ELEMENTOS DE UNA RED

Los principales elementos que necesitamos para instalar una red son :

- Tarjetas de red.
- Cable.
- Protocolos de comunicaciones.
- Sistema operativo de red.
- Aplicaciones capaces de funcionar en red.

TARJETAS DE INTERFAZ DE RED

Las tarjetas de interfaz de red (NICs - Network Interface Cards) son adaptadores instalados en un dispositivo, conectándolo de esta forma en red. Es el pilar en el que sustenta toda red local, y el único elemento imprescindible para enlazar dos ordenadores a buena velocidad (excepción hecha del cable y el software). Existen tarjetas para distintos tipos de redes. Las principales características de una tarjeta de red son :

- Operan a nivel físico del modelo OSI : Las normas que rigen las tarjetas determinan sus características , y su circuitería gestiona muchas de las funciones de la comunicación en red como :
    - Especificaciones mecánicas : Tipos de conectores para el cable, por ejemplo.
    - Especificaciones eléctricas : definen los métodos de transmisión de la información y las señales de control para dicha transferencia.
    - Método de acceso al medio : es el tipo de algoritmo que se utiliza para acceder al cable que sostiene la red.
    - La circuitería de la tarjeta de red determina, antes del comienzo de la transmisión de los datos, elementos como velocidad de transmisión, tamaño del paquete, time-out, tamaño de los buffers. Una vez que estos elementos se han establecido, empieza la verdadera transmisión, realizándose una conversión de datos a transmitir a dos niveles :
- La dirección física es un concepto asociado a la tarjeta de red : Cada nodo de una red tiene una dirección asignada que depende de los protocolos de comunicaciones que esté utilizando. La dirección física habitualmente viene definida de fábrica, por lo que no se puede modificar. Sobre esta dirección física se definen otras direcciones, como puede ser la dirección IP para redes que estén funcionando con TCP/IP.

DETERMINACIÓN DE LA VELOCIDAD DE TRANSMISIÓN EN UNA RED

Existen varios factores que determinan la velocidad de transmisión de una red, entre ellos podemos destacar :

- El cable utilizado para la conexión. Dentro del cable existen factores como :
    - El ancho de banda permitido.
    - La longitud.

Existen otros factores que determinan el rendimiento de la red, son :

- Las tarjetas de red.
- El tamaño del bus de datos de las máquinas.
- La cantidad de retransmisiones que se pueden hacer.

MEDIOS DE TRANSMISIÓN DE UNA RED LOCAL

Se pueden diferenciar dos grupos :

- Los cables.
- Los medios inalámbricos.

CABLES

El cable utilizado para formar una red se denomina a veces *medio*. Los tres factores que se deben tener en cuenta a la hora de elegir un cable para una red son :

- Velocidad de transmisión que se quiere conseguir.
- Distancia máxima entre ordenadores que se van a conectar.
- Nivel de ruido e interferencias habituales en la zona que se va a instalar la red.

Los cables más utilizados son el par trenzado, el cable coaxial y la fibra óptica.

PAR TRENZADO

Se trata de dos hilos de cobre aislados y trenzados entre sí, y en la mayoría de los casos cubiertos por una malla protectora. Los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor (dos pares paralelos constituyen una antena simple, en tanto que un par trenzado no).

Se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer.

Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando. Está dividido en categorías por el EIA/TIA :

- **Categoría 1**: Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbits/seg
- **Categoría 2** : Cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbits/seg.
- **Categoría 3** : Velocidad de transmisión de 10 Mbits/seg. Con este tipo de cables se implementa las redes Ethernet 10-Base-T
- **Categoría 4** : La velocidad de transmisión llega a 16 bits/seg.
- **Categoría 5** : Puede transmitir datos hasta 100 Mbits/seg.

Tiene una longitud máxima limitada y, a pesar de los aspectos negativos, es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico y esto permite utilizarlo sin necesidad de obra. La mayoría de las mangueras de cable de par trenzado contiene más de un par de hilos por lo que es posible encontrar mangueras ya instaladas con algún par de hilos sin utilizarse. Además resulta fácil de combinar con otros tipos de cables para la extensión de redes.

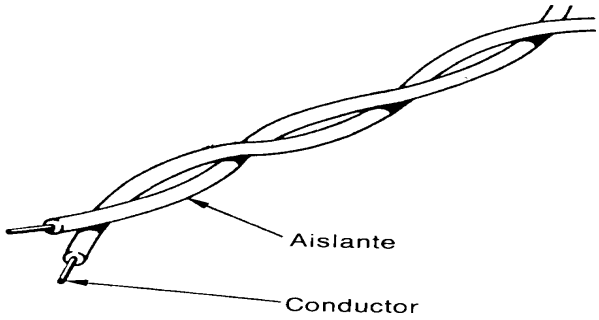


Figura: Cable de par trenzado

CABLE COAXIAL

Consiste en un núcleo de cobre rodeado por una capa aislante. A su vez, esta capa está rodeada por una malla metálica que ayuda a bloquear las interferencias; este conjunto de cables está envuelto en una capa protectora. Le pueden afectar las interferencias externas, por lo que ha de estar apantallado para reducirlas. Emite señales que pueden detectarse fuera de la red.

Es utilizado generalmente para señales de televisión y para transmisiones de datos a alta velocidad a distancias de varios kilómetros.

La velocidad de transmisión suele ser alta, de hasta 100 Mbits/seg; pero hay que tener en cuenta que a mayor velocidad de transmisión, menor distancia podemos cubrir, ya que el periodo de la señal es menor, y por tanto se atenúa antes.

La nomenclatura de los cables Ethernet tiene 3 partes :

- La primera indica la velocidad en Mbits/seg.
- La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD).
- La tercera los metros de segmento multiplicados por 100.

CABLE	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión : 10 Mb/seg. Segmentos : máximo de 500 metros.
10-BASE-2	Cable coaxial fino (Ethernet fino). Velocidad de transmisión : 10 Mb/seg. Segmentos : máximo de 185 metros.
10-BROAD-36	Cable coaxial Segmentos : máximo de 3600 metros. Velocidad de transmisión : 10 Mb/seg.
100-BASE-X	Fast Ethernet. Velocidad de transmisión : 100 Mb/seg.

