E.E. “ANTONIO DE ESCAÑO”
DEPARTAMENTO TCI

REDES DE ÁREA LOCAL

BGDA. CG-ESB RAIMUNDO VILAR PÉREZ

Índice de Contenidos

01.- Generalidades LAN

MODELOS DE REFERENCIA
02.- El modelo de referencia OSI
03.- El modelo de referencia TCP/IP
04.- Diferencias entre OSI y TCP/IP

NIVEL FÍSICO
05.- Medios físicos de transmisión guiados
06.- Medios de transmisión no guiados
07.- anexo. Medidas en FO
08.- anexo. Espectro Electromagnético
09.- Dispositivos de interconexión Capa 1 OSI

NIVEL DE ENLACE
10.- Flujo de la Información
11.- Transmisión analógica y digital de datos
12.- Protocolos de acceso al medio
13.- Arquitectura de redes
14.- Dispositivos de conexión Capa 2 OSI
15.- Protocolos de Enlace

NIVEL DE RED
16.- Protocolos de Comunicación
17.- Direcciones IP
18.- Direcciones de Internet privadas
19.- Cálculo de Subredes
20.- Dispositivos de conexión Capa 3 OSI
21.- Datagrama IP

NIVEL DE TRANSPORTE
22.- El protocolo TCP
23.- El segmento TCP
24.- El protocolo UDP
25.- Encapsulamiento
26.- Puerto de red
27.- anexo - Servicio_Puerto_Protocolo

NIVEL DE SESIÓN, PRESENTACIÓN Y APLICACIÓN
28.- Protocolo de Sesión RPC
29.- Protocolos de Aplicación
30.- Servidores y servicios

GLOSARIO

01.- GENERALIDADES LAN

UN POCO DE HISTORIA

Aunque el primer elemento que apareció en los años 50 conectando dos ordenadores con el objeto de compartir recursos fue el conmutador ABC (donde dos ordenadores podían utilizar el mismo recurso), el verdadero origen de las redes –como en la mayoría de los avances tecnológicos– fue militar.

Se trataba de que varios terminales "tontos" utilizaran a tiempo compartido los recursos de proceso, memoria y almacenamiento de un gran ordenador anfitrión o host.

A principios de los años 60, la **Agencia de Proyectos de Investigación Avanzada (ARPA)** del Departamento de Defensa de Estados Unidos, desarrolla, tras varios intentos, un sistema de cuatro ordenadores de alta velocidad conectados (UCLA, Stanford Research Institute, UC Santa Bárbara, y Universidad de Utah) utilizando unos programas de comunicación llamados protocolos y constituyéndose así la primera red de intercambio de información. Es el origen de **INTERNET**.

El año 1972 fue clave: Ray Tomlinson de BBN inventó el primer programa de correo electrónico.

En 1973 ya se habían unido a esa primera red diecinueve centros universitarios y de investigación de todo el país y los primeros nodos internacionales (Inglaterra y Noruega).

A principios de los 80, Vinton Cerf (el padre de la Internet) y otros socios desarrollan un conjunto de protocolos de comunicación **TCP/IP (Transmition Control Protocol - Internet Protocol)**. TCP/IP es construido dentro de un sistema operativo UNIX. TCP/IP se usaría para enrutar la información entre las diferentes redes, logrando un paso sin precedentes ya que unieron una red militar y una civil. Internet se oficializaría en 1983.

En 1981 aparecen las computadoras personales (IBM), desembocando en el desarrollo de Redes de área local (LAN) para conectar PCs con el fin de compartir información.

DEFINICIÓN DE RED

***Una red se define como la conexión de dos o más sistemas informáticos con el objeto de compartir información y recursos*.**

Esta sencilla definición encierra conceptos que necesitan una pequeña aclaración.

Por un lado hay que resaltar que una red no es la que une aparatos o dispositivos, ya que, por ejemplo, no podemos considerar como una red propiamente dicha la unión de un ordenador a su monitor o a una impresora por su puerto paralelo, ya que estos dispositivos forman parte del mismo sistema informático.

Por otro lado, no es suficiente pensar que una red sólo tiene la misión de compartir información, ya que a esto hay que añadir otro objetivo fundamental, que es el de compartir recursos de hardware –esto es, impresoras, dispositivos de almacenamiento, escáneres, etc.– para optimizar costes.

PROPÓSITO DE LAS REDES

Los propósitos que se persiguen al conectar varios sistemas informáticos son los siguientes:

- **Compartición y transferencia de información.**

Se trata de conseguir el acceso rápido y sencillo a toda la información disponible.

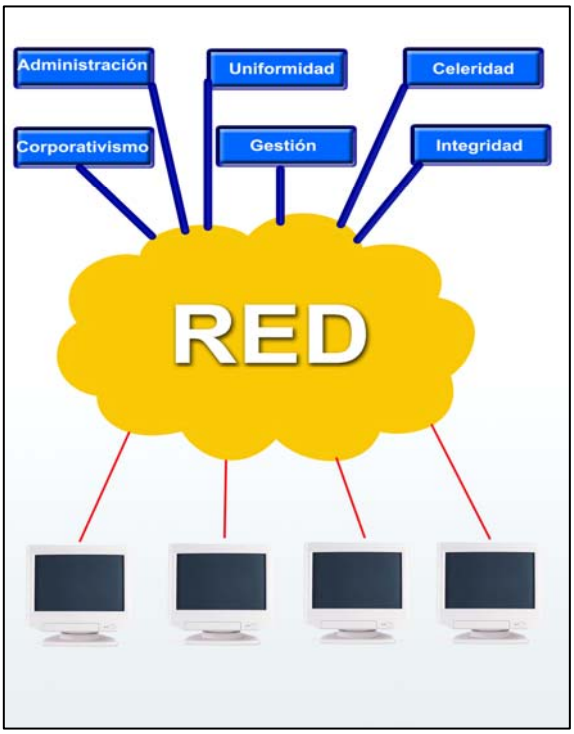
- **Uso común de recursos de hardware**.

Los recursos de hardware pueden ser caros y, por tanto, escasos; se trata de poner a disposición de todos los usuarios estos recursos de tal forma que puedan ser usados de forma compartida con el consiguiente ahorro económico.

- Sincronización y actualización de la información.

La información estará actualizada y a disposición de todos los usuarios con mayor facilidad

VENTAJAS DE UNA RED



Las ventajas añadidas que obtenemos, una vez alcanzados los objetivos anteriores, son las siguientes:

- **Administración centralizada de recursos, usuarios e información**, de tal forma que permite ejercer el control global de todos los puestos de trabajo.

- **Uniformidad corporativa de la información.** Esto es: La información corporativa que llega a los usuarios es igual para todos, de tal manera que no existen interpretaciones erróneas y la empresa o institución mejora en su organización.

- **Rapidez en las comunicaciones.** La mensajería y la transferencia de información entre los puestos de trabajo, es extremadamente mas rápida que por los canales tradicionales como el correo postal u otros.

- Uniformidad en el uso de aplicaciones y programas. Si los puestos de trabajo obtienen de la red (de un servidor de aplicaciones) el software necesario para su trabajo diario, evitamos tener que adquirir aplicaciones para todos los usuarios y prevenimos el uso de software ilegal.

- **Gestión de grupos de trabajo.** Ventaja que permite que los usuarios de cada departamento (o grupo de trabajo) puedan disponer del material que sólo les atañe a ellos, de forma que determinada información no esté disponible para toda la red.

- Seguridad en sus dos vertientes:

Integridad de la información: Si todos los puestos de trabajo guardan sus tareas diarias en un medio de almacenamiento en red, mediante copias de seguridad o backup, se puede garantizar la recuperación del trabajo en caso de averías locales o uso incorrecto del ordenador de trabajo.

Integridad en los ordenadores de los puestos de trabajo: Si los usuarios obtienen todo el software necesario para su trabajo de un servidor de la red, se evitará en gran medida la infiltración de virus informáticos procedentes de software introducido sin el control oportuno.

CLASIFICACIÓN DE LAS REDES:

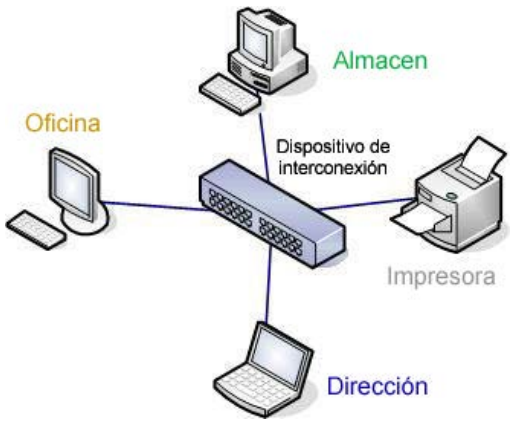
a) Atendiendo a la extensión del ámbito de aplicación

Una clasificación de las redes muy utilizada es la que hace referencia al ámbito que abarcan. No necesariamente se refiere a la extensión de la red sino a la homogeneidad de los usuarios que utilizan.

REDES DE ÁREA LOCAL (LAN – Local Area Network)

Las redes de área local *son el punto de contacto de los usuarios finales*. Su finalidad principal es la de intercambiar información entre grupos de trabajo y compartir recursos tales como impresoras y discos duros. Se caracterizan por abarcar a una oficina, organismo o institución, cuyos usuarios comparten una información y unos recursos homogéneos y comunes.

Ejemplos de este tipo de redes pueden ser un establecimiento con sus oficinas y almacenes; o una sucursal bancaria que une sus diferentes departamentos.



REDES DE ÁREA METROPOLITANA (MAN - Metropolitan Area Network)

Una red de área metropolitana *es la conexión de varias redes LAN* que abarca tal vez a un conjunto de oficinas corporativas, empresas o instituciones (por ejemplo una red de bibliotecas) en una ciudad. En general, a cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros y que conecte entre sí usuarios de diferentes organismos dentro de una población o comarca.

REDES DE ÁREA EXTENSA (WAN – Wide Area Network)

Una red de área amplia *se expande en una zona geográfica de un país, continente o a nivel mundial.*

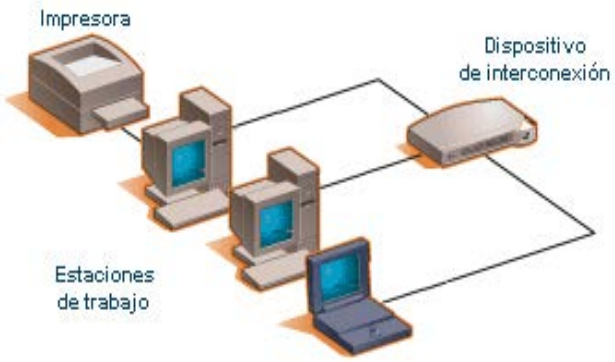
Los usuarios de estas redes, que se ubican en nodos finales, son totalmente heterogéneos y generalmente no siguen ningún criterio corporativo o común. El ejemplo más significativo de este tipo de redes es Internet o las grandes redes de correo electrónico entre las delegaciones de empresas u organismos multinacionales.

b) Atendiendo al sistema operativo de red

Redes de trabajo en grupo

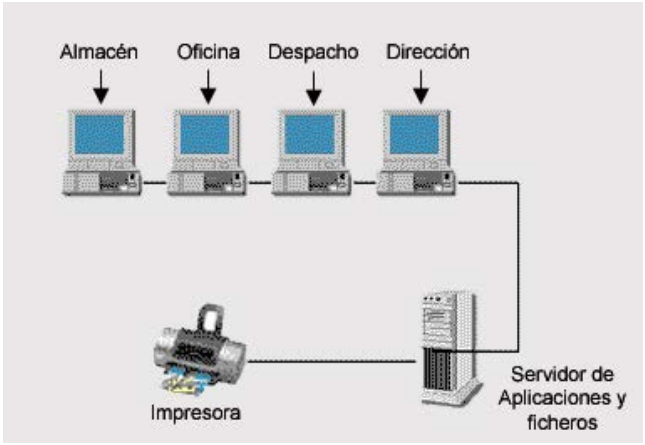
Una red de trabajo en grupo (entre iguales o **peer-to-peer**) resulta *idónea para conectar **pocas** estaciones de trabajo*. En esta configuración, no existe jerarquía: cada usuario administra sus propios recursos e información, y los pone – o no – a disposición del resto de los usuarios de la red. Cada ordenador es un igual, o par, de los otros y pueden compartir archivos y periféricos conectados a la red.

Tiene la ventaja de su sencillez, su económico costo y su facilidad de instalación. Entre las desventajas hay que destacar su **escasa seguridad**, que no garantiza la integridad del sistema, y la dependencia de los demás usuarios para beneficiarse de las posibilidades de la red.



Redes Cliente – Servidor

Cuando hay que *conectar **muchas** estaciones de trabajo y se necesita actualizar de forma periódica grandes archivos* tales como bases de datos o de información, la mejor elección es una red cliente-servidor. La presencia de un **ordenador central o *servidor*** en esta configuración proporciona numerosas ventajas. Como los archivos se almacenan en una única ubicación, se simplifican las tareas de actualización, *backup* (copia de seguridad) y archivo con resultados garantizados.



Generalmente, el servidor es un ordenador con un hardware específico de alto rendimiento que garantiza la rapidez en el acceso y recuperación de datos, y que confiere al la red la plataforma necesaria para añadir funciones tales como centralización de administración, control de los usuarios, control de las aplicaciones utilizadas y “filtros” que impiden la entrada de *virus* u otras aplicaciones dañinas para el sistema, o ilegales.

Por ultimo es necesario destacar que el servidor no se utiliza como estación de trabajo, sino que es una máquina dedicada exclusivamente a prestar servicios de red, con un sistema operativo específico de red. Sistemas operativos de red son:

- Windows 2008 Server ®
- Windows 2003 Server ®
- Windows 2000 Server ®
- Windows NT ®
- Novell Netware ®
- LAN Server de IBM ®
- LINUX Enterprise Server ®

Comparativa entre el modelo trabajo en grupo y cliente–servidor

Modelo peer to peer	Modelo Cliente-Servidor
Sencillez y rapidez de instalación	Instalación y configuración compleja
El sistema operativo de red convive con otras aplicaciones y usos.	Es una máquina dedicada a servidor de red. No convive con otras aplicaciones
Escasa seguridad en la integridad de la información	Implementa plataformas de copia de seguridad y duplicación de la información guardada.
No existe administración centralizada. Cada usuario administra su propia máquina.	La administración es centralizada, con control de los usuarios, derechos restricciones, y aplicaciones en funcionamiento.
La seguridad contra virus e intrusos esta limitada a cada usuario.	La seguridad se implementa de forma centralizada.
Existe riesgo de uso de *software* no controlado o ilegal.	Suministra y controla todas las aplicaciones que funcionan en red.
Imposibilidad de gestionar redes extensas o de elevado número de usuarios.	Desde un solo punto se puede gestionar toda la red independientemente del número de usuarios o su extensión.

c) Atendiendo al tipo de acceso del usuario a la red

Redes Dedicadas

Son aquellas que por motivo de velocidad, seguridad, o ausencia de otro tipo de red, *conectan dos o más puntos de forma exclusiva*. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

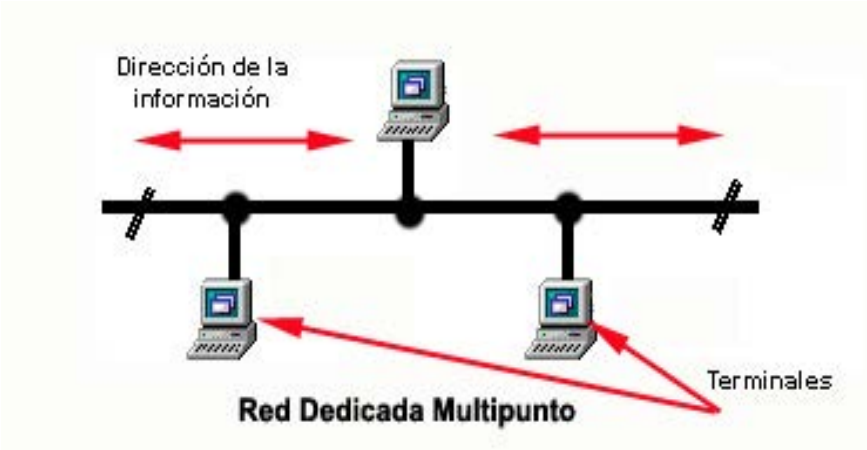
Redes punto a punto

Basada en la *conexión en línea directa entre terminales y ordenadores*. La ventaja de este tipo de conexión se encuentra en la **alta velocidad** de transmisión y la **seguridad** que presenta al no existir conexión con otros usuarios. Su desventaja sería el precio muy elevado de este tipo de red.

Red Dedicada punto a punto

Redes multipunto

En una red multipunto *sólo existe **una línea** de comunicación cuyo uso está **compartido** por todas las terminales en la red*. La información fluye de forma bidireccional y es discernible para todas las terminales de la red. Aunque pierde velocidad y seguridad, tiene la ventaja de tener un coste mas barato.



Red Dedicada Multipunto

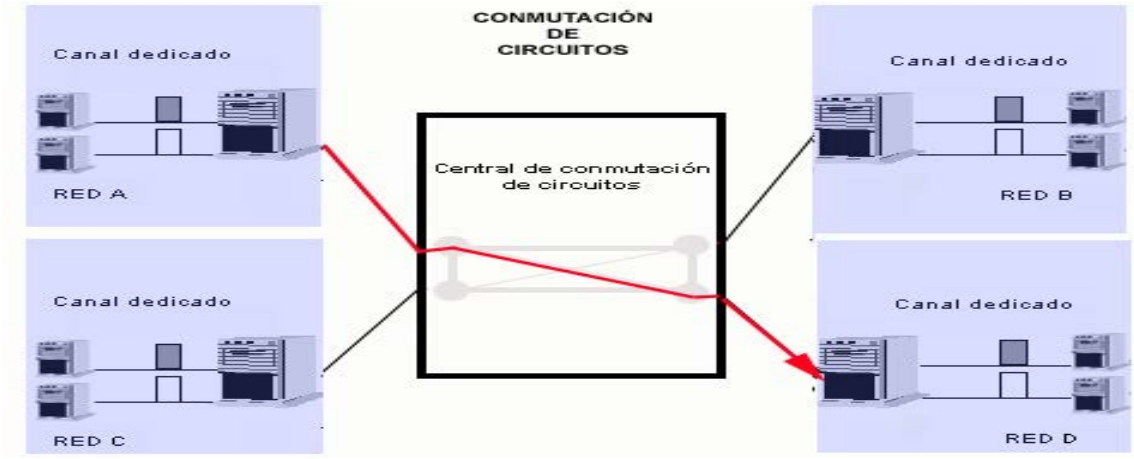
Redes Compartidas

Son aquellas *redes a las que se une un **gran número** de usuarios, compartiendo todas las necesidades de transmisión e incluso con otros tipos de transmisiones.*

Las redes más usuales son las de conmutación de circuitos, la de conmutación de paquetes, la de conmutación de mensajes y la de conmutación por circuitos virtuales.

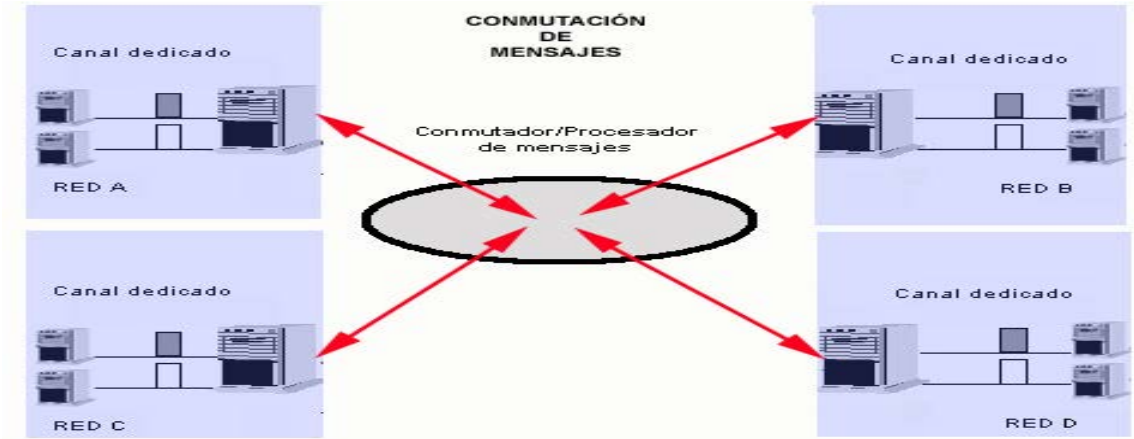
Redes de conmutación de circuitos

Son redes en las que unos centros de conmutación son los que *establecen un circuito dedicado entre dos estaciones que se comunican*. Este sistema recuerda a las antiguas centralitas de teléfono donde se "pinchaban" los conectores de dos líneas para comunicarlas entre sí.



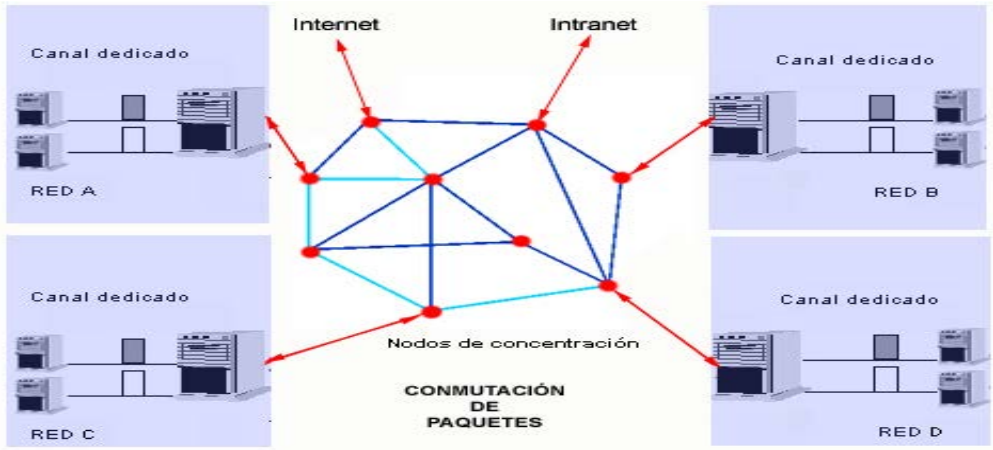
Redes de conmutación de mensajes

En lugar de tener las líneas dedicadas a un origen y un destino, lo que se va a hacer es que *cada mensaje sea conmutado a un circuito*. El mensaje va a llegar al conmutador, y el conmutador va a asignar el mensaje a su nodo correspondiente; así podemos tener varios mensajes, pero ¿Cómo reconoce el conmutador qué mensaje corresponde a cada nodo? Pues con una clave o con un identificador de encabezado del nodo destino (un encabezado del mensaje).



Redes de conmutación de paquetes

Son redes en las que *existen nodos de concentración (dispositivos de interconexión en forma de malla) con capacidad de proceso para regular el tráfico de paquetes*, entendiendo por paquete una pequeña parte de la información que cada usuario desea transmitir. Cada paquete se compone de la información, el identificador de origen y destino y algunos caracteres de control.

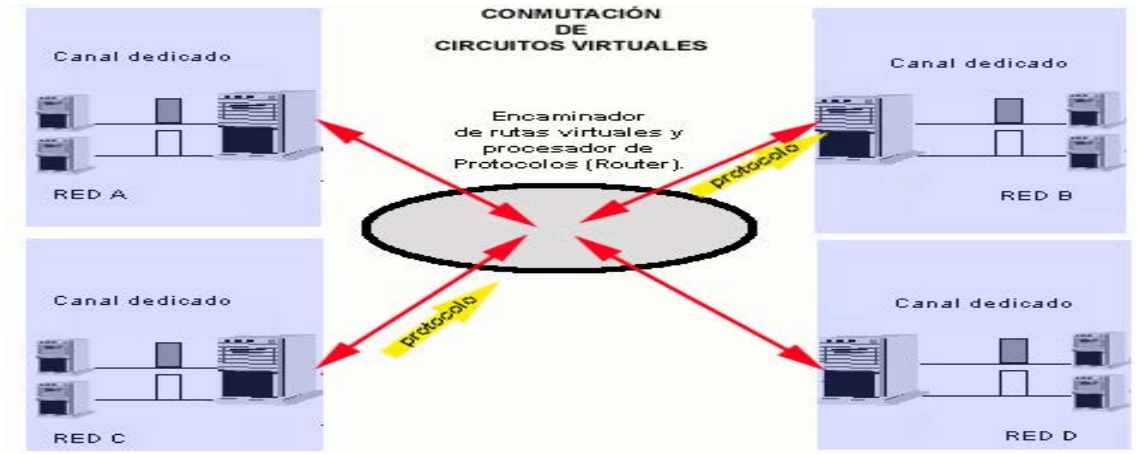


Redes de conmutación de circuitos virtuales

Cada paquete se encamina a través de la red como si fuera una entidad independiente, el camino físico entre los extremos de la conexión puede variar a menudo debido a que los paquetes aprovechan aquellas rutas de menor costo (menor distancia administrativa), y evitan las zonas congestionadas, evitando así colisiones y, por tanto, retrasos en la transmisión de la información. Esto se consigue mediante *protocolos* (conjunto de normas) que:

- Establecen rutas virtuales mediante la identificación de los nodos (transmisores y receptores).

- Aplican una serie de condiciones de cómo debe viajar el paquete de información a través de la red y cuál debe ser el tratamiento que debe recibir cada paquete de información.

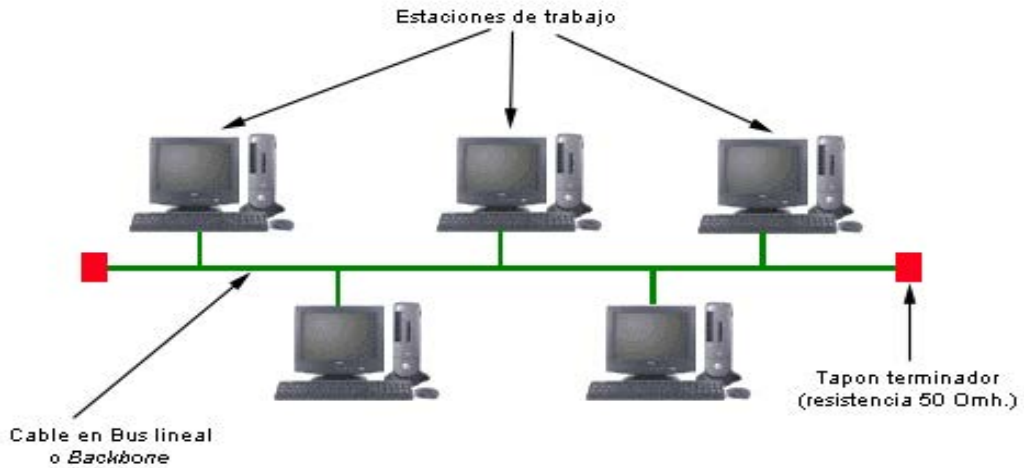


d) Atendiendo a la topología de red

Se entiende por topología de red a la **distribución física** de los puestos de trabajo en esa red.

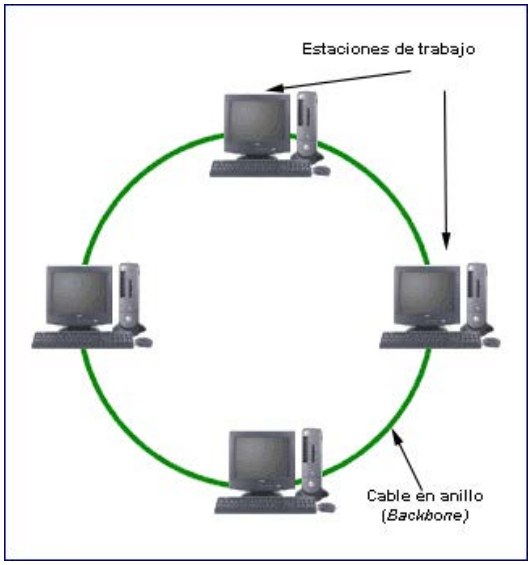
Topología en Bus

Esta topología permite que todas las estaciones reciban la información que se transmite, *una estación transmite y todas las restantes escuchan*. Consiste en *un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red*. Todos los puestos de la red están unidos a este cable: el cual recibe el nombre de **Backbone Cable**. Los nodos o puestos de red en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.



Topología en Anillo

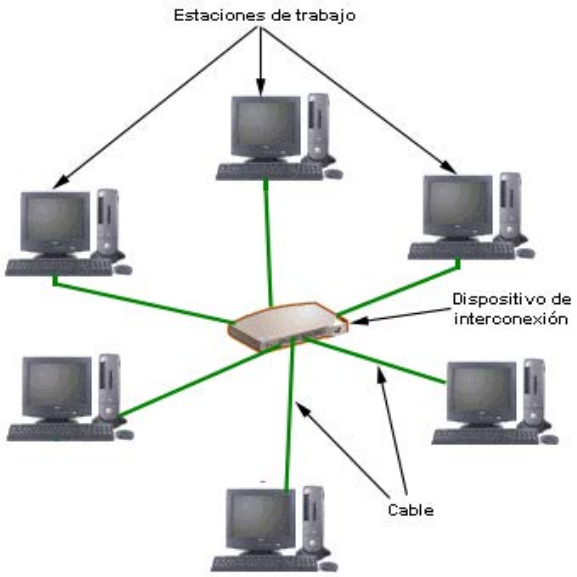
Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se produce una avería en una conexión, se cae la red completa. Con esta topología se evita la instalación de tapones terminadores de 50 Ω.



Topología en Estrella

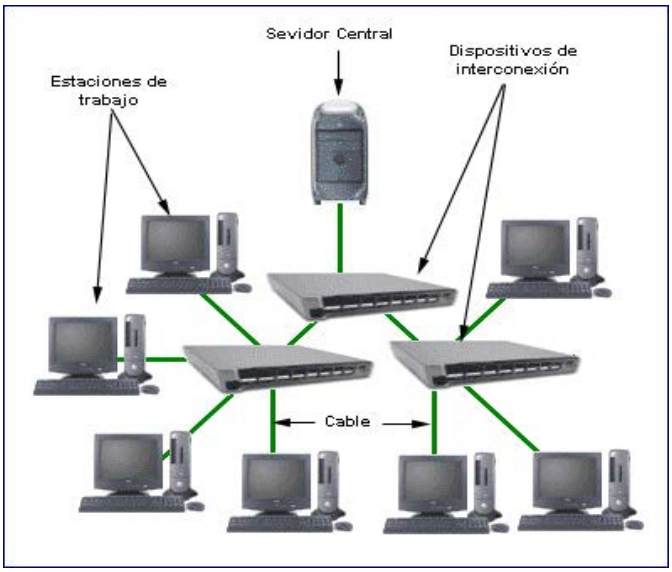
Los datos en estas redes fluyen del nodo emisor hasta un dispositivo de interconexión que realiza todas las funciones de la red, además actúa como amplificador de los datos.

