reto sus conocimientos y de esta forma poder desarrollar nuevas herramientas de trabajo, cabe mencionar también que esto ha originado el crecimiento de usuarios de red denominados hackers, quienes tienen la afición de explorar y conocer sistemas.

Entre los sistemas operativos abiertos más difundidos y populares se encuentra UNIX y LINUX. El código fuente del sistema UNIX, y no el código ejecutable, ha estado disponible a usuarios y programadores. A causa de esto mucha gente ha sido capaz de adaptar el sistema UNIX de firmas diferentes.

Este carácter abierto ha conducido a la introducción de un amplio rango de características nuevas y de versiones personalizadas que se ajustan a

necesidades especiales.

A las personas que han desarrollado esta adaptación del sistema UNIX les ha resultado fácil porque el código correspondiente es sencillo modular, y compacto. Esto ha fomentado la evolución del sistema UNIX, haciendo posible la fusión de las capacidades desarrolladas por diferentes variables del sistema UNIX, necesarias para soportar los entornos de computación de hoy en un sistema operativo único, el UNIX Sistema V Versión 4.

3.4 La integración de servicios.

Desde hace algunos años la tecnología de las comunicaciones a evolucionado a pasos agigantados, Se puede apreciar la evolución en el crecimiento la capacidad de interacción de los distintos medios de comunicación con los usuarios.

Cuando surgió el telégrafo, la interpretación de la información era realizada por el usuario, dando un sentido al mensaje codificado que se recibía o enviaba.

El teletipo realiza esta codificación de manera automática, aunque la interpretación no era del todo buena, era una mejora en la comunicación de ideas.

Cuando surge el teléfono se convierte en uno de los medios universales de comunicación dado que hace posible la compartición de ideas de manera casi directa entre las personas usando el lenguaje, sin embargo, la necesidad de la comunicación escrita a larga distancia es aun más antigua y, la necesidad de compartir información no solo a través de la palabra hablada ha trascendido hasta hoy.

Multimedia.

Con la introducción de las redes de datos, esta necesidad se fue solventando, y abrió la puerta a nuevos horizontes como la compartición de archivos y programas, no obstante, se tiene la visión de llegar a un modelo de comunicación más rápido, más barato, totalmente ubicuo, además cada vez más simple y fácil de usar.

El salto a la comunicación gráfica a partir del texto, una vez más cambia la forma en cómo se percibe el mundo del computo y las comunicaciones e impacta fuertemente los diferentes entes cotidianos donde tiene influencia.

Todos estos antecedentes marcan la tendencia hacia la integración de cada vez mas servicios más sofisticados y potentes, que tratan de aprovechar todo lo que ya existe o adecuándose con muy pocos cambios pero ofreciendo más capacidad y flexibilidad.

Los sistemas de televisión evolucionan al integrar la voz y la imagen como un sistema de comunicación unidireccional, lo cual lo hizo, junto con la radiodifusión, los sistemas de entretenimiento por excelencia en los hogares desde su creación, posteriormente los sistemas de televisión por cable, conjuntan estos servicios en un solo medio de comunicación, ahora la computadora personal pretende abarcar todos estos sistemas en una sola entidad que maneja todos los medios de manera simultánea, surge el concepto **multimedia**.

Tendencias.

Actualmente existen diversas tecnologías para transportar información, ya sea voz datos o Vídeo, a partir de que una señal es digitalizada y convertida en términos de unos y ceros, prácticamente es posible hacer lo que sea con dicha señal, luego entonces, las tecnologías se adaptan al tipo de trafico que se va a enviar o recibir, permitiendo así el transporte de información, multimedia.

Por otro lado, los equipos y programas terminales o de usuario final también han evolucionado rápidamente, planteando nuevas propuestas tecnológicas para aplicaciones que pueden ser soportadas por las tecnologías existentes. Resultado de todo esto es la tendencia a que se tengan diversos equipos y/o programas terminales para diversos tipos de servicios de comunicación que puedan hacer uso de una o varias tecnologías de transporte de información, es decir, la convergencia tecnológica.

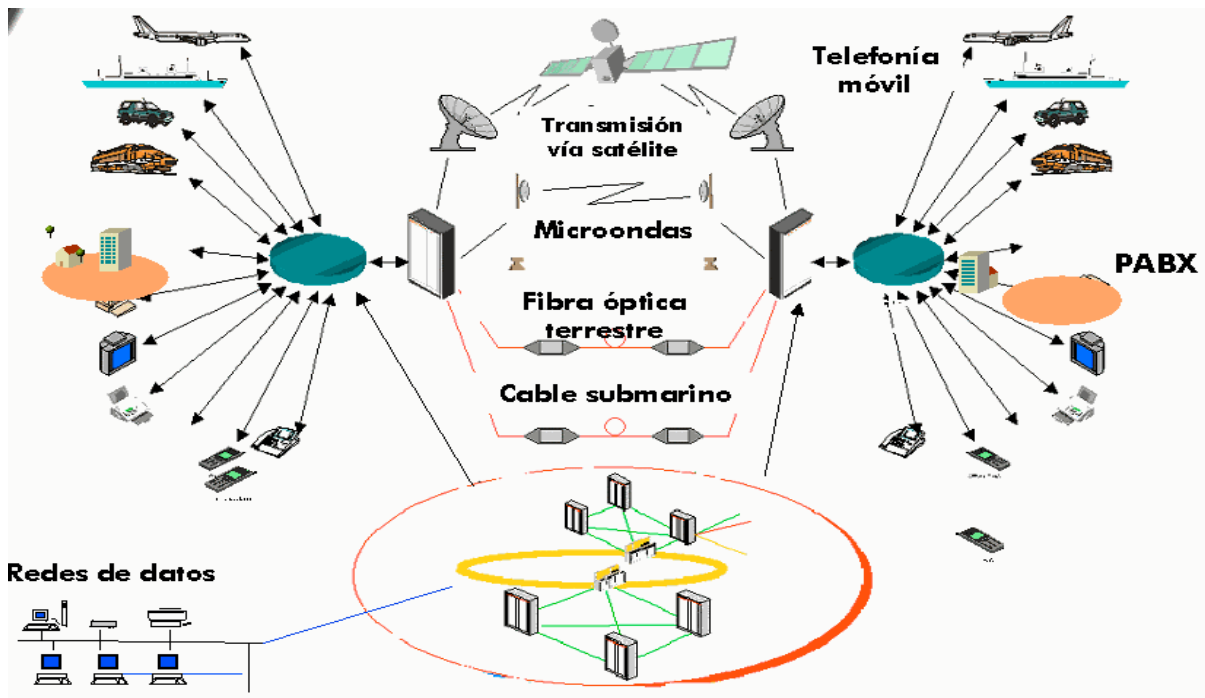


Fig. 3.4 Integración total de servicios.

Ejemplos de aplicaciones de convergencia.

Vamos ahora a conocer algunas de las aplicaciones que se encuentran disponibles en el mercado que hacen uso de la convergencia tecnológica.

Voz sobre IP.

A partir de las redes de datos surge un concepto interesante para transmitir voz sobre una red de datos, con la aparición de Internet la idea se extiende a la larga distancia.

El concepto de voz sobre IP es simple, dada una aplicación que transforma la voz en información de datos, estos pueden ser manipulados de la misma forma que cualquier paquete o datagrama de datos dentro de una red de computadoras, esto hace posible empaquetarlo y enviarlo de la misma forma que se hace con los datos a través de la red LAN o incluso a través de Internet, en el nodo receptor la voz en forma de paquetes es desempaquetada y procesada para devolver la comunicación de voz al receptor.

El soporte de estas características sobre redes tan grandes como Internet, que

además ofrece alcance mundial, ha posicionado esta tecnología como una de las principales opciones para abatir costos en llamadas de larga distancia.

Voz sobre Ethernet.

Las redes de datos están bastante extendidas alrededor del mundo, las redes telefónicas son más antiguas que las redes de datos, sin embargo, cuando se tiene un proyecto nuevo en telecomunicaciones, de voz y datos para oficinas corporativas, es posible implementar servicios de voz y datos sobre la infraestructura de cableado de datos y utilizando las tecnologías de transmisión LAN tal es el caso de Ethernet y sus primos Fast Ethernet y Gigabit.

Existe equipo y facilidades que permiten prescindir de los servicios de un conmutador telefónico mediano, esta tecnología es propietaria de 3Com, y tiene la facilidad de integrar servicios de comunicación de voz con todos los valores agregados de un conmutador digital, con la diferencia de que la información de voz se trasmite por la infraestructura de datos a través de la red.

Las funciones digitales de los teléfonos están integradas (llamadas en espera, conferencia, caller ID.) además de permitir integración con la computadora con aplicaciones de tipo CTI con programas estándares para correo de voz, integración de agenda telefónica con productos de Microsoft o Lotus Notes o cualquier aplicación estándar H.323 del mercado. Más allá de la comunicación local, permite integrarse con aplicaciones de voz sobre IP para hacer llamadas por canales de datos hacia oficinas remotas.

En general es una interesante aplicación de Convergencia tecnológica.

Videoconferencia.

En principio la Televisión como medio de comunicación unidireccional fue implementado en los servicios de educación para impartir clases a distancia, una de las principales desventajas de este sistema es su característica unidireccional, donde no puede haber retroalimentación simultánea por parte de los participantes, Sin embargo la amplia difusión que tiene la televisión además de su poder de penetración en las comunidades, lo hace atractivo para tratar de explotar nuevas capacidades.

Una vez más con la digitalización de la información para su proceso y

transporte, se da oportunidad a los sistemas para transmitir Vídeo digitalizado a través de una infraestructura de transporte que puede llevar voz, datos y Vídeo.

Un sistema de videoconferencia permite la comunicación entre dos o más entidades, cada una de ellas tiene una o varias cámaras de Vídeo, y receptores de Vídeo, además de micrófonos y equipos de computo.

La señal de Vídeo que toma la cámara es procesada en una unidad especial, y es preparada para enviarse a través de alguna tecnología de transporte hacia las entidades remotas, donde se recibe la imagen y el audio con poco retardo y buena calidad de imagen.

Dentro de las aplicaciones más comunes de la videoconferencia están la educación a distancia a todos los niveles, la telemedicina y las juntas virtuales.

Vídeo sobre demanda.

Cuando se encuentra uno de viaje, es común hospedarse en hoteles que tienen servicios de “cine a la carta” es decir, se solicita el servicio y se escoge la película que se desea ver, una vez activado el servicio, la película iniciara en el momento que el huésped lo desee.

Esto es factible gracias a que es posible digitalizar y almacenar grandes cantidades de información como las que compondrían una película con audio y Vídeo de calidad digital, esta información es almacenada en equipos llamados servidores de alto rendimiento, los cuales proporcionan los archivos con las películas a todos los huéspedes que soliciten el servicio, los servidores envían copias de los archivos hacia los cuartos de los huéspedes a través de una infraestructura de comunicaciones con tecnología de alta velocidad, la información es presentada en pantalla para deleite del huésped, más de un huésped puede estar viendo la misma película simultáneamente, sin embargo, la secuencia en la película para cada uno de los espectadores no es simultanea, pues cada huésped inicia la película en el momento que desee.

Videoconferencia al escritorio.

El concepto de videoconferencia inicialmente estaba orientado a equipos que se usaban en salas o auditorios acondicionados para este fin, con la idea de optimizar recursos dados que el equipo y la tecnología de servicio no era barata.

Conforme la tecnología avanza, se observa una tendencia a la disminución de costos y las mejoras continuas, ahora es posible llevar esta funcionalidad al escritorio usando como equipo terminal un equipo PC, con capacidades multimedia, depende del fabricante y el modelo, sin embargo estos equipos permiten la interconexión de varios usuarios en la conferencia y a veces con capacidades de interconexión a través de redes de área amplia y con edición de documentos en línea.

3.5 Características de las redes multiservicio.

Una red de multiservicio es un conjunto de dispositivos de comunicaciones que transportan, y dan acceso a múltiples tipos de servicios de comunicaciones en diversos formatos.

En un inicio, los servicios de comunicación se basan en diferentes técnicas y tecnologías de comunicación, cada una adecuada a sustentar el tipo de necesidades que cada servicio necesitaba, ahora, las redes multiservicio son el resultado de una evolución tecnológica hacia una infraestructura de transporte de información lo suficientemente flexible como para adaptarse a los diferentes requerimientos que cada tipo de tráfico de información necesita solventar sin degradar la calidad del servicio, estas redes pueden transportar y dar acceso a diversos tipos de tráfico y soportar diversos servicios simultáneos ya sea entre dos o más entidades.



Fig. 3.5 Redes Multiservicio.

Dentro de las redes de comunicaciones podemos encontrar 3 subsistemas en los cuales se descomponen:

Sistemas Core.

Son los equipos e infraestructura que proporcionan el núcleo central de la red, aquí se encuentran los equipos que hacen el trabajo de proceso y administración de la comunicación, dichos equipos tienen capacidades muy elevadas.

En los sistemas de voz, estos equipos son las centrales telefónicas, en los Sistemas core datos, se encuentran Switches de alta capacidad. Con la convergencia tecnológica, los sistemas core se interconectan a través de tecnologías de transporte que pueden manejar cualquier tipo de tráfico en alta velocidad y de manera simultánea, tal es el caso de Jerarquías digitales como SDH.

Sistemas de acceso.

Son las tecnologías que permiten conectar los equipos terminales del usuario hacia las redes de transporte, aquí es donde existe una gran variedad de tecnologías, algunas proporcionan características novedosas otras solo se adaptan a la infraestructura de transporte y los equipos del usuario.

Aquí se encuentran la red telefónica, la red de datos, la red de televisión por cable, el sistema de difusión de radio y televisión, la red satelital, la red eléctrica etc.