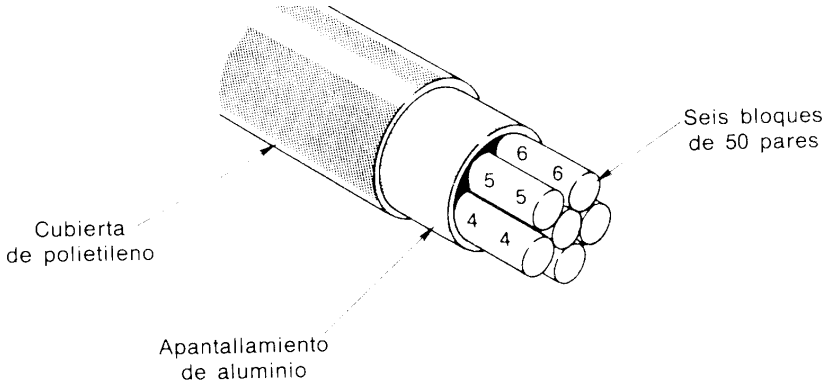


Figura Estructura típica de un cable de pares

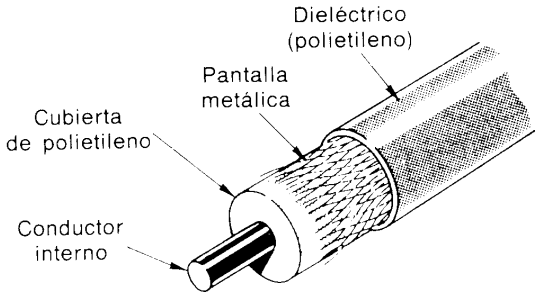


Figura : Estructura típica de un cable coaxial

CABLE DE FIBRA ÓPTICA

Una fibra óptica es un medio de transmisión de la luz que consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura.
En la superficie de separación entre el núcleo y la envoltura se produce el fenómeno de reflexión total de la luz, al pasar éste de un medio a otro que tiene un índice de refracción más pequeño. Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra.
Este conjunto está envuelto por una capa protectora. La velocidad de transmisión es muy alta, 10 Mb/seg siendo en algunas instalaciones especiales de hasta 500 Mb/seg, y no resulta afectado por interferencias.
Los cables de fibra óptica tienen muchas aplicaciones en el campo de las comunicaciones de datos:

- Conexiones locales entre ordenadores y periféricos o equipos de control y medición.
- Interconexión de ordenadores y terminales mediante enlaces dedicados de fibra óptica.
- Enlaces de fibra óptica de larga distancia y gran capacidad.

Los cables de fibra óptica ofrecen muchas ventajas respecto de los cables eléctricos para transmitir datos:

- Mayor velocidad de transmisión. Las señales recorren los cables de fibra óptica a la velocidad de la luz (c = 3 X 10^9 m/s), mientras que las señales eléctricas recorren los cables a una velocidad entre el 50 y el 80 por cien de ésta, según el tipo de cable.
- Mayor capacidad de transmisión. Pueden lograrse velocidades por encima de 1 Gbit/s.
- Inmunidad total ante interferencias electromagnéticas. La fibra óptica no produce ningún tipo de interferencia electromagnética y no se ve afectada por rayos o por pulsos electromagnéticos nucleares (NEMP) que acompañan a las explosiones nucleares.
- No existen problemas de retorno de tierra, crosstalk o reflexiones como ocurre en las líneas de transmisión eléctricas.
- La atenuación aumenta con la distancia más lentamente que en el caso de los cables eléctricos, lo que permite mayores distancias entre repetidores.
- Se consiguen tasas de error típicas del orden de 1 en 10^9 frente a las tasas del orden de 1 en 10^6 que alcanzan los cables coaxiales. Esto permite aumentar la velocidad eficaz de transmisión de datos, reduciendo el número de retransmisiones o la cantidad de información redundante necesaria para detectar y corregir lo errores de transmisión.
- No existe riesgo de cortocircuito o daños de origen eléctrico.
- Los cables de fibra óptica pesas la décima parte que los cables de corte apantallados. Esta es una consideración de importancia en barcos y aviones.
- Los cables de fibra óptica son generalmente de menor diámetro, más flexibles y más fáciles de instalar que los cables eléctricos.
- Los cables de fibra óptica son apropiados para utilizar en una amplia gama de temperaturas.
- Es más difícil realizar escuchas sobre cables de fibra óptica que sobre cables eléctricos. Es necesario cortar la fibra para detectar los datos transmitidos. Las escuchas sobre fibra óptica pueden detectarse fácilmente utilizando un reflectómetro en el dominio del tiempo o midiendo las pérdidas de señal.
- Se puede incrementar la capacidad de transmisión de datos añadiendo nuevos canales que utilicen longitudes de onda distintas de las ya empleadas.
- La fibra óptica presenta una mayor resistencia a los ambientes y líquidos corrosivos que los cables eléctricos.
- Las materias primas para fabricar vidrio son abundantes y se espera que los costos se reduzcan a un nivel similar al de los cables metálicos.
- La vida media operacional y el tiempo medio entre fallos de un cable de fibra óptica son superiores a los de un cable eléctrico.
- Los costos de instalación y mantenimiento para grandes y medias distancias son menores que los que se derivan de las instalaciones de cables eléctricos.

La mayor desventaja es que no se puede "pinchar" fácilmente este cable para conectar un nuevo nodo a la red..

Las transmisiones de la señal a grandes distancias se encuentran sujetas a atenuación, que consiste en una pérdida de amplitud o intensidad de la señal, lo que limita la longitud del cable. Los segmentos pueden ser de hasta 2000 metros.

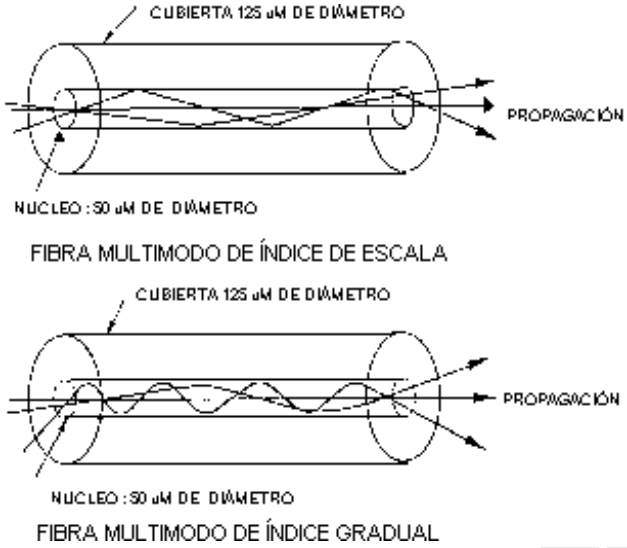


Figura: Propagación multimodo en una fibra óptica de índice de escala y de índice gradualMEDIOS INALÁMBRICOS

ENLACES ÓPTICOS AL AIRE LIBRE

El principio de funcionamiento de un enlace óptico al aire libre es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es un polímero o fibra de vidrio sino el aire.