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones, además si se avería una conexión, el resto de los puestos de red siguen funcionando normalmente.



Topología Jerárquica

También llamada topología en **árbol**, y realmente es una variedad de la topología en estrella, pero con la particularidad de que las estaciones de trabajo están dispuestas de forma jerarquizada. Generalmente *se parte de un servidor y a partir de ahí se van conectando ordenadores en diferentes niveles.* Esta estructura se utiliza en aplicaciones de televisión y otros servicios por cable. Este diseño de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.



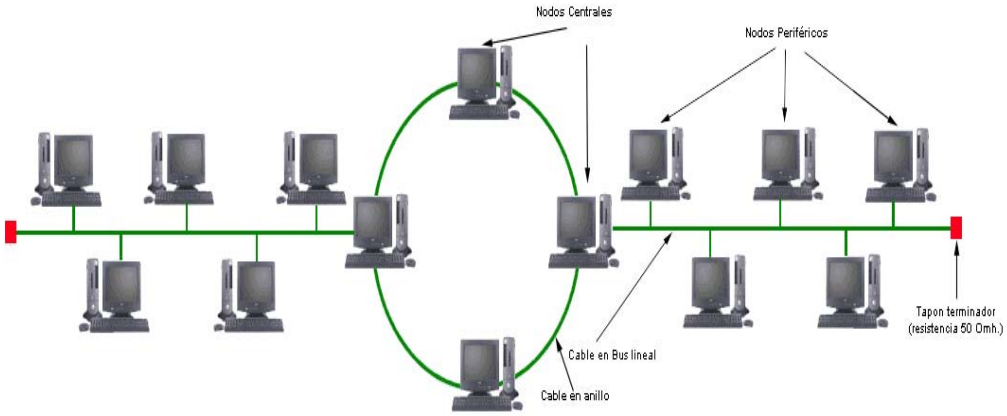
Topologías Híbridas

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

Bus en Anillo: Muy útil para la distribución en amplias zonas geográficas.

Anillo en Estrella: Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

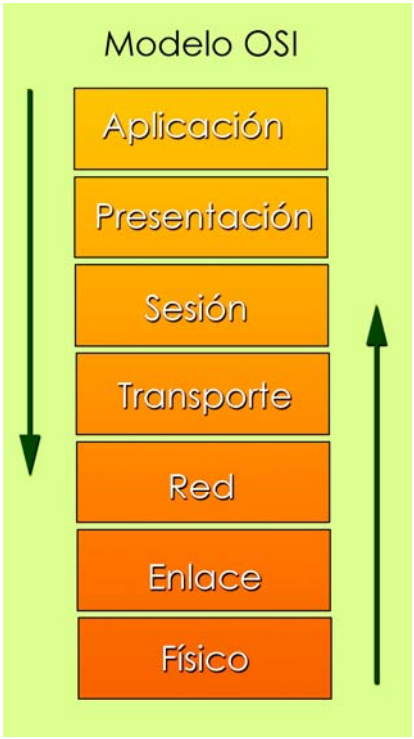
Bus en Estrella: El fin es igual a la topología anterior. En este caso la red es un bus que se cablea físicamente como una estrella por medio de concentradores.



02.- EL MODELO DE REFERENCIA OSI

El modelo **OSI** (Open Systems Interconection) es la propuesta que hizo la Organización Internacional para la Estandarización (**ISO**) para *estandarizar la interconexión de sistemas abiertos*. Un sistema abierto se refiere a que es independiente de una arquitectura específica. Se compone el modelo, por tanto, de **un conjunto de estándares ISO relativos a las comunicaciones de datos**.

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo (o conjunto de normas que debe ser usado en cada capa), sino que es una **referencia**. Este modelo está dividido en **siete capas**:

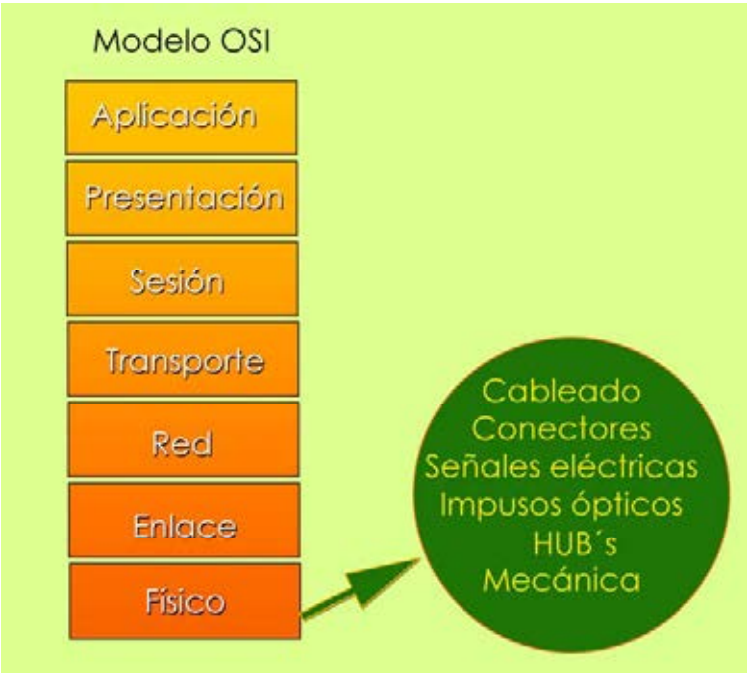


NIVEL FÍSICO

El nivel físico del modelo de referencia OSI ***es el que se encarga de las conexiones físicas del ordenador hacia la red***, en este nivel están, por ejemplo, los estándares de cableado, la forma en que las antenas de microondas deben de estar orientadas para comunicarse, y las características de propagación de ondas radiales.

Es el encargado de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las *propiedades físicas* y *características eléctricas* de los diversos componentes; de la *velocidad de transmisión*, si esta es uni o bidireccional (simplex, duplex o full-duplex). También de *aspectos mecánicos* de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

Se encarga de transformar un paquete de información binaria ("Frame") en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser **eléctricos** (transmisión por cable); **electromagnéticos** (transmisión Wireless) o **luminosos** (transmisión óptica).



Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos.

Sus principales funciones se pueden resumir como:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio.

- Manejar voltajes y pulsos eléctricos.

- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.

- Garantizar la conexión (aunque no la fiabilidad de ésta).

La forma en que estarán físicamente conectadas las estaciones en la red, el tipo de cable ó medio utilizado para la comunicación entre nodos, cómo viajará y será codificada la información eléctricamente en la red, es definida por el nivel 1, la capa física.

La técnica utilizada para lograr que los nodos sobre la red accedan al cable ó medio de comunicación, y evitar que dos o más estaciones intenten transmitir simultáneamente es trabajo del nivel 2, la capa de enlace.

Debido a que la capa física y la capa de enlace tienen cierta independencia del sistema operativo de red, estas son generalmente definidas por el instalador de la red, sobre la base de la conveniencia y diseño de la estructura física de la red, ambas capas están íntimamente ligadas y por lo general sobre la base de un tipo de distribución física de los nodos en la red.

NIVEL DE ENLACE

Una vez establecidas las características físicas de la red, cualquier medio de transmisión debe ser capaz de **proporcionar una transmisión sin errores**. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También debe incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

El nivel de enlace es el segundo nivel del modelo OSI recibe peticiones del nivel de red (tercer nivel) y utiliza los servicios del nivel físico (primer nivel).

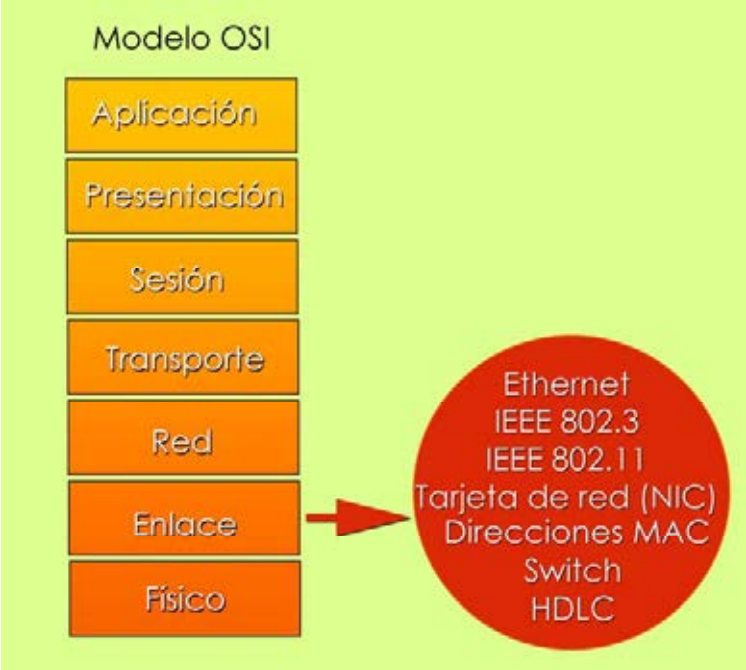
El objetivo del nivel de enlace es ***conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente dentro de una red.***

Para lograr este objetivo tiene que *montar los bloques* de información llamados tramas, *dotarles de una dirección* de nivel de enlace, *gestionar la detección o corrección de errores*, y *ocuparse del control de flujo* entre equipos (para evitar que un equipo más rápido desborde a uno más lento, por ejemplo). A este nivel, por tanto trabajan los **switches.**

Cuando el medio de comunicación está compartido entre más de dos equipos es necesario regular el uso del mismo. Esta tarea se realiza en el subnivel de acceso al medio. Dentro del grupo de protocolos IEEE 802, el subnivel de enlace lógico se recoge en la norma IEEE 802.2 y es común para todos los demás tipos de redes (Ethernet o IEEE 802.3 (cableado), IEEE 802.11 (sin cable), IEEE 802.16 o WiMAX, etc.); todas ellas especifican un subnivel de acceso al medio así como un nivel físico distintos.

Otro tipo de protocolos de nivel de enlace serían **PPP** (Point to Point Protocol o Protocolo punto a punto), **HDLC** (High Level Data Link Control o Protocolo de enlace de alto nivel), por citar dos.

En la práctica *el subnivel de acceso al medio suele formar parte de la propia tarjeta de comunicaciones* (Tarjeta de red), mientras que *el subnivel de enlace lógico estaría en el programa adaptador de la tarjeta es decir su controlador o driver*. Por ello el direccionamiento utilizado es el físico, esto es: las **direcciones MAC** de las tarjetas conectadas a la red.



NIVEL DE RED

En este nivel se decide el **encaminamiento de los paquetes entre el origen y el destino**. Este encaminamiento puede establecerse estáticamente (mediante tablas de rutas prefijadas) o bien dinámicamente (en función del tráfico de la red). También debe detectar y corregir problemas de congestión del tráfico. Un ejemplo de ellos son los routers y los protocolos IP e IPX.

El nivel de red es el tercer nivel del modelo OSI y **su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa**. Para conseguir este objetivo tiene que realizar ciertas tareas:

- Asignación de direcciones de red únicas.
- Interconexión de subredes distintas.
- Encaminamiento de paquetes.
- Control de congestión.

Datagramas o circuitos virtuales

Hay dos formas en las que el nivel de red puede funcionar internamente, mediante datagramas o por circuitos virtuales.

- En una red de datagramas cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo.

- En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión, durante este establecimiento de conexión, todos los encaminadores (o routers) que haya por el camino elegido reservarán recursos para ese circuito virtual.

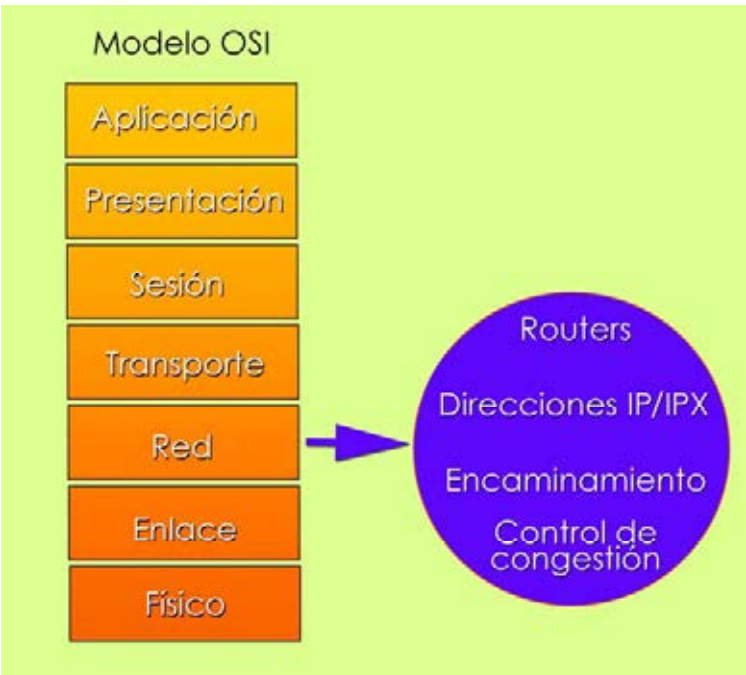
Independientemente de que la red funcione internamente con datagramas o con circuitos virtuales puede dar hacia el nivel de transporte un servicio orientado a conexión o no.

Encaminamiento

El encaminamiento consiste en encontrar un camino óptimo entre un origen y un destino. La optimidad puede tener diferentes criterios: velocidad, retardo, seguridad, regularidad, etc.

Control de congestión

Cuando en una red un nodo recibe más tráfico del que puede cursar se puede dar una congestión. El problema es que una vez que se da congestión en un nodo el problema tiende a extenderse por el resto de la red. Por ello hay técnicas de prevención y control que se pueden y deben aplicar en el nivel de red.



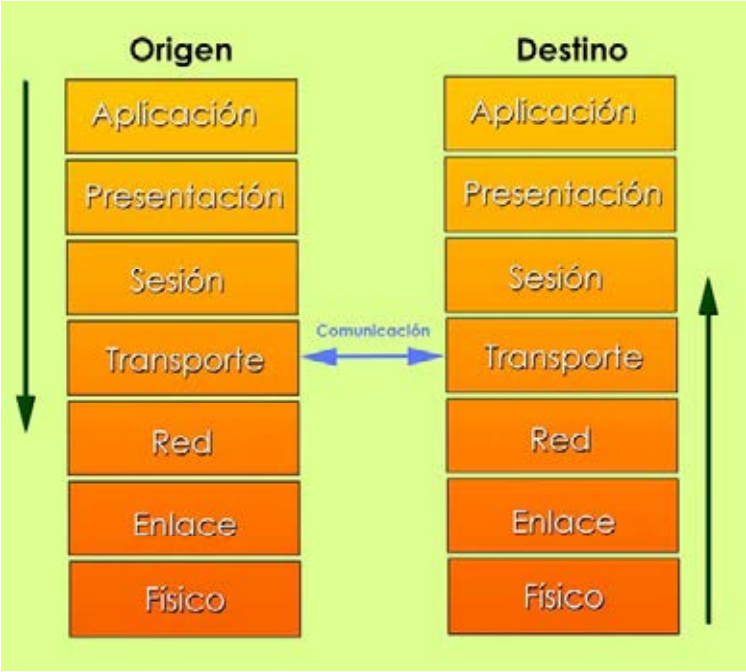
NIVEL DE TRANSPORTE

Recibe los datos de la capa de sesión, los divide si es necesario, y los pasa a la capa de red asegurándose que llegan a su destino. Aísla a las capas superiores de cambios en el hardware de comunicaciones. Es la parte encargada de garantizar la transmisión de datos. En ella podemos encontrar los protocolos UDP, TCP, SPX. A este nivel funcionan las pasarelas.

En sentido contrario cuando la capa de transporte proporciona sus servicios a la capa de sesión, efectúa la transferencia de datos entre dos entidades de sesión.

Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas segmentos, que vuelve a reensamblar en el sistema del host receptor.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos. Además, la capa de transporte es la primera que se comunica directamente con su capa par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.



La capa de transporte intenta suministrar un servicio de transporte de datos que aísle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica y un transporte fiable de datos entre los nodos de la red.

Para ello, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales, proporcionando un servicio fiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Se conocen con el nombre de circuitos virtuales a las conexiones que se establecen dentro de una red. En ellos no hay la necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.

Por tanto las funciones de la capa de transporte son las siguientes:

- Controlar la interacción entre procesos usuarios en las máquinas que se comunican.

- Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.

- Controlar el flujo de transacciones y el direccionamiento de procesos de maquina a procesos de usuario.

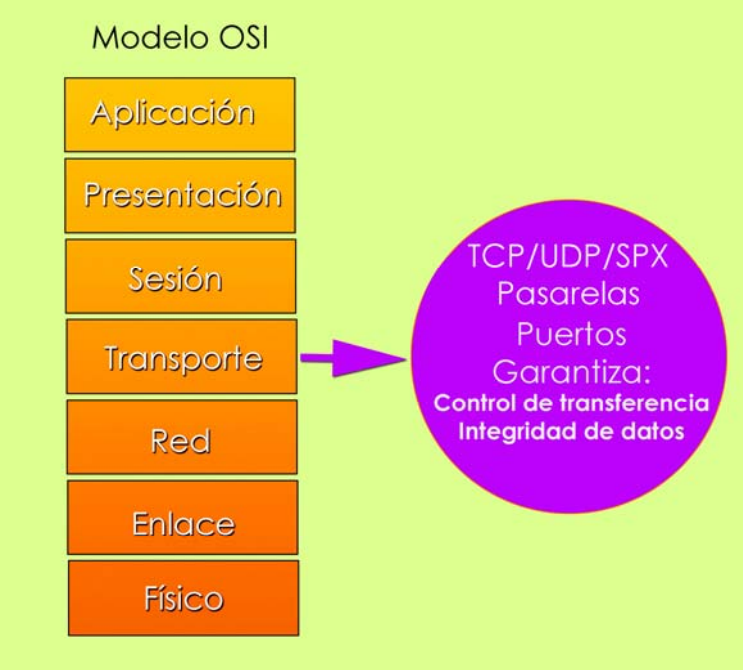
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.

- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas aptas para el transporte fiable, llamadas segmentos, que pasa luego a la capa de red para su envío.

- Realizar funciones de control y numeración de las unidades de información (los segmentos).

- Reensamblar los mensajes en el host destino, a partir de los segmentos que lo forman.

- Garantizar la transferencia de información a través de la red.



NIVEL DE SESIÓN

A este nivel es donde se permite que usuarios de máquinas distintas establezcan sesiones entre ellos. También se encarga de la sincronización y de configurar el sentido del tráfico para que vaya en ambas direcciones a la vez o de forma alternativa.

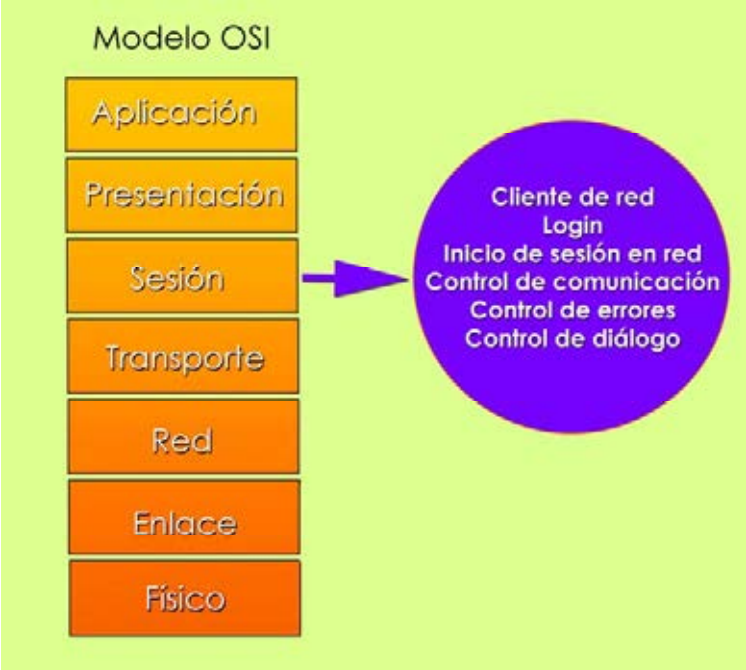
En otras palabras, tiene la responsabilidad de asegurar la entrega correcta de la información a la siguiente capa (capa de presentación). Esta capa tiene que revisar que la información que recibe sea correcta. Para esto la capa de sesión debe realizar algunas funciones:

1. Detección y corrección de errores.

2. Controlar los diálogos entre dos entidades que se estén comunicando, y definir los mecanismos para hacer las Llamadas a Procedimientos Remotos RPC.

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el trasporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

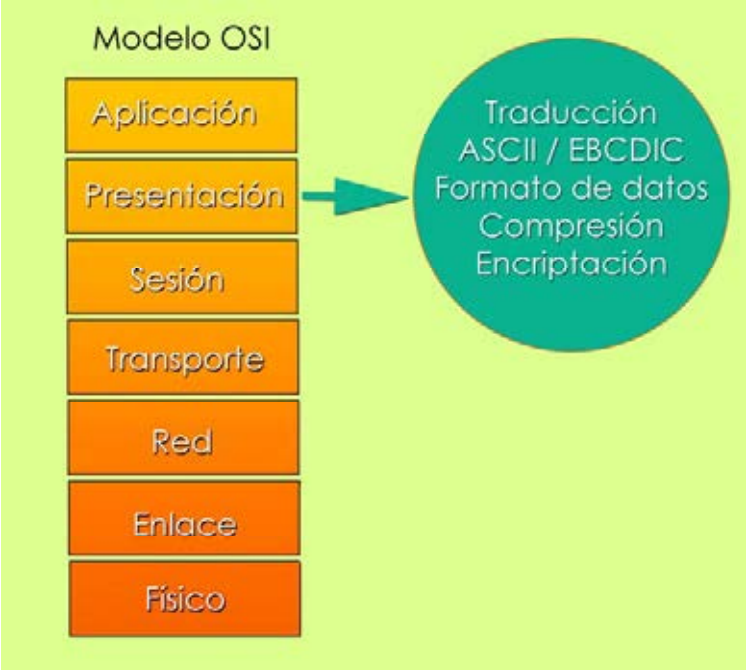
A Este nivel funciona el software de cliente de red, y el acceso por parte del usuario a la red – el Login – mediante un nombre de usuario y una contraseña (o password).



NIVEL DE PRESENTACIÓN

La función del nivel de Presentación es la de proveer un interfaz para que la transferencia de datos que sea idéntica a la tecnología para representarlos en el nivel de aplicación. En definitiva se ocupa de traducir la sintaxis y la semántica de la información que transmite. Opcionalmente puede encriptar o comprimir la información.

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.



Su tarea principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red.

Es también las responsable de la obtención y de la liberalización de la conexión de sesión cuando existan varias alternativas disponibles. Para cumplir estas funciones, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.

- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.

- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).

- Dar formato a la información para visualizarla o imprimirla. Comprimir los datos si es necesario.

- Aplicar a los datos procesos criptográficos cuando sea necesario.

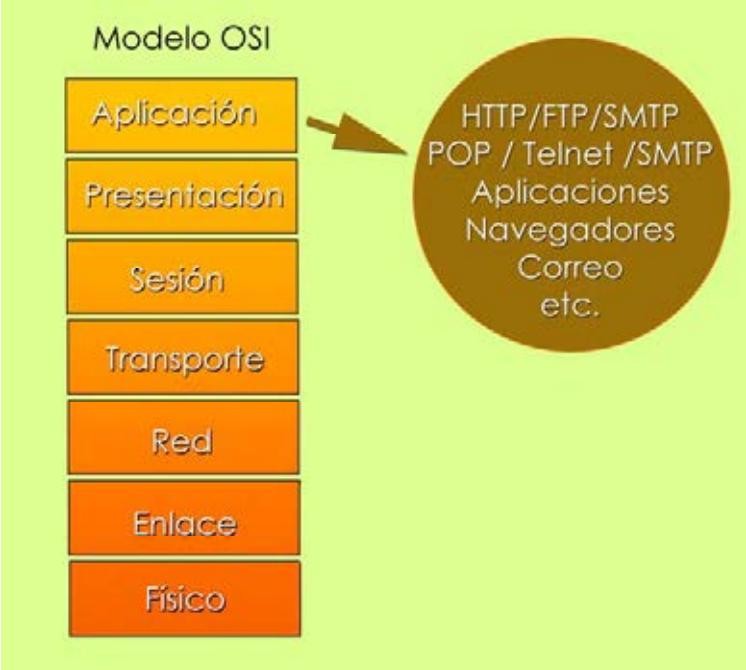
NIVEL DE APLICACIÓN

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el medio por el cual los procesos las aplicaciones de usuario acceden a la comunicación por red mediante el entorno OSI, proporcionando los procedimientos precisos para ello.

Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando éstas controladas por protocolos específicos de la capa de aplicación, que a su vez utilizan los servicios de la capa de presentación, situada inmediatamente debajo en el modelo.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores Web, etc.).



La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Ofrece además la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. Entre sus protocolos más conocidos destacan:

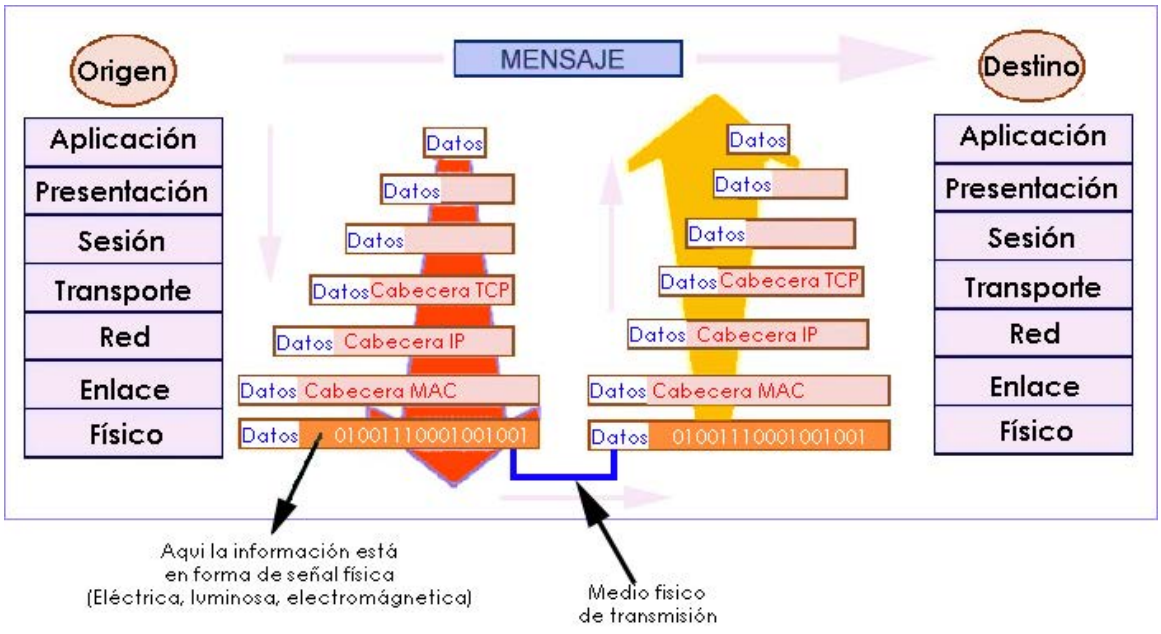
- HTTP, FTP, SMTP, POP, Telnet.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol).
- DNS (Domain Name Server).

Encapsulamiento de los datos en el modelo OSI

Por tanto, conociendo ya el funcionamiento de la torre OSI, la información que envía un usuario a otro a través de una red desde una aplicación (Nivel de aplicación) va sufriendo transformaciones de acuerdo con los niveles de OSI, es decir: la información debe de bajar por todas las capas del nodo origen y subir a las capas del nodo destino. El modo en que cada capa sabe el contenido de la información que le corresponde es por medio del encapsulamiento, tal y como se puede apreciar en el siguiente gráfico:



03.- EL DISEÑO TCP/IP

El diseño TCP/IP esta hoy en día ampliamente difundido, a pesar de no ser un modelo de referencia estandarizado, ningún organismo lo ha definido.

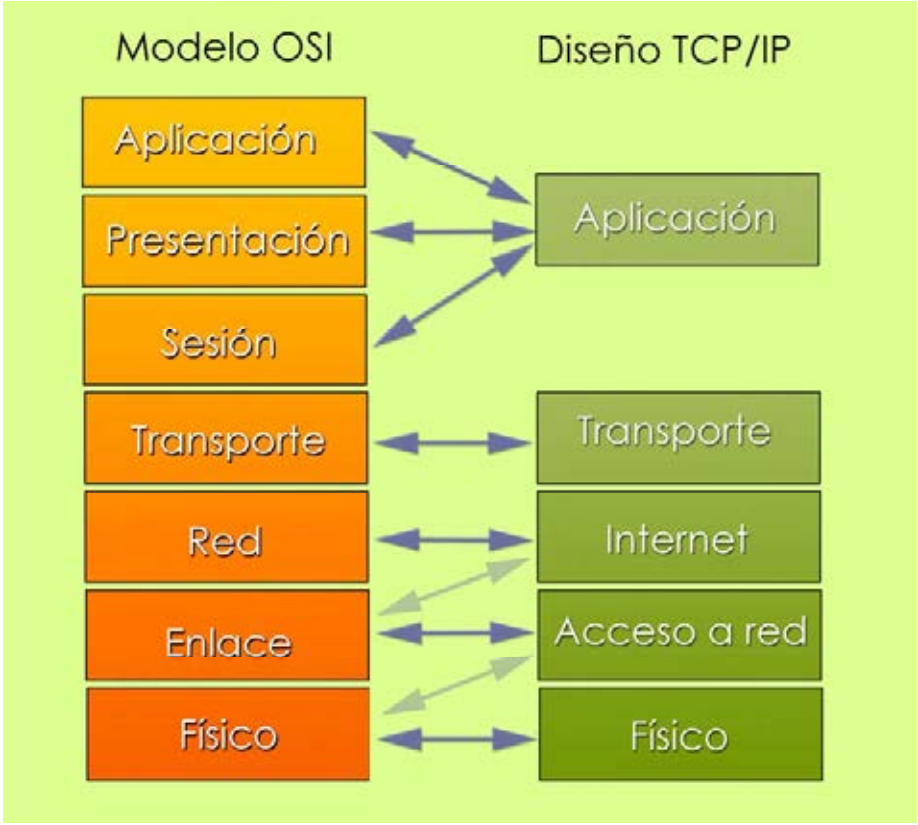
Realmente se ha convertido en una arquitectura *"de facto"* debido a la proliferación de su uso.

Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU.), y con la expansión de INTERNET se ha convertido en una de las arquitecturas de redes más difundida.

Una prueba evidente de que no está estandarizada esta arquitectura es que **no hay uniformidad de criterios a la hora de definirla**: hay autores que la definen en cinco niveles, otro en cuatro, o, incluso, en tres. En este curso se van a considerar cinco niveles ya que es el criterio más extendido.