Cada red tiene sus propias características, la tendencia tecnológica es aprovechar estas redes ya instaladas con mucho tiempo de antigüedad, por lo que las tecnologías nuevas pretenden adaptarse a los medios de acceso ya existentes, sin embargo, hay surgimiento de nuevas tecnologías, en todos los casos la fuerza del cambio se está dando en las aplicaciones del usuario, los equipos terminales del usuario, los medios de acceso al usuario, las tecnologías de acceso y las de transporte.

Sistemas de usuario.

Se vislumbra el equipo de cómputo personal como el sistema universal de control y comunicación por excelencia para el hogar y la oficina, además de que el modelo de comunicación ubicua apunta hacia la computación móvil y la integración de comunicación celular o satelital con servicios integrados de tipo multimedia. Para el usuario final, existe una amplia gama de productos que ofrecen paquetes de servicios, el detalle de elegir hoy por hoy uno u otro es la tendencia, hay equipos que brindan diversos tipos de servicios sin embargo la garantía de que la tecnología que utilizan pudiera llegar a ser predominante en el mercado muchas veces esta fuera del control del usuario, o de los fabricantes e incluso de la misma tecnología, es una combinación de factores.

3.6. Integración de redes corporativas.**Intranet**

Las Intranets son redes privadas que se han creado utilizando las normas y protocolos de Internet. Aportan la interfaz de exploración intuitiva del World Wide Web a la información y servicios almacenados en una red de área local (LAN) corporativa. Las Intranets son atractivas porque disminuyen el costo de

mantenimiento de una red interna y, al mismo tiempo, aumentan la productividad, ya que ofrecen a los usuarios un acceso más eficaz a la información y a los servicios que necesitan.

Aunque el atractivo de las Intranets es evidente, el proceso de instalación no lo es tanto. Algunas organizaciones adoptan el mismo sistema para crear su Web interno que el utilizado para crear el sitio de Internet externo.

Contratan proveedores y diseñadores externos que normalmente se centran en los gráficos, los valores de producción y las últimas tecnologías más populares. Este método puede costar mucho dinero, pero no produce necesariamente una red que se ajuste a las necesidades de una organización.

Un modo rápido y sencillo de empezar.

Una alternativa es comenzar con algo pequeño, con Web locales creadas y mantenidas por equipos y departamentos. Estas sencillas Intranets ofrecen un valor real mejorando la información compartida con costos de configuración y administración relativamente bajos.

Una Intranet sencilla permite a los equipos o departamentos aprovechar el método de exploración intuitivo del Web para buscar y compartir información de forma más eficaz. A diferencia de las soluciones de Intranet más sofisticadas, las Intranets sencillas son muy específicas en su propósito e instalación.

Una Intranet sencilla permite a las organizaciones aprovechar las ventajas de las Intranets a nivel de equipo o de departamento, utilizando tecnologías actuales o fáciles de adquirir. Estas Intranets populares ofrecen sus propias ventajas y son el primer paso para desarrollar una Intranet más completa.

Compartir mejor la información

La principal ventaja de una Intranet es que permite compartir mejor la información. En una organización moderna, el acceso a la información es crucial. Una Intranet proporciona una administración más intuitiva de la información.

El método Web ofrece algunas mejoras respecto a modelos anteriores de administración de la información:

- Vinculación entre documentos.
- Búsqueda fácil.
- Punto de entrada común a toda la información.

- Poca inversión inicial.

Sin una planificación cuidadosa, las ventajas de una Intranet pueden verse ensombrecidas por su costo. Una Intranet sencilla permite a un equipo o departamento aprovechar las ventajas de compartir mejor la información que ofrece el método Web con una inversión gradual relativamente baja, utilizando el hardware y el software existente. Las organizaciones que dispongan de una red LAN y utilicen Office, u otra aplicación como:

Lotus, Corel, Star Office, etc. pueden crear una Intranet sencilla con un costo gradual muy pequeño.

Debido a que las Intranets están limitadas en tamaño y en ámbito por definición, no se producen muchos de los problemas asociados a soluciones de Intranet más sofisticadas: servidores de seguridad, desarrollo de aplicación personalizada, integración de sistemas de herencia. Esto ayuda a mantener un bajo costo de inversión inicial, así como de administración y soporte técnico.

Primer paso al futuro.

Muchas organizaciones configuran Intranets sencillas como primer paso hacia el desarrollo de Intranets más sofisticadas. Una Intranet local de un departamento determinado puede ampliarse y mejorarse para crear una Intranet centralizada para toda una organización.

Opcionalmente, varios Web departamentales pueden administrarse de forma centralizada para crear un Web mayor.

Las organizaciones también se benefician del aprendizaje que se realiza cuando un grupo comienza a utilizar una

Intranet sencilla. Los colaboradores se acostumbran a utilizar la Intranet para compartir información sencilla e incorporarla a su trabajo diario. La utilización de Intranets sencillas permite a las organizaciones obtener una información que aumenta la eficacia de las soluciones de mayor nivel.

El valor de una Intranet depende de que el contenido esté actualizado y sea relevante. Los usuarios necesitan un medio de publicar el contenido en el Web y de obtener acceso a la información una vez publicada. Dado que una Intranet es esencialmente un conjunto de archivos almacenado en un servidor, publicar el contenido es guardar un documento en el servidor. Cada usuario debe disponer de

una carpeta designada para guardar documentos.

El administrador de la Intranet proporciona el nivel de exploración que ayuda a los demás a encontrar la información que necesitan, creando hipervínculos a documentos de prioridad alta o agrupando conjuntos de documentos de una de las siguientes formas:

- Por persona.
- Por asunto.
- Por búsqueda.

Extranet.

Primero fue Internet, la red global de acceso universal en la que todos los contenidos estaban al alcance de todos los usuarios. Luego surgieron las Intranets, que son espacios virtuales reducidos y protegidos de la vista de curiosos y competidores por "muros de fuego" (firewalls), que impiden el acceso a todos aquellos que no pertenecen a la red corporativa. Ultimamente se oye hablar más de las extranets que se perfilan como el nuevo concepto de comunicación (de canal) en tiempo real.

Las empresas han mirado hacia atrás y se han dado cuenta de que sus colaboradores, sus socios e incluso sus clientes se quedaban fuera de esos muros, más allá de los datos esenciales para establecer una relación fluida y continua. Poniendo remedio a esto surge la Extranet: como último golpe en el mundo de la red. La Extranet viene a convertirse en el paso intermedio entre la total apertura de Internet y el hermetismo obligado de las Intranets corporativas.

Un sistema de acceso restringido que permite a las empresas, los clientes y el canal, eliminar limitaciones en sus relaciones y comunicarse en tiempo real. Solo los competidores quedan al otro lado de las barreras.

Más que un nuevo concepto de moda

¿Son las Extranets una palabra de moda que no responden a ningún concepto real? Etimológicamente parecen una redundancia, ya que antepone un sufijo como "extra" (fuera en griego) a lo que en esencia es un sistema de comunicación remota sobre la plataforma de comunicación más abierta que ha conocido la humanidad: Internet.

Según Jim Barksdale, Presidente de Netscape y que acuñó el término extranet, indica que este concepto responde a algo más que a una palabra de moda. "Las compañías construyen Intranets de acceso restringido protegidas por Firewalls, pero no pueden estar seguras sobre quién deberá tener acceso a esas aplicaciones dentro de cinco años y por ello deben esforzarse al máximo para construirlas de modo que garanticen la máxima conectividad y siempre sobre Internet. Pero, bajo esta arquitectura, nos preguntamos: ¿qué pasa con los partners, los usuarios, los clientes y los proveedores que se han quedado al otro lado de las Firewalls? ¿Qué hay del acceso de los empleados que están fuera del departamento original que diseñó el sistema?"

Por eso como suma a las redes internas de las compañías o Intranets, que están detrás de los Firewalls, las compañías no tienen otra solución que diseñar redes externas llamadas "Extranets" que recojan a aquellos que trabajan físicamente fuera de los muros de seguridad pero son una parte importante de la estrategia de negocio, el sistema de entrega de producción o el aparato de soporte al cliente".

Bajo este contexto, una Extranet es una forma de establecer formulas de acceso a una Intranet corporativa a determinadas personas y entidades ajenas a la empresa propiamente dicha, pero laboral, comercial o financieramente relacionadas con ella. Es una forma de comunicación entre webs y por tanto entre entidades diferentes y a diferentes niveles de acceso.

Evidentemente, todo este entramado de comunicación y transmisión de datos exige privacidad y seguridad.

Mantener todo este flujo sobre una plataforma como

Internet exige garantías extremas de que no son posibles las filtraciones, al menos en volúmenes masivos. Como medida de salvaguardar el conocimiento de una empresa se recurrió a una solución positiva. Esto es, en lugar de crear formulas de denegar el acceso se idearon maneras de permitirlo. Así los desarrolladores crearon unas barreras que tiene un nombre tan sonoro como representativo. Nos referimos a los Firewalls (muros de fuego).

Redes privadas virtuales

¿Qué es una red privada virtual (VPN)?

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. Las firewalls o ambos sitios permiten una conexión segura a través de Internet. Las VPNs son una alternativa de costo útil, para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegiendo la información y los passwords.

La tecnología de VPN proporciona un medio para usar el canal público de Internet como una canal apropiada para comunicar los datos privados.

Con las tecnologías de inscripción y encapsulado, una VPN básica, crea un pasillo privado a través de Internet.

Instalando VPNs, se reducen las necesidades de gestión de una red local.

¿Cómo trabaja la tecnología de túneles de una Red Privada Virtual? Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos.

La tecnología de túneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulado", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado

"encapsulado", ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

Una VPN habilita a usuarios de negocios el intercambio de información en forma segura sobre redes privadas y públicas. Esto es una solución segura y efectiva para la expansión de redes a nivel de oficinas sucursales, socios de negocio y usuarios remotos que accesan a Internet.

La seguridad de las VPNs proviene de la confiabilidad e integridad en la información. Si la información es intervenida, esta es encriptado y no puede ser leída. Esto asegura que los datos no han sido modificados en el transporté.

El control de acceso a la red es provisto, previniendo que gente que acceso a la red y traté de robar recursos o atacar la seguridad, sea detectada.

En una VPN, las comunicaciones de red son protegidas por un protocolo de seguridad. El protocolo de red es responsable de la capa de comunicación y de la información entre aplicaciones y sistemas a través de una infraestructura física de red.

3.7 los ISP'S y la industria de internet.

Una vez que se haya decidido establecer un sitio en la Red Mundial, necesitará decidir dónde albergarlos. Sus archivos de la página Web serán albergados en una computadora anfitriona (servidor Web) conectada a la

Internet las 24 horas del día. Este servidor puede ser una computadora ubicada en su casa, en su oficina, o puede usar uno de los crecientes proveedores de servicios de Internet que ofrecen servicios de albergue de sitios Web (Hosting).

Ellos se encargan de los detalles técnicos, lo que le permite concentrarse en el desarrollo del contenido. De cualquier modo, hay que tomar en cuenta los pros y los contras.

Definición de un ISP.

Un proveedor de servicio Internet (Internet Service Provider), en el sentido amplio es una compañía que comercializa servicios de acceso (conexión) a Internet a terceros, ya sea usuarios residenciales o usuarios corporativos, e inclusive a otros ISP.

Dependiendo de su tamaño y cobertura geográfica, a menudo los ISP se clasifican en: Proveedores de Servicios de Internet, ISP, los cuales proporcionan el servicio de acceso a usuarios finales; y Proveedores de Servicio de Red, NSP, los cuales cuentan con su propia infraestructura de Telecomunicaciones y proporcionan servicios de red a los ISP.

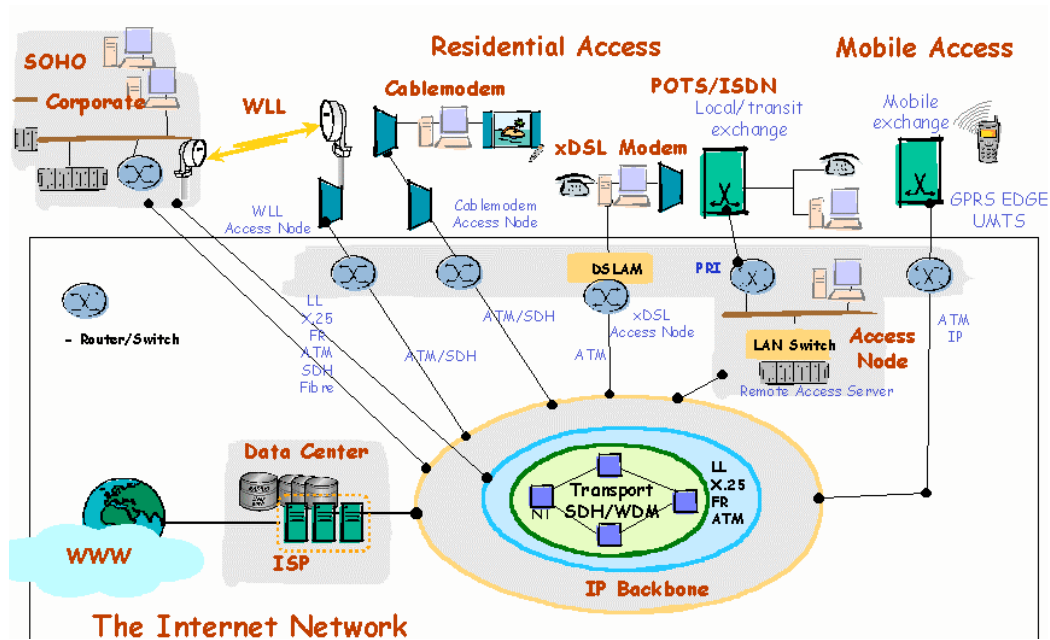


Fig. 3.6 Los ISP'S y la industria del Internet.

Que ofrece un ISP

Un Proveedor Internet nos permite conectar nuestra computadora a la Red Internet. No podemos conectarlo directamente, puesto que las líneas de comunicaciones que forman Internet en sí, sólo las pueden manejar las grandes empresas de telecomunicaciones a nivel Mundial.