El emisor óptico produce un haz estrecho que se detecta en un sensor que puede estar situado a varios kilómetros en la línea de visión. Las aplicaciones típicas para estos enlaces se encuentran en los campus de la universidades, donde las carreteras no permiten tender cables, o entre los edificios de una compañía en una ciudad en la que resulte caro utilizar los cables telefónicos.

Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Las prestaciones de este tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos. Se puede permitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s . El límite para comunicaciones fiables se encuentra sobre los dos kilómetros. Para distancias de más de dos kilómetros son preferibles los enlaces de microondas.

Existen dos efectos atmosféricos importantes a tener en cuenta con los enlaces ópticos al aire libre :

- La dispersión de la luz que atenúa la señal óptica en proporción al número y al tamaño de las partículas en suspensión en la atmósfera. Las partículas pequeñas, como la niebla, polvo o humo, tienen un efecto que es función de su densidad y de la relación existente entre su tamaño y de la longitud de onda de la radiación infrarroja utilizada. La niebla, con una elevada densidad de partículas, de 1 a 10 μm

de diámetro, tienen un efecto más acusado sobre el haz de luz. Las partículas de humo, más grandes, tienen menor densidad y, por tanto, menor efecto.

- Las brisas ascensionales (originadas por movimientos del aire como consecuencia de las variaciones en la temperatura) provocan variaciones en la densidad del aire y, por tanto, variaciones en el índice de refracción a lo largo del haz. Esto da lugar a la dispersión de parte de la luz a lo largo del haz. Este efecto puede reducirse elevando el haz de luz lo bastante con respecto a cualquier superficie caliente o utilizando emisores múltiples. La luz de cada emisor se ve afectada de diferente forma por las brisas, y los haces se promedian en el receptor.

Estos sistemas suelen emplearse para transmisiones digital de alta velocidad en banda base. En EE.UU, todos los fabricantes de productos láser deben tener una certificación que garantiza la seguridad de sus productos.

MICROONDAS

Los enlaces de microondas se utilizan mucho como enlaces allí donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda de SHF, de modo que es necesario dispones de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores.
Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2,4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionara hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo.
Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11} dependiendo de la relación señal/ruido en los receptores. Pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores.
Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

LUZ INFRARROJA

Permite la transmisión de información a velocidades muy altas : 10 Mbits/seg. Consiste en la emisión/recepción de un haz de luz ; debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

COMUNICACIONES VIA SATÉLITE

Los satélites artificiales han revolucionado las comunicaciones desde los últimos 20 años. Actualmente son muchos los satélites de comunicaciones que están alrededor de la tierra dando servicio a numerosas empresas, gobiernos, entidades Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (canal de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (canal de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión. De esta manera se impide que los canales de subida y de bajada se interfieran, ya que trabajan en bandas de frecuencia diferentes.

La capacidad que posee una satélite de recibir y retransmitir se debe a un dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de los gigahertzios. La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria, que se encuentra a 36000 Km sobre el ecuador . Esto permite que el satélite gire alrededor de la tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la tierra.

- Existe un retardo de unos 0.5 segundos en las comunicaciones debido a la distancia que han de recorrer las señales. Los cambios en los retrasos de propagación provocados por el movimiento en ocho de un satélite geoestacionario necesita transmisiones frecuentes de tramas de sincronización.
- Los satélites tienen una vida media de siete a 10 años, pero pueden sufrir fallos que provocan su salida de servicio. Es, por tanto, necesario dispones de un medio alternativo de servicio en caso de cualquier eventualidad.
- Las estaciones terrenas suelen estar lejos de los usuarios y a menudo se necesitan caros enlaces de alta velocidad. Las estaciones situadas en la banda de bajas frecuencias (la banda C) están dotadas de grandes antenas (de unos 30 metros de diámetro) y son extremadamente sensibles a las interferencias. Por este motivo suelen estar situadas lejos de áreas habitadas. Las estaciones que trabajan en la banda Ku disponen de una antena menor y son menos sensibles a las interferencias. Utilizar un enlace de microondas de alta capacidad sólo ayudaría a complicar los problemas de ruido que presente el enlace con el satélite.
- Las comunicaciones con el satélite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estación. Es necesario utilizar técnicas de encriptación para garantizar la privacidad de los datos.
- Los satélites geoestacionarios pasan por periodos en los que no pueden funcionar. En el caso de un eclipse de Sol en el que la tierra se sitúa entre el Sol y el satélite, se corta el suministro de energía a las células solares que alimentan el satélite, lo que provoca el paso del suministro de energía a las baterías de emergencia, operación que a menudo se traduce en una reducción de las prestaciones o en una pérdida de servicio.
- En el caso de tránsitos solares, el satélite pasa directamente entre el Sol y la Tierra provocando un aumento del ruido térmico en la estación terrena, y una pérdida probable de la señal enviada por el satélite.
- Los satélites geoestacionarios no son totalmente estacionarios con respecto a la órbita de la tierra. Las desviaciones de la órbita ecuatorial hace que el satélite describa una figura parecida a un ocho, de dimensiones proporcionales a la inclinación de la órbita con respecto al ecuador. Estas variaciones en la órbita son corregidas desde una estación de control.
- Actualmente hay un problema de ocupación de la órbita geoestacionaria. Cuando un satélite deja de ser operativo, debe irse a otra órbita, para dejar un puesto libre. La separación angular entre satélites debe ser de 2 grados (anteriormente era de 4). Esta medida implicó la necesidad de mejorar la capacidad de resolución de las estaciones terrenas para evitar detectar las señales de satélites próximos en la misma banda en forma de ruido.

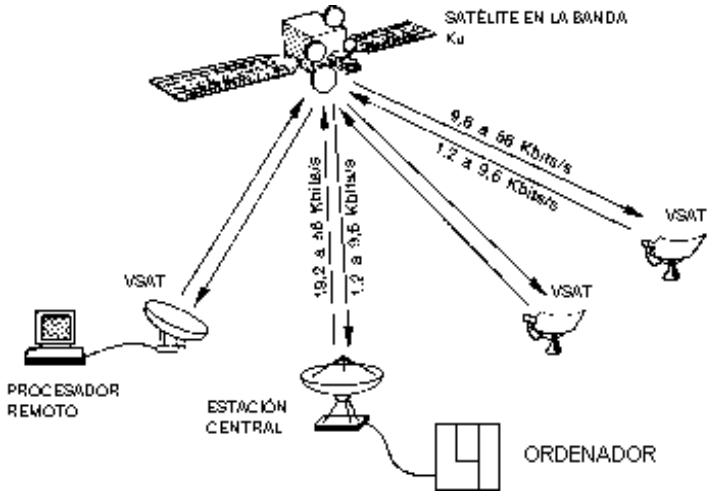


Figura: La red de datos de AT&T utiliza un satélite para conectar las estaciones a una estación central