La relación de esta arquitectura con respecto al modelo de referencia OSI es la siguiente: así como el modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por **5 niveles**:

- Nivel de físico: análogo al nivel físico de OSI.
- Nivel de acceso a la red: análogo al nivel de enlace con aspectos del nivel físico de OSI.
- Nivel de Internet: cubre los aspectos del nivel de red y algunos del nivel de enlace de OSI.
- Nivel de transporte: análogo a nivel de transporte de OSI.
- Nivel de aplicación: engloba los niveles de sesión, presentación y aplicación de OSI.



NIVEL FÍSICO

Análogo al nivel físico de OSI. Cubre los aspectos de la interfaz física entre un dispositivo de transmisión y el medio. Este se ocupa de especificar las características del medio de transmisión, la naturaleza de las señales, el régimen binario y otros asuntos relacionados. TCP/IP se soporta sobre los estándares ya definidos en el modelo OSI.

NIVEL DE ACCESO A LA RED

Es la interfaz para acceder al hardware de la red. TCP/IP no especifica ningún protocolo en este nivel. Se soporta sobre los estándares ya definidos en OSI.

En definitiva es la interfaz de la red real y como no especifica ningún protocolo concreto, corre por las interfaces conocidas, como por ejemplo: Ethernet, 802.3, CSMA/CD, X.25, etc.

NIVEL DE INTERNET

Análoga a la capa de red de OSI, proporciona la imagen de "red virtual" de Internet, es decir, oculta a los niveles superiores la arquitectura de la red.

IP es el protocolo más importante de esta capa. Es un protocolo no orientado a conexión que no garantiza la fiabilidad de las capas inferiores. No suministra fiabilidad, control de flujo o recuperación de errores. Estas funciones debe proporcionarlas una capa de mayor nivel, bien de transporte con TCP, o de aplicación, si se utiliza UDP como transporte. La unidad de un mensaje en una red IP se denomina datagrama IP. Es la unidad básica de información transmitida en redes TCP/IP.

NIVEL DE TRANSPORTE

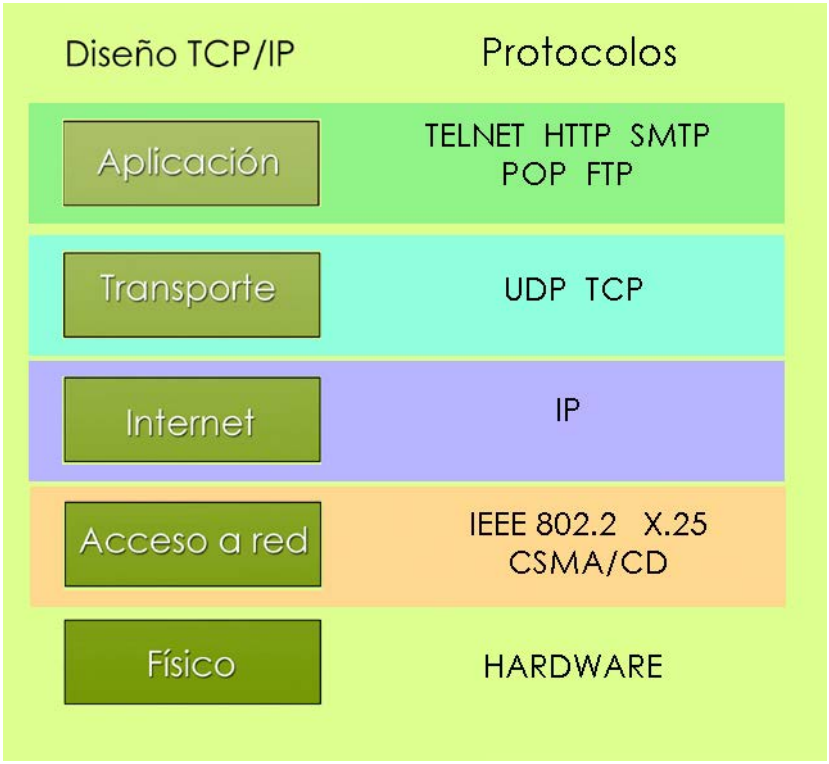
Este nivel se identifica prácticamente con el nivel de transporte de OSI.

Provee comunicación extremo a extremo desde un programa de aplicación a otro, mediante puertos. Puede proveer un transporte fiable asegurándose de que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota.

En esta capa se encuentran los protocolos UDP y TCP.

NIVEL DE APLICACIÓN

El nivel de aplicación se corresponde con los niveles de sesión, presentación y aplicación del modelo OSI, y conecta las aplicaciones a la red. Los interfaces de programación de aplicaciones (API) proporcionan acceso a los protocolos de transporte TCP/IP, los sockets de Windows y NetBIOS. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).


Diseño TCP/IP
Protocolos
Aplicación
TELNET HTTP SMTP
POP FTP
Transporte
UDP TCP
Internet
IP
Acceso a red
IEEE 802.2 X.25
CSMA/CD
Físico
HARDWARE

04.- DIFERENCIAS ENTRE EL MODELO OSI Y EL DISEÑO TCP/IP

El diseño TCP/IP sólo puede equipararse funcionalmente al modelo OSI de ISO, ya que existen diferencias básicas tales como:

- En la pila de protocolos de Internet, una capa representa un encapsulamiento de una función.

- La perspectiva de ISO, por otro lado, trata a las capas como grupos funcionales bastante reducidos, intentando forzar la modularidad al requerir capas adicionales para funciones adicionales.

- En los protocolos TCP/IP, un protocolo dado puede ser usado por otros protocolos en la misma capa, mientras que en el modelo OSI se definirían dos capas en las mismas circunstancias. Ejemplos de estas "dependencias horizontales" son FTP, que usa la misma representación común que TELNET sobre la capa de aplicación, o ICMP, que usa IP para el envío de datagramas en el nivel de red.

- A nivel práctico, lo que se trata aquí es la diferencia entre un estándar "de jure", OSI, y uno "de facto", TCP/IP. El objetivo en el mundo de TCP/IP consiste en establecer de común acuerdo un protocolo estándar que pueda funcionar en una diversidad de redes heterogéneas; siempre se le ha dado mayor importancia al estándar en sí que a su implementación.

- Eficiencia y viabilidad. Las normas de OSI tienden a ser prescriptivas (por ejemplo, la capa "N" debe atravesar todas las capas "por debajo" de ella), mientras que los protocolos TCP/IP tienden a ser descriptivos, y dejan un máximo de libertad a los implementadores. Una de las ventajas del enfoque de TCP/IP es que cada implementación concreta puede explotar características dependientes del sistema, de lo que suele derivarse una mayor eficiencia (menos ciclos de CPU, mayor productividad para las mismas funciones), al mismo tiempo que se asegura la interoperabilidad con otras aplicaciones.

- Otra forma de ver esto es que la mayoría de los protocolos de Internet se han desarrollado primero (codificados y testeados) antes de ser descritos en un RFC (habitualmente por parte del implementador) lo que muestra claramente su viabilidad.

05.- MEDIOS FÍSICOS DE TRANSMISIÓN GUIADOS

A.- CABLE COAXIAL

Se usa normalmente en la conexión de redes con topología de Bus como Ethernet y ArcNet, es llamado así porque su construcción es de forma coaxial; tenemos el conductor central, un recubrimiento dieléctrico, una malla de alambre y un recubrimiento externo que tiene una doble función: como recubrimiento de protección y como aislante.

Una de las cosas más importantes del coaxial es su ancho de banda y su resistencia (*o impedancia*); estas funciones dependen del grosor del conductor central, si varia la malla, varía la impedancia también.

El *Coaxial* es un cable muy usado para las topologías de bus y anillo donde los nodos se conectan a un medio de acceso común. El cable coaxial cobró una gran popularidad en sus inicios por su propiedad idónea de transmisión de voz, audio y video, además de textos e imágenes. El cable coaxial esta estructurado (de adentro hacia afuera) de los siguientes componentes:

a) Un núcleo de cobre sólido, o de acero con capa de cobre, o bien de una serie de fibras de alambre de cobre entrelazadas (dependiendo del fabricante).

b) Una capa de aislante que recubre el núcleo o conductor, generalmente de material de polivinilo, dicho aislante tiene la función de guardar una distancia uniforme del conductor con el exterior.

c) Una capa de blindaje metálico, generalmente cobre o aleación de aluminio entretejido (a veces solo consta de un papel metálico) cuya función es la de mantenerse lo mas apretado posible para eliminar las interferencias, y además evitar de que el eje común se rompa o se sesgue demasiado - ya que si no se mantiene el eje común, trae como consecuencia que la señal se va perdiendo - lo cual afectaría la calidad de la señal.

d) Una capa final de recubrimiento, generalmente de color negro o gris (coaxial delgado) o amarillo (coaxial grueso), y por lo general de vinilo, xelón, polietileno uniforme para mantener la calidad de las señales.

Tipo	Usos
RG-8	**10Base5**
RG-11	**10Base5**
RG-58	**10Base2**
RG-62	**ARCnet**
RG-75	**CTV (Televisión)**

El ancho de banda del cable coaxial esta entre los 500Mhz, esto hace que el cable coaxial sea ideal para transmisión de televisión por cable por múltiples canales. Ahora, como se ve en la tabla, existen varios tipos de cable coaxial.

Cada cable tiene su uso particular, los primeros cables se usan para redes de datos (*10Base2 y 10Base5 ArcNet*) y el último se usa principalmente para televisión. Los RG8 y RG11 son coaxiales gruesos, ya que se están buscando ciertas prestaciones, y de cierta forma el grosor del cable central también va a afectar al factor distancia que podrá viajar una señal sin debilitarse, y estos coaxiales gruesos en particular permiten una transmisión de datos de mucha distancia.

Por otra parte, un metro de coaxial grueso puede llegar a pesar hasta medio kilogramo, y no puede doblarse fácilmente, de hecho, su radio de curvatura no puede ser más que uno o dos kilómetros. Un enlace de coaxial grueso puede ser hasta 3 veces mas largo que un coaxial delgado. Las normas Ethernet 10Base5 y 10Base2, ARCNet y CTV son tecnologías que se profundizarán mas adelante.

TIPOS DE CABLES COAXIALES EMPLEADOS EN REDES LAN

A1.- Cable Coaxial Thinnet (Ethernet fino), 10 BASE 2

El cable Thinnet es un cable coaxial **flexible** de unos **0,64 centímetros** de grueso.

Su alcance es de **185 metros** sin sufrir atenuaciones.

El cable Thinnet está incluido en un grupo que se denomina la **familia RG-58** y tiene una impedancia de **50 ohm**. *(La impedancia es la resistencia, medida en ohmios, a la corriente alterna que circula en un hilo.)*

Este tipo de cable se puede utilizar para la mayoría de los tipos de instalaciones de redes, ya que es un cable flexible y fácil de manejar.

A2.- Cable Coaxial Thicknet (Ethernet grueso), 10 BASE 5

El cable Thicknet es un cable coaxial relativamente **rígido** de aproximadamente **1,27 centímetros** de diámetro.

Al cable Thicknet a veces se le denomina Ethernet estándar debido a que fue el primer tipo de cable utilizado con la conocida arquitectura de red Ethernet.

El núcleo de cobre del cable Thicknet es más grueso que el del cable Thinnet. Es curioso que también se denomine **"cable amarillo"** puesto que en todos los casos su cubierta exterior es de ese color. Puede llevar una señal a **500 metros** sin atenuaciones significativas.

Por tanto, debido a la capacidad de Thicknet para poder soportar transferencia de datos a distancias mayores, a veces se utiliza como enlace central o **backbone** para conectar varias redes más pequeñas basadas en Thinnet.

COMPARATIVA: THINNET FRENTE A THICKNET

Como regla general, los cables más gruesos son más difíciles de manejar. El cable fino es flexible, fácil de instalar y relativamente barato. El cable grueso no se dobla fácilmente y, por tanto, es más complicado de instalar.
Éste es un factor importante cuando una instalación necesita llevar el cable a través de espacios estrechos, como conductos y canales. El cable grueso es más caro que el cable fino, pero transporta la señal más lejos.

Parámetro/Tipo de Cable	**10Base5**	**10Base2**
Tasa de transmisión	10 Mbps	10 Mbps
Longitud máxima	500 mts.	185 mts.
Impedancia	50 ohms	50 ohms, RG58
Diámetro del conductor	2.17 mm	0.9 mm

Hardware de conexión del cable coaxial

Como se refería anteriormente, tanto el cable Thinnet como el Thicknet utilizan un componente de conexión llamado conector BNC, para realizar las conexiones entre el cable y los equipos. Existen varios componentes importantes en la familia BNC, incluyendo los siguientes:

El conector de cable BNC. El conector de cable BNC está soldado, o incrustado, en el extremo de un cable.

El conector BNC T. Este conector conecta la tarjeta de red (NIC) del equipo con el cable de la red y permite conectar varios equipos en serie.

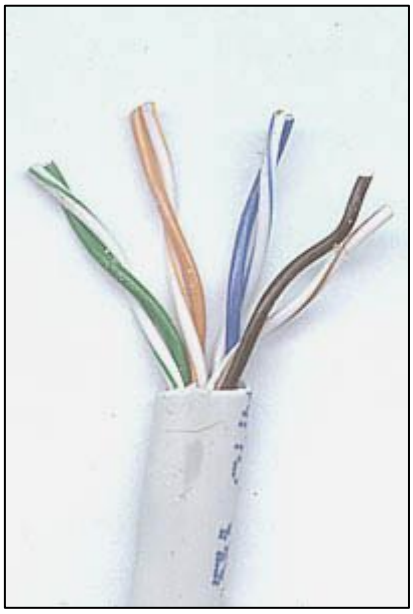
Conector acoplador (barrel) BNC. Este conector se utiliza para unir dos cables Thinnet para obtener uno de mayor longitud.

Terminador BNC. El terminador BNC cierra el extremo del cable del bus para absorber las señales perdidas (con una resistencia de 50 Ω, acorde con su impedancia).

Tipo	Impedancia
RG-8	50 ohms.
RG-11	50 ohms.
RG-58	50 ohms.
RG-62	93 ohms.
RG-75	75 ohms.

El origen de las siglas BNC no está claro, y se le han atribuido muchos nombres, desde «British Naval Connector» a «Bayonet Neill-Councelman». Haremos referencia a esta familia hardware simplemente como BNC, debido a que no hay consenso en el nombre apropiado y a que en la industria de la tecnología las referencias se hacen simplemente como conectores del tipo BNC.

B.- CABLE DE PAR TRENZADO

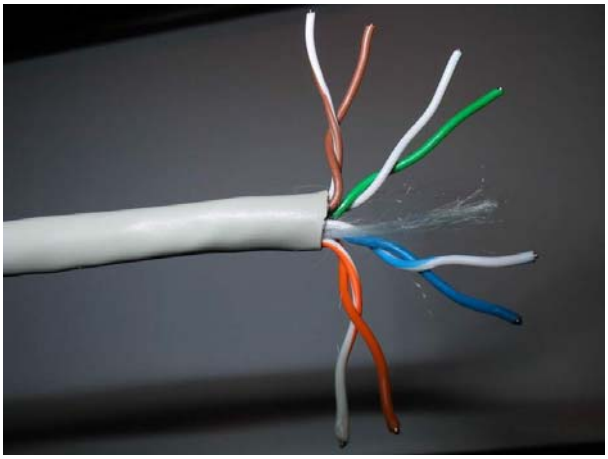


Es de los más utilizados del mercado y el más popular: consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de **1 mm** aproximado. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipares de pares trenzados (de 2, 4, 8...hasta varios centenares de pares).

Un ejemplo de par trenzado es el sistema de telefonía analógica tradicional, ya que la mayoría de aparatos se conectan a la central telefónica por intermedio de un par trenzado. Actualmente se han convertido en un estándar, de hecho en el ámbito de las redes LAN, como medio de transmisión en las redes de acceso a usuarios (típicamente cables de 2 ó 4 pares trenzados). A pesar que las propiedades de transmisión de cables de par trenzado son inferiores y en especial la sensibilidad ante perturbaciones extremas a las del cable coaxial, su gran adopción se debe al costo, su flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, etc.

Básicamente se utilizan ***se utilizan los siguientes tipos de cable pares trenzados:***

B1.- Cable de par trenzado no apantallado UTP (Unshielded twisted pair)



Cable de pares trenzados **más simple** y empleado, sin ningún tipo de apantalla adicional y con una impedancia característica de **100 Ohmios**. El conector más frecuente con el UTP es el **RJ45**, parecido al utilizado en teléfonos RJ11 (pero un poco más grande), aunque también puede usarse otro (RJ11, DB25, DB11, etc.), dependiendo del adaptador de red. Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo, accesibilidad y fácil instalación. Sin embargo a altas velocidades puede resultar **vulnerable a las interferencias electromagnéticas del entorno**: motores eléctricos, alta tensión, reactancias, etc.

B2.- Cable apantallado STP (Shielded twisted pair)

En este caso, **cada par** va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. Su impedancia es de **150 ohmios.**

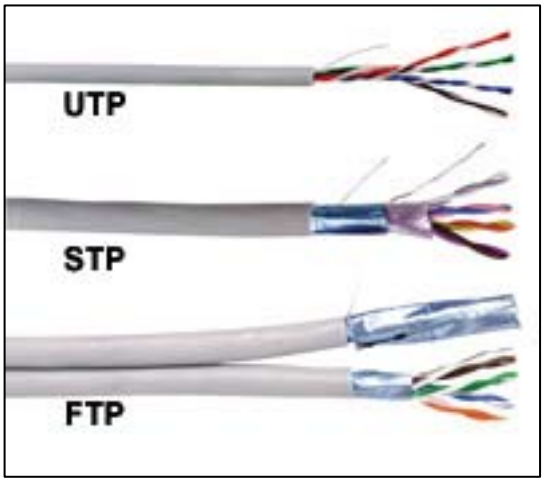
El nivel de protección del STP ante perturbaciones externas es **mayor** al ofrecido por UTP. Sin embargo es **más costoso** y requiere más instalación. La pantalla del STP para que sea más eficaz requiere una configuración de **interconexión con tierra** (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores **RJ49**, aunque se puede utilizar el RJ45.

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable **robusto, caro y difícil de instalar.**

B3.- Cable con apantallado global FTP (Foiled twisted pair)

En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una **pantalla global** para mejorar su nivel de protección ante interferencias externas. Su impedancia característica típica es de 120 ohmios y sus propiedades de transmisión son más parecidas a las del UTP. Además puede utilizar los mismos conectores **RJ45**.

Tiene un precio intermedio entre el UTP y STP.



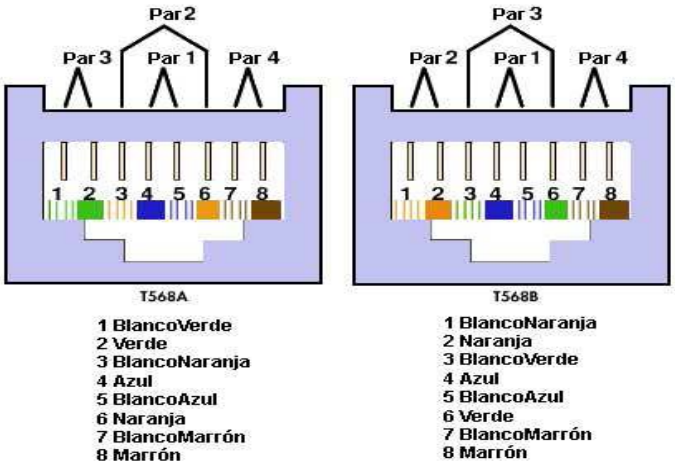
ESTÁNDARES PARA CABLE DE PAR TRENZADO

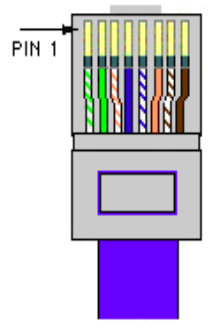
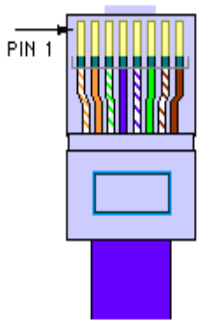
El desmembramiento del sistema Bell en 1984 y la liberación de algunos países en el sistema de telecomunicaciones hizo que quienes utilizaban los medios de comunicación con fines comerciales tuvieran una nueva alternativa para instalar y administrar servicios de voz y datos. Método que se designó como cableado estructurado, que consiste en equipos, accesorios de cables, accesorios de conexión y también la forma de cómo se conectan los diferentes elementos entre sí.

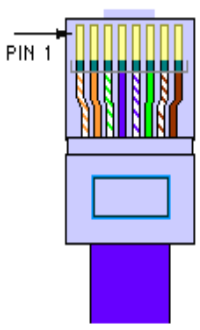
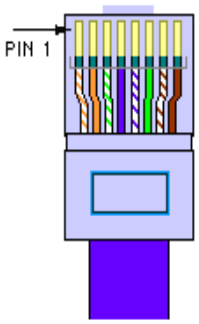
El EIA/TIA define el estándar **EIA/TIA 568** para la instalación de redes locales (LAN). El cable trenzado mas utilizado es el UTP (sin apantallar) que trabajan con las redes 10Base-T de ethernet, Token Ring, etc.

La EIA/TIA-568 selecciona cuatro pares trenzados en cada cable para acomodar las diversas necesidades de redes de datos y telecomunicaciones. Existen dos estándares para los pines de los conectores del cable trenzado denominadas **T568A** y **T568B.**

Para la elaboración de un cable **directo** se utilizará el estándar **T568B**, *esto es, una conexión T568B en cada extremo*; sin embargo para construir un cable **cruzado** *se empleará el estándar T568B en un extremo y T568A en el otro*, según se muestra en le figura siguiente:



Cable Cruzado	
RJ-45 PIN	**RJ-45 PIN**
1 Rx+	3 Tx+
2 Rc-	6 Tx-
3 Tx+	1 Rc+
6 Tx-	2 Rc-
	

Cable Directo	
RJ-45 PIN	**RJ-45 PIN**
1 Tx+	1 Rc+
2 Tx-	2 Rc-
3 Rc+	3 Tx+
6 Rc-	6 Tx-
	

ESTÁNDAR Y PROTOCOLO ETHERNET

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5e ó 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

CATEGORÍAS DEL CABLE DE PAR TRENZADO

El cable par trenzado se especifica según su construcción por categorías:

Categoría 1: Cable de par trenzado sin apantallar, se adapta para los servicios de voz (telefonía), pero no a los datos.

Categoría 2: Cable de par trenzado sin apantallar, este cable tiene cuatro pares trenzados y está certificado para transmisión de datos a **4 Mbps**. Alcance **90 - 100** metros.

Categoría 3: Cable de par trenzado que soporta velocidades de transmisión de **10 Mbps** de ethernet 10Base-T, la transmisión en una red Token Ring es de 4 Mbps. Este cable tiene cuatro pares. Su ancho de banda máximo es de **16 Mhz**. Alcance **90 - 100** metros.

Categoría 4: Cable par trenzado certificado para velocidades de **16 Mbp**s. Este cable tiene cuatro pares y ancho de banda de hasta **20 Mhz**. Alcance **90 - 100** metros.

Categoría 5: Es un cable de cobre par trenzado de **cuatro pares de 100 ohmios**. La transmisión de este cable puede ser a **100 Mbps** para soportar las tecnologías como ATM (Asynchronous Transfer Mode) y Fast Ethernet. Su ancho de banda es de **100 Mhz**. Alcance **90 - 100** metros.

Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque si esta diferenciada por los diferentes organismos. Se ha definido su ancho de banda hasta **250 Mhz** y su transmisión puede soportar Gigabit Ethernet (**1000 Mbps**). Alcance **90 - 100** metros.

Categoría 6: Es una mejora de la categoría anterior. Las características de transmisión del medio están especificadas hasta una frecuencia superior a **250 Mhz**. Certificándose para transmisiones de **1000 Mbps**. Alcance **90 - 100** metros.

Categoría 6a: definido en TIA/EIA-568-B, usado en redes 10 gigabit ethernet **(10000 Mbps)**. Diseñado para transmisión a frecuencias de hasta **500 Mhz.**

Categoría 7: actualmente no reconocido por TIA/EIA. Es una mejora de la categoría 6, puede transmitir datos hasta **10 Gbps** y las características de transmisión del medio están especificadas hasta una frecuencia superior a **600 Mhz.**

C.- FIBRA ÓPTICA

La fibra óptica puede usarse del mismo modo que los cables de cobre convencionales, tanto en pequeños entornos (tales como sistemas de procesamiento de datos de aviones o buques), como en grandes redes geográficas (como los sistemas de largas líneas urbanas mantenidos por compañías telefónicas y de información).

Básicamente, la fibra óptica está compuesta por una región cilíndrica, por la cual se efectúa la propagación, denominada núcleo y de una zona externa al núcleo y coaxial con él, totalmente necesaria para que se produzca el mecanismo de propagación, y que se denomina envoltura o revestimiento.

La capacidad de transmisión de información que tiene una fibra óptica depende de tres características fundamentales:

a) Del diseño geométrico de la fibra.

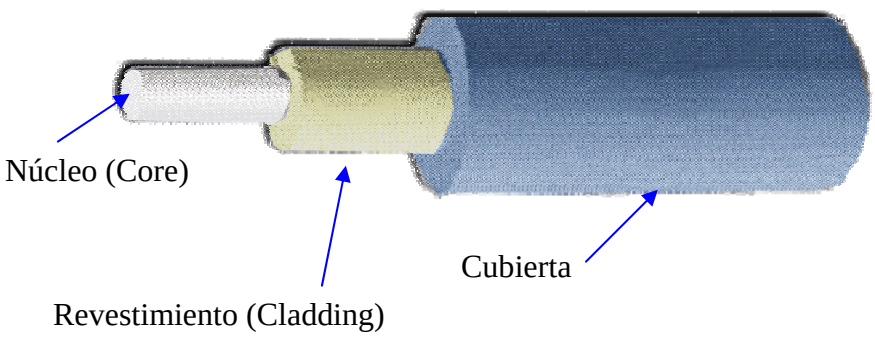
b) De las propiedades de los materiales empleados en su elaboración. (Diseño óptico)

c) De la anchura espectral de la fuente de luz utilizada. Cuanto mayor sea esta anchura, menor será la capacidad de transmisión de información de esa fibra.

Presenta dimensiones más reducidas que los medios preexistentes. Un cable de 10 fibras tiene un diámetro aproximado de 8 o 10 mm. y proporciona la misma o más información que un coaxial de 10 tubos. El peso del cable de fibras ópticas es muy inferior al de los cables metálicos, redundando en su facilidad de instalación.

Estructura de los cables de fibra óptica

La estructura física de los cables de datos de la fibra óptica sean cual sean sus características tecnológicas siempre es similar:

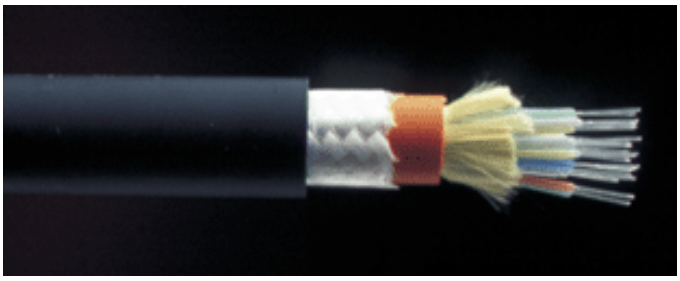


Núcleo (Core): Es el hilo central de vidrio por donde circula la onda luminosa. Su diámetro varía, según la tecnología empleada, entre los **8 μm y los 125 μm**.

Revestimiento (Cladding): Es la primera capa de vidrio que rodea el núcleo – con un índice de refracción diferente a éste – y donde va "rebotando" el haz luminoso en su trayecto. Evita que la luz salga del núcleo. Su diámetro va desde **125 μm a 140 μm.**

Recubrimiento (Coating): Es el la primera cubierta plástica que da resistencia al cable, evita roturas e impide que la luz exterior pueda perturbar la señal luminosa. Su diámetro oscila entre **250 μm y 900 μm.**

A partir de esta capa el cable puede llevar otros elementos de protección y refuerzo dependiendo de su aplicación.

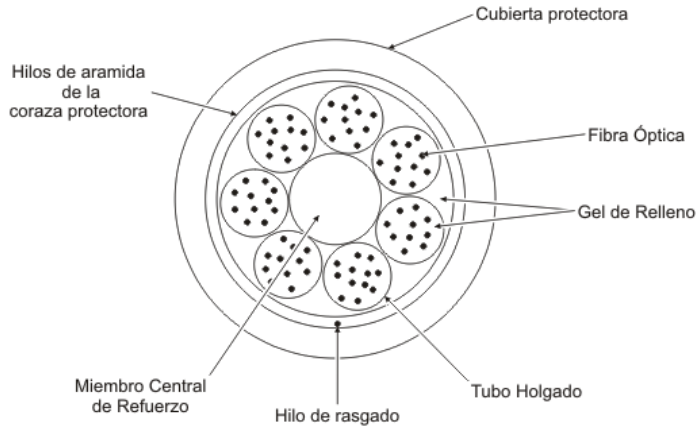


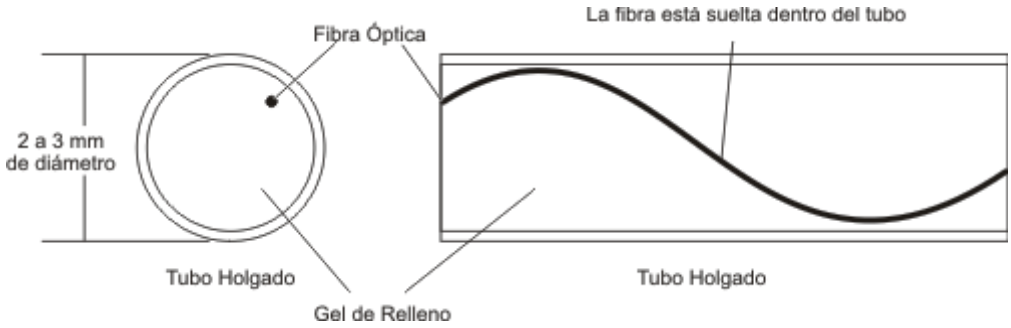
a) Clasificación de la fibra óptica con respecto a su construcción

Los cables de fibra se pueden clasificar en holgados y ajustados.

Fibra óptica holgada

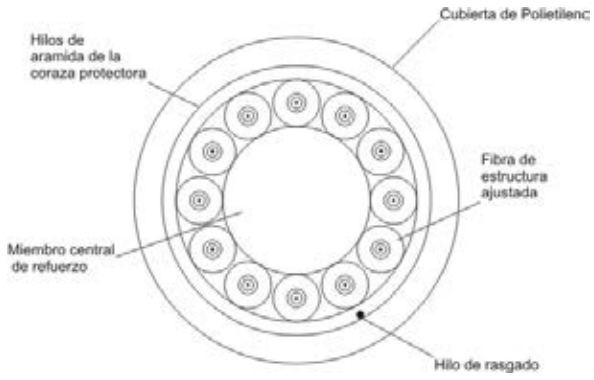
Este tipo de fibra se caracteriza por tener un gel interno que hace que se pueda desplazar longitudinalmente dentro de su cubierta. Es **poco flexible,** pero **resistente** al manejo. Se usa fundamentalmente en **exteriores y para largas distancias**. Es de compleja instalación, pero se hace ideal para transporte de señal.