Los Proveedores conectan a muchos usuarios (normalmente varios miles de ellos por proveedor) a estas grandes líneas de telecomunicaciones. Como tienen tantos clientes, pueden permitirse el lujo de negociar las conexiones a Internet con las grandes empresas de telecomunicaciones. Aparte de esta principal funcionalidad, los Proveedores también ofrecen otros servicios: instrucciones de instalación de la conexión, ayuda telefónica, archivos de datos y programas, servicios de conversación, tramites de asignación de nombres de dominio, Servidor de correo electrónico, consultoría, Hospedaje de tiendas virtuales, redes virtuales corporativas, etc.

Últimamente, algunos Proveedores están ofreciendo con el costo de la conexión, el módem e incluso una segunda línea de teléfono para nuestra casa, para evitar

ocupar el teléfono cuando nos conectamos a la Red.

En principio las conexiones que nos vende nuestro proveedor son privadas. Para que nadie pueda acceder a Internet por la conexión que nosotros hemos contratado, el proveedor asigna un nombre de usuario y una clave secreta a cada cliente. Siempre existe la posibilidad de compartir nuestra conexión con otra persona, con el único inconveniente de que no podremos conectarnos simultáneamente.

Interno contra externo.

Los servidores Web ahora se configuran y activan más fácilmente, pero todavía requieren tiempo considerable y conocimiento técnico de manejo, sin mencionar el costo del equipo. Muchas compañías y personas empiezan colocando su sitio con un ISP u otro servicio de hospedaje.

A medida que el tamaño del sitio aumenta y se hace más complicado, se podría reconsiderar la situación para decidir si tiene sentido albergar el sitio Web internamente.

Con un ISP no tendrá que incurrir en gastos de hardware o software, que podrían estar entre US\$ 2,000 y US\$10,000, dependiendo del tipo de servidor que desee.

Tampoco tendrá que incurrir en los gastos de emplear a alguien para que administre el sitio, aunque podría querer tener un asesor a medio tiempo que le ayude con el mantenimiento necesario. El costo de su conexión a Internet será probablemente mucho menor con un proveedor externo.

Si no tiene su propio hardware o ya tiene un personal dedicado, la diferencia en costos para su primer año puede ser impresionante. Con los costos de adquisición y del personal, poner a funcionar su propio servidor podría costarle hasta US \$50,000 en el primer año. Por otro lado, si es externo le costará mucho menos, quizás unos cuantos dólares.

Estas cifras pueden variar significativamente dependiendo de su localización geográfica y los diferentes paquetes que ofrece su ISP. Los precios son más competitivos en zonas urbanas más grandes.

Los costos de desarrollo y mantenimiento podrían elevarse dramáticamente a medida que el tamaño y complejidad de su sitio aumente. Cuanto más tráfico genere su sitio, más caro resultará utilizar un proveedor externo. Si su compañía

ya tiene un sólido sistema de computadoras y un administrador de sistema interno que tenga el tiempo para administrar el sitio, la mejor opción podría ser poner a funcionar su propio servidor.

Otra opción es la llamada "co-localización". Con esta elección un ISP le da mantenimiento físico a una computadora en su sitio, pero usted es responsable de todo el contenido de la máquina. Esta es una buena opción si tiene acceso a especialistas de software y puede comprar su propio equipo, pero no quiere la molestia de mantener una conexión constante a la Red, las 24 horas del día.

Proveedores de paquetes.

Algunos ISP's ofrecen paquetes "llave en mano", que incluyen desde planear y diseñar los sitios hasta programarlos y darle mantenimiento físico.

Si realiza una negociación amplia, debería evaluar cuidadosamente cada opción. Asegúrese de obtener una cotización escrita con las tarifas por horas y un tope de los costos para cada etapa del proyecto.

¿Cómo elegir un proveedor de servicio de Internet?

Si se decide por un proveedor externo, localice uno que sea estable, económico y amigable para el usuario. Los ISP's pueden variar considerablemente en los paquetes que ofrecen y los servicios que proveen. Aquí le mencionamos algunas preguntas que le pueden servir de directriz:

¿Qué tan rápida y estable es su conexión a la Internet? ¿Garantiza un servicio y contribución las 24 horas? ¿Tiene servicio ininterrumpido de electricidad y sólidos sistemas de copia de seguridad?

Lo peor es gastar miles de dólares para preparar su sitio y luego escuchar quejas de los clientes con respecto a la lentitud o indisponibilidad del servidor. Su ISP debería tener por lo menos dos conexiones de alta velocidad a la Internet.

¿Por cuánto tiempo ha estado en negocios? ¿Cuántos empleados tienen?

Evite las operaciones individuales de nuevas empresas.

Son excelentes si está buscando un arreglo para su página principal personal. Pero cuando se trata de su empresa, necesitará una administración que tenga programadores profesionales, especialistas en redes y personal de servicio al cliente.

¿Ofrece el ISP reportes resumidos de las estadísticas de uso?

Incluso si lo hacen, asegúrese de que pueda acceder a las estadísticas reales de visitas a su sitio, y no simplemente los resúmenes del ISP.

¿Ofrecen servicio completo de nombre de dominio?

Algunos ISP's no quieren tener el problema de crear los alias completos de los nombres de rutas requeridos para soportar diferentes nombres de dominios. En vez de ofrecerle la opción de un nombre de dominio,

www.minombre.com, le ofrecerán algo así como:

www.proveedorperezoso.com/minombre.

Este tipo de URL luce poco profesional, y generalmente es demasiado largo y difícil de escribir en tarjetas de negocios y material de mercadeo. (También es difícil de recordar). Si el ISP no ofrece el nombre completo del dominio, busque otro sitio.

¿Cuántos megabytes de almacenamiento de datos le permiten?

¿Hay recargos si hay mucha circulación en su sitio?

Algunos ISP's ofrecen al menos 5 megabytes o menos de espacio de almacenamiento gratuito con un recargo por megabytes si los sobrepasa. Eso podría estar bien para algunas páginas pequeñas, pero una vez que usted añada gráficos y algunos códigos cgi-bin para procesar formularios, necesitará más espacio. Busque un proveedor que ofrezca alta capacidad de almacenamiento. Los ISP's cobran recargos por mucho tráfico en sitios específicos, especialmente cuando esto impacta el funcionamiento de su servidor o si afecta a otros clientes.

¿Cómo actualizará usted sus páginas? ¿Tiene acceso vía FTP y Telnet?

El método más común para actualizar páginas es editarlas en su computadora y cargar los archivos al servidor con un programa de FTP. Alternadamente, los archivos pueden ser editados utilizando Telnet para entrar al servidor remotamente y editar los archivos con un editor de texto. Esto es más difícil y, si es posible, debería evitarse.

¿Soporta su proveedor CGI de modo tal que usted pueda usar formularios, búsqueda en base de datos y mapas de imágenes?

Si usted quiere que en su sitio haya formularios y mapas de imágenes, necesitará tener acceso completo a un directorio cgi-bin (el directorio donde son

almacenados los códigos CGI y otros programas ejecutables). Ahora la mayoría de los grandes ISP's ofrecen esto. Aléjese de aquellos que le dicen que es demasiado difícil de establecer o es un riesgo de seguridad. Se puede hacer si están comprometidos a respaldar a sus clientes.

¿Cuáles son las estipulaciones de seguridad y para contrarrestar a los intrusos en la Red?

Primero, recuerde que su proveedor está tan preocupado por la seguridad como usted. Todo su negocio depende de que los clientes estén contentos. Seguramente, la gran mayoría de clientes no están contentos si sus datos no están seguros. La seguridad ideal, absoluta e inquebrantable no existe actualmente en la Internet. Sin embargo, usted puede reducir los riesgos si sabe qué buscar en un ISP. La primera pregunta es si ellos utilizan un experto en seguridad. Si usted tiene una preocupación especial, solicite hablar con esta persona. Si no tienen, y esto es algo muy importante para usted, busque otro proveedor.

Lo que usted quiere escuchar de su ISP es que tiene bajo control la actividad en su sitio las 24 horas del día, de manera que se pueda detectar cualquier actividad sospechosa antes de que llegue a causar daños, y que tenga un programa que activamente instale y utilice la tecnología más revolucionaria de cortafuegos (firewalls) u otros métodos para tratar los problemas de seguridad conocidos. El National Institute of Computer Security Resource Clearinghouse (Instituto de recursos para la seguridad informática de los Estados Unidos) (en inglés) tiene un completo sitio Web con información general sobre la seguridad en Internet.

3.8 Nuevos servicios de acceso a internet.

Para que un usuario pueda hacer uso de los servicios de Internet requiere establecer un contrato con un proveedor de acceso a Internet (ISP), el cual proporciona la conexión, los protocolos TCP/IP y el software necesario para las herramientas de navegación.

Además de la conexión física a Internet, el usuario deberá contar con los programas de "software" necesarios para el establecimiento de la conexión a la red y los programas para la búsqueda e intercambio de información.

La conexión de usuarios a la red de Internet, puede ser utilizando líneas telefónicas conmutadas, líneas dedicadas o a través de una red de conmutación de paquetes (basada en X.25, Frame Relay, RDSI, etc).

En años recientes, con la aparición de nuevas tecnologías de acceso como son: ISDN, xDSL, CATV e inclusive enlaces satelitales, en algunos países ya se cuenta con esta tecnología, los ISP las están ofreciendo a sus usuarios como una alternativa de alta velocidad para el acceso a Internet.

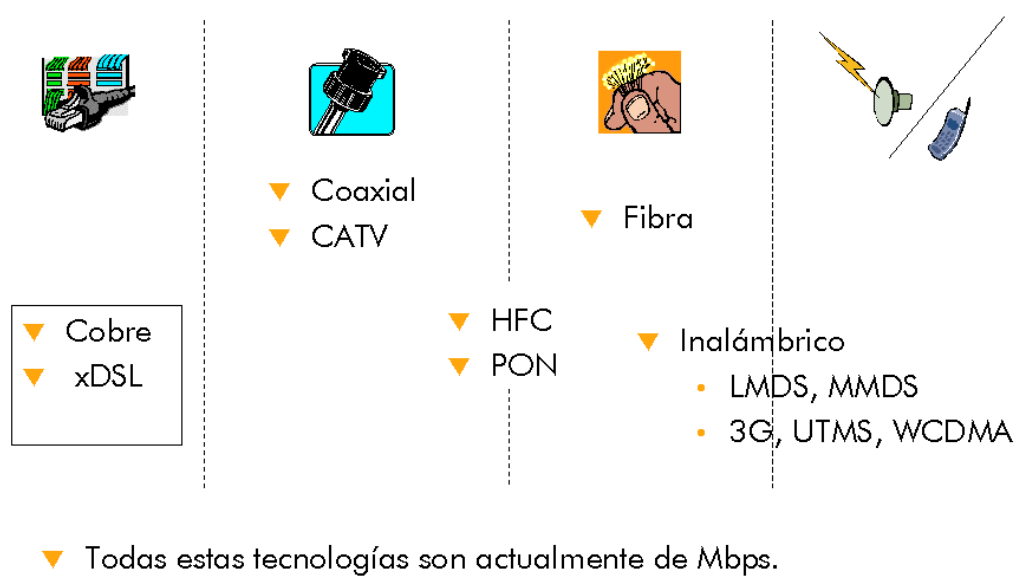


Fig. 3.7 Acceso de Banda Ancha

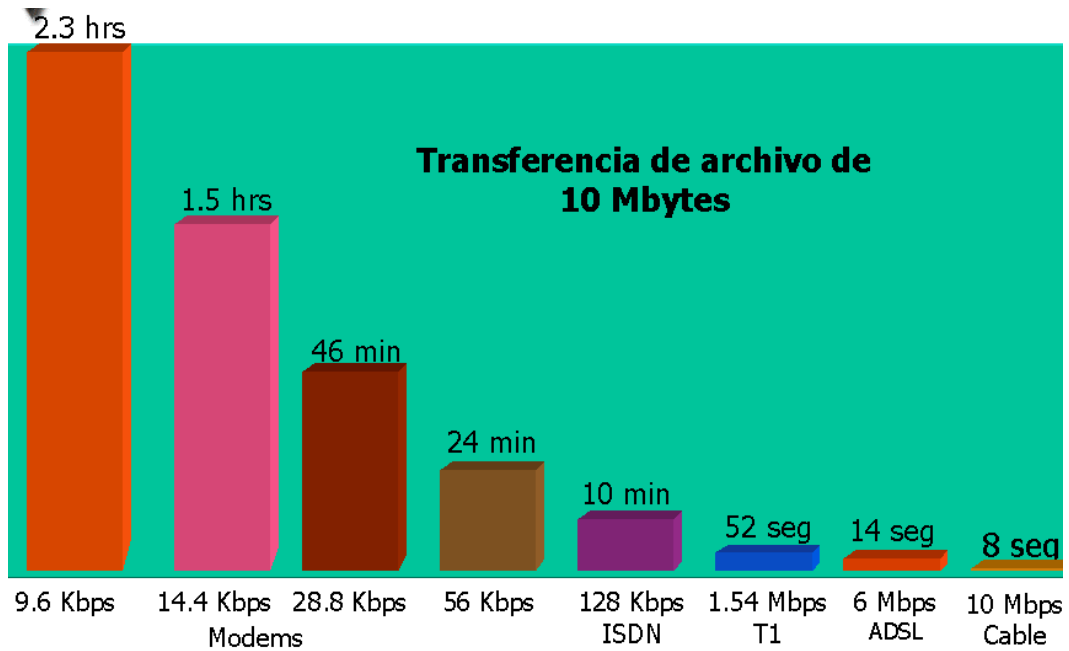


Fig. 3.8 Comparación entre tecnologías.