CONCEPTOS GENERALES DE REDES – PROTOCOLO TCP/IP

Desde el momento que surge la necesidad de realizar una conexión entre distintas redes, se fija como primer objetivo ocultar no sólo el hardware sino, tambien, el tipo de red sobre el que se sustenta la comunicación, para lo que se define una serie de servicios universales de comunicación.
Este objetivo de transparencia puede alcanzarse a través de los programas de aplicación que de encarguen de tratar en cada máquina con la red y el hardware específico con que ésta cuenta proporcionando un sistema uniforme en la red. Sin embargo, este enfoque si bien es más intuitivo y concreto y a veces se emplea en programas reducidos para resolver un problema bien definido, presenta grandes problemas en cuanto el escenario aparece como un conjunto heterogéneo más o menos numeroso y, sobre todo, cuando se persigue cierta generalidad. Así, si en determinado momento se desea incorporar una nueva funcionalidad, es necesario desarrollar código para cada diferente arquitectura.
Es este planteamiento el que se emplea en todo sistema abierto que se ha dado a llamar networking.

¿Qué es Networking?

Se define como Networking o redes de computadoras, a la interconexión de un conjunto de equipos mediante un medio de transmisión, por lo que se permite a determinados datos llegar de un origen a un destino determinados.

•Sin networking :

–Redundancia de datos.
–Inconsistencia de información.
–Duplicación de equipos y recursos.
–Imposibilidad de comunicarse en forma eficiente.
–Falta de administración de la red.

•Con networking :

–Datos únicos. Actualizacion autom.
–Consistencia de información.
–Recursos mejor aprovechados.

–Comunicación optimizada entre procesos y usuarios.
–Posibilidad de administración de los recursos.**ISO (International Organization for Standardization)**

Comienza a investigar un modelo para unificar criterios (mediados de los 80s) por la gran diversidad de protocolos de comunicación que empezaron a aparecer en base a la implementacion del networking.
ISO se trata de una organización reconocida mundialmente de normalización. Su objetivo es el de promover y desarrollar normas para el intercambio internacional. Establece normas de estandarización en muchísimos campos, estableciendo modelos a seguir para todos y cada uno de ellos. Abarca campos tan dispares como el diámetro de algunos tipos de conectores, el paso de rosca de tornillos, el grosor de un modelo concreto de cable, etc. En cuanto al campo de las comunicaciones, la ISO ha desarrollado un modelo, al que llamó OSI. Sus normas fomentan los entornos abiertos de conexión de red, que permiten a sistemas de diferentes casas comerciales comunicarse entre sí mediante el uso de protocolos.

OSI (Open System Interconnection): se trata de un modelo elaborado por la ISO que define los protocolos de comunicación en siete niveles diferentes. Estos niveles son los siguientes: aplicación, presentación, sesión, transporte, red, enlace y físico. Cada nivel se encarga de una parte en el proceso de transmisión (en el proceso de elaboración de la información a transmitir), apoyándose en los servicios que le ofrece el nivel inferior y dando servicios a niveles superiores.
Cada nivel tiene funciones muy definidas, que se interrelacionan con las funciones de niveles contiguos. Los niveles inferiores definen el medio físico, conectores y componentes que proporcionan comunicaciones de red, mientras que los niveles superiores definen cómo acceden las aplicaciones a los servicios de comunicación.

PROTOCOLO TCP-IP

Con el fin de comprender la naturaleza de los ataques contra los sistemas de información, los métodos de detección y protección, se procederá a describir en el presente capítulo algunos de los protocolos que intervienen en el intercambio de información en redes y sus características

TCP/IP y su relación con Internet.

TCP/IP no es un protocolo solo, sino una familia de protocolos relacionados que ejecutan tareas dedicadas.
TCP/IP es una familia de protocolos que se ocupa de una amplia variedad de tareas, todas entrelazadas e interrelacionadas de alguna forma. Conforme ha crecido la popularidad de Internet y los sistemas operativos UNIX, se ha producido un aumento continuo en el número de redes TCP/IP. UNIX y TCP/IP ha estado entrelazadas desde el principio mismo de la historia del protocolo, lo que resulta evidente en varios de los archivos de configuración, así como en la arquitectura de TCP/IP. En los últimos años han surgido implementaciones TCP/IP para prácticamente todas las plataformas de hardware y sistemas operativos disponibles. casi todas ellas compatibles.

¿ Qué es TCP/IP ?

Es un protocolo de comunicaciones que se basa en software utilizado en redes. Aunque el nombre TCP/IP implica que el ámbito total del producto es la combinación de dos protocolos - protocolo de control de transmisión - (transmission control protocol) y protocolo Internet (Internet protocol) , el término TCP/IP no es una

entidad única que combina dos protocolos, sino un conjunto de programas de software más grande que proporciona servicios de red, como registro de entrada remoto, transferencia de archivos remota y correo electrónico. TCP/IP ofrece un método de transferir información de una máquina a otra. un protocolo de comunicaciones debe manejar los errores en la transmisión, administrar el encaminamiento y entrega de los datos, así como controlar la transmisión real mediante el uso de señales de estado predeterminadas. TCP/IP se ocupa de todo lo anterior.

Breve Historia de TCP/IP

Internet fue propuesta originalmente por la precursora de DARPA, la agencia de proyectos de investigación avanzada de la defensa (advanced research projets agency, ARPA), como una forma de probar la viabilidad de las redes de conmutación de paquetes. (Cuando el enfoque de ARPA se volvió de naturaleza militar, se cambió el nombre). Durante su estadía en el proyecto, ARPA previó una red de líneas rentadas conectadas por nodos de conmutación. La red se denominó ARPAnet y los nodos se conocieron como procesadores de Mensajes de Internet (IMPs).

ARPAnet inicialmente está formada pro cuatro IMPs. En 1971 ARPAnet entró en servicio normal. Las máquinas utilizaron ARPAnet mediante la conexión a un IMP y utilizando el protocolo "1822" (Número del documento técnico que describía el sistema).

Una necesidad comúnmente reconocida era la capacidad de transferir archivos de una máquina a otra, así como la capacidad de aceptar registro de entrada remoto no podían ser realizados hasta que se implementaron en un protocolo conocido como Programa de Control de Red (Network Control Program, NCP) que cumplía con estos requisitos. Más adelante, a través de FTP (Protocolo de Transferencia de Archivo, File Transfer Protocol) se añadió el correo electrónico y junto con el registro y la transferencia de archivos remotas de NCP, se conformaron los servicios de ARPAnet.