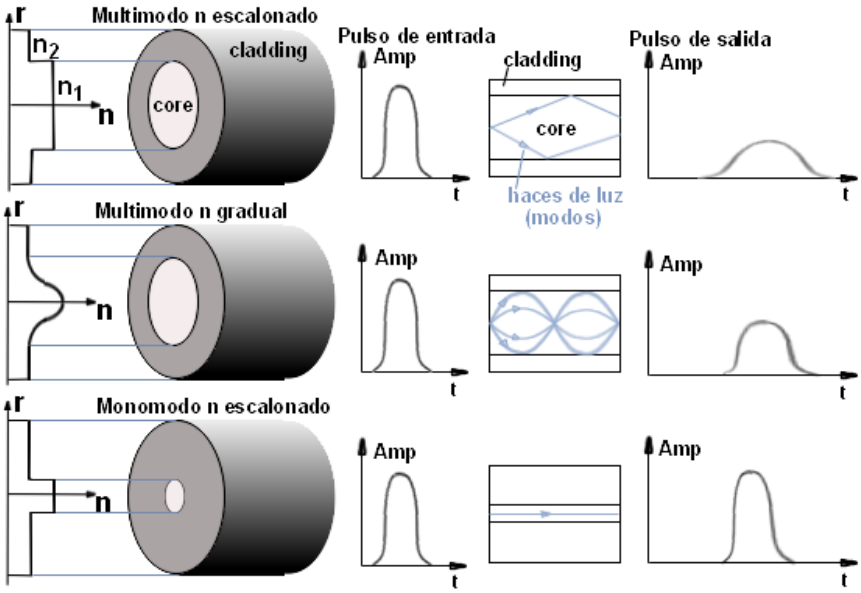
Fibra óptica ajustada

Se caracteriza por estar la fibra solidariamente pegada a su cubierta. Posee **buena flexibilidad**. Tiene un gel externo a la cubierta que evita la entrada de humedad (gel higrófobo). Durante su manejo e instalación hay que observar mucha precaución ya que es de **fácil rotura**. Se utiliza fundamentalmente en **interiores y en cortas distancias**. Es muy apropiada para llegar a los dispositivos finales.



b) Clasificación de la fibra óptica con respecto a su tecnología

Con respecto a la tecnología de propagación de la señal luminosa la fibra se puede diferenciar en Fibra Multimodo (MM) y Fibra Monomodo (SM).



Fibra Multimodo (Multi-Mode)

En este tipo de fibra viajan **varios rayos ópticos** reflejándose a diferentes ángulos, los diferentes rayos ópticos recorren diferentes distancias y se desfasan al viajar dentro de la fibra. Por esta razón, la distancia a la que se puede trasmitir está limitada a **3000 mts**. Tiene la ventaja de su facilidad de instalación, conectorización y empalme. Además su costo es relativamente bajo.

Fibra multimodo con índice graduado

En este tipo de fibra óptica el núcleo está hecho de **varias capas concéntricas** de material óptico con **diferentes índices de refracción**. En estas fibras el número de rayos ópticos diferentes que viajan es menor y, por lo tanto, sufren menos el severo problema de las multimodales.

Fibra monomodo (Single-Mode)

Esta fibra óptica es la de **menor diámetro** y solamente permite viajar al rayo óptico central. No sufre del efecto de las otras dos pero es más difícil de construir y manipular. Es también más costosa pero permite distancias de transmisión mucho mayores: **hasta 40.000 mts**. Su instalación, soldadura y conectorización es muy compleja.

Emisores y detectores

Los dispositivos utilizados como emisores y detectores de radiación luminosa en los sistemas de comunicaciones ópticas son el **láser de semiconductores** (diodo láser) y el **LED** (diodo electroluminiscente). Ningún otro tipo de fuente óptica puede modularse directamente a las altas velocidades de transmisión requeridas, con tan baja excitación y tan baja salida. En función del sistema, escogemos uno u otro. Las longitudes de onda utilizadas son 850 y 1300 nm para fibra multimodo y 1500 nm para monomodo.

*El **láser** ofrece mejor rendimiento en anchos de banda grandes y largos alcances. Para anchos de banda menores y cortas distancias se suele escoger el **LED***, pues tanto el circuito de ataque como el de control son más sencillos.

Los componentes utilizados para emitir luz en la ventana de los 850 nm, son galio (Ga), aluminio (Al) y arsénico (As); si agregamos indio (In) y fósforo (P) podemos emitir en las ventanas de los 1300 y 1500 nm.

Emisores

LED:

*El proceso de generación de luz en un LED se basa en el efecto de **electroluminiscencia**.* En un LED la luz se emite según los 360º que corresponden a una radiación esférica, pero en la práctica, esto queda limitado por la construcción metálica del diodo, la reflexión en el material utilizado y la absorción en el metal semiconductor.

Un ancho de banda típico de un LED es de 200 MHz, con rendimientos de 50 μW/mA. Los LED presentan un espectro de emisión más ancho que los láser.

DIODO LÁSER:

El proceso de generación de luz en un diodo láser es similar al del LED, pero con un volumen de generación menor y una alta concentración de portadores inyectados. Se consigue así una **elevada ganancia óptica** y un espectro de emisión muy estrecho que da lugar a luz coherente.

La luz de este tipo de láser puede acoplarse fácilmente va una fibra multimodo juntando simplemente a tope un extremo de la raya del láser contra el extremo del núcleo de la fibra, que tiene un diámetro mucho mayor. También puede acoplarse a una fibra monomodo.

Receptores

Básicamente el detector es un **dispositivo que convierte fotones en electrones.** Los fotodetectores utilizados en las comunicaciones ópticas son el fotoconductor, el diodo PIN y el fotodiodo de avalancha (APD). La mayor parte de sistemas instalados usan diodos PIN.

PIN: El fotodiodo PIN es el detector **más utilizado** en los sistemas de comunicación óptica. Es relativamente fácil de fabricar, altamente fiable, tiene bajo ruido y es compatible con circuitos amplificadores de tensión. Además es sensible a un gran ancho de banda debido a que no tiene mecanismo de ganancia.

El diodo PIN se compone básicamente de unas zonas p y n altamente conductoras junto a una zona intrínseca poco conductiva. Los fotones entran en la zona intrínseca generando pares electrón-hueco. El diodo se polariza inversamente para acelerar las cargas presentes en esta zona intrínseca, que se dirigen a los electrodos, donde aparecen como corriente. El proceso es rápido y eficiente. Como no hay mecanismo de ganancia, la máxima eficiencia es la unidad y el producto ganancia por ancho de banda coincide con ésta última.

APD: Los APD también **son diodos polarizados en inversa**, pero en este caso las tensiones inversas son elevadas, originando un fuerte campo eléctrico que acelera los portadores generados, de manera que estos colisionan con otros átomos del semiconductor y generan mas pares electrón-hueco. Esta ionización por impacto determina la ganancia de avalancha. La ganancia de un APD tiene influencia sobre el ancho de banda. El máximo ancho de banda se da para ganancia 1. Con ganancias mas elevadas, el ancho de banda se reduce debido al tiempo necesario para que se forme la fotoavalancha.

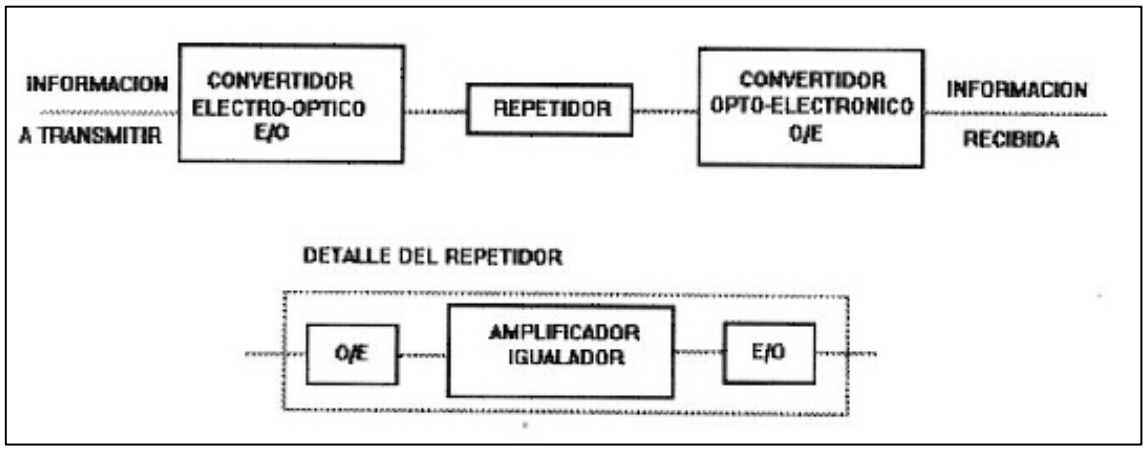
Elementos de un sistema de fibra óptica

Estos sistemas están compuestos por un **transmisor**, cuya misión es la de convertir la señal eléctrica en señal óptica susceptible de ser enviada a través de una fibra óptica. En el extremo opuesto de la fibra óptica se encuentra el **receptor**, cuya misión es la de convertir la señal óptica en señal eléctrica nuevamente.

El **transmisor** puede emplear un LED o un diodo láser como elemento de salida. A estos elementos se los denomina **conversores electro-ópticos (E/O).**

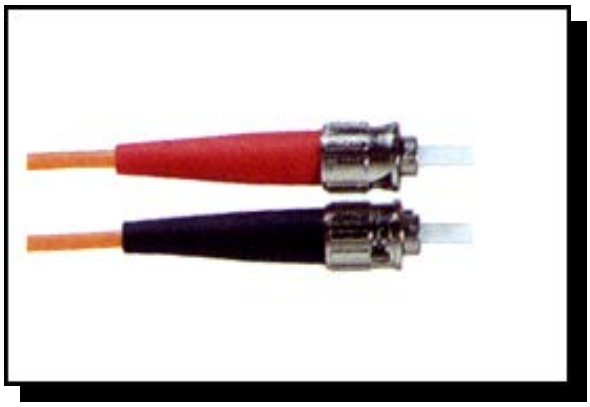
El **receptor** consiste en un diodo PIN o un APD, que se acopla a la fibra óptica. Se le denomina **convertidor opto-electrónico (O/E).**

La señal óptica que se propaga a través de la fibra óptica se degrada por la atenuación y restricción de la anchura de banda de la fibra, y entonces, es preciso **regenerar** la señal transmitida. El mejor método es tratar la señal en **forma eléctrica.** Por lo tanto, Los conversores E/O y O/E son componentes indispensables en un repetidor óptico. El amplificador e igualador de la señal eléctrica son similares a los de los sistemas de transmisión convencionales.



Conectores para fibra óptica

El acoplamiento óptico en la mayoría de los conectores se produce enfrentando las caras previamente preparadas de las fibras ópticas y manteniéndolas muy juntas. Las **pérdidas** en un conector se producen por varios factores: *mala alineación* (radial y angular), *reflexión en las superficies aire-vidrio*, *separación entre las fibras* (necesaria para que no se rayen entre si), *variaciones del tamaño del núcleo*, *de la apertura numérica de la fibra*, etc. **Los conectores más utilizados son los SC y los ST.**



Conectores ST

Aplicable en monomodo y multimodo.
Anclaje de bayoneta
Ferrule: Cerámica 2,5 mm ∅ o acero.
Tipo FO: 125 – 140 µm ∅ cladding
Tipo cable: Ajustado/holgado
Pérdidas inserción:
<150 dB (Typ. 0,35 dB) en MM
<150 dB (Typ. 0,30 dB) en SM
Compatibilidad ST Estándar

Mejor aplicación en **instalaciones que no requieran conexión/desconexión frecuente.**

Conectores SC

Monomodo y multimodo
Anclaje Push - Pull
Ferrule: Cerámica 2,5 mm ∅
Tipo FO: 125 µm ∅ cladding
Tipo cable: Ajustado/holgado
Pérdidas inserción:
<150 dB (Typ. 0,35 dB) en MM
<150 dB (Typ. 0,25 dB) en SM
Compatibilidad ST Estándar

De aplicación en **dispositivos en los que se requiera conexión/desconexión frecuente.**

Existen en el mercado otra gran variedad de conectores dependiendo de las necesidades específicas, algunos ejemplos son los FC, Euro2000 o LC.

DIN

FC

Euro 2000

LC

Empalmes para unión de fibra óptica

Debido a que una **bobina** de cable de fibra óptica no llega a superar los **2 Km** de longitud, mientras que la distancia entre dos **repetidores** o centrales puede ser de **30 o 40 Km**., deben realizarse empalmes entre los tramos, y entre cada final y los conectores.

Existen tres tipos de empalmes para la fibra óptica: ***Acopladores***, ***Empalmes mecánicos*** y ***Soldadura por fusión.***

Acopladores

Requiere que los dos cables a unir tengan **conectores en sus extremos** con el consiguiente coste y con las **atenuaciones** intrínsecas a los conectores. Se trata de un adaptador **doble hembra** que une los dos conectores machos de los cables a unir y por donde pasa la señal de luz libre. Las atenuaciones oscilan entre **0,30 y 0,80 Db.**

SC

ST

Empalme mecánico

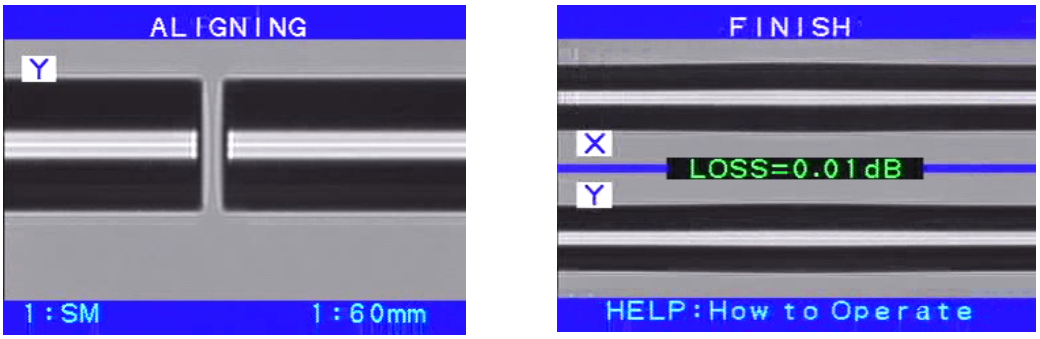
Son empalmes rápidos, permanentes o provisionales, que pueden usarse, por ejemplo, para probar bobinas. Producen **atenuaciones altas**, del orden de 0,20 a 1dB.

Vienen rellenos con gel para mejorar la continuidad de la luz.

Pueden ser cilindros con un orificio central, o bandejitas cerradas con dos pequeñas llaves que nos permiten introducir las fibras.

Soldadura por fusión

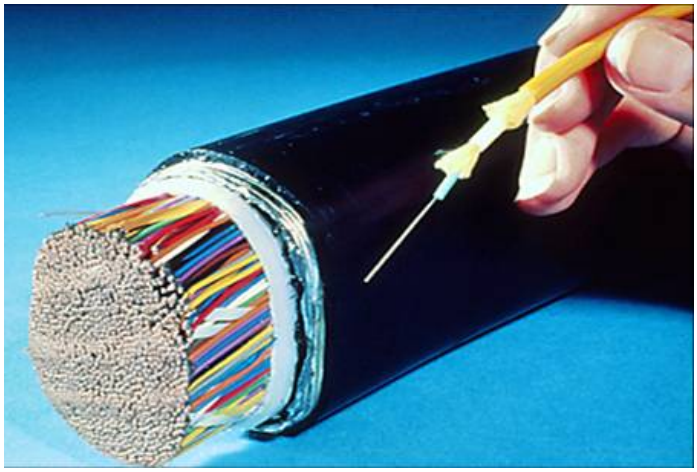
Son empalmes permanentes y se realizan con máquinas empalmadoras, manuales o automáticas, que luego de cargarles las fibras sin coating y cortadas a 90º realizan un alineamiento de los núcleos de una y otra, para luego fusionarlas con un arco eléctrico producido entre dos electrodos.
Llegan a producir atenuaciones casi imperceptibles (0.01 a 0.10 dB)



Antes y después de una soldadura por fusión

Protección de los empalmes

La zona del empalme es **delicada** por lo que se protege de diferentes maneras: pegándose sobre unas ***almohadillas autoadhesivas*** existentes en algunos cassettes de empalmes, rodeándose con una ***bisagra autoadhesiva***, o con ***manguitos termocontraíbles*** (sleeves) los cuales poseen un nervio metálico.

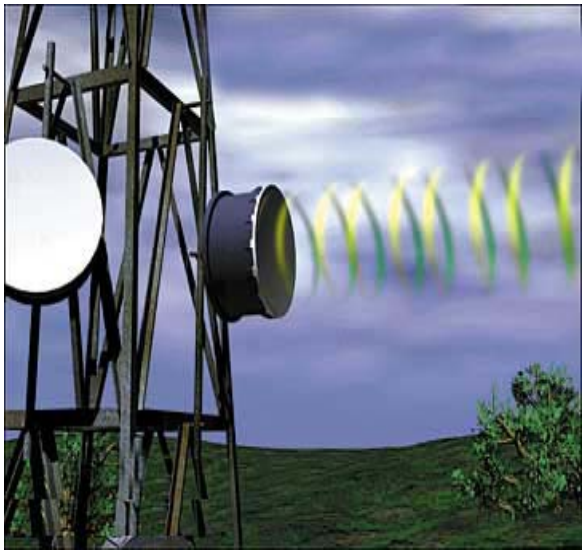


06.- MEDIOS DE TRANSMISIÓN NO GUIADOS

Consideramos como medios de transmisión no guiados aquellos que no utilizan ningún tipo de cable para transmitir la señal dentro de una red.

Dependiendo del tipo de tecnología empleada, las transmisiones inalámbricas se clasifican en:

- ***Microondas terrestres***
- ***Microondas por satélite***
- ***Radiofrecuencia***
- ***Infrarrojos***
- ***Bluetooth***



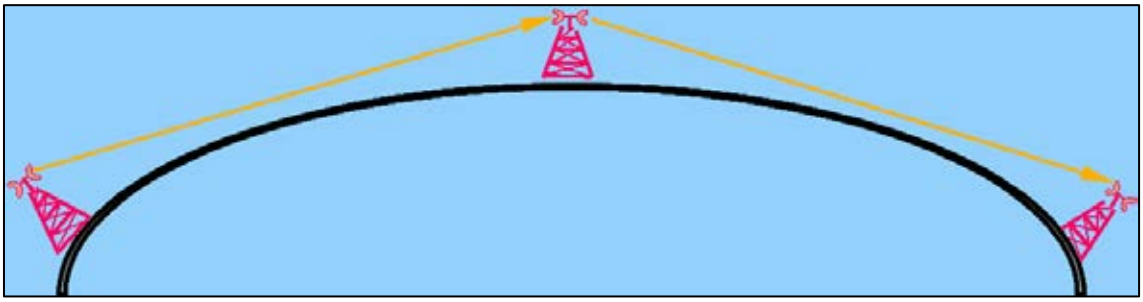
MICROONDAS TERRESTRES

Son **ondas electromagnéticas** del extremo superior del espectro de radio. Están situadas entre los rayos **infrarrojos** (cuya frecuencia es mayor) y las ondas de **radiofrecuencia**.

Sus frecuencias se miden en Gigahertzios y su longitud de onda es del orden de **centímetros**. Debido a su alta frecuencia no son reflejados por la **ionosfera**.

En las comunicaciones por microondas terrestres se utilizan unas antenas **unidireccionales**, que producen un haz (aprox. 1.4 grados de apertura) que se propaga en línea recta, por tanto debe existir **línea de vista** entre el transmisor y el receptor.

Son afectadas por fenómenos atmosféricos, lo que obliga a tener circuito de backup. Tienen buena capacidad de transmisión: aunque la capacidad máxima depende mucho de la frecuencia, las velocidades de datos habituales para un único rango de frecuencia oscilan entre **1** y **10 Mbps (2400 canales de voz).** Son fáciles de instalar y relocalizar.



MICROONDAS POR SATÉLITE

Cuando no hay posibilidad de que las antenas terrestres se vean entre sí se utilizan satélites ubicados a **36.000 kilómetros** de la tierra y son los encargados de retransmitir la señal de información. Cada satélite está compuesto de **transpondedores** (unidades de recepción y transmisión independientes.)

Los satélites **Geo-estacionarios** *rotan a la misma velocidad de la tierra, siendo así estacionarios en relación a la superficie de la tierra.* Esto simplifica enormemente, el trabajo de mantenerlos dentro del rango de los platos receptores en la tierra.

Existen dos clasificaciones de satélites usados en transmisiones:

Satélites BANDA-C: que utilizan frecuencias entre **3,7 y 4,2 Ghz** y desde **5,9 hasta 6,4 Ghz.**

Satélites BANDA-Ku: que utilizan frecuencias entre **11 y 12 Ghz.**

Satélites Banda-C

La banda-C fue el primer rango de frecuencia satelital utilizado en transmisiones. Comparado con la Banda-Ku, la Banda-C requiere unas parábolas de transmisión y recepción, **relativamente grandes.**

Sin embargo con respecto a la Banda-Ku, la Banda-C es **más fiable bajo condiciones adversas**, principalmente lluvia fuerte y granizo. Al mismo tiempo, las frecuencias de banda-C están **más congestionadas** y son **más vulnerables** hacia interferencia terrestre.

Satélites Banda-Ku

Las antenas Banda-Ku son aproximadamente **un tercio del tamaño** utilizado para Banda-C. La razón de que Banda-Ku también tiene menos restricciones técnicas, es la que hace que los usuarios puedan rápidamente instalar enlaces satelitales y empezar a transmitir. Esto es una ventaja importante a la hora de transmitir y recibir información.

RADIOFRECUENCIA

El término **radiofrecuencia**, también denominado **espectro de radiofrecuencia** o **RF**, se aplica a la porción menos energética del espectro electromagnético, situada entre unos **3 Hz y unos 300 GHz**. *El hercio es la unidad de medida de la frecuencia de las ondas radioeléctricas, y corresponde a un periodo por segundo.* Las ondas electromagnéticas de esta región del espectro se pueden transmitir aplicando la corriente alterna originada en un generador a una antena.

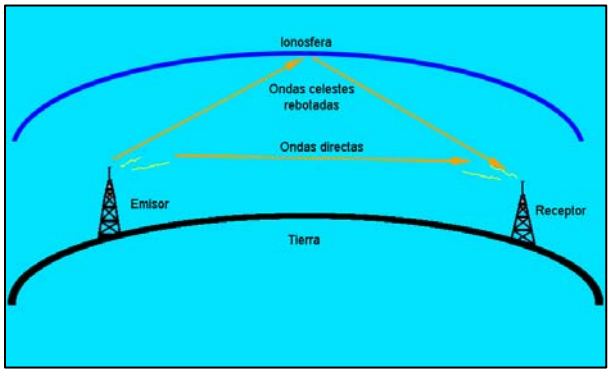
Se emplean en **telecomunicaciones** y se usan para radiotelegrafía, radiofonía, telefonía celular, redes de comunicación personal y otros como controles remotos, teléfonos inalámbricos, etc.

Sus antenas son conductores que transmiten y captan las ondas electromagnéticas. Pueden ser de dos tipos:

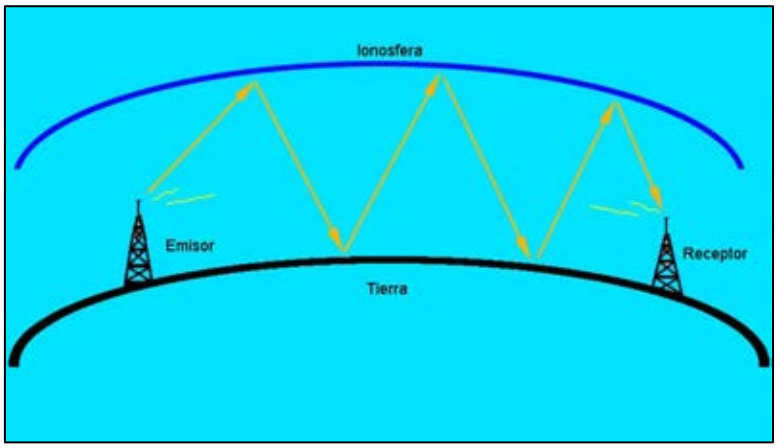
Omnidireccionales: transmiten ondas hacia todas las direcciones.

Unidireccionales: las ondas que envían tienen una dirección específica.

Las frecuencias mas bajas del espectro son las ondas de radio que comprende las bandas **VLF, LF, MF** y **HF** son reflejadas por la ionosfera (capa más alta de la atmósfera).



En grandes distancias la señal va *rebotando* entre la Ionosfera y la Tierra como esquematiza la figura siguiente.



Estas frecuencias **NO** son apropiadas para transmisiones digitales – y por tanto para redes de datos - puesto que se producen **retardos** en los rebotes que pueden modificar el valor de dos bits consecutivos.

Las frecuencias más altas de este espectro son las **VHF, UHF** y **SFH**. Estas frecuencias **NO** rebotan en la Ionosfera por tanto son de ***propagación directa:*** *emisor y receptor se tienen que ver*.

VHF (Very High Frecuency)

Gama de Frecuencia: de **30 Mhz** a **300 Mhz**

Longitud de Onda: de **10** a **1 metro**

Características: Prevalentemente propagación directa, esporádicamente propagación Ionosférica o Troposférica.

Uso Típico: **Enlaces de radio a corta distancia, Televisión, Radiodifusión en Frecuencia Modulada; no tiene demasiada aplicación en redes de datos.**

UHF (Ultra High Frecuency)

Gama de Frecuencia: de **300 Mhz** a **3.000 Mhz.**

Longitud de Onda: de **1 metro** a **10 centímetros.**

Características: **Exclusivamente propagación directa**, posibilidad de enlaces por reflexión o a través de satélites artificiales. Esta banda de frecuencia es la utilizada en las cada vez más populares **redes inalámbricas**, donde, por medio de tarjetas TX/RX de red se pueden unir los diferentes puestos y dispositivos de la red.

Los estándares para redes WLAN han sido desarrollados por organismos reconocidos internacionalmente, tal como el **IEEE** (Institute of Electrical and Electronics Engineers) o el **ETSI** (European Telecommunications Standards Institute). Entre los principales **estándares** se encuentran:

IEEE 802.11: El estándar original de WLANs que soporta velocidades entre 1 y 2 Mbps.

IEEE 802.11a: El estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.

IEEE 802.11b: El estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.

HiperLAN2: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 GHz.

HomeRF: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 GHz.

IEEE 802.11g: Soporta velocidades de hasta 54 Mbps en la banda de 2,4 GHz.

Estándar	Velocidad máxima	Ancho de banda de canal	Frecuencia
802.11b	11 Mbps	25 MHz	2.4 GHz
802.11a	54 Mbps	25 MHz	5.0 GHz
802.11g	54 Mbps	25 MHz	2.4 GHz
HomeRF2	10 Mbps	5 MHz	2.4 GHz
HiperLAN2	54 Mbps	25 MHz	5.0 GHz
5-UP	108 Mbps	50 MHz	5.0 GHz

El gran éxito de las WLANs es que utilizan **frecuencias de uso libre**, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varía de país a país.

La desventaja de utilizar este tipo de bandas de frecuencias es que las comunicaciones son **propensas a interferencias** y **errores de transmisión**. Estos errores ocasionan que sean **reenviados** una y otra vez los paquetes de información.

Una razón de error del 50% ocasiona que se reduzca el caudal eficaz real (throughput) dos terceras partes aproximadamente. Por eso la velocidad máxima especificada teóricamente no es tal en la realidad. Si la especificación IEEE 802.11b nos dice que la velocidad máxima es 11 Mbps, entonces el máximo caudal eficaz será aproximadamente 6 Mbps y menos.

INFRARROJOS

Son ondas electromagnéticas de **frecuencia muy elevada**, entre las microondas y la luz, del orden de **100.000 GHz (100 THz)**. Los estándares IrDA soportan una amplia gama de dispositivos eléctricos, informáticos y de comunicaciones, permite la comunicación **bidireccional** entre dos extremos a velocidades que oscilan entre los **9.600 bps** y los **4 Mbps**. Se utiliza para transmisión de información en **áreas reducidas**: mandos a distancia, conexiones de impresora a un ordenador, etc. Usados también en **redes LAN** en áreas pequeñas que requieren línea de vista.

En redes de área local para el IRDA (Infrared Data Association) ha definido un estándar para capacidades de **1** a **4 Mbps.** El FIR (Fast Infrared) se encuentra en estudio, con unas velocidades teóricas de hasta 16 Mbps.

No necesitan licencia por ser para **interiores** y **cortas distancias** principalmente.

TECNOLOGÍA BLUETOOTH

Propuesta por Ericsson en 1994, en la actualidad muchos fabricantes la desarrollan. Bluetooth es una tecnología inalámbrica que permite comunicaciones entre ordenadores portátiles, PDAs (Personal Digital Assistants), teléfonos celulares y otros dispositivos portátiles en un **área relativamente pequeña**.

Está diseñada para **áreas reducidas**, en **banda de 2.4 Ghz.** Tiene una capacidad de hasta **720 Kbps** y **no requiere línea de vista**. Es muy **resistente a las interferencias**, y permite implementar seguridad mediante **encriptamiento**. No requieren licencia.

En marzo del 2002 la IEEE aprobó el estándar **IEEE 802.15.1** compatible totalmente con la tecnología **Bluetooth v1.1**. En este estándar se definen las especificaciones de la capa física y MAC (medium access control) para las redes WPANs (Wireless PAN).

Este nuevo estándar permite una mayor validez y soporte en el mercado de las especificaciones de Bluetooth, además es un recurso adicional para aquellos que implementaron dispositivos basados en esta tecnología. Anteriormente a la estandarización, dispositivos Bluetooth no podían coexistir con los dispositivos basados en IEEE 802.11b debido a que ambos se interferían entre sí.

07.- anexo. BANDAS DEL ESPECTRO ELECTROMAGNÉTICO

Para su estudio, el espectro electromagnético se divide en segmentos o bandas, aunque esta división es inexacta. Existen ondas que tienen una frecuencia, pero varios usos, por lo que algunas frecuencias pueden quedar en ocasiones incluidas en dos rangos.