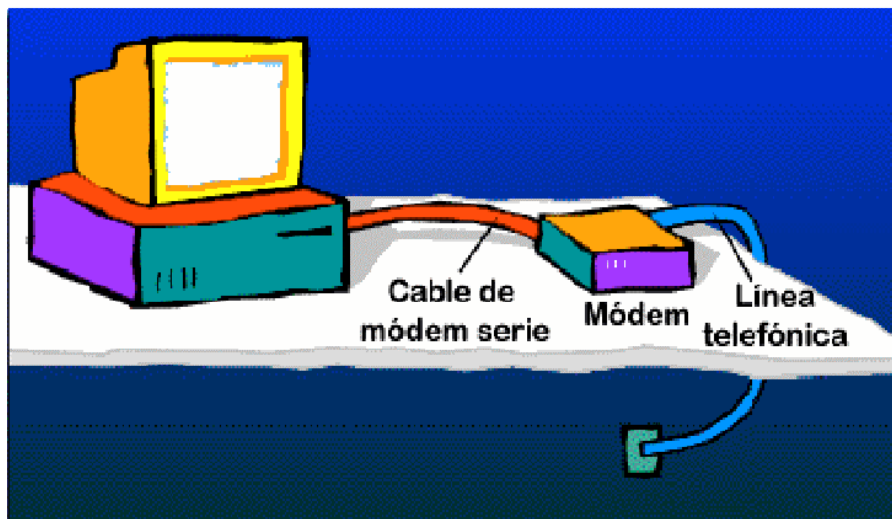


Fig. 3.9 Modems POTS e ISDN

Acceso por cobre

Las principales tecnologías de acceso por par de cobre para Internet son:

- Modems POTS
- ISDN
- XDSL

Módems POTS.

Para conectarse a la Internet, su computadora debe estar equipada con un módem, un dispositivo que convierte las señales digitales de su computadora en señales análogas que pueden viajar por una línea telefónica tradicional. Un módem del otro lado de la línea puede entenderlo y convertir el sonido de retorno en información digital. Los módems tienen distintas velocidades y se miden en bps o bits por segundos. Un módem de 28.8 Kbps envía datos a 28,800 bits por segundo. Un módem de 56 Kbps es el doble de rápido, enviando y recibiendo datos a una velocidad de 56,000 bits por segundos. La mayoría de módems de hoy son de 56 Kbps.

¿Qué tan importante es la velocidad? En la Internet, se están constantemente intercambiando datos con otras computadoras. Algunos de estos archivos digitales pueden ser muy grandes.

ISDN O RDSI

Red Digital de Servicios Integrados.

ISDN es una tecnología que ha tomado mucha fuerza en estos días, ya que es una alternativa para conexiones rápidas a costos bajos. Las siglas se derivan de Integrated Service Digital Network, que en español es Red Digital de Servicios Integrados. ISDN es un completo sistema de procesamiento de llamadas que permiten transportar por la red telefónica: voz y datos, desde una única interfaz de red. Entre las ventajas que posee respecto a las conexiones por módem son: la velocidad y confiabilidad de la conexión. Usando ISDN se puede lograr conexiones a más de 64 Kbps lo cual es un aumento al menos de 50% en comparación a un módem.

Hay maneras más veloces de transmitir datos. Esto se logra usando una línea ISDN o línea arrendada. En muchos lugares de los EE.UU, las compañías

telefónicas están ofreciendo ISDN para uso doméstico por menos de 30 dólares por mes (en México aproximadamente 400 pesos) . Las ISDN requieren de un adaptador de ISDN en vez de un módem y una línea telefónica con una conexión especial, que le permite enviar y recibir señales digitales.

Una línea ISDN tiene una tasa de transferencia de datos que oscila entre 64,000 y 128,000 bits por segundo, que es al menos el doble de la velocidad de un módem de 28.8 Kbps. Las líneas arrendadas en México pueden solicitarse a varias velocidades entre 64 Kbps y 2048 Kbps (E1) y hasta 34 Mbps (E3) para empresas muy grandes. A diferencia de la ISDN, estas conexiones arrendadas son conexiones dedicadas, lo que quiere decir que está permanentemente conectada a la Internet.

Esto es útil para los servidores de redes u otras computadoras que tienen que estar conectadas todo el tiempo. Usualmente cuando se arrendan estas líneas, se utiliza el protocolo Frame Relay.

Como ya se dijo, se pueden arrendar en bloques que varían de 128 Kbps a 2.04 Mbps. No vale la pena entrar en detalles sobre las diferencias, pero la conexión fraccional E-1 será más cara a las velocidades más bajas disponibles, y la Frame Relay será ligeramente más cara a menos que se acerque a la velocidad total de la E-1 de 2.04 Mbps. Una línea T-3 es significativamente más veloz, alcanzando unos 45 millones de bits por segundo. El backbone de la Internet consiste en líneas T-3.

Las líneas arrendadas son muy caras y generalmente son usadas sólo por compañías cuyos negocios dependen de la Internet o necesitan transferir enormes cantidades de datos. La ISDN, por otro lado, está disponible en algunas ciudades a un precio muy razonable. No todas las compañías de teléfonos ofrecen líneas residenciales ISDN.

Infórmese con su compañía telefónica local sobre la disponibilidad en su área.

XDSL.

Actualmente se están desarrollando tecnologías de acceso de alta velocidad para redes de telecomunicaciones como son las denominadas xDSL(x Digital Subscriber line): ADSL, HDSL, SDSL, etc.

La DSL (Digital Subscriber Line o Línea Digital de Suscriptor) es otra tecnología de alta velocidad que cada vez es más popular. Las líneas DSL están siempre conectadas a la Internet así que no se necesita marcar.

Típicamente los datos pueden ser transferidos a ritmos de hasta 2 Mbps en carga y cerca de 128 Kbps en descarga, en líneas ordinarias de teléfono.

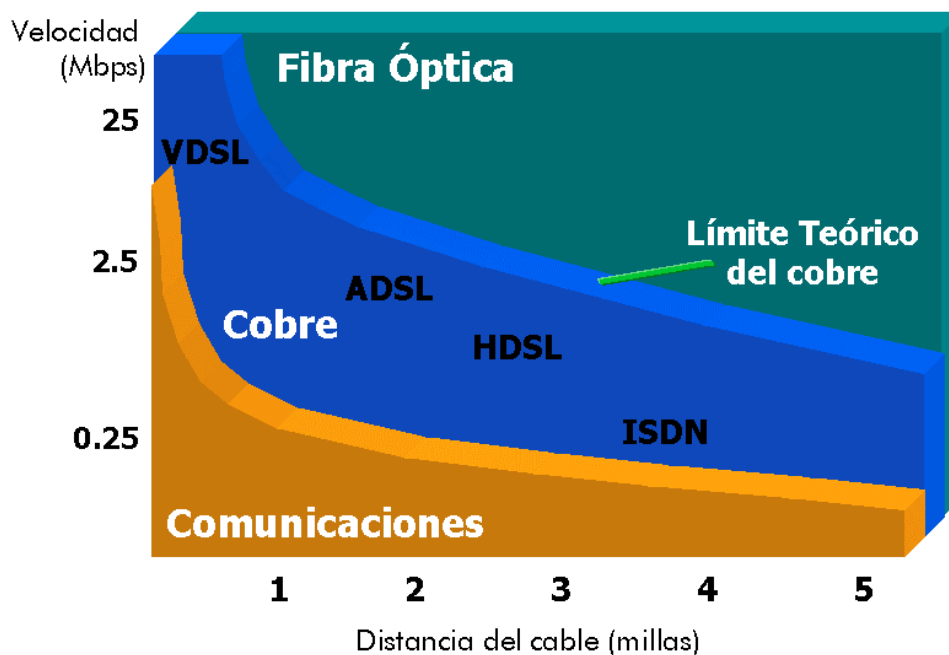


Fig. 3.10 Límite teórico del cobre.

Ya que una línea DSL transporta ya sea voz o datos, no hay que instalar otra línea telefónica. Puede usar su línea existente para establecer un servicio de DSL, si ese servicio está disponible en su área y usted está dentro de la distancia especificada por la oficina de conmutación principal de la compañía telefónica.

El servicio de DSL requiere un módem especial. Los precios para el equipo, la instalación de la DSL y el servicio mensual pueden variar considerablemente. La buena noticia es que los precios están bajando a medida que la competencia se vuelve más ardua.

ADSL en internet.

ADSL (Asimetric Digital Subscriber Line) es una tecnología de acceso de esta familia, que tiene como principal característica el que la recepción de la red es mucho mayor (Máximo 8Mbps) que la transmisión a la red (Máximo 1 Mbps), lo que lo hace ideal para aplicaciones como el acceso a la red Internet.

Esto es, los “browsers” en Internet no siempre demandan rangos simétricos, por lo general se accesa a bases de datos utilizando solo comandos de control y se reciben grandes volúmenes de información.

Adsl es una red que aprovecha la infraestructura de cobre y ofrece conexiones de alta velocidad, las cuales desbordan hacia una Red pública de ATM. Con esta solución, los usuarios obtienen respuestas a sus grandes demandas de información y el operador de servicios, redirecciona el tráfico hacia una red independiente de la RTPC, con lo optimiza sus recursos de voz y datos.

Acceso por Coaxial**Cable-Módem (CATV)**

Una creación relativamente nueva en México es un dispositivo que provee acceso a la Internet a alta velocidad mediante una red de televisión por cable. Con velocidades de hasta 36 Mbps, los módems de cable pueden descargar datos en segundos, acción que podría tardar cincuenta veces más con una conexión telefónica.

Ya que funciona con el cable de su televisor, no ocupa una línea telefónica. Lo mejor de todo es que siempre está activado.

Este servicio está disponible solo en algunas localidades ó ciudades, ya que es un sistema particular. La aparición de sistemas de acceso por coaxial es una buena alternativa para los usuarios, Ya que pueden aprovechar una conexión de Televisión privada de la que dispongan. En la actualidad es una tecnología que tiene demanda interesante en el mercado, ya que se ofrecen enlaces desde 64kbps a precios accesibles.

Tanto como ADSL y CATV se perfilan como protagonistas para el mercado de acceso a Internet.

Aplicaciones de DirectPC.

Empresas, Organizaciones y Personas independientes han aplicado el Sistema DirectPC, para incrementar su eficiencia al reducir tiempos de recepción de información (datos, audio, vídeo).

Hoy en día DirectPC, se ha comercializado tanto por sus grandes beneficios que ofrece para la Navegación en Internet:

- Velocidad en la navegación por Internet.
- Rapidez y eficiencia en la recepción de información
- Mayor comodidad para el envío y recepción de correo electrónico
- Navegación sin exceso de tráfico en servidores públicos
- Y un sin fin de beneficios relacionados con este gran medio innovador llamado **INTERNET**.

Un ejemplo comercial son los Cibercafés, gran parte de estos comercios, cuentan ya con el sistema DirectPC, ya que les otorga los beneficios indispensables para el negocio o comercio y un servicio satisfactorio.

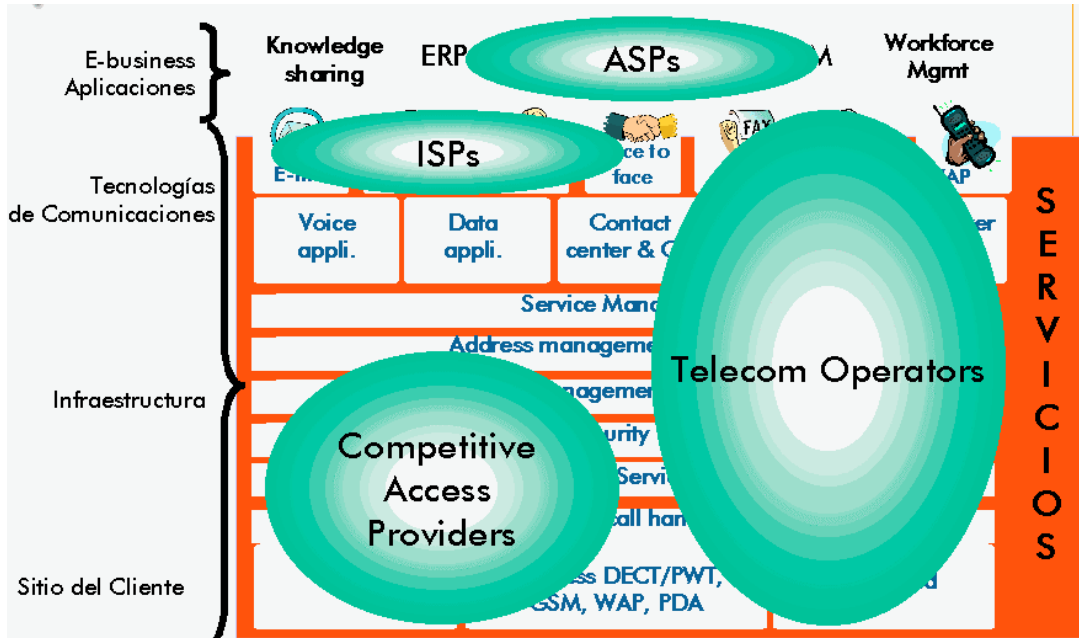


Fig. 3.11 Arquitectura Del E-Business.

3.9 Business Intelligence (BI), piedra angular Del e-Business.

En el lenguaje empresarial se agregaron nuevas palabras al vocabulario cotidiano, conceptos como Data Warehouse, Data Mart, Data Mining, Metadatos, OLAP (Online Analytical Processing) y sus Tipos y Modelos.

Todos estos se transforman en herramientas para realizar Business Intelligence o simplemente (BI).

Que pasaría sí, tuviera la oportunidad de acceder a los distintos datos que tenemos en nuestras empresas, alojados en distintos aplicativos, donde lo más común sería que estén corriendo en distintos entornos operativos, y con toda esta información disponible en nuestras manos, transformarla en conocimiento, para descubrir nuevas oportunidades de negocios, determinar comportamientos de productos, clientes, personas, y disponer la posibilidad de anticipar comportamientos, analizarlos y adelantarnos a nuestros competidores.