Al llegar 1973 resultaba claro que NCP era incapaz de manejar el volumen de tráfico y la nueva funcionalidad propuesta. Se inició un proyecto con el objetivo de desarrollar un nuevo protocolo. El nacimiento de TCP/IP y las arquitecturas de los routers fueron propuestos por primera vez en 1974. El artículo publicado por Cerf y Kahn describía un sistema que incluía un protocolo de aplicación estandarizada, que también utilizaba confirmaciones de extremo a extremo.
También, proponían conectividad universal a través de la red. Estas dos ideas eran radicales en un mundo de hardware y software propietarios, porque permitirían que cualquier tipo de plataforma participara en la red. El protocolo fue creado y se conoció como TCP/IP.

OSI y TCP/IP

La adopción de TCP/IP no entraba en conflicto con los estándares OSI, porque ambos se desarrollaron en forma simultánea. De alguna manera TCP/IP contribuyo con OSI y viceversa.
Sin embargo hay varias diferencias de importancia, que se originan en los requerimientos básicos de TCP/IP:

· Un conjunto común de aplicaciones
· Enrutamiento dinámico
· Protocolos sin conexión en nivel de red
· Conectividad universal
· Conmutación de paquetes

Las diferencias entre la arquitectura OSI y la de TCP/IP están relacionadas con las capas encima del nivel de transporte, y las que corresponden al nivel de red. OSI tiene tanto una capa de sesión como una capa de presentación, en tanto que TCP/IP combina ambas en una capa de aplicación. El requisito de un protocolo sin conexión también hacia que TCP/IP combinara las capas física y de vínculo de datos de OSI en el nivel de red. En la figura 1 aparece una vista esquemática de la estructura en capas de TCP/IP (en comparación con el modelo de siete capas de OSI). TCP/IP denomina a los distintos elementos de niveles de red como subredes.

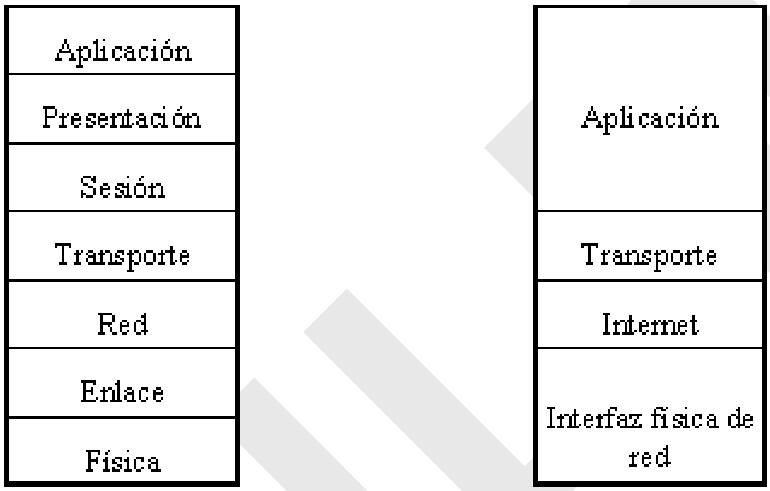


Figura 1: Estructuras en capas OSI y TCP/IP

OSI y TCP/IP no son incompatibles, pero tampoco son perfectamente compatibles. Ambos tienen una arquitectura en capas. La arquitectura OSI está definida con mucho más rigor y TCP/IP las capas son más independientes.
La combinación de dos capas en una sola tenía una ventaja importante: permitía que se diseñara una subred que resultaba independiente de muchos protocolos de control de transmisión (TCP) o alguna de las variables como protocolo de datagrama de usuario (UDP). Sin embargo hay un solo protocolo para el nivel de red. El protocolo Internet (IP) esto es lo que asegura la conectividad universal del sistema, una de las prioridades principales del diseño.

CARACTERÍSTICAS DE TCP/IP

Las principales características son:

- Utiliza conmutación de paquetes.
- Proporciona una conexión fiable entre dos máquinas en cualquier punto de la red.
- Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.
- Se apoya en los protocolos de más bajo nivel para acceder a la red física (Ethernet, Token-Ring).

FUNCIONAMIENTO DE TCP/IP

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetess conteniendo :

- La información a transmitir.
- La dirección IP del destinatario.
- La dirección IP del remitente.
- Otros datos de control.

PROTOCOLO IP

Se trata de un protocolo a nivel de red cuyas principales caraterísticas son:

- Ofrece un servicio no orientado a la conexión; esto significa que cada trama en la que ha sido dividido un paquete es tratado por independiente. Las tramas que componen un paquete pueden ser enviadas por caminos distintos e incluso llegar desordenadas.
- Ofrece un servicio no muy fiable porque a veces los paquetes se pierden, duplican o estropean y este nivel no informa de ello pues no es consciente del problema.

DIRECCIONAMIENTO DE INTERNET

Una dirección se representa por cuatro valores decimales separados por puntos, para que sea más fácil su escritura y memorización.

Las direcciones de red son análogas a las direcciones de correos, en el sentido de que le indican a un sistema donde debe entregar un datagrama. Tres términos utilizados comúnmente en Internet se relacionan con el direccionamiento: nombre, dirección y ruta.

Un nombre es una identificación especifica de una máquina, un usuario o una aplicación. Por lo general es único y proporciona un objetivo absoluto para el datagrama.

Una dirección típicamente identifica la localización del objetivo, por lo general su localización física o lógica en una red.
Una ruta le dice al sistema como hacer llegar el datagrama a la dirección.

DIRECCIONES IP

TCP/IP utiliza una dirección de 32 bits para identificar una maquina y la red a la cual esta conectada.

[0..255] . [0..255] . [0..255] . [0..255]

Las direcciones IP identifican la conexión de la maquina a la red, no la máquina misma. Siempre que se modifique la localización de la máquina en la red, también deberá modificarse la dirección IP. Esta es el conjunto de números que muchas personas ven en sus estaciones de trabajos o en sus terminales, como 127.40.8.72, y que identifican en forma única al dispositivo.