Banda	Longitud de onda (m)	Frecuencia (Hz)	Energía (J)
Rayos gamma	< 10 pm	> 30,0 EHz	$> 20 \cdot 10^{-15}$ J
Rayos X	< 10 nm	> 30,0 PHz	$> 20 \cdot 10^{-18}$ J
Ultravioleta extremo	< 200 nm	> 1,5 PHz	$> 993 \cdot 10^{-21}$ J
Ultravioleta cercano	< 380 nm	> 789 THz	$> 523 \cdot 10^{-21}$ J
Luz Visible	< 780 nm	> 384 THz	$> 255 \cdot 10^{-21}$ J
Infrarrojo cercano	< 2,5 µm	> 120 THz	$> 79 \cdot 10^{-21}$ J
Infrarrojo medio	< 50 µm	> 6,00 THz	$> 4 \cdot 10^{-21}$ J
Infrarrojo lejano/submilimétrico	< 1 mm	> 300 GHz	$> 200 \cdot 10^{-24}$ J
Microondas	< 30 cm	> 1 GHz	$> 2 \cdot 10^{-24}$ J
Ultra Alta Frecuencia - Radio	< 1 m	> 300 MHz	$> 19.8 \cdot 10^{-26}$ J
Muy Alta Frecuencia - Radio	< 10 m	> 30 MHz	$> 19.8 \cdot 10^{-28}$ J
Onda Corta - Radio	< 180 m	> 1,7 MHz	$>11.22 \cdot 10^{-28}$J
Onda Media - Radio	< 650 m	> 650 kHz	$> 42.9 \cdot 10^{-29}$ J
Onda Larga - Radio	< 10 km	> 30 kHz	$> 19.8 \cdot 10^{-30}$ J
Muy Baja Frecuencia - Radio	> 10 km	< 30 kHz	$< 19.8 \cdot 10^{-30}$ J

RADIOFRECUENCIA

En radiocomunicaciones, los rangos se abrevian con sus siglas en inglés. Los rangos son:

Nombre	Abreviatura inglesa	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
Extra baja frecuencia Extremely low frequency	**ELF**	1	3-30 Hz	100.000 km – 10.000 km
Super baja frecuencia Super low frequency	**SLF**	2	30-300 Hz	10.000 km – 1000 km
Ultra baja frecuencia Ultra low frequency	**ULF**	3	300–3000 Hz	1000 km – 100 km
Muy baja frecuencia Very low frequency	**VLF**	4	3–30 kHz	100 km – 10 km
Baja frecuencia Low frequency	**LF**	5	30–300 kHz	10 km – 1 km
Media frecuencia Medium frequency	**MF**	6	300–3000 kHz	1 km – 100 m
Alta frecuencia High frequency	**HF**	7	3–30 MHz	100 m – 10 m
Muy alta frecuencia Very high frequency	**VHF**	8	30–300 MHz	10 m – 1 m
Ultra alta frecuencia Ultra high frequency	**UHF**	9	300–3000 MHz	1 m – 100 mm
Super alta frecuencia Super high frequency	**SHF**	10	3-30 GHz	100 mm – 10 mm
Extra alta frecuencia Extremely high frequency	**EHF**	11	30-300 GHz	10 mm – 1 mm
			Por encima de los 300 GHz	< 1 mm

- **Frecuencias extremadamente bajas (*ELF, Extremely Low Frequencies*)** : son aquellas que se encuentran en el intervalo de 3 a 30 Hz. Este rango es equivalente a aquellas frecuencias del sonido en la parte más baja (grave) del intervalo de percepción del oído humano. Cabe destacar aquí que el oído humano percibe ondas sonoras, no electromagnéticas, sin embargo se establece la analogía para poder hacer una mejor comparación.

- **Frecuencias super bajas (*SLF*, *Super Low Frequencies*)** : son aquellas que se encuentran en el intervalo de 30 a 300 Hz. En este rango se incluyen las ondas electromagnéticas de frecuencia equivalente a los sonidos graves que percibe el oído humano típico.

- **Frecuencias ultra bajas (*ULF, Ultra Low Frequencies*) :** son aquellas en el intervalo de 300 a 3000 Hz. Este es el intervalo equivalente a la frecuencia sonora normal para la mayor parte de la voz humana.

- **Frecuencias muy bajas *(VLF*, *Very Low Frequencies) :*** Se pueden incluir aquí las frecuencias de 3 a 30 kHz. El intervalo de VLF es usado típicamente en comunicaciones gubernamentales y militares.

- **Frecuencias bajas *(LF*, *Low Frequencies)* :** son aquellas en el intervalo de 30 a 300 kHz. Los principales servicios de comunicaciones que trabajan en este rango están la navegación aeronáutica y marina.

- **Frecuencias medias *(MF, Medium Frequencies)*** : están en el intervalo de 300 a 3000 kHz. Las ondas más importantes en este rango son las de radiodifusión de AM (530 a 1605 kHz).

- **Frecuencias altas *(HF, High Frequencies) :*** son aquellas contenidas en el rango de 3 a 30 MHz. A estas se les conoce también como "onda corta". Es en este intervalo que se tiene una amplia gama de tipos de radiocomunicaciones como radiodifusión, comunicaciones gubernamentales y militares. Las comunicaciones en banda de radioaficionados y banda civil también ocurren en esta parte del espectro.

- **Frecuencias muy altas *(VHF, Very High Frequencies) :*** van de 30 a 300 MHz. Es un rango popular usado para muchos servicios, como la radio móvil, comunicaciones marinas y aeronáuticas, transmisión de radio en FM (88 a 108 MHz) y los canales de televisión del 2 al 12 [según norma CCIR (Estándar B+G Europa)]. También hay varias bandas de radioaficionados en este rango.

- **Frecuencias ultra altas *(UHF, Ultra High Frequencies) :*** abarcan de 300 a 3000 MHz, incluye los canales de televisión de UHF, es decir, del 21 al 69 [según norma CCIR (Estándar B+G Europa)] y se usan también en servicios móviles de comunicación en tierra, en servicios de telefonía celular y en comunicaciones militares.

- **Frecuencias super altas *(SHF, Super High Frequencies) :*** son aquellas entre 3 y 30 GHz y son ampliamente utilizadas para comunicaciones vía satélite y radioenlaces terrestres. Además, pretenden utilizarse en comunicaciones de alta tasa de transmisión de datos a muy corto alcance mediante UWB. También son utilizadas con fines militares, por ejemplo en radares basados en UWB.

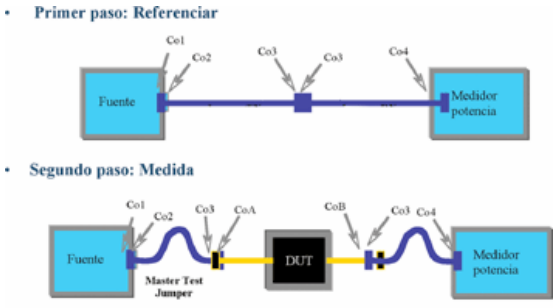
- **Frecuencias extremadamente altas *(EHF, Extrematedly High Frequencies) :*** se extienden de 30 a 300 GHz. Los equipos usados para transmitir y recibir estas señales son más complejos y costosos, por lo que no están muy difundidos aún.

Existen otras formas de clasificar las ondas de radiofrecuencia. Como ejemplo, cabe destacar que las frecuencias entre 1 GHz y 300 GHz, son llamadas microondas. Estas frecuencias abarcan parte del rango de UHF y todo el rango de SHF y EHF. Estas ondas se utilizan en numerosos sistemas, como múltiples dispositivos de transmisión de datos, radares y hornos microondas.

08.- anexo. MEDIDAS EN FIBRA ÒPTICA: REFLECTOMETRÍA Y POTENCIA

INSTRUMENTOS DE MEDIDA

Una vez finalizado el montaje de un enlace óptico, es preciso realizar las medidas necesarias para comprobar su adecuada realización. El técnico debe asegurarse de que los resultados obtenidos; en términos de atenuación y pérdidas de retorno, en su caso, se corresponden con las exigencias del proyecto; esto es, con el balance de pérdidas, o pérdidas admisibles previstas.



Para ello cuenta con dos familias de equipos de medida: los **medidores de potencia óptica** y los **reflectómetros ópticos (OTDRs).**

EQUIPOS DE MEDIDA DE POTENCIA ÓPTICA: (OLTS)

Un **OLT (Optical Loss Test Set: Conjunto de medida de pérdidas ópticas)** está formado por varios elementos:

- Una **fuente de luz**, estable y con capacidad de emisión en las longitudes de onda (λ) previstas en la instalación (850 y 1300 nm para las fibras MM; 1310, 1550, 1490 nm en SM)

- Un **medidor de potencia**, con posibilidad de reconocimiento de la λ en la que emite la fuente, calibrado para las λ previstas en el proyecto. La potencia de emisión de la fuente y la sensibilidad del medidor deben ser suficientes para que, conjugados, permitan superar el rango de pérdidas previsto.

- Un **conjunto de accesorios** (latiguillos de medida, enfrentadores, elementos de limpieza,…) que permitan seguir la operativa básica.

En consecuencia, las pérdidas registradas se corresponderán exactamente con las pérdidas reales del circuito a medir; sin otra información adicional. Para reproducir exactamente todas las posibilidades de trabajo del circuito, las medidas de potencia deberán ser bidireccionales, y en todas las longitudes de onda previstas para la transmisión.

En función de las características propias de los equipos (posibilidad de registro automático de datos, de conexión a ordenador, de reconocimiento automático de λ, número de ellas para las que esté calibrado el medidor o emita la fuente, posibilidad de fijación de umbrales, etc.) los OLTS serán más o menos rápidos en su manejo o emisión de informes. Es preciso acceder a los dos extremos de la fibra.

REFLECTÓMETROS ÓPTICOS (OTDRS)

Los OTDR emiten, desde uno de sus extremos, una **señal lumínica pulsada** en el seno de la fibra a medir, que **la recorre hasta su final**. Posteriormente, el equipo recoge y analiza las porciones de esta señal que han sido retornadas, como consecuencia de las reflexiones de Fresnel y de Rayleigh (backscattering).

El resultado es una **gráfica Atenuación/ Distancia** en la que quedan reflejados todos los eventos, tanto reflexivos (conectores, enfrentamientos) como de atenuación (Curvaturas, empalmes).

La gráfica reflectométrica proporciona toda la información precisa sobre las incidencias en el cable, siendo un auxiliar indispensable para la **localización de eventos** *(curvaturas, conectores, empalmes, etc.)* dada la precisión de la medida. En este caso, también deben realizarse medidas bidireccionales, y en diferentes λ, ya que, además de las razones apuntadas para los OLTS nos permitirá identificar determinado tipo de un OTDR viene dada por la adecuación de sus características (Rango dinámico, zonas muertas de atenuación y eventos, λ de trabajo) a las necesidades de medida.

CONCLUSIÓN: ¿OTDRS U OLTS?

Tal y como comentamos anteriormente, cada tipo de instrumento proporciona medidas de gran precisión y validez, una vez conocidas sus características específicas. No obstante, en líneas generales, las medias de potencia con ***OLTS serán suficientes al finalizar tramos cortos con pocos eventos (Enlaces LAN, por ej.),*** mientras que l***as gráficas OTDR serán precisas en enlaces de larga distancia, con eventos múltiples (Redes WAN enlaces Telecom).***

No obstante, siempre será preciso realizar medidas bidireccionales y en varias λ. (Las previstas de trabajo, además de 1625 nm, si nuestro equipo lo permite)

09.- DISPOSITIVOS DE INTERCONEXIÓN DE REDES NIVEL FÍSICO (capa 1 OSI)

Los dispositivos de interconexión son aquellos elementos de una red LAN que permiten conectar los diferentes puestos (ordenadores, impresoras etc.) entre si. Además también son aquellos que permiten conectar diferentes redes, como por ejemplo, una red LAN interna con Internet.

Como dispositivos englobados en el **nivel físico** (**capa 1** del modelo OSI) veremos **repetidores** y **concentradores** (HUB).

REPETIDORES

En una línea de transmisión, la señal sufre distorsiones y se vuelve más débil a medida que la distancia entre los dos elementos activos se vuelve más grande. Dos nodos en una red de área local, generalmente, no se encuentran a más de unos cientos de metros de distancia. Es por ello que se necesita equipo adicional para ubicar esos nodos a una distancia mayor.

Un **repetidor** es un *dispositivo sencillo utilizado para* ***regenerar*** *una señal entre dos nodos de una red*. De esta manera, se extiende el alcance de la red. El repetidor funciona solamente en el **nivel físico** (**capa 1** del modelo OSI), es decir que sólo actúa sobre la información binaria que viaja en la línea de transmisión y que **no puede** interpretar los paquetes de información.

Por otra parte, un repetidor puede utilizarse como una **interfaz** entre dos medios físicos de tipos diferentes, es decir que puede, por ejemplo, *conectar un segmento de par trenzado a una línea de fibra óptica.*

CONCENTRADOR

Un **concentrador** (hub) es un elemento de hardware que ***permite concentrar el tráfico de red que proviene de múltiples hosts y regenerar la señal*****.** El concentrador es una entidad que cuenta con determinada cantidad de puertos (posee tantos puertos como equipos a conectar entre sí, generalmente 4, 8, 16 ó 32). **Su único objetivo es recuperar los datos binarios que ingresan a un puerto y enviarlos a los demás puertos**.

Al igual que un repetidor, el concentrador funciona en el **nivel físico** (**capa 1** del modelo OSI). Es por ello que a veces se lo denomina *repetidor multipuertos*.

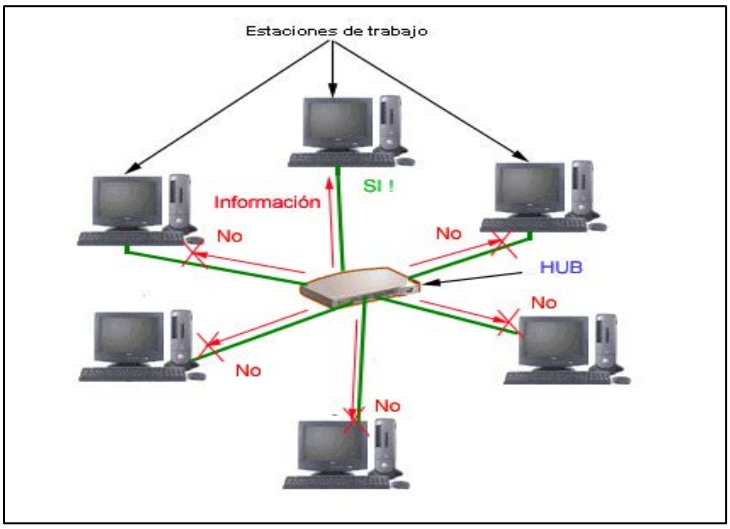
Un HUB tal como dice su nombre es un **concentrador**. *Simplemente une conexiones y no altera la información que le llega*. Para entender como funciona veamos paso a paso lo que sucede (aproximadamente) cuando llega una trama con información.

El HUB **envía la información a todos los ordenadores (estén o no interesados):** a este nivel sólo hay un destinatario de la información, pero el HUB envía la información a todos los ordenadores que están conectados a él, y aquellos que no son destinatarios la rechazan.

Este tráfico añadido genera más probabilidades de **colisión**. ***Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea que otro ordenador que hace lo mismo.*** Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

Un HUB **funciona a la velocidad del dispositivo más lento de la red**. Si observamos cómo funciona vemos que el HUB **no tiene capacidad de almacenar nada**. Por lo tanto si un ordenador que emite a 100 Mbps le trasmitiera a otro de 10 Mbps algo se perdería el mensaje. En el caso del ADSL los routers suelen funcionar a 10 megabit, si lo conectamos a nuestra red casera, toda la red funcionará a 10, aunque nuestras tarjetas sean 10/100.

Un HUB es un dispositivo **simple**, esto influye en dos características: el precio; es **barato** y el retardo: un HUB en una red de oficina o doméstica casi no añade **ningún retardo** a los mensajes; pero si la red comienza a ampliarse se empiezan a notar retrasos, precisamente por las colisiones que se originan, y que obligan a reenviar la información.



El concentrador (hub) conecta diversos equipos entre sí, a veces dispuestos en forma de **estrella**, de donde deriva el nombre de HUB (que significa cubo de rueda en inglés; la traducción española exacta es **repartidor**) para ilustrar el hecho de que se trata del punto por donde se cruza la comunicación entre los diferentes equipos.

Tipos de concentradores

Existen diferentes categorías de concentradores (hubs):

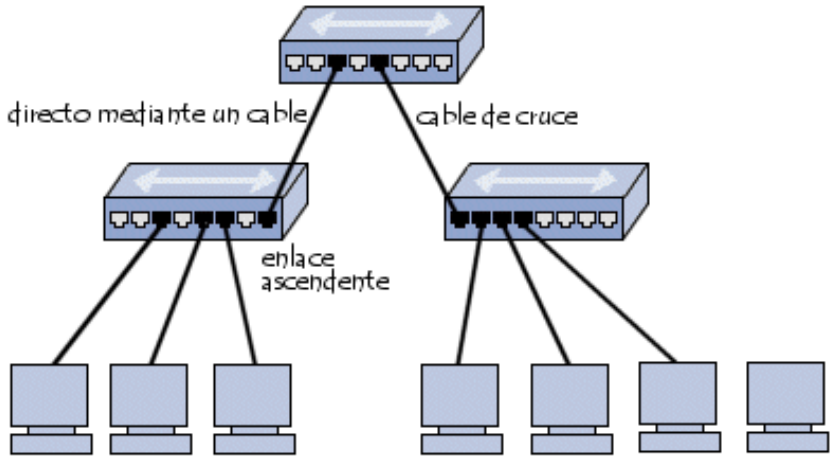
- concentradores "**activos**": Están conectados a una fuente de alimentación eléctrica y permiten **regenerar** la señal que se envía a los diferentes puertos

- puertos "**pasivos**": Simplemente envían la señal a todos los hosts conectados, sin amplificarla.

Conexión de múltiples concentradores

Es posible conectar varios concentradores (hubs) entre sí para centralizar un gran número de equipos. Esto se denomina **conexión en cadena margarita** (“daisy chains” en inglés). Para ello, sólo es necesario conectar los concentradores mediante un **cable cruzado**, es decir un cable que conecta los puertos de entrada/salida de un extremo a aquéllos del otro extremo.

Los concentradores generalmente tienen un puerto especial llamado "**enlace ascendente**" para conectar dos concentradores mediante un cable de conexión. Algunos concentradores también pueden cruzar o descruzar automáticamente sus puertos, en función de que se encuentren conectados a un host o a un concentrador.



Se pueden conectar en cadena hasta tres concentradores.

Si desea conectar varios equipos a su conexión de Internet, un concentrador no será suficiente. Necesitará un router o un conmutador, o dejar el equipo conectado directamente como una pasarela (permanecerá encendido mientras los demás equipos de la red deseen acceder a Internet).

10.- FLUJO DE LA INFORMACIÓN

TIPOS DE ENLACES

Atendiendo al modo de acceso de un terminal a otro, los enlaces se clasifican en: **Punto a punto**, **multipunto**, **directo** e **indirecto**.

Punto a punto

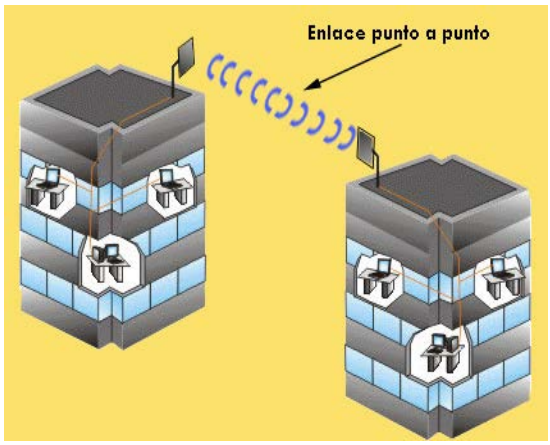
Es aquel que conecta únicamente dos estaciones en un instante dado. Se puede establecer enlaces punto a punto en circuitos dedicados o conmutados, como ya se ha explicado, que a su vez pueden ser simplex, half-dúplex o full-dúplex. Estos enlaces presentan las siguientes ventajas:

- Alta disponibilidad de servicio. Una conexión permanente entre dos puntos asegura que cada uno de los extremos se encontrara "visible" las 24 horas, los 365 días del año.

- Confidencialidad del enlace. Esta es otra de las características de los enlaces Punto a Punto. Al no existir más de dos puntos conectados, se reduce considerablemente el riesgo de intrusión en la comunicación.

- Ancho de banda estable. Al disponer de un enlace de alta disponibilidad de servicio y dedicado, no se producen fluctuaciones en el ancho de banda, ya que no se añaden usuarios a esta comunicación.

Entre los inconvenientes podemos encontrar su elevado coste económico.



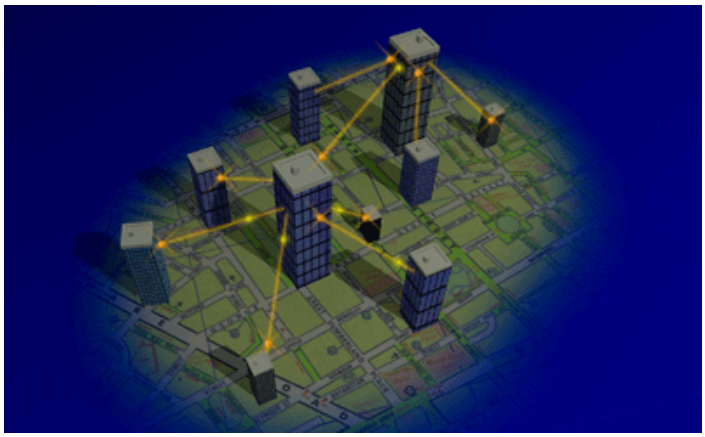
Multipunto

Un enlace multipunto es aquel que conecta más de dos estaciones a la vez.

Este tipo de enlace puede ser a su vez **half-duplex** o **full-duplex**, por regla general no es fácil encontrar un enlace multipunto simplex. El enlace multipunto presenta las siguientes ventajas:

- Compartir recursos e información entre sus redes con facilidad.
- Disponibilidad de la información por muchos puestos de forma inmediata.
- Administración centralizada de los todos los puestos de red.
- Bajo costo de instalación y mantenimiento, teniendo en cuenta el número de estaciones que se manejan.

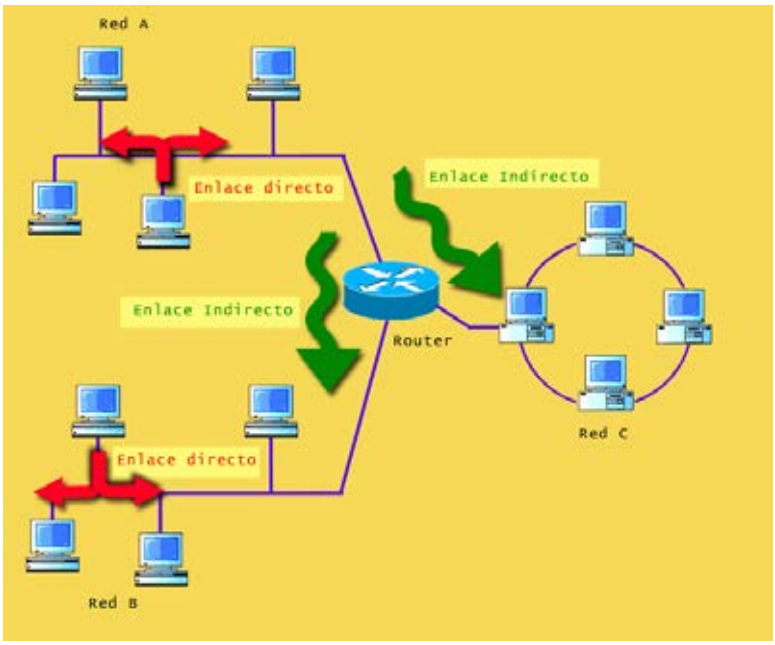
Este tipo de enlaces tiene los inconvenientes de su baja seguridad, ya que no es fácil controlar a todos los usuarios conectados, y la inestabilidad de su ancho de banda, puesto que se producen conexiones y desconexiones con relativa frecuencia.



Enlaces directos

Son aquellos enlaces que se producen *entre dos ordenadores dentro de la misma red*. En esta clase de enlaces no se necesita **ningún** dispositivo de interconexión que gestione o filtre el tráfico entre redes diferentes.

En este tipo de enlace, el ordenador de origen envía la información directamente con la dirección del ordenador de destino.



Enlaces indirectos

Son aquellos enlaces que se producen a través de un dispositivo de interconexión, es decir: atraviesan ***routers*** o ***bridges*** para conectar con otros ordenadores que se encuentran **en redes distintas** a la del origen.

En los enlaces indirectos, el ordenador de origen envía la información al primer dispositivo de interconexión (el router o el bridge) y es éste el que encamina la información hacia el ordenador de destino, o hacia el siguiente router.

TIPOS DE FLUJO DE LA INFORMACIÓN

Atendiendo a la forma en la que fluye la información de un sitio a otro de la red, los enlaces se pueden clasificar en **simplex** (o unidireccional), **half-duplex** (o bidireccional no simultáneo) y **full duplex** (o bidireccional simultáneo).

Simplex

En este tipo, también llamado **unidireccional**, la información se transmite en una sola dirección. Los cables de datos están dedicados a la transmisión en un solo sentido. Un ejemplo de este tipo de comunicación es el flujo de datos desde un ordenador hacia una impresora, puesto que este flujo no se produce en sentido inverso.

En esta comunicación están perfectamente definidas las funciones del emisor y el receptor, y la transmisión de datos siempre se efectúa en una dirección: emisor --> receptor.

En este tipo de comunicación se dice que hay un **único** canal físico y un **único** canal lógico unidireccional.

Half-Duplex

El mismo canal o línea se utiliza para transmitir **en los dos sentidos, pero no simultáneamente**. La comunicación es bidireccional; emisor y receptor pueden intercambiar los papeles, sin embargo la bidireccionalidad no puede ser simultánea.

Ejemplo: Las emisiones de radioaficionados, donde se utilizan códigos vocales especiales ("cambio") para que se produzca la conmutación de los papeles de emisor y receptor. Hay un canal físico y un canal lógico bidireccional.

En los diseños de redes de información, conectadas con cable coaxial en banda base, también se produce este tipo de comunicación: mientras una estación transmite no puede recibir, y si le llegara un paquete de información desde otro puesto, éste **colisionaría** con el recién enviado, y se perderían ambos.

Full-Duplex

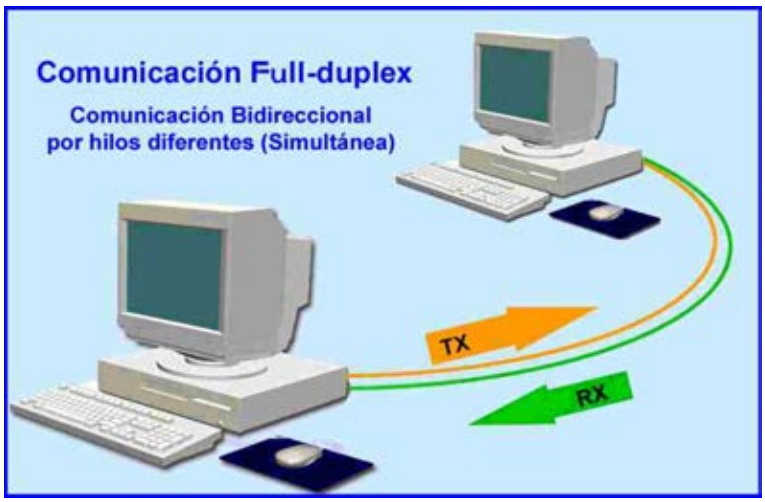
En las comunicaciones full-duplex la transmisión es **bidireccional** y **simultánea**. La emisión y la recepción se producen *por canales diferentes*. Es importante tener en cuenta que, aunque haya canales diferentes para transmitir y recibir, las estaciones de red también tienen que estar en disposición de poder hacerlo; es decir: deben de tener tarjetas de red full-duplex.

El flujo de información full-duplex es el más utilizado en las redes de área local.

En los cables utilizados, ya sean de par trenzado o de fibra óptica, siempre se reservan unos hilos para transmisión y otros para recepción.

Ventajas de full-duplex:

- Rapidez: Se puede enviar y recibir a la vez.
- Ausencia total de colisiones en el cable: los envíos y las recepciones circulan por canales diferentes.



PERTURBACIONES DE LA TRANSMISIÓN

En general todos los dispositivos eléctricos y electrónicos emiten interferencias y además son susceptibles a éstas. Por tanto las transmisiones de datos tampoco están libres de perturbaciones.

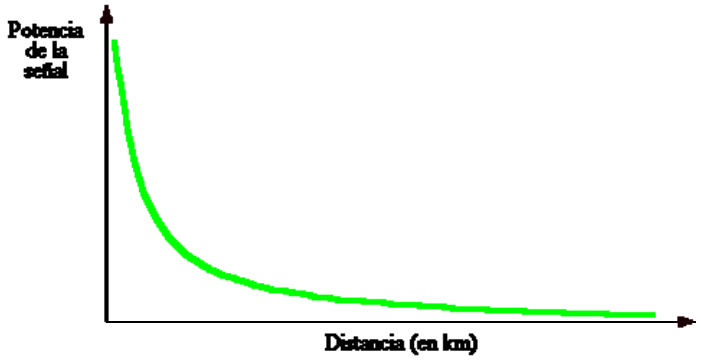
Las perturbaciones más frecuentes que sufren las transmisiones de datos son las siguientes:

- La atenuación
- La distorsión de retardo
- El ruido

Atenuación

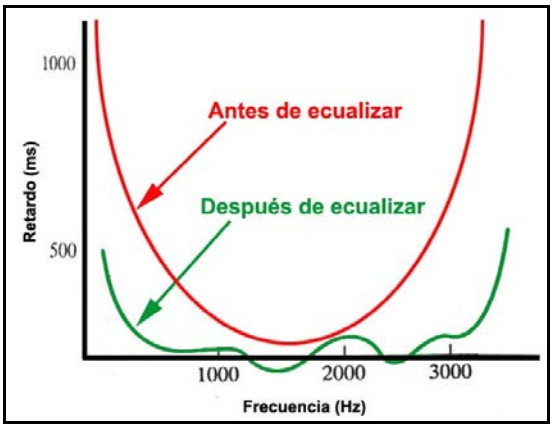
Como ya se sabe, los datos son transmitidos a través del canal mediante señales eléctricas. Esta energía eléctrica que conforma una señal decae con la distancia, por lo que hay que asegurarse que llegue con la suficiente energía como para ser captada por la circuitería del receptor y además, el ruido debe ser sensiblemente menor que la señal original. Para conseguir este objetivo se utilizan amplificadores de señal o repetidores.

Debido a que la atenuación varía en función de la frecuencia, las señales analógicas llegan distorsionadas, por lo que hay que utilizar sistemas que le devuelvan a la señal sus características iniciales. Esto se consigue mediante bobinas que cambian las características eléctricas o amplificando más las frecuencias más altas.