La respuesta a esta pregunta se encuentra, en aplicaciones de Business Intelligence, donde es obvio que no es posible la sustitución de la intuición y análisis humano, pero estas aplicaciones, servirán como auxiliares tácticos y estratégicos para empresarios, analistas técnicos y usuarios de información dentro de las empresas.

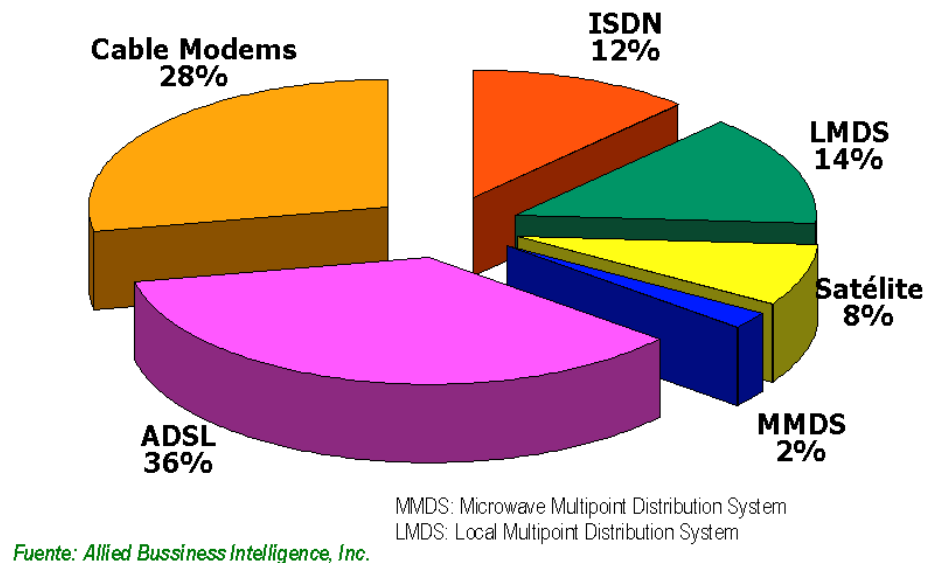


Fig. 3.12 Mercado de acceso de banda ancha para el 2008.

Objetivo del: Business Intelligence

El objetivo de las herramientas que se utilicen en Business Intelligence debe proveer a los usuarios finales de:

- Aplicaciones para toma de decisiones en circunstancias que atraviesan las empresas hoy en día, la exigencia de ser más competitivas, la necesidad de nuevas aplicaciones de soporte de decisiones.
- Consultas y generación de informes con herramientas de consulta y generaciones de informes, rápidas y fáciles de usar, posibilidad de explorar datos, recuperar la información necesaria y presentarla en un formato acorde.

Cómo extraer, limpiar, transformar y consolidar datos provenientes de múltiples fuentes heterogéneas para construir y mantener datamarts y data warehouses.

Sin duda que el primer paso es la definición de las necesidades de negocios del data warehouse. Una vez completado, debe analizarse el software que guíe a lo largo del proceso de especificación de relaciones entre los datos fuente y aquéllos almacenados en el warehouse. En algunos casos, el mismo software ayudará a acelerar la transformación y carga de los datos en el warehouse. Esto incluye limpieza, reestructuración, correlación, estandarización, sumarización y distribución de los datos según las necesidades de análisis y generación de informes. Para proyectos data warehousing complejos, también es conveniente considerar herramientas especializadas para ETML (extracción, transformación, movimiento y carga, por los términos en inglés) si se quiere asegurar un flujo de trabajo sin sobresaltos durante el proceso.

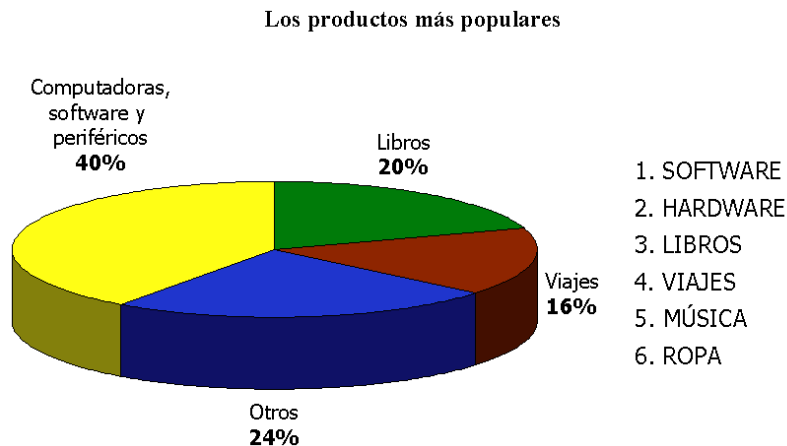


Fig. 3.13
Compra en línea.

Cómo automatizar y administrar los procedimientos de construcción y mantenimiento para data warehouses, datamarts y proceso.

Para procesos exploratorios. Los analistas que quieran usar el servidor OLAP para escenarios <what-if>, para presupuestación y pronosticación, deben reescribir los datos en el depósito de datos OLAP.

Aplicaciones OLAP distribuidas.

Otro resultado de la implementación de OLAP en una empresa es el desarrollo de aplicaciones OLAP individuales, cada una con sus propios cubos.

Acceso SQL

Al utilizar una base de datos relacional como depósito multidimensional, los usuarios pueden acceder a los datos empleando consultas SQL estándar.

Posibilidad de acceder a los cubos de Información, tanto de redes locales, como en Internet y Extranet.

Posibilidad de correr, en distintas plataformas de Hardware/Software.

Posibilidad de consolidar información proveniente de diferentes sistemas, aplicaciones propietarias, u otras fuentes de datos, sin necesidad de construir interfaces específicas.

Contar con niveles de control de acceso a la información, y de fijación del alcance del nivel.

Data Warehouse, Data Mart y Data Mining

La revolución del Data Warehouse (DW) está impulsada por la esperanza de que esta aproximación será capaz de ofrecer a las personas que toman decisiones en la organización un acceso integrado, consistente, fiable y rápido a los datos, que les permite tomar decisiones basadas en una mejor información. Históricamente, los datos de la corporación suelen residir en Bases de Datos (BD) que se diseñaron principalmente para introducir y almacenar datos, mediante el llamado Proceso de Transacciones En Línea (OLTP/OLAP). Este método es idóneo para insertar, modificar o borrar registros, pero no lo es tanto para responder a complejas consultas. La relación entre los datos responde, cuando existe, a unas técnicas llamadas de Entidad - Relación (Modelo Relacional). Los Data Warehouse surgen precisamente en respuesta a los problemas asociados a

realizar análisis de datos sobre Bases de Datos del tipo OLTP. La solución propuesta por el Data Warehouse es extraer los datos de una (o más) bases operacionales y moverlos a una Base de Datos independiente y orientada a las consultas.

Data Mining

Esta técnica consiste en extraer información de grandes basas de datos en función de estos mismos. se trata de un proceso automatizado de presentación de patrones, normas o funciones a un usuario informado para su revisión y estudio.

Análisis Multidimensional

_ Dimensiones (geografía, tiempo, producto, etc.).

_ Interrelaciones entre las anteriores jerarquías. Día, mes=año fiscal, tri=año.

_ Servicios---navegación, cálculos, profundización y resumen, piloto,

Pero ¿qué ocurre cuando los DW crecen y se van haciendo más complejos? El rendimiento de las consultas vuelve a sufrir y el modelo centralizado deja de ser el más eficiente. En estos casos, la solución propuesta es crear unos almacenes de datos" especializados " por áreas como Ventas o Compras, que reciben los datos desde el almacén centralizado (Data Warehouse) y que pueden residir en diferentes máquinas, BD, redes, etc. Estos almacenes se conocen como Data Marts (DM). Dado que un Data Mart soporta menos usuarios que un Data Warehouse se puede optimizar para recuperar más rápidamente los datos que necesitan los usuarios. La arquitectura de 3 Capas de un Data Mart es muy aconsejable porque:

- Menores cantidades de datos implican que se procesan antes tanto las cargas de datos como las consultas.
- Las peticiones pueden acotarse al área o red que sirve esos datos, sin afectar al resto de usuarios.
- La aplicación cliente que pide la consulta es independiente del servidor que la procesa y del Servidor de Base de Datos que almacena la
- Información.

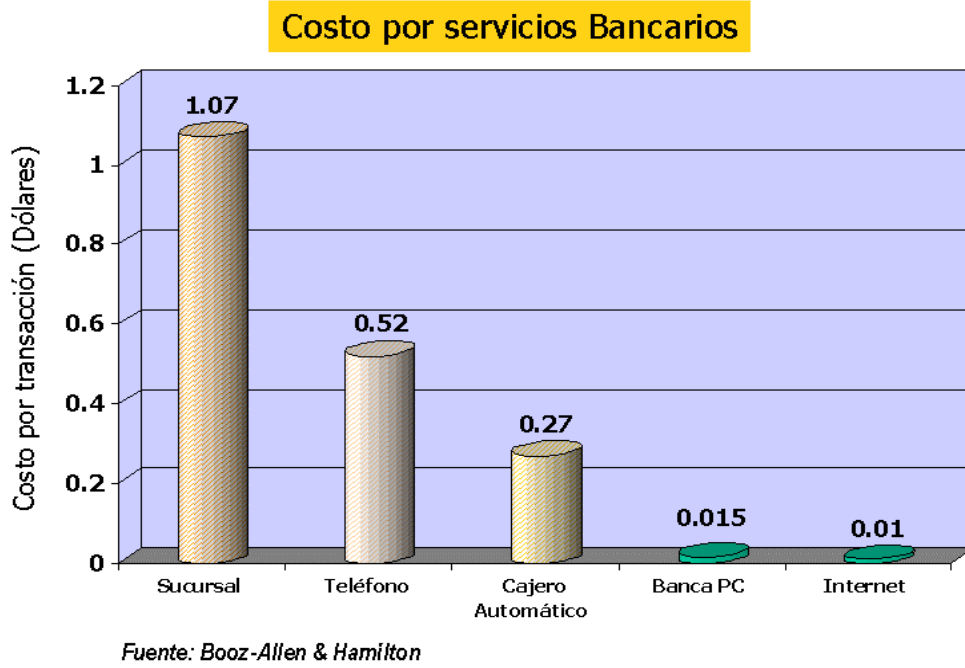


Fig. 3.14 Nuevas formas de hacer negocios.

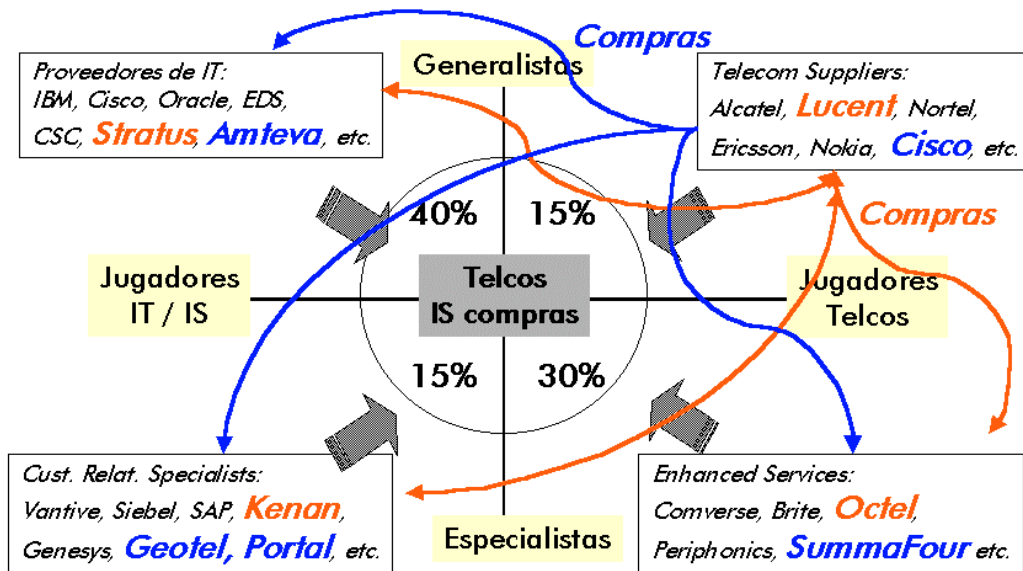


Fig. 3.15 Jugadores de servicios y aplicaciones.

3.10 Plataformas accesibles para sus clientes.

La reciente crisis de las dot.com (Expresión por la cual se identifican las empresas virtuales) ha dejado al descubierto la inviabilidad, al menos en el entorno económico actual, de los modelos de negocio de buen número de las iniciativas desarrolladas tanto en B2C (Business to Customer, es la comercialización al cliente final.) como en B2B (Business to Business, es la negociación entre empresas, ganar-ganar)

Esta circunstancia, no obstante, no debe inducirnos al error de extender esta situación y sus implicaciones de forma estructural a todo lo que "suene" a nueva economía, incluso a pesar de los mensajes pesimistas de algunas entidades bancarias de nuestro país. Lejos de ello, lo que ocurre es que por fin se han introducido criterios de racionalidad en el mercado e-business.

Por explicarlo de otro modo, se ha pasado de una primera fase emprendedora, donde la iniciativa era el factor clave de éxito principal y casi único y el objetivo era lanzar múltiples proyectos para demostrar actividad y diversificar riesgos, a una fase de consolidación donde la robustez de los modelos de negocio subyacentes prima sobre cualquier otra consideración y la calidad de cada proyecto es crítica.

En este nuevo contexto, tanto las empresas tradicionales como los nuevos entrantes o startups deben hacer frente y sacar el máximo provecho a los mismos retos estratégicos (redefinición de la cadena de valor, mayores rendimientos de la propiedad intelectual y el fondo de comercio, reducción de oportunidades basadas en la asimetría de la información, posibilidad de propuestas de valor personalizadas, capacidad de expansión rápida) y tecnológicos (disponibilidad y escalabilidad de sistemas, sofisticados sistemas de gestión de contenidos, operaciones y soporte a clientes, integración con sistemas transaccionales), pero su interpretación no puede ser la misma o igual de simplista que en el pasado.