Unicamente el Centro de Informacion de Red (NIC) asigna las direcciones IP (o Internet), aunque si una red no esta conectada a Internet, dicha red puede

determinar su propio sistema de numeración. Sin embargo, las direcciones IP deberán ser registradas ante el NIC para todos los accesos a Internet.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, clase A hasta clase D, se muestran en la figura 3.

figura 3: Las cuatro estructuras de clases de dirección IP

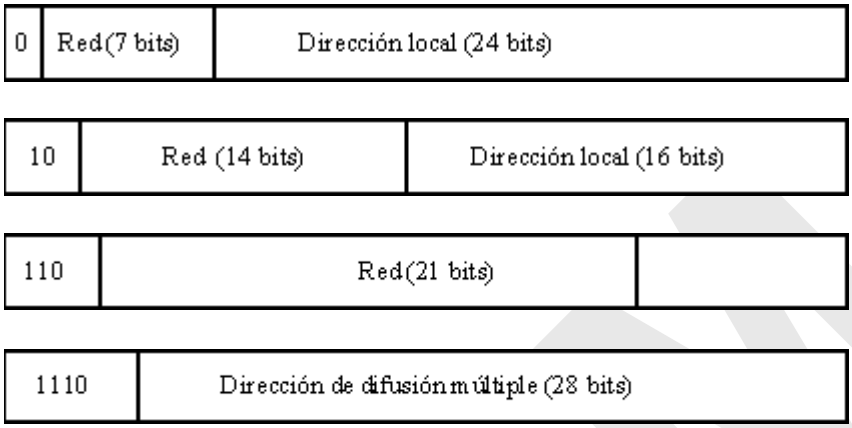


figura 3: Las cuatro estructuras de clases de dirección IP

Las direcciones de clase A corresponden a redes grandes con muchas máquinas.

Las direcciones de clase B sirven para redes de tamaño intermedios.

La red de clase C limita el numero de dispositivos a 256.

Las redes de clase D y E se utilizan con fines de multidifusión, cuando se requiere una difusión general a mas de un dispositivo.

CLASES DE REDES

El tipo depende de el número de máquinas que forman la red; atendiendo esto se pueden distinguir tres clases de redes :

Redes de clase A : Las principales características son :

Se tratan de redes de mayor tamaño, redes que tengan más de 2^{16} hosts.
El espacio reservado para la dirección de red es más pequeño por dos motivos:
- Porque existen menos redes de este tipo.
- Porque al tener más hots necesitamos dejar más espacios para direccionar a estos.

La parte que identifica la red consta de

- un cero (0)
- 7 bits más.

Se podrán direccionar por tanto 2^7 redes que hace un total de 128 redes diferentes. Cada una de estas redes podrá tener 2^{24} posibles hosts. La dirección 127 no se utiliza.

1……..7	8……..32
Dirección de la red 0…..	Identificador de la máquina

Redes de clase B: Son redes de tamaño mediano que tienen entre 2^8 y 2^{16} hosts. La parte que identifica la red consta de

- La secuencia uno-cero (10).
- 14 bits con cualquier valor.

Por tanto, el rango de valores para el primer byte de los dos asignados a la red es de :128-191.

Estas redes pueden tener 2^{16}=65536 hosts cada una de ellas. El formato de las direcciones es:

1……..……16	17…….……..32
Dirección de la red 10…..	Identificador de la máquina

Redes de clase C: Son redes menor tamaño que pueden tener hasta 2^8 hosts. La parte que identifica la red consta de

- La secuencia uno-uno-cero (110).
- 21 bits con cualquier valor.

Por tanto, el rango de valores para el primer byte de los dos asignados a la red es de :192-223.

Estas redes pueden tener 2^8=256 hosts cada una de ellas. El formato de las direcciones es:

0……..……23	24……..31
Dirección de la red 110…..	Identificador de la máquina

TABLA ESQUEMÁTICA DE LOS FORMATOS DE DIRECCIONES

	Byte 1	**Byte 2**	**Byte 3**	**Byte 3**
Clase A	0…126	0…255	0…255	0…255
Clase B	128 …191	0…255	0…255	0…255
Clase C	192…223	0…255	0…255	0…255

Existen más clases de redes, como la D, E y F cuyo rango de direcciones oscila entre 224.0.0.0 y 254.0.0.0 . Este tipo de redes son experimentales o se reservan para un uso futuro.

Ejemplo: la dirección 156.35.41.20 identifica el host 41.20 de la red 156.35.

A partir de la dirección IP, una red puede determinar si los datos serán enviados a través de un router. El router que reciba los datos que se transmitirán a otra red, tendrá entonces que determinar el enrutamiento con base en la dirección IP de los datos y una tabla interna que contiene información de enrutamiento.

LAS CAPAS DE INTERNET

El concepto de capas ayudan en la tarea de desarrollar las aplicaciones para las interredes. Este diseño en capas también muestra como funcionan juntas las distintas partes de TCP/IP.

Hay que recordar que estas capas son solo conceptuales; no son verdaderamente capas físicas ni de software como tal (a diferencia de las capas OSi o TCP/IP).
Resulta conveniente pensar en Internet como formado por cuatro capas. Esta arquitectura Internet en capas se muestra en la figura 2. Tales capas no deben confundirse con la arquitectura de cada maquina, descripta en el modelo de siete capas de OSI, sino como un método para apreciar como funcionan juntos la interred, la red local, TCP/IP y cada una de las maquinas individuales. Las maquinas independientes residen en la capa de subred en la parte inferior de la arquitectura, conectadas juntas en una red de área local (LAN) e identificadas como la subred.

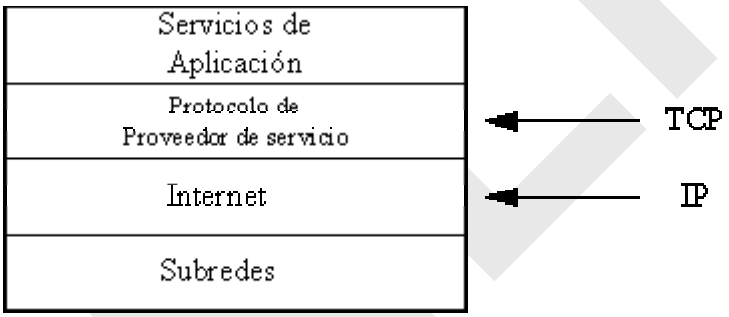


figura 2: Arquitectura de Internet

Por encima de la capa de subred esta la interred, que proporciona la funcionalidad para las comunicaciones entre redes a través de routers. Cada subred utiliza routers para conectarse a otras subredes en la interred. En estas capas los datos son transferidos de un router a otro hasta que llegan a su destino, y entonces pasan a la capa de subred. El protocolo Internet corre en la capa de interred.

La capa del protocolo del proveedor de servicios es responsable de las comunicaciones extremo a extremo de la red. Esta es la capa donde corre el Protocolo de Control de Transmisión (TCP), así como otros protocolos. Por si misma maneja el flujo de trafico de datos y asegura la confiabilidad de la transferencia del mensaje.

La capa mas alta es la de los servicios de aplicación, que soporta las interfaces con las aplicaciones de usuario. Esta capa es la interfaz para el correo electrónico, las transferencias remotas de archivos y el acceso remoto.

Arquitectura de protocolos TCP/IP

La arquitectura TCP/IP se basa en un mecanismo de internetworking basado en cuatro premisas:

1- Los programas de aplicación no deben tener conocimiento del hardware para realizar la comunicación.
2- La interfaz del usuario debe ser independiente del sistema, lo que permite que los programas no necesiten conocer el tipo de red sobre el que se encuentran.
3- La Internet no impone el uso de ninguna topología en especial.
4- El protocolo de red considera redes enteras como sistemas finales y permite transmitir información a través de redes intermedias que actúan como nodos intermedios en las redes.