Distorsión de retardo

El retardo se produce debido a que, en medios guiados, la velocidad de propagación de una señal varía con la frecuencia, hay frecuencias que llegan antes que otras dentro de la misma señal, y por tanto, las diferentes componentes en frecuencia de la señal, llegan en instantes diferentes al receptor. Para atenuar este problema se usan técnicas de ecualización.



Ruido

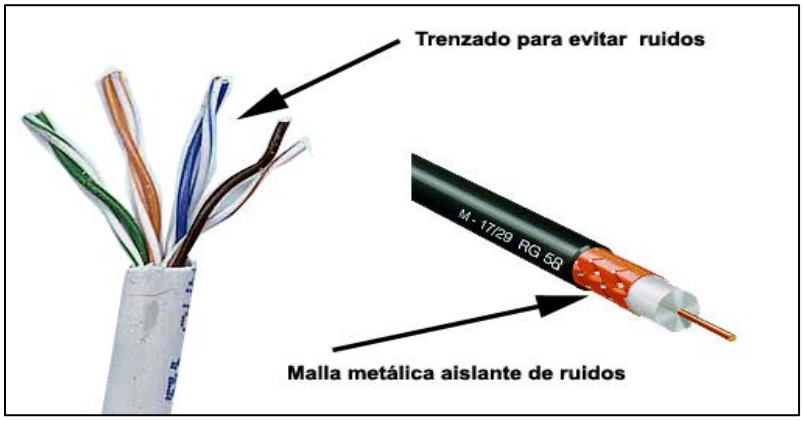
El ruido es toda aquella señal no deseada que se inserta entre el emisor y el receptor de una señal dada. Hay diferentes tipos de ruido:

Ruido térmico: debido a la agitación térmica de electrones dentro del conductor.

Ruido de intermodulación: cuando distintas frecuencias comparten el mismo medio de transmisión.

Diafonía: se produce cuando hay un acoplamiento entre las líneas que transportan las señales.

Ruido impulsivo: son pulsos discontinuos de poca duración y de gran amplitud que afectan y distorsionan la señal. Precisamente, el objetivo del trenzado de los hilos- dos a dos- en los cables de pares, y la malla metálica de los cables coaxiales, es evitar las interferencias por ruido.



11.- TRANSMISIÓN ANALÓGICA Y DIGITAL

En las redes de ordenadores, los datos a intercambiar siempre están disponibles en forma de señal digital. No obstante, para su transmisión podemos optar por la utilización de señales digitales o analógicas. La elección no será, casi nunca, una decisión del usuario, sino que vendrá determinada por el medio de transmisión a emplear.

No todos los medios de transmisión permiten señales analógicas ni todos permiten señales digitales. Como la naturaleza de nuestros datos será siempre digital, es necesario un proceso previo que adecue estos datos a la señal a transmitir. A continuación examinaremos los 2 casos posibles:

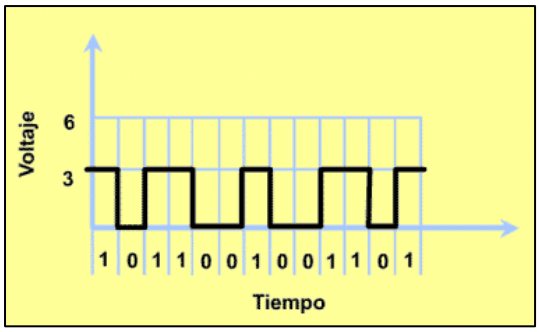
INFORMACIÓN DIGITAL Y TRANSMISIÓN DE SEÑAL ANALÓGICA: TRANSMISIÓN ANALÓGICA DE DATOS

La Capa de Enlace de Datos de OSI prepara la información para su envío en forma de trenes de bits, sucesiones de ceros y unos binarios que contienen los datos a transmitir junto a las cabeceras necesarias para el funcionamiento correcto de los diferentes protocolos.

Ahora bien; si pensamos en que un ordenador es un dispositivo eléctrico/electrónico, que funciona a base de impulsos de corriente eléctrica continua, comprenderemos claramente cómo estos ceros y unos lógicos son interpretados por nuestra máquina como variaciones de tensión eléctrica.

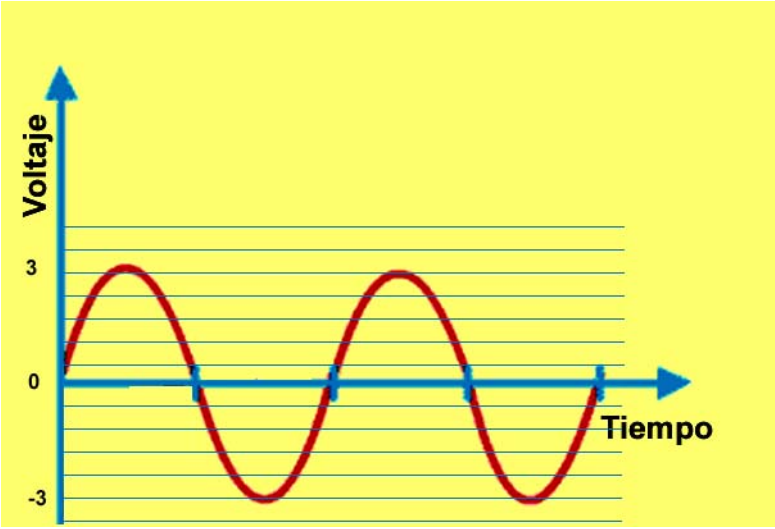
Es decir, que la información que maneja un ordenador son dígitos binarios convertidos en impulsos de electricidad continua. El mecanismo general de transformar información (datos) en "algo" que la represente y que sea apto para su transmisión por un medio cualquiera se denomina **Codificación**, y a ese "algo" que representa la información son las **señales**.

Para codificar datos binarios por medio de señales de corriente continua se pueden usar diversos métodos, como la determinación de un determinado voltaje (3 voltios) para representar un 1 y otro voltaje menor (0 voltios) para representar un cero, cuya representación gráfica sería:



El inconveniente de las señales en corriente continua -señales digitales- es que cuando deben ser transportadas a través de determinadas redes y cableados, como la red de telefonía convencional, se deben convertir en corriente alterna, es decir en señales analógicas.

Las señales analógicas mediante corriente alterna, a diferencia de las digitales, son señales continuas en el tiempo, es decir en un instante cualquiera, su valor instantáneo puede ser cualquiera, solo limitado por la potencia máxima que se puede transmitir. Su representación gráfica sería:



Los parámetros a considerar en una señal analógica son:

Frecuencia: Se mide en Hertzios y es el número de ciclos que se producen en un segundo.

Amplitud: Se mide en voltios.

Fase: Instante en que la señal toma un valor respecto a una referencia, se mide en grados

Longitud de Onda: es la distancia que recorre la onda en el intervalo de tiempo transcurrido entre dos máximos consecutivos de una de sus propiedades.

Ancho de Banda: es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal y se mantienen igual o inferior a 3 dB comparada con la frecuencia central de pico (f_c). Es la característica más importante que define a una señal analógica.

Se pude concluir, por tanto, que la transmisión analógica es una forma de transmitir señales analógicas que pueden contener datos analógicos o datos digitales convertidos.

Las ventajas de las transmisiones analógicas son fundamentalmente dos:

Alta disponibilidad de medios de transmisión: ya que los datos analógicos se pueden transmitir por cualquier línea telefónica convencional.

Reducido coste económico: ya que no requiere instalación alguna si se dispone de un a línea de teléfono.

El principal inconveniente de la transmisión analógica es que la señal se debilita con la distancia, lo que obliga a utilizar amplificadores de señal cada cierta distancia.

EL MODEM

Un Módem (**MO**dulador - **DEM**odulador) es un dispositivo que **convierte la señal digital** -utilizada en un sistema informático- **en señal analógica y viceversa**, para posibilitar que el mensaje enviado por un ordenador pueda llegar a otros ordenadores a través de líneas analógicas.

Al proceso por el cual obtenemos una señal analógica a partir de unos datos digitales se le denomina **modulación**. Esta señal la transmitimos y el receptor debe realizar el proceso contrario, denominado **demodulación** para recuperar la información. El módem es el encargado de realizar dicho proceso. Algunos esquemas simples de modulación son:

FSK (Modulación por desplazamiento de la frecuencia): Se modifica la frecuencia de la portadora según el valor de bit a transmitir.

ASK (modulación por desplazamiento de la amplitud): En esta técnica no se modifica la frecuencia de la portadora sino su amplitud. Los dos valores binarios se representan mediante diferentes niveles de amplitud de esta señal.

PSK (Modulación por desplazamiento de fase): La frecuencia y la amplitud se mantiene constantes y se varía la fase de la portadora para representar los niveles uno y cero con distintos ángulos de fase.

Los Modems podemos seleccionarlos de acuerdo a:

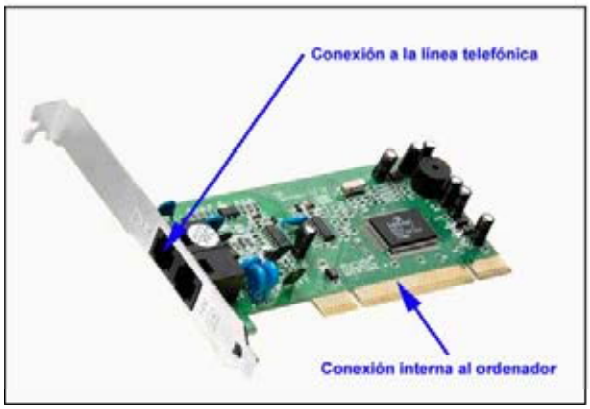
- La velocidad de transmisión: Generalmente a 56.000 bits por segundo.
- El tipo de línea que utiliza: dedicada, conmutada o ambas.
- La modulación que emplea: FSK, PSK, DPSK, QAM, TCM.
- Las posibilidades de compresión de datos para transmisión.
- La modalidad de trabajo: punto a punto o multipunto.

Si se instala interno o externo al terminal de datos: compatible con las ranuras internas de expansión (ISA o PCI) del ordenador; o con conexión externa por el puerto COM o USB.

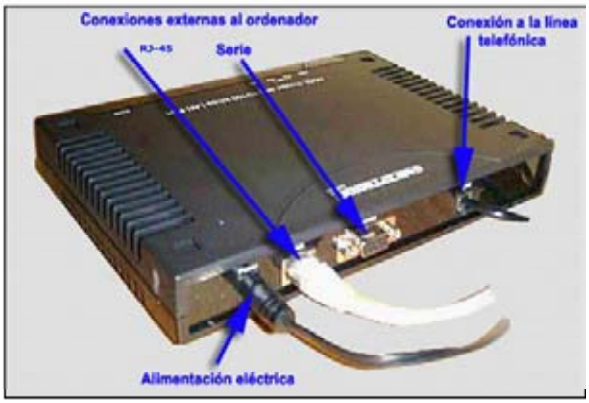
En la práctica, el mercado de los módems crea dos grupos:

- **Modems empleados en centros de transmisión** con una permanente o casi permanente actividad, las cuales cuentan con mecanismos sofisticados de diagnostico, control y administración centralizados y remotos.
- **Modems de escritorio** cuyo principal uso es la conexión a través de la red telefónica convencional, con cierta regularidad pero nunca con carácter permanente ni con uso exhaustivo.

Modem interno

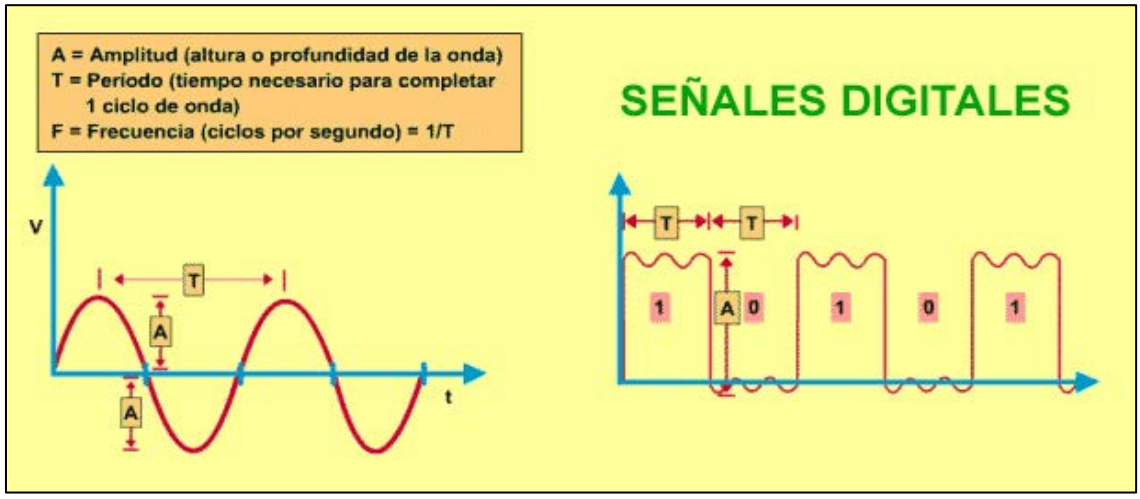


Modem

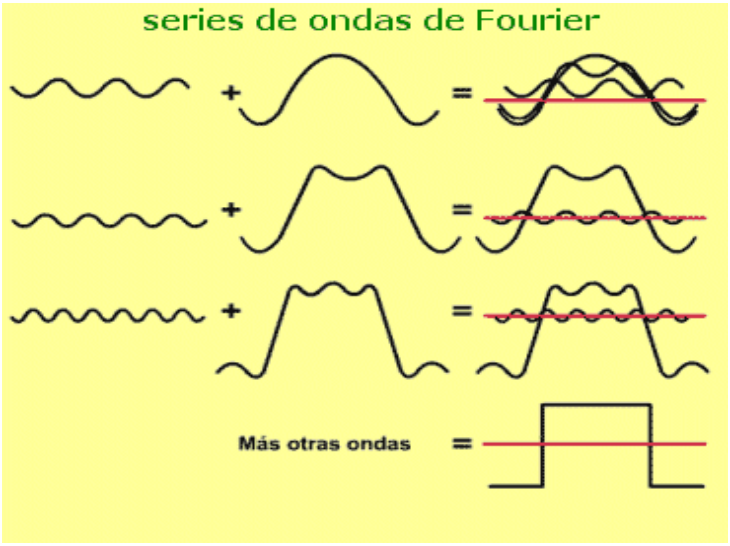


MODULACIÓN

El principal problema que plantea la codificación en señales de corriente alterna (señales analógicas) es que, por propia definición, la corriente va variando entre dos valores extremos con el tiempo, por lo que no podemos usar de antemano el sistema aplicado en el caso de corriente continua, a no ser que consiguiéramos variar la forma ondulante de la corriente alterna en una forma pulsante, con la que podríamos obtener señales parecidas a las conseguidas en el caso de corriente continua. Estas ondas alternas pulsantes se denominan señales digitales.

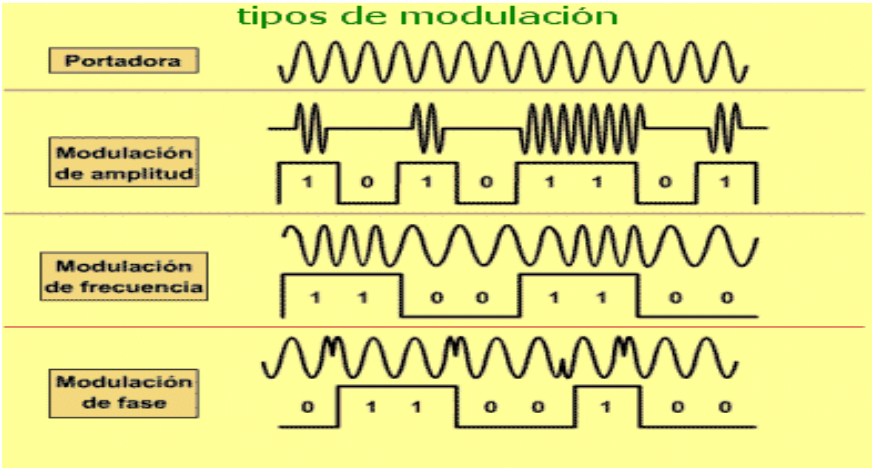


Este método sería ideal, pero el problema era cómo poder realizar la transformación. Así estaban las cosas hasta que Jean Baptiste Fourier demostró que una suma especial de ondas sinusoidales, de frecuencias relacionadas armónicamente, que son múltiplos de cierta frecuencia básica, se pueden sumar para crear cualquier patrón de onda. Con esto, las ondas complejas se pueden crear a partir de ondas simples, y *una onda rectangular, o un* ***pulso rectangular****, se puede generar usando la combinación correcta de ondas sinusoidales.*



Estos pulsos pueden ser usados para transportar información, proceso que también se conoce con el nombre de **Modulación**. Esto es, precisamente, lo que hace un MODEM: modular y demodular una señal. *La modulación se basa en la modificación de una onda primaria de forma que pueda seguir un patrón de pulsos capaz de transmitir información de forma correcta por una línea digital.*

Existen tres formas de modulación: De amplitud, de frecuencia y de fase.

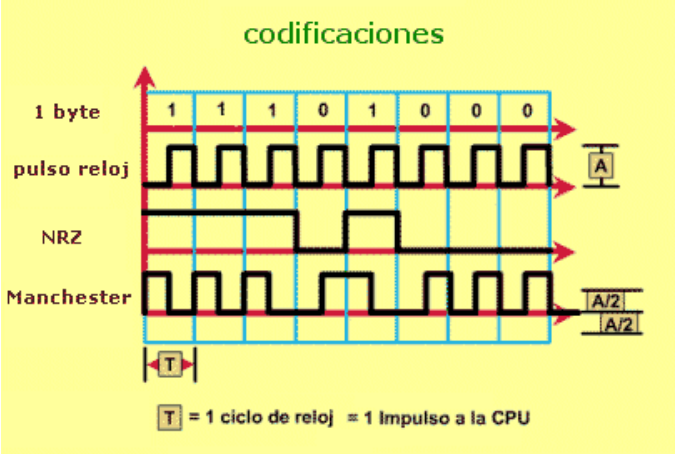


INFORMACIÓN DIGITAL Y TRANSMISIÓN DE SEÑAL DIGITAL: TRANSMISIÓN DIGITAL DE DATOS

Esta es la base de la codificación usada para transmitir datos entre redes LAN, transformándose los bits en algo tangible, físico, como un pulso eléctrico en un cable, un pulso luminoso en una fibra óptica o un pulso de ondas electromagnéticas en el espacio. *Para obtener la secuencia que compone la señal digital a partir de los datos digitales se efectúa un proceso denominado* ***codificación***. Existen dos métodos principales de codificación: **NRZ (No Return to Zero) y Manchester.**

Codificación NRZ **(No Return to Zero)*:*** o de código sin retorno a cero, es la codificación más sencilla. Se caracteriza por *una señal alta y una señal baja* (a menudo +5 o +3,3 V para 1 binario y 0 V para 0 binario). En el caso de las fibras ópticas, el 1 binario puede ser un LED o una luz láser brillante, y el 0 binario oscuro o sin luz. En el caso de las redes inalámbricas, el 1 binario puede significar que hay una onda portadora y el 0 binario que no hay ninguna portadora.

Codificación de Manchester: el voltaje del cable de cobre, el brillo del LED o de la luz láser en el caso de la fibra óptica o la energía de una onda EM en el caso de un sistema inalámbrico hace que *los bits se codifiquen como transiciones*. Así, la codificación Manchester da como resultado que los 0 se codifiquen como una transición de baja a alta y que el 1 se codifique como una transición de alta a baja (un flanco de bajada representa un cero y un flanco de subida un uno). Dado que tanto los 0 como los 1 dan como resultado una transición en la señal, el reloj se puede recuperar de forma eficaz en el receptor.



Otras codificaciones son: **NRZI** (No Return to Zero Inverted), **RZ** (Return to Zero) y **Manchester diferencial**

NRZI (No Return to Zero Inverted): La señal no cambia si se transmite un uno, y se invierte si se transmite un cero.

RZ (Return to Zero): Si el bit es uno, la primera mitad de la celda estará a uno. La señal vale cero en cualquier otro caso.

Manchester diferencial: Manteniendo las transiciones realizadas en el método Manchester, en este método introduce la codificación diferencial. Al comienzo del intervalo de bit, la señal se invierte si se transmite un cero, y no cambia si se transmite un uno.

Por tanto la **Capa de Enlace de Datos** prepara la información a transmitir en trenes de bits (0 y 1 lógicos), representados internamente por **impulsos de corriente continua**. Para su transmisión por los medios de red, el host emisor debe transformar estas señales continuas en señales en **corriente alterna**, y para ello usa un sistema de codificación, generalmente el de Manchester, creando ondas pulsantes basadas en las series de ondas de Fourier.

Normalmente este proceso se lleva a cabo en chips especiales de la tarjeta de red del host o en dispositivos especiales, como un modem.

Cuando los trenes de bits han sido convertidos en señales apropiadas, éstas son enviadas por los medios físicos hasta el host destino, en donde se procede el proceso inverso, transformándose las señales en sus trenes de bits originales, pudiendo ser procesados entonces por los diferentes protocolos de capa, recuperándose el mensaje original.

LA TARJETA DE RED (NETWORK INTERFACE CARD - NIC)

Una **tarjeta de interfaz de red** o Network Interface Card (**NIC**) (también conocida como *adaptadora* o *tarjeta adaptadora*) es una placa de circuito instalada en un componente de equipo de informática, como un PC, por ejemplo, que *le permite conectar el ordenador a una red mediante una línea digital.*

A diferencia del modem, *la tarjeta de red no modula ni demodula la señal, puesto que no es necesaria la conversión analógica a digital, ya que los datos en el ordenador son digitales y la línea por donde van a ser transmitidos también*. Pero sí se encarga de preparar los datos para poder ser transmitidos y recibidos por el canal (alámbrico o inalámbrico) hacia y desde la red.

Los parámetros o consideraciones que ha que tener en cuenta a la hora de elegir una tarjeta de red son los siguientes:

La velocidad de transmisión y funcionamiento de la red a la que se va a conectar Ethernet (10Mbps), Fast Ethernet (100Mbps) o Giga Ethernet.

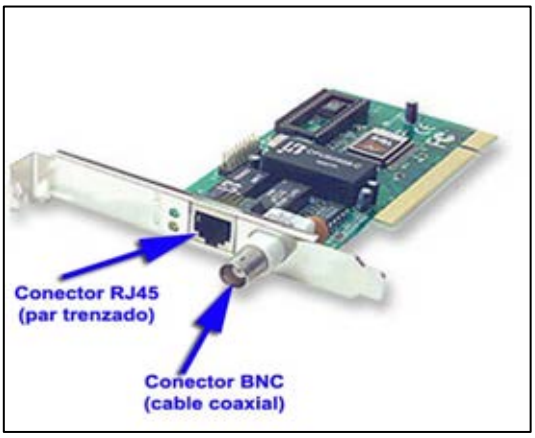
Con respecto a la velocidad de transmisión debe utilizarse un HUB o Switch que soporte la velocidad de transmisión de la tarjeta de red. Existen en el mercado dispositivos de interconexión **multi speed** que admiten varios valores: 10, 100 y 1000 Mbps y permiten utilizar una tarjeta de red de cualquier velocidad de transmisión, puesto que ajustan su velocidad automáticamente para que coincida con la velocidad más alta admitida por ambos extremos de la conexión.

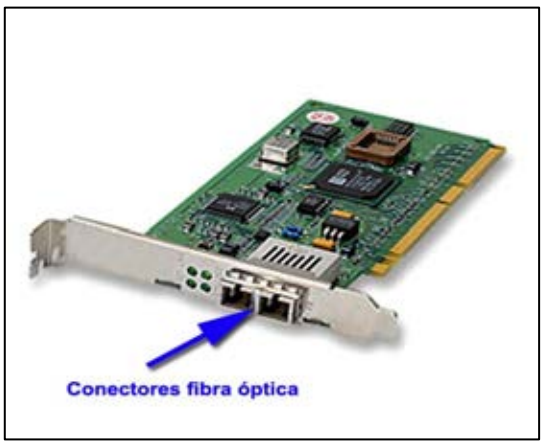
De un modo semejante, si se dispone de una NIC 10/100, podrá conectarse al concetrador Ethernet de 10Mbps o al concentrador Fast Ethernet de 100Mbps. La NIC 10/100 ajustará su velocidad para que coincida con la velocidad más alta soportada por ambos extremos de la conexión.

El modo de transmisión: Half duplex o Full duplex.

La tarjeta de red debe de soportar el modo de transmisión que se utilice en la red a la que está conectada. Actualmente la totalidad de las tarjetas soportan los modos half y full duplex; y además, mediante la opción "*Auto"*, se ajustan automáticamente al modo de transmisión de la red.

El tipo de conexión que se necesita: RJ-45 para par trenzado, BNC para cable coaxial o conectores de fibra óptica.



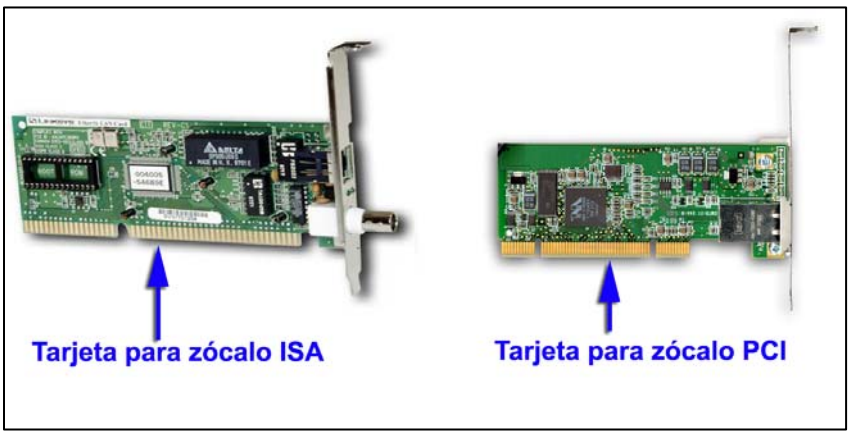


El tipo de ranura interna del ordenador: (ISA o PCI).

Hay dos tipos comunes de conectores de NIC para PC:

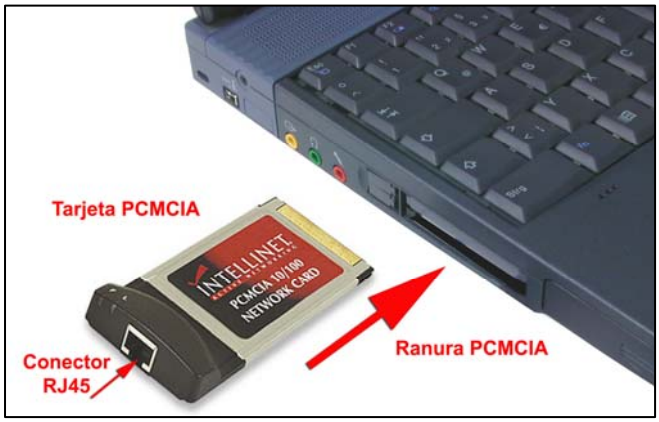
Los zócalos ISA (Arquitectura de normas industriales) miden unos 14cm de largo.

Los zócalos PCI (Interconexión de componente periférico) se utilizan en todos los PC Pentium de sobremesa. Los zócalos PCI tienen un mayor rendimiento que los ISA. Los zócalos PCI miden unos 9cm de longitud.



Es necesario conocer el tipo zócalo interno que tiene el ordenador al que se le va a instalar la tarjeta de red.

En algunos casos, es necesario utilizar tarjetas especiales: es el caso de los ordenadores portátiles que utilizan tarjetas PCMCIA.



MAC

Las tarjetas de red tipo **Ethernet** tienen una pequeña memoria en la que alojan un dato único para cada tarjeta de este tipo. Se trata de la **dirección MAC**, y está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis parejas (cada pareja se separa de otra mediante dos puntos ":" o mediante guiones "-"). Por ejemplo, una dirección MAC podría ser **F0:E1:D2:C3:B4:A5**.

MAC son las siglas de **Media Access Control** y se refiere al control de acceso al medio físico. O sea que la dirección MAC es una **dirección física** (también llamada **dirección hardware**), porque identifica físicamente a un elemento del hardware: cada tarjeta Ethernet viene de fábrica con un número MAC distinto. Windows la menciona como **Dirección del adaptador**. Esto es lo que finalmente permite las transmisiones de datos entre ordenadores de la red, puesto que cada ordenador es reconocido mediante esa dirección MAC, de forma inequívoca.

La mitad de los bits de la dirección MAC son usados para identificar al fabricante de la tarjeta, y los otros 24 bits son utilizados para diferenciar cada una de las tarjetas producidas por ese fabricante.

Casi todas las redes de hoy día (y concretamente Internet) utilizan el **protocolo IP**, que usa otro sistema de direcciones no relacionadas con el hardware. Las direcciones IP responden a un sistema de convencionalismos más abstractos. Cuando un software quiere enviar datos a otro ordenador, normalmente sabe la dirección IP del ordenador destinatario, pero no sabe realmente cómo hacerle llegar los datos (físicamente). Hay otro protocolo llamado **ARP** (**Protocolo de Resolución de Direcciones**) que es el encargado de averiguar la dirección MAC correspondiente a una dirección IP, y así se pueden enviar físicamente los datos desde un ordenador a otro.

No hay relación alguna entre la dirección IP y la dirección MAC, pero el protocolo ARP y la red cuentan con mecanismos para averiguar en cualquier momento cuál es esa correspondencia.

¿Que pasa si no tenemos tarjeta de red y conectamos por módem? Pues en ese caso no se usa la dirección MAC ni tampoco funciona el protocolo ARP. La conexión por módem funciona mediante otro protocolo llamado **PPP** (**Point to Point Protocol, protocolo de punto a punto**), que actúa como enlace directo entre los dos ordenadores conectados por medio de la línea telefónica. A todos los efectos (visto desde el resto de Internet), nuestro ordenador tiene la misma dirección MAC que el servidor con el que enlazamos mediante módem. Pero hay que tener en cuenta que si tenemos instalada una tarjeta de red, la dirección MAC de esa tarjeta puede resultar visible desde Internet, incluso aunque conectemos por módem y sin usar la tarjeta de red.