Fig. Plataforma para los clientes.

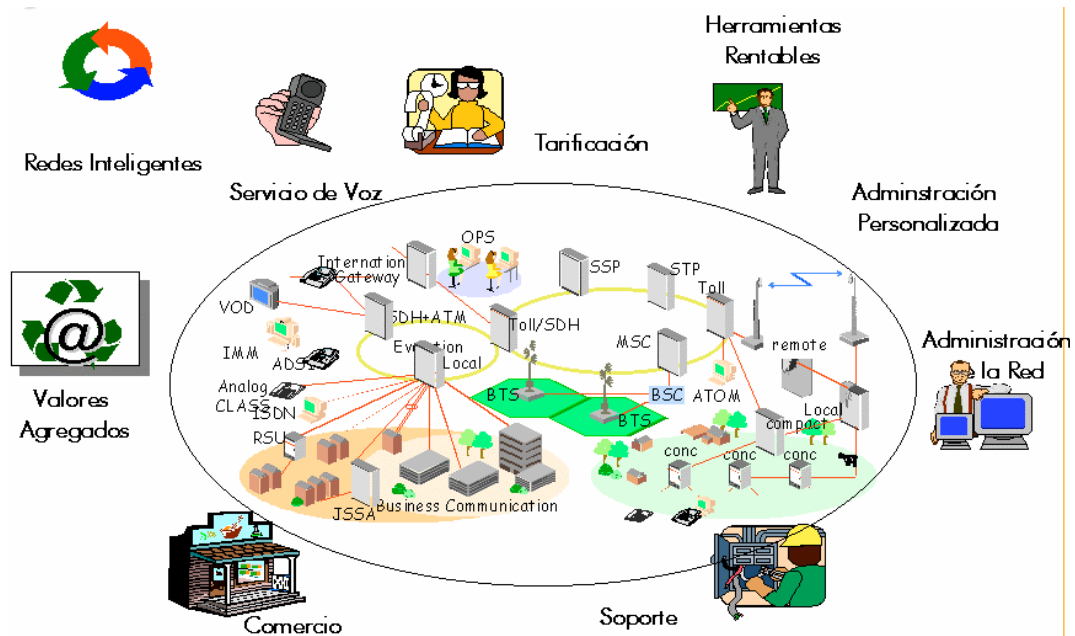


Fig. 3.17 Aplicaciones reales

Partiendo de la Economía Tradicional

Si estamos ante el caso de una empresa de la economía tradicional, financiera y operativamente consolidada, la gran oportunidad de mejora y, por tanto, el objetivo fundamental debe ser dotar su cadena de valor de las capacidades intrínsecas al nuevo medio digital, es decir: redefinir sus elementos, para optimizar las relaciones existentes con clientes, socios, empleados y proveedores; y añadir valor en todas sus dimensiones posibles, aumentando los ingresos (captación y retención de clientes, time to market, mejora de productos / servicios), reduciendo los costes (eficiencia operativa, economías de escala) y mejorando la imagen de marca (satisfacción de clientes y empleados, reconocimiento de analistas).

Para cada elemento de la cadena de valor, los beneficios y posibles soluciones tecnológicas existentes son múltiples.

Además, es posible optar por distintas maneras de recibir el servicio prestado por dichas soluciones y sacar el máximo partido de la tecnología disponible sin incurrir en fuertes inversiones, optando por un mayor o menor grado de externalización:

- Desarrollo "in-house". Permite el máximo grado de control y personalización de los servicios, a cambio de importantes inversiones propias en tecnología.
- Outsourcing de ciertos servicios de operación de sistemas, como el hosting de aplicaciones.
- ASP, es decir, suministro por contrato a largo plazo de los servicios de implantación, hosting, gestión, operación y alquiler de aplicaciones, pudiendo variar su alcance en función del nivel de complejidad de éstas y de la extensión de los servicios de operación.

Existentes en el mercado son muy numerosas y la forma de recibir su servicio también, por lo que resulta imprescindible haber desarrollado previamente una clara visión de las necesidades de negocio a cubrir y su centralizado para seleccionar las más adecuadas en cada caso y planificar su desarrollo.

Es muy importante que la estrategia de implantación sea progresiva, dando a la organización tiempo suficiente para internalizar los cambios derivados de ella (conflictos entre canales, responsabilidad operativa,

etc.). En términos generales, podría hablarse de cuatro etapas en el proceso de migración paulatina hacia la operación online de cualquier compañía:

- Etapa 1. Establecimiento de presencia en la red.
- Etapa 2. Transformación de la Cadena de Valor para dar cabida al e-business: reducción de costes operativos, mejoras del conocimiento y relación con clientes, etc.
- Etapa 3. Redefinición del modelo de negocio para el e-business: nuevas oportunidades, gestión de transiciones y conflictos, etc.
- Etapa 4. Creación de nuevos negocios en la red.

Conclusiones.

Uno de los avances más significativos para el mundo ha sido el surgimiento de las telecomunicaciones, pues a través de estas se pueden emitir o recibir signos, señales, imágenes fijas o en movimiento, sonidos o datos de cualquier naturaleza, entre dos o más puntos geográficos a cualquier distancia, mediante el uso de cables, radioelectricidad, medios ópticos u otros sistemas electromagnéticos, ya al tener dos puntos conectados entre sí, se habla de la presencia de una red de comunicaciones, si se viera a través de dos PCs, se estaría hablando de una red de computadoras.

El concepto de telecomunicaciones, es relativamente nuevo, pues hasta mediados de los sesenta fue incluido en los diccionarios, el cual se usa como sinónimo de transmisión de datos, de radiodifusión, de comunicación de voz y también se le identifica con algunos componentes de la industria del entretenimiento.

La instalación de medios de comunicación, específicamente el que abordamos en el presente trabajo “Sistema de cableado estructurado y consideraciones de diseño para redes de datos corporativas” hace que el desarrollo en una empresa sea significativo, hoy por hoy una organización que tenga PCs interconectadas, y que lleven a cabo procesos determinados, implementando y explotando tan importante medio de comunicación, estará alcanzando niveles de eficiencia y efectividad notables, en comparación con aquellas que se rehúsen al cambio. La implementación de redes de computadoras en instituciones u organizaciones, buscan como principal meta, crear grupos de trabajo organizados y que permiten llevar al éxito, tanto personal como institucional u organizacional.

La instalación de una red, implica un análisis previo, que involucra desde la elección de la topología dependiendo de la infraestructura que tenga la institución hasta su configuración, administración y mantenimiento preventivo como etapa final de la misma.

Actualmente con la globalización, y con la crisis que estamos viviendo, se incrementa la importancia de los sistemas de cómputo, que a su vez pertenecen a las redes, pues estos optimizan el rendimiento de los usuarios y minimizan costos.

Además el día de hoy desde los pequeños hasta los grandes empresarios, requieren de una computadora, y por ende de una red por pequeña que esta sea, ya que un servidor bien administrado almacena bases de datos, e información importante de cada cliente, o cada usuario, sin olvidar que el administrador puede tomar control de todo lo que en el servidor se almacene, pues la implementación de un adecuado sistema de redes, y la elección de los medios, materiales y del personal, son elemento clave para la buena ejecución y consecución de la misma. Toda red de computadoras está sujeta a limitaciones y depende del equipo de diseño y análisis, el elegir aquella topología y el protocolo adecuado, así como también el hardware necesario para la infraestructura o el terreno, en el cual la red se desempeñará.

Tanto la conexión de dos PCs utilizando el puerto serial de las mismas como enlace, hasta la creación de la Internet utilizando el Modem como puente físico de conexión, las comunicaciones ocupan un lugar importante en la actualidad, la cantidad de información que fluye y se comparte, conlleva a una abrumadora realidad institucional, donde la principal meta es la de lograr el éxito pleno y total, utilizando para ello herramientas tecnológicas de gran magnitud, como las redes de computadoras, y lo más importante la creación de éstas son una importante fuente de empleo para los ingenieros.

Glosario.

10Base2 Especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial delgado de 50 ohms. 10Base2, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia de 185 metros por segmento.

10Base5 Especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial estándar (grueso) de 50 ohms. 10Base5, que forma parte de la especificación de capa física de banda base. IEEE 802.3, tiene un límite de distancia de 500 metros por segmento. Véase también Ethernet e IEEE 802.3.

10BaseF Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BaseFB, 10BaseFL y 10BaseFP para Ethernet a través de cableado de fibra óptica.

10BaseFB Especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFB forma parte de la especificación IEEE.

10BaseFL Especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFL forma parte de la especificación IEEE 10BaseF y, al poder interoperar con FOIRL, está diseñada para reemplazar a la especificación FOIRL. Los segmentos 10BaseF pueden tener una longitud de hasta 1.000 metros si se los utiliza con FOIRL y de hasta 2.000 metros si se utiliza exclusivamente 10BaseFL.

10BaseFP Especificación Ethernet de banda base de fibra pasiva de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFP forma parte de la especificación IEEE 10BaseF. Organiza una serie de computadoras dentro de una topología en estrella sin el uso de repetidores. Los segmentos 10BaseFP pueden tener una longitud de hasta 500 metros.

10BaseT Especificación Ethernet de banda base de 10 Mbps que utilizados pares del cableado de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y el otro para recibir datos.

10BaseT, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia aproximado de 100 metros por segmento. Véase también Ethernet e IEEE 802.3.

10Broad36 Especificación Ethernet de banda ancha de 10 Mbps que utiliza cable coaxial de banda ancha. 10Broad36, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia de 3.600 metros por segmento. Véase también Ethernet e IEEE 802.3 10 Mbps Millones de bits por segundo. Unidad de velocidad de transferencia de información. Ethernet porta 10 Mbps.

100BaseFX Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una

correcta temporización de la señal, un enlace 100BaseFX no puede exceder los 400 metros de longitud. Basada en el estándar IEEE 802.3.

100BaseT Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la cual se base 100BaseT envía impulsos de enlace a través del segmento de la red cuando no se detecta tráfico. Sin embargo, estos impulsos de enlace contienen más información que los utilizados en 10BaseT. Basada en el estándar IEEE 802.3.

100BaseT4 Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cuatro pares del cableado UTP Categoría 3, 4 ó 5. Para garantizar una correcta temporización de las señales, un segmento 100BaseT4 no puede exceder los 100 metros de longitud. Basada en el estándar IEEE 802.3.

100BaseTX Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos pares del cableado UTP o STP. El primer par de cables se emplea para recibir datos y el segundo para transmitir. Para garantizar una correcta temporización de las señales, un segmento 100 Base TX no puede exceder los 100 metros de longitud. Basada en la norma IEEE 802.3.

100BaseX Especificación Fast Ethernet de banda base de 100 Mbps que se refiere a los estándares 100BaseFX y 100BaseTX para Fast Ethernet sobre cableado de fibra óptica. Basada en el estándar IEEE 802.3

ARP (Address Resolution Protocol). Protocolo de resolución de direcciones. Protocolo de Internet que se utiliza para mapear una dirección IP a una dirección MAC. Definido en RFC826.

ARP Inverso (Inverse Address Resolution Protocol). Protocolo de resolución de direcciones inversas. Método de construcción de rutas dinámicas dentro de una red. Permite que un servidor de acceso descubra la dirección de red de un dispositivo asociado con un circuito virtual.

ARP Proxy Protocolo de resolución de direcciones Proxy. Variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un ruteador) envía una respuesta ARP en nombre de un nodo extremo al Host solicitante. ARP Proxy puede disminuir el uso del ancho de banda en enlaces WAN de baja velocidad.

ARPA (Advanced Research Projects Agency) Agencia de proyectos de investigación avanzada. Organización de investigación y desarrollo que es parte de DoD. ARPA es responsable de numerosos avances tecnológicos en comunicaciones y networking. ARPA se convirtió en DARPA y luego volvió a ser ARPA nuevamente (en 1994).

ARPANET (Advanced Research Projects Agency Network) Red de la agencia de proyectos de investigación avanzada. Red de conmutación de paquetes que marcó un hito en 1969. ARPANET fue desarrollada en los años '70 por BBN y financiada por ARPA (luego, DARPA). Finalmente, se convirtió en Internet. El término ARPANET fue retirado oficialmente en 1990.

Arquitectura abierta

Arquitectura con la cual los desarrolladores de terceras partes pueden legalmente desarrollar productos para los cuales existen especificaciones de dominio público.

Arquitectura cliente-servidor Término utilizado para describir los sistemas de red de informática distribuida en los cuales las responsabilidades de la transacción se dividen en dos partes: cliente (frontal) y servidor (nodo). Ambos términos (cliente y servidor) pueden aplicarse a programas de software o a dispositivos reales de computación. También llamado informática distribuida.

Backbone. La parte de una red que actúa como ruta primaria para el tráfico que sale y llega de otras redes con mayor frecuencia.

Banda ancha Sistema de transmisión que multiplexa varias señales independientes en un cable. En terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que un canal con grado de voz (4 kHz). En terminología LAN, un cable coaxial sobre el cual se utiliza señalización analógica.

Banda base Característica de una tecnología de red donde se utiliza sólo una frecuencia portadora. Ethernet es un ejemplo de red de banda base. También llamada banda estrecha.

Baudio Unidad de velocidad de señalización igual al número de elementos de señal discontinua que se transmiten por segundo.
Baudio es sinónimo de bits por segundo (bps), si cada elemento de señal representa exactamente 1 bit.

BITNET ("Because It's Time" Networking Services) Red académica de bajo costo y baja velocidad que consiste principalmente en mainframes IBM y en líneas arrendadas de 9600 bps. BITNET actualmente forma parte de CREN.

Bps (bits per second) bits por Segundo.