Descomposición en niveles de TCP/IP

Toda arquitectura de protocolos, al menos desde un punto de vista abstracto o de referencia, se suele descomponer en un modelo en capas o niveles en los que se sitúan diversos protocolos que especifican como transmitir la información entre máquinas. Esto obedece a una necesidad de atenuación de complejidad. El problema global se subdivide en distintas áreas con problemas aislados, y a cada una de ellas se asocia un nivel.

La arquitectura TCP/IP, que al contrario de OSI no proviene de ningún comité, se puede considerar (a priori) dividida en cuatro niveles software y un quinto nivel correspondiente al hardware de comunicaciones.

Distintos niveles:

NIVEL DE APLICACIÓN: constituye el nivel más alto de la torre TCP/IP, se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet invocadas por el usuario. Las aplicaciones pueden elegir el tipo de transporte que necesitan, ya sea transmisión fiable de un flujo de bits o transmisión no fiable de mensajes delimitados, e interactúan con los protocolos de transporte únicamente para enviar y recibir datos.

NIVEL DE TRANSPORTE: el nivel de transporte análogo al nivel cuatro OSI, proporciona una comunicación extremo a extremo entre programas de aplicación.

En caso de emplear un transporte fiable se gestionan retransmisiones, confirmaciones y se realiza control de flujo. El nivel de transporte divide los datos que le proporciona el nivel de aplicación en paquetes (terminología TCP/IP) que pasa al siguiente nivel junto con la dirección de destino. Como existe la posibilidad de atender a varias aplicaciones añade información adicional a estos paquetes para identificar la aplicación remitente y la destinataria.

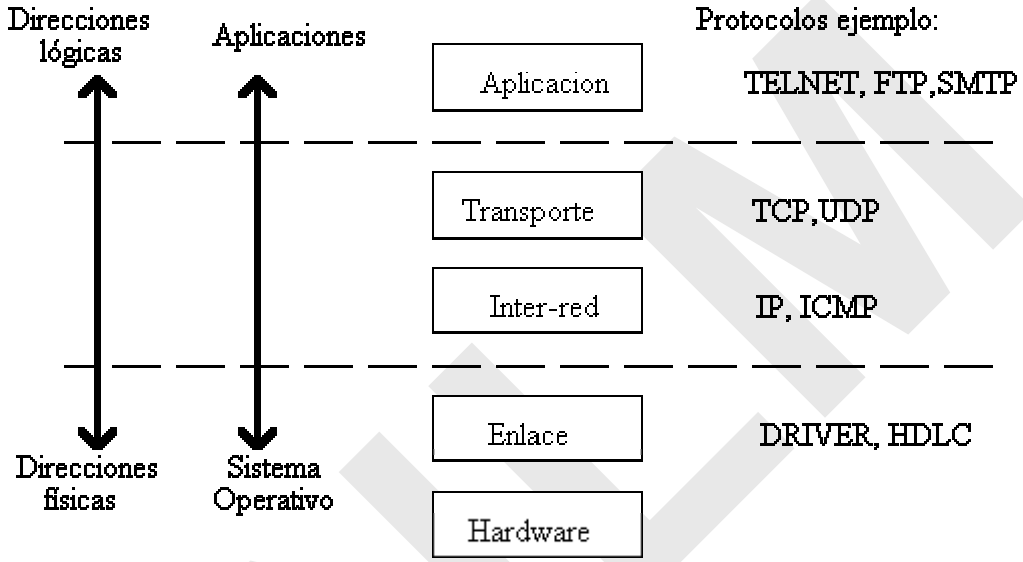
El **nivel de transporte**, intercambia mensajes delimitados o flujos de bits con su homólogo en la máquina remota (comunicación horizontal, entre entidades homólogas) y no paquetes, que es lo que pasa al nivel inferior (comunicación vertical, entre niveles de la misma máquina).

NIVEL INTER-RED (INTERNET): el nivel inter-red es el que genera la red virtual (Internet). Para ello coloca la información que le proporciona el nivel de transporte en datagramas IP (unidad básica de transferencia), que añade unas cabeceras con información necesaria para el nivel, y los pasa al nivel de interfaz de red. Es en este nivel donde se emplean los algoritmos de encaminamiento. Por ejemplo, al recibir un datagrama del nivel inferior decide en función de su dirección de destino si debe

procesarlo y pasarlo a un nivel superior o si por el contrario debe realizar un forwarding, es decir, si debe dejarlo "pasar a través", y retransmitirlo, colocándole una nueva dirección de destino y devolviéndolo al nivel inferior. También será este nivel el que procese los mensajes de error y control del protocolo ICMP, que circula encapsulados en datagramas IP.

NIVEL DE ENLACE: Este nivel se limita a recibir del nivel superior los datagramas IP y transmitirlos por la red local, pro lo que actúan como una interfaz de acceso a la red. Puede ser tan simple como un driver de dispositivo o todo un subsistema con un protocolo de enlace propio como HDLC.

MODELOS DE NIVELES TCP/IP



PROBLEMAS DE LA INTERRED

· No todo funciona perfectamente al transferir los datos de una subred a otra. A pesar de que toda la red usa un solo protocolo, diversos problemas pueden ocurrir. Un problema típico es la limitación en el tamaño de los datagramas (unidad básica de datos usada en TCP/IP). La red emisora quizás soporte datagramas de 1024 bytes, pero la red receptora tal vez solo maneje datagramas de 512 bytes.

· Los métodos de direccionamientos reales utilizados por las distintas subredes pueden causar conflictos al enrutar o encaminar datagramas. Debido a que las subredes en comunicación quizá no tenga el mismo software de control de red, a pesar de que los métodos de comunicación estén basados en TCP/IP.

· La distinta tolerancia que cada red tiene a problemas de sincronización. Los valores de intervalos de retardo y de reintento pueden ser distintos, por lo que cuando dos subredes estén intentando establecer comunicación, quizás una ya desistió y paso a otra tarea, en tanto la segunda todavía esta esperando una señal de confirmación.

· Los métodos de enrutamiento y la velocidad de las maquinas en la red pueden afectar también el rendimiento de la interred. Si un router es administrado por una

maquina particularmente lenta, puede acumularse el trafico que pasa por el router, causando retrasos y transmisiones incompletas en toda la interred.

También resulta muy importante desarrollar un sistema de interred que pueda adaptarse dinámicamente a la carga y reenrutamiento de datagramas cuando ocurra un cuello de botella.