12.- PROTOCOLOS DE ACCESO AL MEDIO

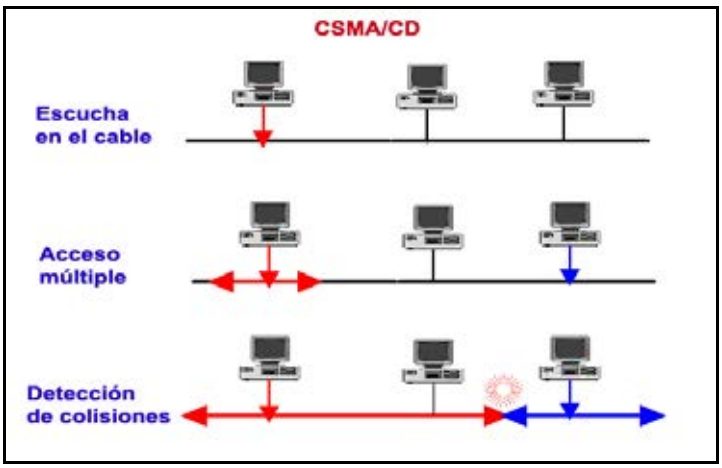
CSMA/CD (IEEE 802.3)

Siglas que corresponden a **Carrier Sense Multiple Access with Collision Detection** (en castellano: "Acceso Múltiple con Escucha de Portadora y Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por ello apareció primeramente la técnica CSMA que fue posteriormente depurada a la técnica CSMA/CD, es decir se implementó la detección de posibles colisiones.

Acceso múltiple con escucha de portadora significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir **previamente escucha** el canal antes de emitir. Si el canal está ocupado espera un tiempo aleatorio y vuelve a escuchar. Cuando detecta libre el canal puede actuar de dos formas distintas: emitiendo de inmediato o esperando un tiempo aleatorio antes de emitir.

Si emite con una probabilidad "p", se dice que es un sistema CSMA p-persistente, mientras que si emite de inmediato se dice que es un sistema CSMA 1-persistente.

Una vez comenzado a emitir, no para hasta terminar de emitir la trama completa. Esto supone que se puede producir una colisión si dos estaciones intentan transmitir a la vez, de forma que las tramas emitidas por ambas serán incompresibles para las otras estaciones y la transmisión habrá sido infructuosa.



Finalmente CSMA/CD supone una mejora sobre CSMA, pues la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión para inmediatamente la transmisión.
La ganancia producida es el tiempo que no se continúa utilizando el medio para realizar una transmisión que resultará inútil, y que se podrá utilizar por otra estación para transmitir.

Funcionamiento de CSMA/CD

El primer paso a la hora de transmitir será, obviamente, saber si el medio está libre. Y ¿cómo podemos saberlo? Pues nos quedamos callados y escuchamos lo que dicen los demás. Si hay portadora en el medio, es que está ocupado y, por tanto, seguimos escuchando; en caso contrario, el medio está libre y podemos transmitir.

A continuación, esperamos un tiempo mínimo necesario para poder diferenciar bien una trama de otra y comenzamos a transmitir. Si durante la transmisión de una trama se detecta una colisión, entonces las estaciones que colisionan abortan el envío de la trama y envían una señal de reinicio. Después de una colisión, las estaciones esperan un tiempo aleatorio (Tiempo de Backoff) para volver a transmitir una trama.

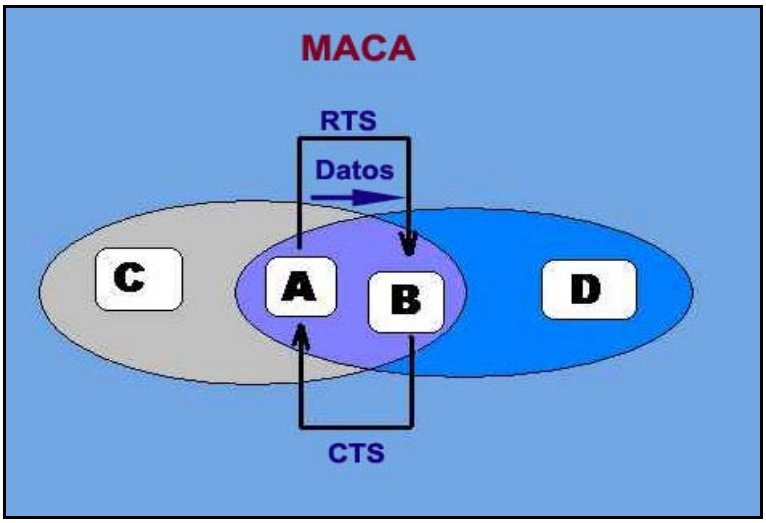
MACA (IEEE 802.11)

En redes inalámbricas, resulta a veces complicado llevar a cabo el primer paso (escuchar al medio para determinar si está libre o no). Por este motivo, surgen dos problemas que pueden ser detectados:

Problema del nodo oculto: La estación cree que el medio está libre cuando en realidad no lo está, pues está siendo utilizado por otro nodo al que la estación no “oye”.

Problema del nodo expuesto: La estación cree que el medio está ocupado, cuando en realidad lo está ocupando otro nodo que no interferiría en su transmisión a otro destino.

Para resolver estos problemas, la **IEEE 802.11** (protocolo para redes inalámbricas) propone **MACA** (MultiAccess Collision Avoidance – Evasión de Colisión por Acceso Múltiple).



La modificación incluida en este protocolo, respecto a CSMA/CD, es que ahora las estaciones, antes de transmitir, deben enviar una trama **RTS** (Request To Send – Solicitud para enviar).

Dicha trama, indica la longitud del paquete de datos a enviar. Ante esto, el resto de estaciones actuarán de tal forma que, si "escuchan" un RTS, esperarán por el **CTS** (Clear to send – Libre para enviar) y, si "escuchan" un CTS, esperarán el tiempo necesario para que se transmita la longitud indicada en dicho CTS.

TOKEN BUS (IEEE 802.4)

Token Bus es un protocolo para redes de área local con similitudes a Token Ring, pero en vez de estar destinado a topologías en anillo está diseñado para topologías en bus.

Es un protocolo de acceso al medio en el cual los nodos están conectados a un bus o canal para comunicarse con el resto. En todo momento hay un testigo (*token*) que los nodos de la red se van pasando, y únicamente el nodo que tiene el testigo tiene permiso para transmitir. El bus principal consiste en un cable coaxial.

Token bus está definido en el estándar IEEE 802.4. Se publicó en 1980 por el comité 802 dentro del cual crearon 3 subcomites para 3 propuestas que impulsaban distintas empresas. El protocolo ARCNET es similar, pero no sigue este estándar.

Token Bus se utiliza principalmente en aplicaciones industriales. Fue muy apoyado por GM. Actualmente en desuso por la popularización de Ethernet.

Características

- Tiene una topología en bus (configuración en bus física), pero una topología lógica en anillo. Las estaciones están conectadas a un bus común pero funcionan como si estuvieran conectadas en anillo.

- Todas las estaciones o nodos conocen la identidad de los nodos siguiente y anterior. El último nodo conoce la dirección del primero y de su anterior, así como el primer nodo conoce la dirección del último y de su sucesor.

- La estación que tiene el testigo o *token* tiene el control sobre el medio y puede transmitir información a otro nodo.

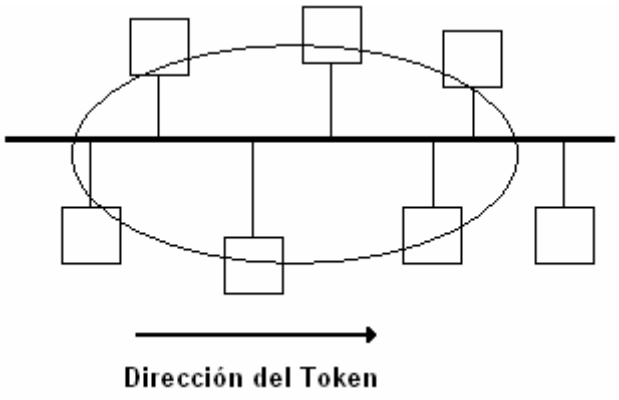
- Cada estación tiene un receptor y un transmisor que hace las funciones de repetidor de la señal para la siguiente estación del anillo lógico.

- No existen colisiones.

- Todas las estaciones tienen igual probabilidad de envío.

- Es un protocolo eficaz en la producción en serie.

Funcionamiento



- El testigo pasa de un nodo al siguiente siguiendo el orden del anillo lógico. Los nodos fuera del anillo no reciben testigo.

- Siempre hay un testigo (*token*) el cual las estaciones de la red se van pasando en el orden en el que están conectadas. Solamente un único nodo puede transmitir en un momento dado y éste nodo es el que tiene el testigo.

- El testigo es usado durante un tiempo para transmitir, pasando después el testigo a su *vecino lógico* para mantener el anillo.

- Si el nodo no tuviera que enviar ningún dato, el testigo es inmediatamente pasado a su nodo sucesor.

- La idea de anillo lógico se usa para que cualquier ruptura del anillo desactive la red completa.

- Es necesario que un protocolo notifique las desconexiones o adhesiones de nodos al anillo lógico.

Medio Físico

- Los nodos están conectados a un cable coaxial de 75Ω como el usado en TV.

- Se emplean 3 tipos de modulaciones analógicas:

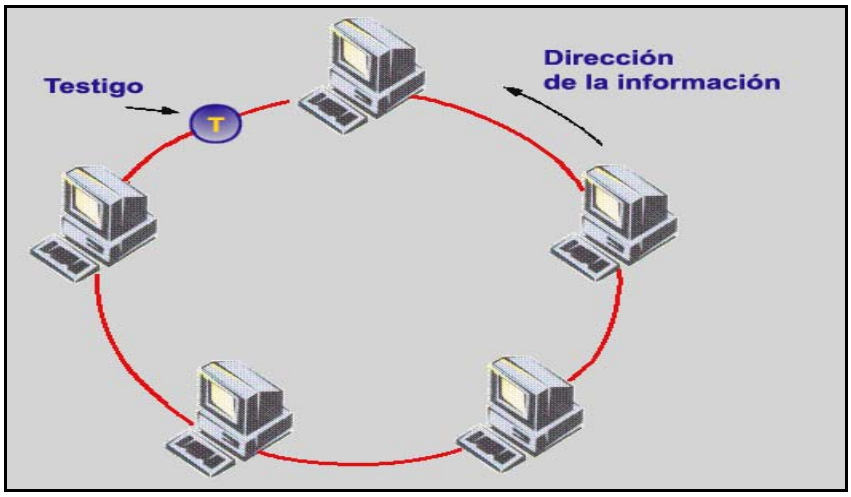
  1. Modulación por desplazamiento de frecuencia continua (FSK).
  2. Modulación por desplazamiento de frecuencia coherente (FSK).
  3. Modulación por desplazamiento de fase de amplitud modulada (PSK).

- La velocidad de transmisión son de 1,5 y 10 Mbps.

PASO POR TESTIGO (Token Ring IEEE 802.5)

Esta técnica es propia de las redes en anillo. Con la red en anillo con paso de testigo, cuando una estación quiere enviar un mensaje a un dispositivo de la red, debe esperar por un testigo que viaja de estación en estación. Si está disponible, la estación toma control del testigo y envía su paquete de información.

Con esta tecnología se asegura que las estaciones no tengan que competir por el acceso a la red. Pero también abre las puertas a los fallos. Si la red en anillo con paso de testigo no está cableada con un conjunto de cables redundante, cualquier rotura en el anillo principal detendrá de forma inmediata todas las comunicaciones entre estaciones de trabajo.



El paso por testigo es una trama de control y por tanto puede presentar los siguientes problemas:

- *Que se pierda el testigo*. Se espera un tiempo determinado, si no viene significa que se perdió el testigo y en tal caso se genera un nuevo testigo.

- *Que se genere más de un testigo*, si es así se eliminan estos. Y hay otra estación que genera otro testigo. A la hora de generar los testigos normalmente se suele usar una estación que genere dichos testigos.

- *Que las estaciones estén numeradas y tenga que saber cual es la estación siguiente y la anterior* (porque hay que saber quien tiene el testigo). Puede surgir un problema y es que se conecte otro ordenador a la red

El paso por testigo presenta las siguientes ventajas.

- Rápida, no hay colisiones.

- Seguridad: garantiza que llega el paquete de información.

- Todas las estaciones tienen la misma posibilidad de enviar información.

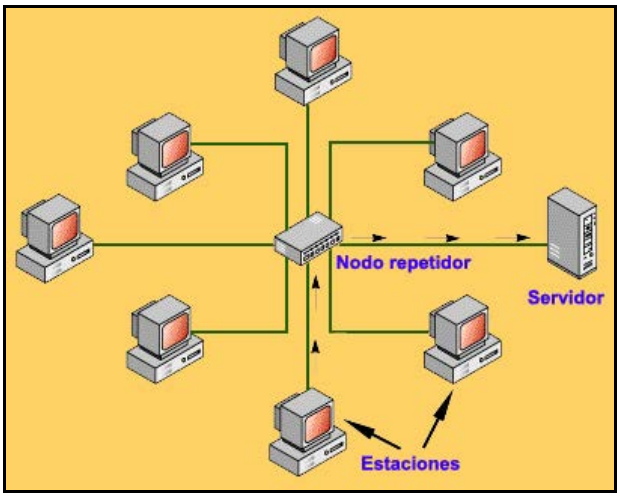
PRIORIDAD DE DEMANDAS (IEEE 802.12)

La prioridad de demandas, Demand Priority Protocol **(DPP)**, es un método de acceso relativamente nuevo y está diseñado para el estándar Ethernet 100 Mbps conocido como **100VG-AnyLAN**.

Consiste en un hub o repetidor central de nivel 1 o raíz con un enlace a cada nodo, creándose así una topología en estrella. Los hubs realizan continuas búsquedas de los nodos que quieren enviar datos. Si dos dispositivos coinciden en querer enviar al mismo tiempo, la petición de más alta prioridad será la atendida en primer lugar, a menos que las prioridades sean iguales en cuyo caso las peticiones son atendidas a la vez (alternando tramas).

El hub sólo sabe de dispositivos conectados y de otros repetidores así que la comunicación está únicamente dirigida a ellos antes que hacer broadcast a todos los dispositivos de un dominio (que podrían ser cientos de ellos). Los paquetes de datos son direccionados solo a su puerto destino deseado.

Este método de acceso está basado en el hecho de que los nodos repetidores y finales son los dos componentes que forman todas las redes 100VG-AnyLAN. Los repetidores gestionan el acceso a la red haciendo búsquedas round-robin de peticiones de envío de todos los nodos de red. El repetidor o hub es el responsable de conocer todas las direcciones, enlaces y nodos finales, y de comprobar que todos están funcionando. De acuerdo con la definición de 100VG-AnyLAN, un nodo final puede ser un equipo, un bridge, un router o un switch.



Retención de datos en prioridad de demandas

Al igual que en CSMA/CD, dos equipos que utilicen el método de acceso con prioridad de demandas pueden causar una retención si transmiten exactamente en el mismo instante. Sin embargo, con prioridad de demandas, es posible implementar un esquema en que ciertos tipos de datos tengan prioridad si existe contención. Si el hub o repetidor recibe dos peticiones al mismo tiempo, primero se servirá la petición que tenga mayor prioridad. Si las dos peticiones tienen la misma prioridad, ambas peticiones se servirán alternando entre las dos.

En una red con prioridad de demandas, los equipos pueden recibir y transmitir al mismo tiempo (Full duplex) debido al esquema de cableado definido por este método de acceso. En este método se utilizan cuatro pares de hilos, que permiten dividir por cuatro las transmisiones, transmitiendo cada uno de los hilos del cable señales a 25 MHz.

Consideraciones sobre la prioridad de demandas

En una red con prioridad de demandas, sólo hay comunicación entre el equipo que envía, el hub y el equipo que recibe. Esto es más eficiente que CSMA/CD, que transmite avisos a toda la red. En prioridad de demandas, cada hub conoce los nodos finales y los repetidores que están conectados a él directamente, mientras que en el entorno CSMA/CD, cada hub conoce la dirección de cada nodo de la red.

La prioridad de demandas tiene varias ventajas respecto a CSMA/CD, entre las que se incluyen:

- El uso de cuatro pares de hilos. Al utilizar cuatro pares de hilos, los equipos pueden enviar y recibir al mismo tiempo.

- Las transmisiones se realizan a través del dispositivo de interconexión.

- Las transmisiones no se envían a todos los equipos de la red.
- Los equipos no compiten por acceder al cable, pero trabajan bajo el control centralizado del hub.

Hoy en día es la técnica más utilizada en las redes de área local en la Armada con la conocida topología física en estrella o en árbol.

OTROS PROTOCOLOS DE LA CAPA DE ENLACE

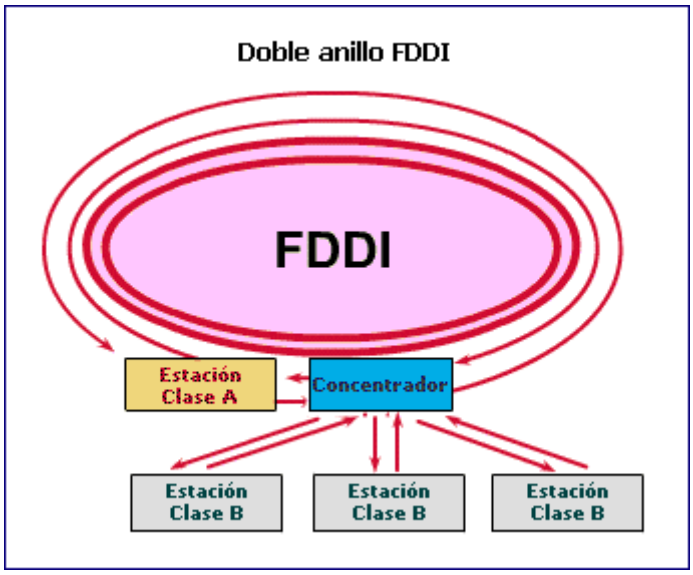
FDDI (Fiber Distributed Data Interface) es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante **cable de fibra óptica**. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex. Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

Sus características son:

- Esquema MAC de paso de testigo basado en IEEE 802.5
- Compatibilidad con LAN´s basadas en IEEE 802
- Fibra óptica o trenzado
- Doble anillo con tolerancia a fallos
- Velocidad de 100 Mbps
- Hasta 500 dispositivos
- Hasta 100 Km. por anillo de fibra
- Asignación dinámica de ancho de banda (servicios síncronos y asíncronos)

Se utiliza mucho como red dorsal de varias LAN´s y como anillo de alta velocidad para interconexión de servidores de alto tráfico.

Una red FDDI utiliza dos arquitecturas token ring, una de ellas como apoyo en caso de que la principal falle. En cada anillo, el tráfico de datos se produce en dirección opuesta a la del otro. Empleando uno solo de esos anillos la velocidad es de 100 Mbps y el alcance de 200 km, con los dos la velocidad sube a 200 Mbps pero el alcance baja a 100 km. La forma de operar de FDDI es muy similar a la de token ring, sin embargo, el mayor tamaño de sus anillos conduce a que su latencia sea superior y más de una trama puede estar circulando por un mismo anillo a la vez.



También existe una implementación de FDDI en cables de hilo de cobre conocida como CDDI. La tecnología de Ethernet a 100 Mbps (100BASE-FX y 100BASE-TX) está basada en FDDI.

HDLC (High-Level Data Link Control, Control de Enlace Síncrono de Datos) es un protocolo de comunicaciones de propósito general punto a punto, que opera a nivel de enlace de datos. Se basa en ISO 3309 e ISO 4335. Surge como una evolución del anterior SDLC. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable entre el transmisor y el receptor.
De este protocolo derivan otros como LAPB, LAPF y PPP.

ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrona) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

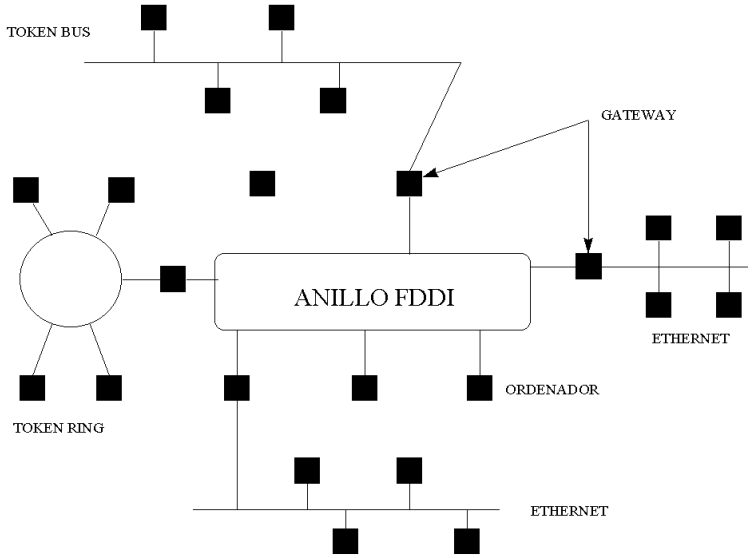
Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente mediante el uso de los denominados *canales virtuales* y *trayectos virtuales*.

PPP (Point to Point Protocol - Protocolo Punto a Punto) es un protocolo de nivel de enlace para hacer conexión entre dos puntos (dos computadoras o nodos). El PPP fue desarrollado por el grupo de trabajo IETF (Internet Engineering Task Force).

Permite conectar computadoras utilizando cable serial, línea telefónica, teléfono celular, enlace de fibra óptica, etc. *Generalmente es empleado para establecer la conexión a internet desde un usuario al proveedor de internet a través de un módem telefónico.* A veces es usado para conexiones de banda ancha tipo DSL.

El protocolo PPP permite transporte de datos, autentificación a través de una clave de acceso y asignación dinámica de IP.

PPP fue diseñado para trabajar con múltiples protocolos de capas de red, como IP, IPX, NetBEUI y AppleTalk.



13.- ARQUITECTURA DE REDES

ETHERNET

Con el paso del tiempo, Ethernet se ha convertido en el medio de acceso más utilizado en la Armada y se utiliza en entornos de red pequeños y grandes. Ethernet es un estándar que no pertenece a ninguna industria, y que ha tenido una gran aceptación por los fabricantes de hardware de red. Casi no existen problemas relacionados con la utilización de productos hardware para Ethernet de distintos fabricantes.

Orígenes de Ethernet

A finales de los sesenta la Universidad de Hawai desarrolló una WAN denominada ALOHA. La universidad ocupaba un área extensa y buscaba cómo conectar los equipos que estaban dispersos por el campus. Una de las características fundamentales de la red de la universidad era que utilizaba CSMA/CD como método de acceso.

Esta red fue la base para la arquitectura de red Ethernet actual. En 1972, Robert Metcalfe y David Boggs inventaron un esquema de cableado y comunicación en el Centro de Investigación de Xerox en Palo Alto (PARC) y en 1975 introdujeron el primer producto Ethernet. La versión original de Ethernet estaba diseñada como un sistema de 2.94 megabits por segundo (Mbps) para conectar unos 100 equipos sobre un cable de 1 km.

La Ethernet de Xerox tuvo tanto éxito que Xerox, Intel Corporation y Digital Equipment Corporation diseñaron un estándar para Ethernet a 10 Mbps.

Características de Ethernet

Actualmente, Ethernet es la arquitectura de red más popular. Esta arquitectura de banda base utiliza una topología en bus o en estrella, normalmente transmite a **10, 100 o 1000 Mbps** y utiliza **CSMA/CD** para regular el segmento de cable principal.

El medio Ethernet es pasivo, lo que significa que no requiere una fuente de alimentación, por lo que no fallará a no ser que el medio esté cortado físicamente o no esté terminado correctamente.

Aspectos básicos de Ethernet:

- Topologías: Bus lineal o bus en estrella
- Método de acceso: CSMA/CD.
- Especificación: IEEE 802.3.
- Velocidad de transferencia: 10, 100 ó 1000 Mbps.
- Tipo de cable: Grueso, fino, UTP, STP y F.O.

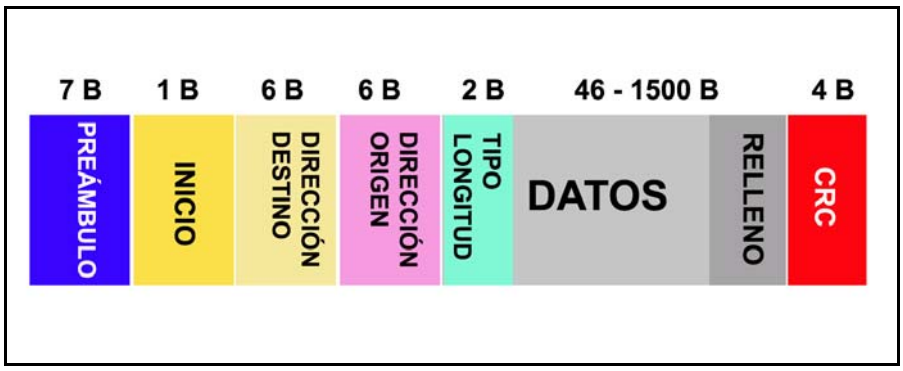
Formato de trama Ethernet

Ethernet divide los datos en paquetes en un formato que es diferente al de los paquetes de otras redes: Ethernet divide los datos en **tramas**.

Se pueden utilizar los términos de «paquete» y «trama» de forma indistinta.

Una **trama** es un paquete de información transmitido como una unidad. Una trama Ethernet puede tener entre 64 y 1.518 bytes, pero la propia trama Ethernet necesita utilizar al menos 18 bytes; así pues, el tamaño de los datos de una trama Ethernet está entre 46 y 1.500 bytes. Cada trama contiene información de control y tiene la misma estructura básica.

Por ejemplo, la trama Ethernet II, utilizada por TCP/IP, que se transmite a través de la red, consta de las secciones que aparecen en la siguiente figura:



- ***Preámbulo:*** Indica el principio de la trama. Es de 7 Bytes.
- ***Inicio:*** Delimitador de trama que se utiliza para sincronizar las tramas en recepción. 1 Byte.

- ***Destino y origen:*** Las direcciones de origen y destino. 2 ó 6 Bytes cada una.

- ***Tipo y longitud:*** Se utiliza para identificar el protocolo del nivel de red, normalmente, IP o IPX (Intercambio de paquetes entre redes de Novell). E indica la cantidad de Bytes que tiene el campo datos.

- ***Datos:*** Campo donde van los datos propiamente dichos, la información que circula por la red.

- ***Relleno:*** La trama Ethernet debe tener un mínimo de 64 Bytes según la norma IEEE 802.3. Si el campo datos es muy pequeño, se debe rellenar hasta 64 Bytes.

- ***Comprobación de redundancia cíclica (CRC):*** Campo de comprobación de errores para determinar si la trama ha llegado sin errores. 4 Bytes.

Tecnología y velocidad en Ethernet

Hace ya mucho tiempo que Ethernet consiguió situarse como el principal protocolo del nivel de enlace. Ethernet 10Base2 consiguió, ya en la década de los 90s, una gran aceptación en el sector. Hoy por hoy, 10Base2 se considera como una "tecnología de legado" respecto a 100BaseT. Hoy los fabricantes ya desarrollaron adaptadores capaces de trabajar tanto con la tecnología 10baseT como la 100BaseT y esto ayuda a una mejor adaptación y transición.

Las tecnologías Ethernet que existen se diferencian en estos conceptos:

Velocidad de transmisión
- Velocidad a la que transmite la tecnología.

Tipo de cable
- Tecnología del nivel físico que usa la tecnología.

Longitud máxima
- Distancia máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).

Topología
- Determina la forma física de la red. Bus si se usan conectores T (hoy sólo usados con las tecnologías más antiguas) y estrella si se usan hubs (estrella de difusión) o switches (estrella conmutada).

A continuación se especifican los anteriores conceptos en las tecnologías más importantes:

Tecnologías Ethernet

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5e ó 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

Hardware usado

Los elementos de una red Ethernet son: tarjeta de red, repetidores, concentradores, puentes, los conmutadores, los nodos de red y el medio de interconexión. Los nodos de red pueden clasificarse en dos grandes grupos: **equipo terminal de datos (DTE)** y **equipo de comunicación de datos (DCE)**.

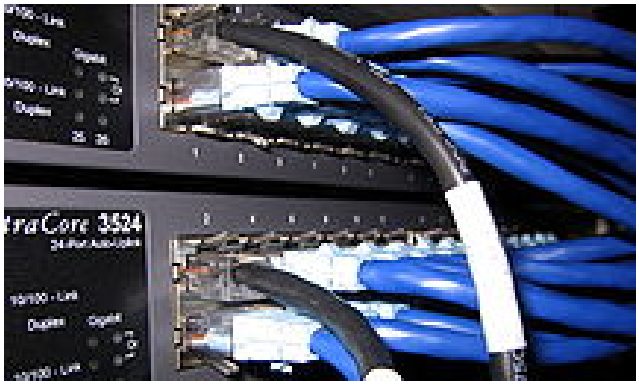
Los **DTE** son dispositivos de red que generan el destino de los datos: los PC, las estaciones de trabajo, los servidores de archivos, los servidores de impresión; todos son parte del grupo de las estaciones finales. Los **DCE** son los dispositivos de red intermediarios que reciben y retransmiten las tramas dentro de la red; pueden ser: ruteadores, conmutadores (switch), concentradores (hub), repetidores o interfaces de comunicación.

- **NIC, o Tarjeta de Interfaz de Red** - permite que una computadora acceda a una red local. Cada tarjeta tiene una *única* dirección MAC que la identifica en la red. Una computadora conectada a una red se denomina **nodo**.

- **Repetidor o *repeater*** - aumenta el alcance de una conexión física, recibiendo las señales y retransmitiéndolas, para evitar su degradación, a través del medio de transmisión, lográndose un alcance mayor. Usualmente se usa para unir dos áreas locales *de igual* tecnología y sólo tiene *dos* puertos. Opera en la capa física del modelo OSI.

- **Concentrador o *hub*** - funciona como un repetidor pero permite la interconexión de *múltiples* nodos. Su funcionamiento es relativamente simple pues recibe una trama de ethernet, por uno de sus puertos, y la repite por todos sus puertos restantes sin ejecutar ningún proceso sobre las mismas. Opera en la capa física del modelo OSI.

- **Puente o *bridge*** - interconecta segmentos de red haciendo el cambio de *frames* (tramas) entre las redes de acuerdo con una tabla de direcciones que le dice en qué segmento está ubicada una dirección MAC dada.



Conexiones en un switch Ethernet

- **Conmutador o *Switch*** - permite la interconexión de múltiples segmentos de red, funciona en velocidades rápidas y es más sofisticado. Los *switches* pueden tener otras funcionalidades, como *Redes virtuales* , y permiten su configuración a través de la propia red. Funciona básicamente en la capa 2 del modelo OSI (enlace de datos).

Son capaces de procesar información de las tramas; su funcionalidad más importante es en las tablas de dirección. Por ejemplo, una computadora conectada al puerto 1 del conmutador envía una trama a otra computadora conectada al puerto 2; el *switch* recibe la trama y la transmite a todos sus puertos, excepto aquel por donde la recibió; la computadora 2 recibirá el mensaje y eventualmente lo responderá, generando tráfico en el sentido contrario; ahora el *switch* conocerá las direcciones **MAC** de las computadoras en el puerto 1 y 2; cuando reciba otra trama con dirección de destino de alguna de ellas, sólo transmitirá la trama a dicho puerto disminuyendo así el tráfico de la red y contribuyendo al buen funcionamiento de la misma.