Bridge (puente) Dispositivo que conecta y pasa paquetes entre dos segmentos de red que utilicen el mismo protocolo de comunicaciones. El bridge opera en la capa de enlace de datos (capa 2) del modelo de referencia OSI. En general, el bridge filtra, envía o inunda un Frame entrante basándose en la dirección MAC de dicho Frame.

Broadcast (emisión) Paquete de datos que se enviará a todos los nodos de una red. Los broadcasts se identifican por medio de direcciones de broadcast.

Bucle Ruta donde los paquetes nunca alcanzan su destino, en lugar de ello, pasan por ciclos repetidamente a través de una serie constante de nodos de red.

Byte Término empleado para referirse a una serie de dígitos binarios consecutivos sobre los cuales se opera como una unidad (por ejemplo, un byte de 8 bits).

Cable coaxial Cable que consta de un conductor cilíndrico exterior hueco que envuelve a un único alambre conductor interno. En las LANs se utilizan normalmente dos tipos de cable coaxial, cable de 50 ohms que se utiliza para la señalización digital y cable de 75 ohms que se utiliza para la señal analógica y la señalización digital de alta velocidad.

Cable de fibra óptica Medio físico capaz de conducir una transmisión de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más costoso, pero no es susceptible a la interferencia electromagnética y es capaz de mayores velocidades de datos. Llamado a veces fibra óptica.

Cableado de categoría 1. Una de las cinco categorías de cableado UTP descritas en la norma EIA/TIA-568B. El cableado de categoría 1 se utiliza para comunicaciones telefónicas y no resulta adecuado para la transmisión de datos. Compárese con cableado de categoría 2, cableado de categoría 3, cableado de categoría 4 y cableado de categoría 5.

Cableado de categoría 2. Una de las cinco categorías de cableado UTP descritas en la norma EIA/TIA-568B. El cableado de categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Compárese con cableado de categoría 1, cableado de categoría 3, cableado de categoría 4 y cableado de categoría 5.

Cableado de categoría 3. Una de las cinco categorías de cableado UTP descritas en la norma EIA/TIA-568B. El cableado de categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps. Compárese con cableado de categoría 1, cableado de categoría 2, cableado de categoría 4 y cableado de categoría 5..

Cableado de categoría 4. Una de las cinco categorías de cableado UTP descritas en la norma EIA/TIA-568B. El cableado de categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Compárese con cableado de categoría 1, cableado de categoría 2, cableado de categoría 3 y cableado de categoría 5.

Cableado de categoría 5.

Una de las cinco categorías de cableado UTP descritas en la norma EIA/TIA-568B. El cableado de categoría 5 se utiliza para correr CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Compárese con cableado de categoría 1,

cableado de categoría 2, cableado de categoría 3 y cableado de categoría 4.

Cableado del backbone. Cableado que permite realizar interconexiones entre los armarios para el cableado, entre los armarios para el cableado y el POP y entre los edificios que forman parte de la misma LAN.

Capa de aplicación. Capa 7 del modelo de referencia OSI. Esta capa provee servicios a procesos de aplicaciones (como correo electrónico, transferencia de archivos y emulación de terminal) que no pertenecen al modelo OSI. La capa de aplicación identifica y establece la disponibilidad de las partes que se tiene pensado comunicar (y de los recursos necesarios para conectarse con ellos), sincroniza aplicaciones cooperativas y aprueba los procedimientos para recuperación de errores y control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción en el modelo SNA

Capa de control de enlace de datos. Capa 2 del modelo de arquitectura SNA. Responsable de la transmisión de datos sobre un enlace físico particular. Corresponde aproximadamente a la capa de enlace de datos del modelo OSI. Véase también capa de control de flujo de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capas de servicio de transacción y capa de control de transmisión. Capa de control de flujo de datos. Capa 5 del modelo de arquitectura SNA. Esta capa determina y administra las interacciones entre las partes de la sesión, particularmente el flujo de datos. Corresponde a la capa de sesión del modelo OSI.

Capa de control físico. Capa 1 del modelo de arquitectura SNA. Esta capa es responsable de las especificaciones físicas de los enlaces físicos entre sistemas finales. Corresponde a la capa física del modelo OSI. Véase también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

Capa de enlace de datos. Capa 2 del modelo de referencia OSI. Esta capa brinda un tránsito confiable de datos a través de un enlace físico. La capa de enlace de datos tiene correspondencia con el direccionamiento físico, topología de red, disciplina de línea, notificación de error, entrega solicitada de frames y control de flujo. El IEEE ha dividido esta capa en dos subcapas: la subcapa MAC y la subcapa LLC. Algunas veces se la denomina simplemente capa de enlace del modelo SNA.

Capa de control de ruta. Capa 3 del modelo de arquitectura SNA. Esta capa cumple servicios de secuenciamiento relacionados con el reensamblado adecuado de los datos. La capa de control de ruta es asimismo responsable del enrutamiento. Corresponde generalmente a la capa de red del modelo OSI.

Capa de control de transmisión. Capa 4 del modelo de arquitectura SNA. Esta capa es responsable de establecer, mantener y terminar sesiones SNA, secuenciar mensajes de datos y controlar el flujo de nivel de sesión. Corresponde a la capa de transporte del modelo OSI. Véase también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación y capa de servicios de transacción.

Capa de presentación. Capa 6 del modelo de referencia OSI. Esta capa garantiza que la información enviada por la capa de aplicación de un sistema sea legible por la capa de aplicación de otro. La capa de presentación también se encuentra involucrada con las estructuras de datos utilizadas por los programas y, por lo tanto, negocia la sintaxis de transferencia de datos para la capa de aplicación. Tiene correspondencia en lo general con la capa de servicios de presentación del modelo SNA.

Capa de red Capa 3 del modelo de referencia OSI. Esta capa provee conectividad y selección de rutas entre dos sistemas terminales. La capa de red es la capa donde tiene lugar un enrutamiento. Corresponde aproximadamente a la capa de control de ruta del modelo SNA.

Capa de servicios de transacción. Capa 7 en el modelo de arquitectura SNA. Representa funciones de aplicaciones para usuarios, como planillas de cálculo, procesamiento de palabras, o correo electrónico, por las cuales los usuarios interactúan con la red. Corresponde aproximadamente a la capa de aplicación del modelo de referencia OSI.

Capa de sesión Capa 5 del modelo de referencia OSI. Esta capa establece, gestiona y termina sesiones entre aplicaciones y gestiona el intercambio de datos entre entidades de la capa de presentación. Corresponde a la capa de control de flujo de datos del modelo SNA.

Capa de transporte. Capa 4 del modelo de referencia OSI. Esta capa es responsable de una comunicación de red confiable entre nodos extremos. La capa de transporte provee mecanismos para el establecimiento, mantenimiento y terminación de circuitos virtuales, detección y recuperación de fallos en el transporte y control de flujo de información. Corresponde a la capa de control de transmisión del modelo SNA.

Capa física. Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para la activación, mantenimiento y desactivación de la capa física entre sistemas finales. Corresponde con la capa de control físico en el modelo SNA.

Capas de servicios de presentación. Capa 6 del modelo de arquitectura SNA. Esta capa brinda gestión de recursos de red, servicios de presentación de sesión y alguna gestión de aplicación. Tiene correspondencia en lo general con la capa de presentación del modelo OSI.

Capa de control físico, capa de servicios de transacción y capa de control de transmisión. CD (Carrier Detect) Detección de portadora. Señal que indica si una interfaz se encuentra activa. Asimismo, una señal generada por un módem que indica que se ha conectado una llamada. Circuito virtual Circuito lógico creado para garantizar una comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por medio de un par VPI/VCI y puede ser permanente (PVC) o conmutado (SVC). Los circuitos virtuales se utilizan en Frame Relay y en X.25. En ATM, un circuito virtual se llama canal virtual. Algunas veces abreviado VC. Codificación Proceso por el cual los bits son representados por tensiones. Técnicas eléctricas utilizadas para transportar señales binarias. Código de corrección de errores. Código que tiene suficiente inteligencia e incorpora suficiente información de señalización como para permitir la detección y corrección de muchos errores en el receptor.

Código de detección de errores. Código que puede detectar errores de transmisión mediante un análisis de los datos recibidos, basándose en la adherencia de los datos a pautas estructurales apropiadas. Colisión En Ethernet, el resultado de dos nodos transmitiendo en forma simultánea. Los frames provenientes de cada dispositivo impactan y se dañan al encontrarse en el mismo medio físico Computación peer-to-peer. Llamadas de informática peer-to-peer para cada dispositivo de red para correr tanto las porciones del cliente como del servidor de una aplicación. Asimismo describe la comunicación entre las implementaciones de la misma capa del modelo de referencia OSI en dos dispositivos de red diferentes.

Conector BNC (British Naval Connector). Conector estándar que se utiliza para conectar el cable coaxial 10Base2 IEEE 802.3. Conector RJ (registered jack). Conector tipo ficha registrado. Conectores estándar normalmente empleados para conectar las líneas telefónicas. Los conectores RJ se utilizan actualmente para las conexiones telefónicas y 10BaseT como así también para otros tipos de conexiones de red. RJ-11, RJ-12 y RJ-45 son algunos de los tipos de conectores RJ más difundidos

Conmutador de paquetes Dispositivo WAN que enruta los paquetes a lo largo de la ruta más eficiente y permite que un canal de comunicaciones sea compartido por múltiples conexiones. Algunas veces denominado como nodo de conmutación de paquetes (PSN) y anteriormente denominado un IMP. CRC (Cyclic redundancy check) Verificación por redundancia cíclica. Técnica de verificación de errores en la que el receptor del Frame calcula un resto dividiendo el contenido de un Frame por un divisor binario primo y compara el resto calculado con un valor almacenado en el Frame por el nodo emisor. CSMA/CD (Carrier Sense Multiple Access Collision Detect) Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso al medio en el cual los dispositivos listos para transmitir datos primero verifican el canal en busca de una portadora. Si no se detecta ninguna portadora por un lapso especificado, un dispositivo puede transmitir. Si dos dispositivos transmiten a la vez, tiene lugar una colisión y ésta es detectada por todos los dispositivos que entran en colisión. En consecuencia, la

colisión demora las retransmisiones desde dichos dispositivos por un lapso al azar. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3. DARPA (Defense Advanced Research Projects Agency) Agencia de proyectos de investigación avanzada para la defensa. Agencia del gobierno de los Estados Unidos que brindó los fondos para la investigación y experimentación con la Internet. Evolucionó a partir de ARPA y luego en 1994 retornó a ARPANET. Datagrama Agrupamiento lógico de información enviada como una unidad de capa de red por un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información en la Internet. Los términos Frame, mensaje, paquete y segmento también se utilizan para describir los agrupamientos lógicos de información en las diferentes capas del modelo de referencia OSI y en varios círculos de tecnología.

Demodulación Proceso de retornar una señal modulada a su forma original. Los módems realizan la Demodulación, tomando una señal analógica y retornándola a su forma original (digital).

Dirección de broadcast Dirección especial reservada para enviar un mensaje a todas las estaciones. En general, la dirección de broadcast es una dirección de destino MAC con todos

Dirección de punto Se refiere a la notación común para las direcciones IP en la forma <a.b.c.d>, donde cada número a representa, en formato decimal, 1 byte de la dirección IP de 4 bytes. También denominada notación de punto o anotación punteada en cuatro partes.

Dirección de red Dirección de capa de red que se refiere a un dispositivo de red lógico, en vez de físico. También llamada dirección de protocolo. Dirección de subred Parte de una dirección IP que la máscara de subred especifica como subred.

DNS (Domain Naming System). Sistema de denominación de dominio. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones. Domain Sistema de networking desarrollado por Apollo Computer (actualmente parte de Hewlett-Packard) para utilizarse en sus estaciones de trabajo de ingeniería. Dominio 1.En Internet, una parte del árbol de jerarquía de nombres que se refiere a los agrupamientos generales de redes basadas en tipo de organización o geografía. 2.En SNA, un SSCP y los recursos que controla. 3.En IS-IS, un conjunto lógico de redes.

Dominio de broadcast. Conjunto de todos los dispositivos que recibirán frames de broadcast provenientes de cualquier dispositivo del conjunto. Los dominios de broadcast son limitados típicamente por los ruteadores ya que éstos no envían frames de broadcast.

Dominio de colisión En Ethernet, el área de la red dentro de la cual se propagan los frames que han colisionado. Los repetidores y los hubs propagan las colisiones; los Switches LAN, Bridges y ruteadores no lo hacen. Véase también colisión.

Dominio de enrutamiento Grupo de sistemas finales y de sistemas intermedios que operan bajo el mismo conjunto de normas administrativas. Dentro de cada dominio de enrutamiento hay una o más áreas, cada una de las cuales está identificada en forma única por medio de una dirección de área.

Dominio de fallo Área donde se ha producido un fallo en Token Ring, definida por la información contenida en una baliza. Cuando una estación detecta un problema serio en la red (tal como un cable cortado), envía un Frame baliza que comprende la estación que informa del fallo, su NAUN y todo lo que haya en medio. La baliza a su vez inicia un proceso llamado auto-reconfiguración.

DS-0 (Digital Signal Level 0) Nivel 0 de la señal digital. Especificación de entramado que se utiliza para transmitir señales digitales en un único canal a 64-kbps en una facilidad T1.

DS-1 (Digital Signal Level 1). Nivel 1 de la señal digital. Especificación de entramado que se utiliza para transmitir señales digitales a 1,544-Mbps en una facilidad T1 (en los Estados Unidos) o a 2,108-Mbps o en una facilidad E1 (en Europa).

DS-3 (Digital Signal Level 3). Nivel 3 de la señal digital. Especificación de entramado que se utiliza para transmitir señales digitales a 44,736-Mbps en una facilidad T3.

E1 Sistema de transmisión digital de área amplia, utilizado predominantemente en Europa, que transporta datos a una velocidad de 2,048 Mbps. Las líneas E1 se pueden arrendar de portadoras comunes para uso privado.