Tipos de Redes LAN, MAN y WAN

Un criterio para clasificar redes de ordenadores es el que se basa en su extensión geográfica, es en este sentido en el que hablamos de redes LAN, MAN y WAN, aunque esta documentación se centra en las redes de área local (LAN), nos dará una mejor perspectiva el conocer los otros dos tipos: MAN y WAN.

Redes de Área Local (LAN)

Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo.
Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.
Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red.
Suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas.
Operan a velocidades entre 10 y 100 Mbps.
Tienen bajo retardo y experimentan pocos errores.

Redes de Área Metropolitana (MAN)

Son una versión mayor de la LAN y utilizan una tecnología muy similar. Actualmente esta clasificación ha caído en desuso, normalmente sólo distinguiremos entre redes LAN y WAN.

Redes de Área Amplia (WAN)

Son redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host acceden a la subred de la WAN por un router. Suelen ser por tanto redes punto a punto.
La subred tiene varios elementos:

- Líneas de comunicación: Mueven bits de una máquina a otra.
- Elementos de conmutación: Máquinas especializadas que conectan dos o más líneas de transmisión. Se suelen llamar encaminadores o routers.

Cada host está después conectado a una LAN en la cual está el encaminador que se encarga de enviar la información por la subred.
Una WAN contiene numerosos cables conectados a un par de encaminadores. Si dos encaminadores que no comparten cable desean comunicarse, han de hacerlo a través de encaminadores intermedios. El paquete se recibe completo en cada uno de los intermedios y se almacena allí hasta que la línea de salida requerida esté libre.
Se pueden establecer WAN en sistemas de satélite o de radio en tierra en los que cada encaminador tiene una antena con la cual poder enviar y recibir la información. Por su naturaleza, las redes de satélite serán de difusión.

TOPOLOGÍA DE UNA RED

La topología de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores, es decir, es el mapa de distribución del cable que forma la intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son :

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba :

- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

TOPOLOGÍA FÍSICA

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen tres topología físicas puras :

- Topología en anillo.
- Topología en bus.
- Topología en estrella.

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por mas de una topología física.

TOPOLOGÍA EN BUS

Consta de un único cable que se extiende de un ordenador al siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada **terminador,** que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus.

Sus principales ventajas son :

- Fácil de instalar y mantener.

- No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría inoperativas a todas las estaciones.

Sus principales inconvenientes son :

- Si se rompe el cable en algún punto, la red queda inoperativa por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unirlas todas a través de un bus troncal.

TOPOLOGÍA EN ANILLO

Sus principales características son :

- El cable forma un bucle cerrado formando un anillo.
- Todos los ordenadores que forman parte de la red se conectan a ese anillo.
- Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo "paso de testigo".

Los principales inconvenientes serían :

- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Requiere mantenimiento.

TOPOLOGÍA EN ESTRELLA

Sus principales características son :

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.
- Habitualmente sobre este tipo de topología se utiliza como método de acceso al medio poolling, siendo el nodo central el que se encarga de implementarlo.
- Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de uno hacia el otro debe pasar por el punto central.
- existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.
- La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.
- Este tipo de topología se utiliza cuando el trasiego de información se va a realizar preferentemente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.
- Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.
- es fácil de detectar y de localizar un problema en la red.

La tabla siguiente refleja las longitudes máximas de los segmentos dependiendo de las diferentes topologías de red.

TOPOLOGÍAS	LONGITUD
Ethernet gruesa	500 metros

Ethernet fina	185 metros
Ethernet de par trenzado	100 metros
Ethernet de fibra óptica	2.000 metros
Token-Ring de par trenzado	100 metros

CÓMO FUNCIONA UNA RED

Se puede pensar por un momento en el servicio de correos. Cuando alguien desea mandar una carta a otra persona, la escribe, la mete en un sobre con el formato impuesto por correos, le pone un sello y la introduce en un buzón; la carta es recogida por el cartero, clasificada por el personal de correos, según su destino y enviada a través de medios de transporte hacia la ciudad destino; una vez allí otro cartero irá a llevarla a la dirección indicada en el sobre; si la dirección no existe, al cabo del tiempo la carta devolverá al origen por los mismos cauces que llegó al supuesto destino.

Más o menos, esta es la forma en que funciona una red : la carta escrita es la información que se quiere transmitir; el sobre y sello es el paquete con el formato impuesto por el protocolo que se utiliza en la transmisión; la dirección del destinatario es la dirección del nodo destino y la dirección del remitente, será la dirección del nodo origen, los medios de transporte que llevan la carta cerca del destino es el medio de transmisión (cable coaxial, fibra óptica …); las normas del servicio de correos, carteros y demás personal son los protocolos de comunicaciones establecidos.

Si se supone que se está utilizando el modelo OSI de la ISO. Este modelo tiene 7 niveles, es como decir que la carta escrita pasa por 7 filtros diferentes (trabajadores con diferentes cargos) desde que la ponemos en el buzón hasta que llega al destino. Cada nivel de esta torre se encarga de realizar funciones diferentes en la información a transmitir. Cada nivel por el que pasa la información a transmitir que se ha insertado en un paquete, añade información de control, que el mismo nivel en el nodo destino irá eliminando. Además se encarga de cosas muy distintas: desde el control de errores, hasta la reorganización de la información transmitida cuando esta se ha fragmentado en tramas.

Si la información va dirigida a una red diferente (otra ciudad en el caso de la carta), la trama debe llegar a un dispositivo de interconexión de redes (router, gateway, bridges), que decidirá, dependiendo de su capacidad, el camino que debe seguir la trama. Por eso es imprescindible que el paquete lleve la dirección destino y que esta contenga, además de la dirección que identifica al nodo, la dirección que identifica la red a la que pertenece el nodo.

Glosario

*** IP (Internet Protocol)**
Es un protocolo de datagrama, es decir, no orientado a conexión, con mensajes con un tamaño máximo. Cada datagrama IP se gestiona la forma independiente por lo que dos datagramas que formen parte de la misma comunicación pueden llegar a su destino por rutas distintas lo que puede provocar que lleguen en distinto orden al que salieron, que se pierda alguno, incluso, que lleguen duplicado. El protocolo IP no es

fiable, es decir, no se encarga de corregir estos problemas ni tampoco de informar de ellos o detectarlos.
los datagramas IP contienen una cabecera y un cuerpo de datos. Además de los datos que provienen del nivel superior, incorporan información de fragmentación

*** ICMP (Internet Control Message Protocol)**
Proporciona una forma de informar acerca de los errores de la red. Los paquetes ICMP se transporta mediante el uso del protocolo IP y proporciona información sobre los errores producidos por los datagramas o proporciona un modo de consulta acerca de las condiciones de los lugares remotos.

UNLM