E3 Sistema de transmisión digital de área amplia, utilizado predominantemente en Europa, que transporta datos a una velocidad de 34,368 Mbps. Las líneas E3 se pueden arrendar de portadoras comunes para uso privado.

Error de alineación En redes IEEE 802.3, un error que tiene lugar cuando la cantidad total de bits de un Frame recibido no es divisible por ocho. Los errores de alineación son provocados en general por un Frame dañado debido a colisiones. Ethernet Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y corren por una variedad de tipos de cable a 10 Mbps. Ethernet es similar a la serie de normas IEEE 802.3.

Fast Ethernet Cualquiera de varias especificaciones de Ethernet de 100- Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de Frame, mecanismos MAC y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes de Fast Ethernet. Basada en una extensión de la especificación IEEE 802.3.

FDDI (Fiber Distributed Data Interface) Interfaz de datos distribuida por fibra. Norma LAN, definida por ANSI X3T9.5, que especifica una red de tokenpassing de 100-Mbps que utiliza un cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble para dar redundancia. DDI II Norma ANSI que mejora FDDI. FDDI II proporciona una transmisión isócrona para circuitos de datos sin conexión y para circuitos de voz y vídeo orientados a conexión.

FDM Multiplexación de división de frecuencia. Técnica por la cual se puede asignar un ancho de banda a información desde varios canales en un único cable, basándose en la frecuencia. Fragmentación Proceso de dividir un paquete en unidades más pequeñas cuando se transmite por un medio de red que no puede soportar el tamaño original del paquete.

Frame Agrupación lógica de información, enviada como unidad de la capa de enlace de datos por un medio de transmisión. A menudo, se refiere al encabezado y al trailer, utilizados para la sincronización y el control de errores, que rodean a los datos del usuario que contiene la unidad. Los términos Datagrama, mensaje, paquete de datos y segmento también se utilizan para describir agrupaciones lógicas de información en diversas capas del modelo de referencia OSI y en diversos círculos de tecnología.

Frame Relay Protocolo de la capa de enlace de datos conmutados, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficaz que X.25, el protocolo para el cual se considera por lo general un reemplazo Gateway En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, se utiliza el término ruteador para describir los nodos que realizan esta función, mientras que gateway se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro Half dúplex Capacidad de transmisión de datos solamente en una dirección a la vez, entre una estación de envío y una estación de recepción. Compárese con full dúplex y simplex. Host (anfitrión) Sistema de computación en una red. Similar al término nodo excepto que el Host usualmente implica un sistema de computación, mientras que un nodo generalmente se aplica a cualquier sistema en red, incluyendo los servidores de acceso y ruteadores.

Hub (concentrador) En forma general,

- Es un término utilizado para describir un dispositivo que sirve como centro de una red de topología en estrella.

- Dispositivo de hardware o software que contiene múltiples módulos independientes pero conectados de equipo de red e internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten, sino que meramente dividen las señales enviadas a través de ellos).
- En Ethernet e IEEE 802.3, un repetidor Ethernet multipuerto, algunas veces denominado como concentrador. Hub activo Dispositivo de varios puertos que amplifica las señales de transmisión LAN.

Internet. Término utilizado para referirse a la mayor internetwork global que conecta a decenas de miles de redes de todo el mundo y que tiene una “cultura” que apunta básicamente a la investigación y a la estandarización basándose en el uso en la vida real. Muchas tecnologías de red líderes provienen de la comunidad de Internet. La Internet evolucionó en parte a partir de la ARPANET. Antes llamada también Internet DARPA. No debe confundirse con el término general Internet.

InterNIC Organización que sirve a la comunidad de Internet brindando asistencia al usuario, documentación, capacitación, servicio de registro de nombres de dominio de Internet y otros servicios. Antiguamente llamado Network Information Center (NIC) (Centro de Información de Redes).

IP (Internet Protocol). Protocolo Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado y seguridad. Documentado en RFC 791.

LAN (Local Area Network) Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas física y de enlace datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas MAC (Media Access Control. Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos, por ejemplo, si se utilizará token passing o contención.

LLC (Logical Link Control) Control de enlace lógico. La más alta de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa LLC maneja el control de errores, el control de flujo, el entramado y el direccionamiento de subcapa MAC. El protocolo LLC que más prevalece es IEEE 802.2, que incluye tanto la variante sin conexión como la orientada a conexión.

MAN (metropolitan área network). Red de área metropolitana. Red que abarca un área metropolitana. En general, una MAN abarca un área geográfica más vasta que una LAN, pero cubre un área geográfica más pequeña que una WAN.

Máscara de dirección. Combinación de bits que se utiliza para describir qué porción de una dirección se refiere a la red o subred y cuál parte se refiere al Host. A veces se la llama simplemente máscara. Máscara de subred Máscara de dirección de 32 bits que se utiliza en el IP para indicar los bits de una dirección IP que se están utilizando para la dirección de subred. También llamada simplemente máscara Modelo de referencia OSI Modelo de referencia de interconexión de sistemas abiertos. Modelo de arquitectura de redes desarrollado por ISO e ITU-T. El modelo consiste en siete capas, cada una de las cuales especifican funciones particulares de la red, como por ejemplo direccionamiento, control de flujo, control de errores, encapsulación y transferencia confiable de mensajes. La capa superior (capa de aplicación) es la más próxima al usuario; la capa inferior (capa física) es la más próxima a la tecnología de medios. La capa siguiente a la capa inferior está implementada en hardware y en software mientras que las cinco capas superiores están implementadas únicamente en software. El modelo de referencia OSI se utiliza mundialmente para enseñar y comprender la funcionalidad de una red. Es similar en ciertos aspectos a SNA. Véase capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

Módem Modulador-demodulador. Dispositivo que convierte señales digitales y análogas. En el punto de origen, un módem convierte señales digitales a una forma apropiada para la transmisión por facilidades de comunicación análogas. En el punto de destino, las señales análogas se recuperan a su forma digital. Los módem permiten la transmisión de datos por líneas telefónicas de grado voz.

Multicast Paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.

NET (network entity title). Identificador de la entidad de la red. Direcciones de red, definidas por la arquitectura de red ISO y utilizadas en redes basadas en CLNS.

NetBIOS (Network Basic Input/Output System) Sistema de básico de entrada/salida de red. API utilizada por aplicaciones en una LAN IBM para solicitar servicios de procesos de red de menor nivel. Estos servicios podrían incluir inicio y terminación de sesiones y transferencia de información. Networking. Conexión de cualquier conjunto de computadoras, impresoras, ruteadores, Switches y otros dispositivos, con el fin de enviar comunicación por un medio de transmisión.

NIC (Network interface card). Tarjeta de interfaz de red. Tarjeta que provee capacidades de comunicación de red hacia y desde un sistema de computación. También llamada adaptador. Nodo Punto final de una conexión de red, o unión común a dos o más líneas en una red. Los nodos pueden ser procesadores, controladores, o estaciones de trabajo. Los nodos, que pueden variar según su capacidad de enrutamiento y otras capacidades funcionales, pueden estar interconectados por enlaces y servir como puntos de control en la red. El término

nodo se emplea a veces de modo genérico para indicar cualquier entidad que puede tener acceso a una red y es utilizado a menudo en forma intercambiable con dispositivo.

Número del Host Parte de una dirección IP que designa qué nodo se está direccionando en la subred. Asimismo denominado una dirección del Host. Paquete Agrupamiento lógico de información que incluye un encabezado que contiene información de control y (usualmente) datos del usuario. Los paquetes se utilizan más frecuentemente para hacer referencia a las unidades de datos de las capas de red. Los términos Datagrama, Frame, mensaje y segmento también se utilizan para describir agrupamientos de información lógica en diferentes capas del modelo de referencia OSI y en varios círculos de tecnología Par trenzado. Medio de transmisión de velocidad relativamente baja que consiste en dos cables aislados, dispuestos en forma de espiral regular. Los cables pueden ser blindados o sin blindaje. Par trenzado es común en aplicaciones telefónicas y es cada vez más común en redes de datos.

RARP (Reverse Address Resolution Protocol). Protocolo de resolución de direcciones inversa. Protocolo en el stack TCP/IP que brinda un método para encontrar direcciones IP en base a las direcciones MAC.

RFC (Request For Comments) Petición de comentarios. Serie de documentos empleada como medio de comunicación primaria para transmitir información acerca de la Internet. Algunas RFC son designados por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFCs pueden encontrarse en línea en distintas fuentes. Ruteador Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los ruteadores envían paquetes de una red a otra en base a la información de capa de red. Ocasionalmente llamado gateway (aunque esta definición de gateway va cayendo en desuso día a día).

Señal digital Lenguaje de computadoras que consta solamente de dos estados, encendido y apagado, los cuales se indican mediante una serie de impulsos de tensión. Señalización Proceso que consiste en enviar una señal de transmisión sobre un medio físico a los fines de la comunicación. Servidor de acceso Procesador de comunicaciones que conecta dispositivos asíncronos con una LAN o WAN mediante una red y un software de emulación de terminal. Realiza tanto enrutamiento asíncrono como síncrono de los protocolos soportados. Llamado a veces servidor de acceso a la red. Servidor de comunicaciones Procesador de comunicaciones que conecta dispositivos asíncronos a una LAN o WAN a través de un software de red y emulación de terminal. Lleva a cabo solamente un enrutamiento asíncrono de IP e IPX. Servidor de impresión Sistema de computación en red que registra, administra y ejecuta (o envía para ejecución) solicitudes de impresión desde otros dispositivos de red.

SMTP (Simple Mail Transfer Protocol). Protocolo SMTP. Protocolo de Internet que brinda servicios de correo electrónico SNMP (Simple Network Management Protocol). Protocolo simple de administración de redes. Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad. Véase también SGMP y SNMP2. SNMP2 SNMP Versión 2. Versión 2 del popular protocolo de administración de redes. SNMP2 soporta estrategias de gestión de redes tanto centralizadas como distribuidas, e incluye mejoras al protocolo SMI, a las operaciones del protocolo, a la arquitectura de gestión y a la seguridad.

SONET (Synchronous Optical Network) Red óptica síncrona. Especificación de red síncrona de alta velocidad (hasta 2,5 Gbps) desarrollada por Bellcore y diseñada para correr por una fibra óptica. STS-1 es el bloque de construcción básico de SONET. Aprobado como estándar internacional en 1988. Subred 1. En redes IP, red que comparte una dirección de subred particular. Las subredes son redes segmentadas arbitrariamente por un administrador de red para brindar una estructura de enrutamiento multinivel, jerárquico, protegiendo a la subred de la complejidad del direccionamiento de las redes conectadas. Llamada a veces subnet.2. En las redes OSI, grupo de ES e IS bajo el control de un único dominio administrativo que utilizan un mismo protocolo de acceso a la red. Subvector Segmento de datos de un vector en un mensaje SNA. Un subvector consiste en un campo de longitud, una clave que describe el tipo de subvector y datos específicos del subvector.

T1. Facilidad de portadora de WAN digital. T1 transmite datos formateados en DS-1 a 1,544 Mbps por la red de conmutación telefónica, mediante una codificación AMI o B8ZS. T1 canalizado Enlace de acceso que opera a 1,544 Mbps, que se encuentra subdividido en 24 canales (23 canales B y un canal D) de 64 Kbps cada uno. Los canales o grupos de canales individuales se conectan a diferentes destinos. Soporta DDR, Frame Relay y X.25. También denominado T1 fraccionario. T3 Facilidad de portadora de WAN digital. T3 transmite datos formateados en DS-3 a 44,736 Mbps por la red de conmutación telefónica. Compárese con E3. Comando que utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red. Es un mecanismo de prueba muy básico. Portadora Onda electromagnética o corriente alterna de frecuencia única, apropiada para la modulación por otra señal, que transporte datos. UDP (User Datagram Protocol) Protocolo de Datagrama de usuario. Protocolo sin conexión de capa de transporte en el stack de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC

WAN (wide área network) Red de área amplia. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

BIBLIOGRAFÍA.

Protocolos de Internet. Diseño e Implementación

Ángel López, Alejandro Novo
Alfaomega. Ra-ma. 2002.

Tecnología de interconectividad de redes

Merilee Ford, H. Kim Lew.
Prentice Hall Hispanoamericana,
S.A.

Redes Globales de información con Internet y TCP/IP

Douglas E. Comer
Prentice Hall Hispanoamericana,
S.A.

The Switching Book II.

Xylan: An Alcatel Company

PC/TIPS.

Jorge Mondragón
Año 2 Número 15, 15/Abr./1998.

El círculo de comunicaciones de Token-Ring.

José Daniel Sánchez Navarro
Capítulo 1, pp. 3-7, 14
Editorial McGraw Hill
Feb. /1999
Serie Enter: El camino fácil a Internet.

REFERENCIAS DE INTERNET

www.m-w.com
www.wordreference.com
http://news.internet2.com
http://gopher.gopher.unam
ftp://ftp.netscape.com
ftp://ftp.ipswitch.com
http://www.internic.net/
http://www.isoc.org
http://www.iana.org
http://www.ietf.org
http://www.iab.org
http://www.rfc.net/
www.whowhere.com
www.pregunta.com
www.nettools.com

http://www.itu.org/
www.atmforum.com
www.frforum.com
http://abcdatos.com/
http://www.tutoriales.com/
http://www.ciberteca.net/
www.speedtest.com
www.monografías.com
www.recursosvoip.com
www.iec.org
http://www.howstuffworks.com/
www.intermaqnagers.com
www.nordxcdt.com
www.alcatel.com
www.belden.com
www.tiaonline.com
www.siemon.com
www.lucent.com
www.anixter.com
www.bertek.com
www.siecor.com
www.pouyet.com
www.rittal.com
www.blackbox.com
www.cofetel.gob.mx
www.telmex.com.mx
www.conocer.gob.mx