TOKEN RING

La arquitectura Token Ring fue desarrollada a mediados de los ochenta por IBM. Este método está basado en el **paso por testigo** y es el que se suele encontrar en instalaciones de minis y mainframes de IBM. Aunque la popularidad en el mercado ha descendido en favor de Ethernet, sigue jugando un papel importante en el mercado de las redes.

En 1985, la Token Ring de IBM se convirtió en un estándar del Instituto de estandarización nacional americano IEEE, estableciendo la especificación IEEE 802.5.

Características

La arquitectura de una red Token Ring típica comienza con un anillo físico. Sin embargo, en su implementación de IBM, es un anillo cableado en estrella, es decir: los equipos de la red se conectan a un hub central. El anillo lógico representa el sentido de circulación para los testigos entre equipos. El anillo de cable físico actual está en el hub. Los usuarios son parte de un anillo, pero se conectan a él a través de un hub.

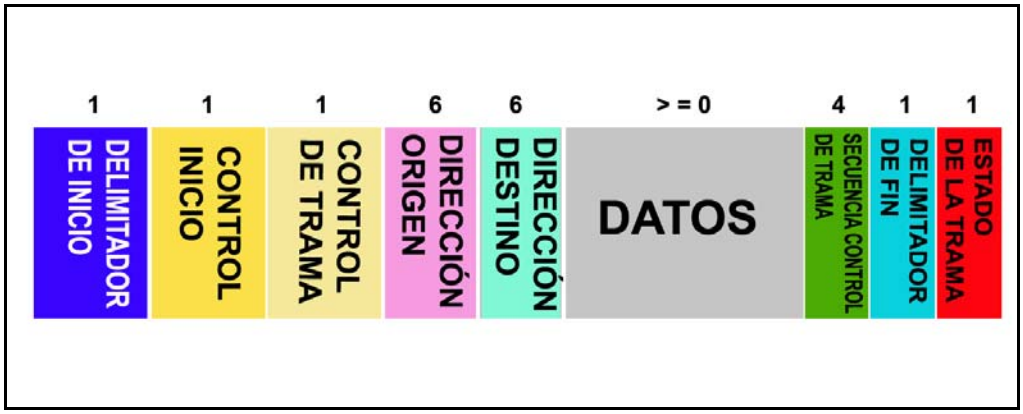
Especificaciones básicas

- Topología del cableado en anillo o en estrella.
- Método de acceso de paso de testigo.
- Cableado coaxial y de par trenzado apantallado y sin apantallar.
- Velocidades de transferencia entre 4 y 16 Mbps.
- Transmisión banda base.

- Estándar IEEE 802.5.

Formatos de trama Token Ring

El formato básico de la trama de datos de Token Ring consta de cabecera, datos y final. El campo de datos suele formar la mayor parte de la trama.



Componentes de una trama de datos Token Ring

- **Delimitador de inicio:** Indica el inicio de la trama. 1 Byte.
- **Control de acceso:** Indica la prioridad de la trama y se trata de un testigo o de una trama de datos. 1 Byte.
- **Control de trama:** Contiene información sobre el Control de acceso al medio para todos los equipos o información de «estación final» para un solo equipo. 1 Byte.
- **Dirección de destino:** Indica la dirección del equipo que recibe la trama. 6 Bytes
- **Dirección de origen:** Indica el equipo que envió la trama. 6 Bytes.
- **Información o datos:** Contiene los datos enviados. Igual o mayor a 0 Bytes.
- **Secuencia de control de la trama:** Contiene información de comprobación de errores CRC. 4 Bytes.
- **Delimitador de fin:** Indica el final de la trama. 1 Byte.
- **Estado de la trama:** Indica si la trama fue reconocida, copiada, o si la dirección de destino estaba disponible. 1 Byte.

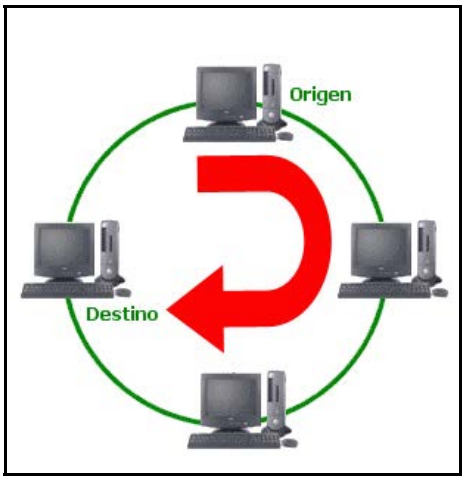
Funcionamiento de una red Token Ring

Cuando el primer equipo de Token Ring entra en línea, la red genera un testigo. El anillo es una formación de bits predeterminada (una serie de datos) que permite a un equipo colocar datos en los cables. El testigo viaja a través de la red preguntando a cada equipo, hasta que un equipo indica que quiere transmitir datos y se apodera del testigo, y, en ese instante, ningún equipo puede transmitir hasta que no tome el control del testigo.

Una vez que un equipo se apodera del token (testigo), envía una trama de datos a través de la red. La trama viaja por la red hasta que alcanza el equipo con una dirección que coincida con la dirección de destino de la trama. El equipo de destino copia la trama en su búfer de recepción y marca la trama en el campo de estado de la trama para indicar que se ha recibido la información.

La trama continúa por el anillo hasta que llegue al equipo que la envió, de forma que se valida la transmisión. A continuación, el equipo que envía retira la trama del anillo y transmite un testigo nuevo a éste.
En la red sólo puede haber un testigo activo y el testigo puede viajar sólo en una dirección del anillo.

¿Circula el testigo en el sentido de las agujas del reloj o en sentido contrario? El estándar IEEE 802.5 dice que es en el sentido de las agujas del reloj, y la sección 3 de la publicación SC30-3374 de IBM dice que es en el sentido contrario de las agujas del reloj. Depende entonces del estándar utilizado. En la Armada se sigue el IEEE 802.5 .



El paso de testigos es determinante, lo que significa que un equipo no puede imponer su turno en la red, tal y como ocurre en un entorno CSMA/CD. Si el testigo está disponible, el equipo puede utilizarlo para enviar datos. Cada equipo actúa como un repetidor unidireccional, regenera el testigo y lo continúa pasando.

Control del sistema

El primer equipo que se active queda designado por el sistema Token Ring para controlar la actividad de la red. El equipo encargado del control asegura que las tramas se están entregando y recibiendo correctamente. Esto se realiza comprobando las tramas que circulan por el anillo más de una vez y asegura que sólo hay un testigo en la red.

El proceso de monitorización se denomina de baliza (beaconing). El equipo encargado del control envía una baliza cada siete segundos. La baliza pasa de equipo en equipo por todo el anillo. Si un equipo no recibe la baliza de su vecino, notifica a la red su falta de conexión. Envía un mensaje que contiene su dirección y la dirección del vecino que no le ha enviado la baliza y el tipo de baliza. A partir de esta información, se intenta diagnosticar el problema y tratar de repararlo sin dividir la red. Si no se puede realizar la reconfiguración de forma automática es necesaria la intervención manual.

Reconocimiento de un equipo

Cuando un equipo de la red entra en línea, el sistema Token Ring lo inicializa de forma que pueda formar parte del anillo. Esta inicialización incluye:

- Comprobación de direcciones duplicadas.
- Notificación a otros equipos de la red de su existencia.

Componentes hardware

El hardware para redes Token Ring está basado en el hub, que es el que forma el anillo. Una red Token Ring puede tener varios hubs. El cableado que se utiliza para conectar los equipos a los hubs es STP o UTP; para extender las conexiones se pueden utilizar cables adaptadores. El cable de fibra óptica es especialmente apropiado para redes Token Ring.
Junto con los repetidores, el cable de fibra óptica puede extender enormemente el rango de las redes Token Ring. El cableado para componentes se realiza con cuatro tipos de conectores. Otro tipo de hardware para Token Ring incluye a los filtros, paneles de conexiones y tarjetas de red.

El HUB

En una red Token Ring, el hub es conocido con varios nombres y todos con el mismo significado. Entre estos están:

- MAU (Unidad de acceso multiestación).
- MSAU (Unidad de acceso multiestación).
- SMAU (Unidad de acceso multiestación inteligente).

Los cables conectan los clientes y los servidores a la MSAU, que funciona como otros hubs pasivos. El anillo interno se convierte automáticamente en un anillo externo por cada conexión que se realice.

MAU Token ring de IBM

Tolerancia a fallos incorporada

En una red con paso de testigo pura, un equipo que falle detiene la continuación del testigo. De hecho, esto detiene la red. Los hub se diseñaron para detectar la ocurrencia de fallos de una NIC. Este procedimiento salta el equipo que falla de forma que el testigo pueda continuar.

En los hub de IBM, las conexiones o los equipos que no funcionen correctamente se saltan automáticamente y se desconectan del anillo. Así pues, un fallo en un equipo o en una conexión no afectará al resto de la red Token Ring.

Cableado

Aunque todavía se pueden encontrar en la Armada tramos de red con cable coaxial, la mayor parte de las redes token ring se estructuran con cable de par trenzado.

El cable STP o UTP conecta los equipos con los hubs en una red Token Ring. El cableado para Token Ring es IBM del Tipo 1, 2 y 3. La mayoría de las redes utilizan cableado UTP de Tipo 3 del sistema de cableado IBM.

El cable conexión entre el equipo y el hub no puede tener más de 101 metros, si es del Tipo 1. Cuando se utiliza cable STP, el equipo puede llegar a estar a una distancia máxima de 100 metros del hub. En cambio esta distancia es de 45 metros (unos 148 pies) cuando se utilice cable UTP. La longitud mínima para cable con o sin apantallar es de 2,5 metros (unos 8 pies).

De acuerdo con IBM, la longitud máxima del cable de Tipo 3 desde una HUB hasta un equipo o un servidor de archivos es de 46 metros. Sin embargo, algunos fabricantes afirman que la transmisión de datos entre HUB y equipo es fiable hasta 152 metros.

La longitud máxima entre una HUB y otra está limitada a 152 metros (500 pies). Cada red Token Ring sólo puede acomodar a 260 equipos con cable STP y 72 equipos con UTP.

Conectores

Las redes Token Ring suelen utilizar estos tipos de conectores para conectar los cables a los componentes:

- Conectores de teléfono RJ-45 (8 pines) para cable de cuatro pares.
- Conectores de teléfono RJ-11 (4 pines) para cable de dos pares.
- Filtros para realizar la conexión entre una NIC Token Ring y un conector de teléfono estándar RJ-11/RJ-45.

Filtros

Los filtros son necesarios en equipos que utilizan cable telefónico de par trenzado de Tipo 3, ya que reducen el ruido de la línea.

Paneles de distribución de conectores (PATCH PANEL)

Un panel de conexión (patch panel) se utiliza para organizar los cables que hay entre un HUB y un módulo de conexiones telefónicas. (Un módulo de conexiones es un tipo de hardware que proporciona conexiones terminales para conectar los extremos del cable de red.)

Tarjetas de red

Las tarjetas de red para Token Ring están disponibles en los modelos 4 Mbps y 16 Mbps. Las tarjetas de 16 Mbps permiten una trama de mayor longitud que realiza menos transmisiones para la misma cantidad de datos.

La implementación de tarjetas para Token Ring necesita una atención especial, ya que una red Token Ring sólo puede funcionar a dos velocidades: 4 Mbps o 16 Mpbs. Si la red es una red a 4 Mbps, puede utilizar las tarjetas de 16 Mbps ya que pueden trabajar en el modo de 4 Mbps. Sin embargo, una red a 16 Mbps no aceptará las tarjetas de 4 Mbps, ya que no pueden aumentar su velocidad.

Tarjeta Token ring

Aunque hay varios fabricantes que fabrican NIC y componentes para Token Ring, la mayoría son vendidas por IBM.

REDES FDDI

Las redes FDDI (Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra) surgieron a mediados de los años ochenta para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades. Pueden ser implementadas con cable STP o UTP con inferiores prestaciones.

Están implementadas mediante una topología física de estrella (lo más normal) y lógica de anillo doble de token, uno transmitiendo en el sentido de las agujas del reloj (anillo principal) y el otro en dirección contraria (anillo de respaldo o back up), que ofrece una velocidad de 100 Mbps sobre distancias de hasta 2000 metros, soportando hasta 1000 estaciones conectadas (500 x anillo). Su uso más normal es como una tecnología de backbone para conectar entre sí redes LAN de cobre o computadores de alta velocidad.

El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Los dos anillos de la FDDI se conocen con el nombre de primario y secundario. El anillo primario se usa para la *transmisión de datos*, mientras que el anillo secundario se usa generalmente como *respaldo.*

Las redes FDDI utilizan un mecanismo de transmisión de tokens (testigos) similar al de las redes Token Ring, pero además, acepta la asignación en tiempo real del ancho de banda de la red, mediante la definición de dos tipos de tráfico:

- ***Tráfico Síncrono***: Puede consumir una porción del ancho de banda total de 100 Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.

- ***Tráfico Asíncrono***: Se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono.

El ancho de banda síncrono se asigna a las estaciones que requieren una capacidad de transmisión continua. Esto resulta útil para transmitir información de voz y vídeo. El ancho de banda restante se utiliza para las transmisiones asíncronas.

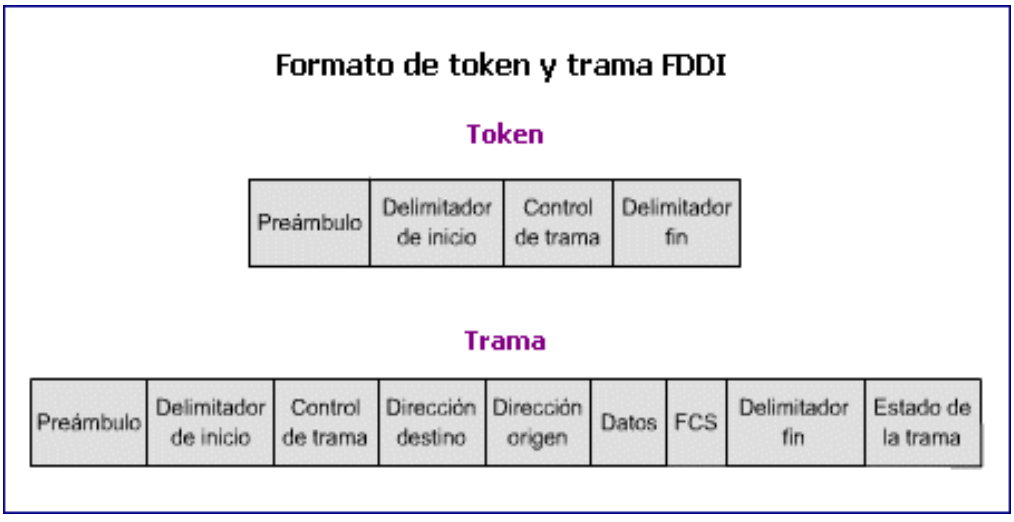
FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono.

El mecanismo de prioridad de la FDDI puede bloquear las estaciones que no pueden usar el ancho de banda síncrono y que tienen una prioridad asíncrona demasiado baja.

Las fuentes de señales de los transceptores de la FDDI son **LED**s (diodos electroluminiscentes) o **lásers**. Los primeros se suelen usar para tendidos entre máquinas, mientras que los segundos se usan para tendidos primarios de backbone.

Tramas FDDI

Las tramas en la tecnología FDDI poseen una estructura particular. Cada trama se compone de los siguientes campos:



- **Preámbulo**, que prepara cada estación para recibir la trama entrante.

- **Delimitador de inicio**, que indica el comienzo de una trama, y está formado por patrones de señalización que lo distinguen del resto de la trama.

- **Control de trama**, que contiene el tamaño de los campos de dirección, si la trama contiene datos asíncronos o síncronos y otra información de control.

- **Dirección destino**, que contiene la dirección física (6 bytes) de la máquina destino, pudiendo ser una dirección unicast (singular), multicast (grupal) o broadcast (cada estación).
- **Dirección origen**, que contiene la dirección física (6 bytes) de la máquina que envió la trama.

- **Secuencia de verificación de trama (FCS)**, campo que completa la estación origen con una verificación por redundancia cíclica calculada (CRC), cuyo valor depende del contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado durante el tránsito. La trama se descarta si está dañada.

- **Delimitador de fin**, que contiene símbolos que indican el fin de la trama.

- **Estado de la trama**, que permite que la estación origen determine si se ha producido un error y si la estación receptora reconoció y copió la trama.

Medios de transmisión en las redes FDDI

Una de las características de FDDI es el uso de la fibra óptica como medio de transmisión. La fibra óptica ofrece varias ventajas con respecto al cableado de cobre tradicional, por ejemplo:

- **Seguridad:** la fibra no emite señales eléctricas que se pueden interceptar.

- **Fiabilidad:** la fibra es inmune a la interferencia eléctrica.

- **Velocidad:** la fibra óptica tiene un potencial de rendimiento mucho mayor que el del cable de cobre.

14.- DISPOSITIVOS DE INTERCONEXIÓN DE REDES NIVEL DE ENLACE (capa 2 OSI)

Los dispositivos de interconexión son aquellos elementos de una red LAN que permiten conectar los diferentes puestos (ordenadores, impresoras etc.) entre si. Además también son aquellos que permiten conectar diferentes redes, como por ejemplo, una red LAN interna con Internet.

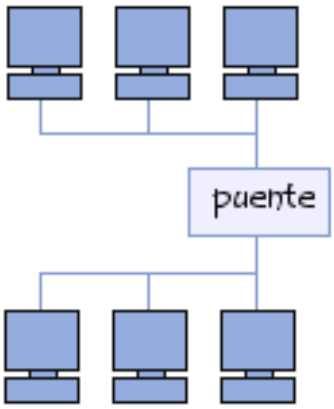
Como dispositivos englobados en el **nivel de enlace** (**capa 2** del modelo OSI) veremos **PUENTES (Bridges)** e **INTERRUPTORES (Switches)**.

PUENTES O BRIDGES

Un **puente** es un dispositivo de hardware ***utilizado para conectar dos redes que funcionan con el mismo protocolo***. A diferencia de un repetidor, que funciona en el nivel físico, el puente funciona en el **nivel de enlace** (**capa 2** del modelo OSI). Esto significa que *puede filtrar tramas para permitir sólo el paso de aquellas cuyas direcciones de destino se correspondan con un equipo ubicado del otro lado del puente*.

El puente, de esta manera, se utiliza para **segmentar** una red, ya que retiene las tramas destinadas a la red de área local y transmite aquellas destinadas para otras redes. Esto reduce el tráfico (y especialmente las colisiones) en cada una de las redes y aumenta el nivel de privacidad, ya que la información destinada a una red no puede escucharse en el otro extremo.

Sin embargo, el filtrado que lleva a cabo el puente puede provocar una **leve demora** al ir de una red a otra, razón por la cual los puentes deben ubicarse con buen criterio dentro de una red.



La función normal de un puente es enviar paquetes entre dos redes del mismo tipo.

Concepto

Un puente cuenta con dos conexiones a dos redes distintas. Cuando el puente recibe una trama en una de sus interfaces, analiza la **dirección MAC** del emisor y del destinatario. Si un puente no reconoce al emisor, almacena su dirección en una tabla para "recordar" en qué lado de la red se encuentra el emisor. De esta manera, el puente puede averiguar si el emisor y el destinatario se encuentran del mismo lado o en lados opuestos del puente. Si se encuentran en el mismo lado, el puente ignora el mensaje; si se encuentran en lados opuestos, el puente envía la trama a la otra red.

Cómo funciona un puente

Un puente funciona en la capa de enlace de datos del modelo OSI, es decir que funciona con las **direcciones físicas** de los equipos. En realidad, el puente está conectado a varias redes de área local, denominadas **segmentos**. El puente crea una tabla de correspondencia entre las direcciones de los equipos y los segmentos a los que pertenecen, y "escucha" los datos que circulan por los segmentos.

Al momento de realizarse la transmisión de datos, el puente controla en la tabla de correspondencia el segmento al que pertenecen los equipos remitentes y destinatarios **(utiliza su dirección física, denominada dirección MAC, y no su dirección IP)**. Si pertenecen al mismo segmento, el puente no hace nada; de lo contrario, conmuta los datos al segmento del equipo destinatario.

¿Para qué se utiliza un puente?

Un puente se utiliza para **segmentar una red**, *es decir, (en el caso presentado anteriormente) para que la comunicación entre los tres equipos de la parte superior no bloquee las líneas de la red que pasa a través de los tres equipos de la parte inferior*. La información sólo se transmite cuando un equipo de un lado del puente envía datos a un equipo del lado opuesto.

Además, estos puentes pueden conectarse a un módem para que también puedan funcionar con una red de área local remota.

CONMUTADORES O SWITCH

Un **conmutador** (switch) es un puente con múltiples puertos, es decir que es un elemento activo que trabaja en el **nivel de enlace** (**capa 2** del modelo OSI).

Cuando hablamos de un switch hablamos de un dispositivo que añade un nivel de "i**nteligencia**" a la unión de dispositivos.

El conmutador *analiza las tramas que ingresan por sus puertos de entrada y filtra los datos para concentrarse solamente en los puertos correctos* (esto se denomina **conmutación** o **redes conmutadas**). Por consiguiente, el conmutador puede funcionar como puerto cuando filtra los datos y como concentrador (hub) cuando administra las conexiones. A continuación, encontrará el diagrama de un conmutador:

Es capaz de conmutar la información enviando ésta ***solamente a su destinatario****, y prescindiendo de los demás ordenadores, con el consiguiente ahorro de tiempo y colisiones*. Su funcionamiento es el siguiente:

El "switch" conoce los ordenadores que tiene conectados a cada uno de sus puertos (enchufes). Cuando en la especificación del un "switch" leemos algo como "**8k MAC address table**" se refiere a la memoria que el "switch" destina a almacenar las direcciones. Un "switch" cuando se enchufa no conoce las direcciones de los ordenadores de sus puertos, las **aprende** a medida que circula información a través de él. Con 8k hay más que suficiente.

Por tanto, cuando un "switch" no conoce la dirección MAC de destino envía la trama por todos sus puertos, al igual que un HUB ("**Flooding**", inundación). Cuando hay más de un ordenador conectado a un puerto de un "switch" este aprende sus direcciones MAC y cuando se envían información entre ellos no la propaga al resto de la red, a esto se llama **filtrado**.

El "switch" almacena la trama antes de reenviarla. A este método se llama "**Store&Forward**", es decir "almacenar y enviar".

Hay otros métodos como por ejemplo "**Cut-Through**" que consiste en recibir los 6 primeros bytes de una trama que contienen la dirección MAC y a partir de aquí ya empezar a enviar al destinatario. "Cut-through" no permite descartar paquetes defectuosos. Un "switch" de tipo "Store&forward" controla el CRC de las tramas para comprobar que no tengan error, en caso de ser una trama defectuosa la descarta y ahorra tráfico innecesario.

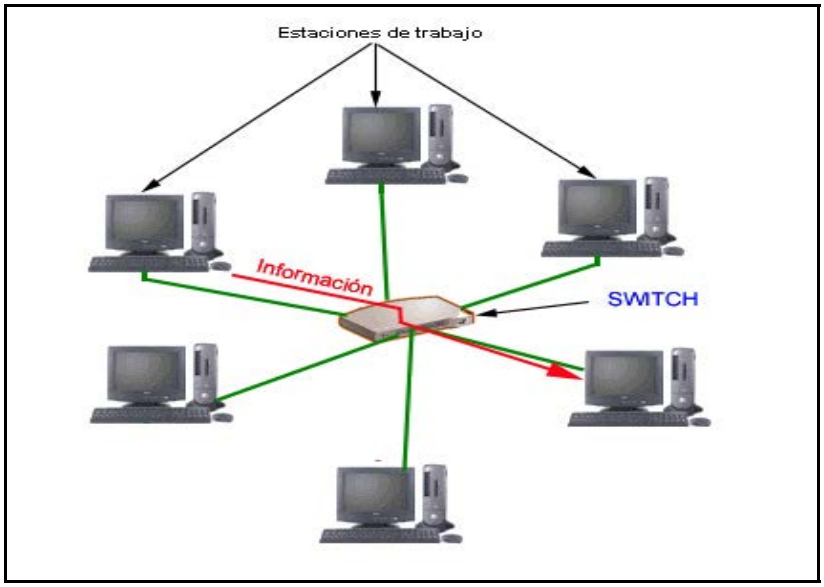
El "Store&forward" también permite adaptar velocidades de distintos dispositivos de una forma más cómoda, ya que la memoria interna del "switch" sirve de "**buffer**". Obviamente si se envía mucha información de un dispositivo rápido a otro lento otra capa superior se encargará de reducir la velocidad.

Un "switch" moderno también suele tener lo que se llama "**Auto-Negotiation**", es decir, negocia con los dispositivos que se conectan a él la velocidad de funcionamiento, 10 megabits ó 100, así como si se funcionara en modo "Full-Duplex" o "Half-Duplex". "Full-Duplex" se refiere a que el dispositivo es capaz de enviar y recibir información de forma simultánea. "Half-Duplex" por otro lado, sólo permite enviar o recibir información, pero no a la vez.

Todo lo anterior explicado requiere que el "switch" tenga un **procesador** y una **memoria**. También hay un parámetro conocido como "**Back-Plane**" o plano trasero que define el **ancho de banda** máximo que soporta un "switch". El "Back-Plane" dependerá del procesador, del número de tramas que sea capaz de procesar.

Si hacemos números vemos lo siguiente: 100 Mbps x 2 (cada puerto puede enviar 100 Mbps y recibir 100 más en modo “Full-Duplex”) x 8 puertos = 1,6 Gbps. Así pues, un “switch” de 8 puertos debe tener un “Back-Plane” de 1,6 Gbps para funcionar correctamente.

Si un nodo puede tener varias rutas alternativas para llegar a otro un “switch”, tiene problemas para aprender su dirección ya que aparecerá en dos de sus entradas. A esto se le llama “**loop**”. El protocolo de **Spanning Tree Protocol IEEE 802.1d** se encarga de solucionar este problema.



Conmutación

El conmutador utiliza un mecanismo de filtrado y de conmutación que redirige el flujo de datos a los equipos más apropiados, en función de determinados elementos que se encuentran en los paquetes de datos.

Un **conmutador de nivel 4**, que funciona en la **capa de transporte** del modelo OSI, inspecciona las **direcciones** de origen y de destino de los mensajes y crea una tabla que le permite saber qué equipo está conectado a qué puerto del conmutador (en general, el proceso se realiza por autoaprendizaje, es decir automáticamente, aunque el administrador del conmutador puede realizar ajustes complementarios.

Una vez que conoce el puerto de destino, el conmutador sólo envía el mensaje al puerto correcto y los demás puertos quedan libres para otras transmisiones que pueden llevarse a cabo de manera simultánea. Por consiguiente, cada intercambio de datos puede ejecutarse a la velocidad de transferencia nominal (más uso compartido de ancho de banda) sin colisiones. El resultado final será un aumento significativo en el ancho de banda de la red (a una velocidad nominal equivalente).

Los conmutadores más avanzados, denominados **conmutadores de nivel 7** (que corresponden a la **capa de aplicación** del modelo OSI), pueden redirigir los datos en base a los datos de aplicación avanzada contenidos en los paquetes de datos, como las cookies para el protocolo HTTP, el tipo de archivo que se envía para el protocolo FTP, etc. Por esta razón, un conmutador de nivel 7 puede, por ejemplo, permitir un equilibrio de carga al enrutar el flujo de datos que entra en la empresa hacia a los servidores más adecuados: los que poseen menos carga o que responden más rápido.

15.- PROTOCOLOS DE COMUNICACIÓN DE RED

PROTOCOLO NETBIOS (NETWORK BASIC INPUT/OUTPUT SYSTEM)

En 1984, IBM diseñó un simple protocolo para conectar en red sus computadoras, llamado Network Basic Input/Output System (NetBIOS). El protocolo NetBIOS proporcionaba un diseño rudimentario para que una aplicación se conectara y compartiese datos con otras computadoras.

A finales de 1985, IBM lanzó dicho protocolo NetBIOS para convertirse en NetBIOS Extended User Interface (NetBEUI). NetBEUI fue diseñado para redes de área local (LANs), y permitía a cada máquina usar un nombre (de hasta 15 caracteres) que no estuviera siendo usado en la red.

El protocolo NetBIOS se volvió muy popular en las aplicaciones de red, incluyendo a las que corrían bajo Windows para Grupos. Más tarde, emergieron también implementaciones de NetBIOS sobre protocolos IPX de Novell. Sin embargo, los protocolos de red escogidos por la comunidad de Internet eran TCP/IP y UDP/IP, y las implementaciones de los protocolos NetBIOS sobre dichos protocolos pronto se convirtió en una necesidad para poder acceder a Internet.

NetBIOS es un protocolo rápido y sencillo de implementar, pero muy poco seguro, ya que abre conexiones en los ordenadores de forma indiscriminada permitiendo el acceso al propio ordenador desde cualquier punto de la red con escasos mecanismos de seguridad.

PROTOCOLO NETBEUI (NETBIOS EXTENDED USER INTERFACE)

NetBEUI (Interfaz extendida de usuario de NetBIOS) fue presentado por primera vez por IBM en 1985. NetBEUI es un protocolo compacto, eficiente y rápido, pero poco seguro.

En 1985, cuando fue desarrollado el protocolo NetBEUI, se consideró que las redes locales estarían segmentadas en grupos de trabajo de entre 20 y 200 Pc's y que se utilizarían ruoters para conectar cada segmento de red local con otro segmento de red local, o con un servidor.

NetBEUI está optimizado para obtener un rendimiento muy elevado cuando se utiliza en redes locales o segmentos de redes locales departamentales. En cuanto al tráfico cursado dentro de un segmento de red local, NetBEUI es el más rápido de los protocolos.

Fue concebido expresamente para la comunicación dentro de redes locales pequeñas y, por lo tanto, es muy rápido. Tiene buena protección frente a errores y utiliza poca memoria. Sin embargo, no admite encadenamientos y su rendimiento en redes de área amplia (WAN) es pobre.

Puesto que NetBEUI es muy rápido para comunicaciones dentro de redes locales de pequeño tamaño, pero su rendimiento es peor para las comunicaciones con redes de área amplia (WAN), un método recomendable para configurar una red es utilizar NetBEUI y otro protocolo, como TCP/IP, en cada uno de los ordenadores que necesiten acceder a otro a través de un router o una red de área amplia.

PROTOCOLO IP (INTERNET PROTOCOL)

El protocolo IP es el más utilizado para la interconexión entre redes y cuando se diseñó ya se tuvo en cuenta la interconexión entre redes. Su trabajo es proporcionar un medio para el transporte de datagramas con información del origen al destino, sin importar si estas máquinas están en la misma red, o si hay otras redes entre ellas.

IP está implementado en todos los ordenadores y dispositivos de encaminamiento (Routers). Se preocupa de la retransmisión de los datos de un ordenador a otro ordenador, pasando por uno o varios dispositivos de encaminamiento nodo a nodo. No conoce para que aplicación son los paquetes, únicamente sabe de máquina son.

Por tanto el protocolo IP:

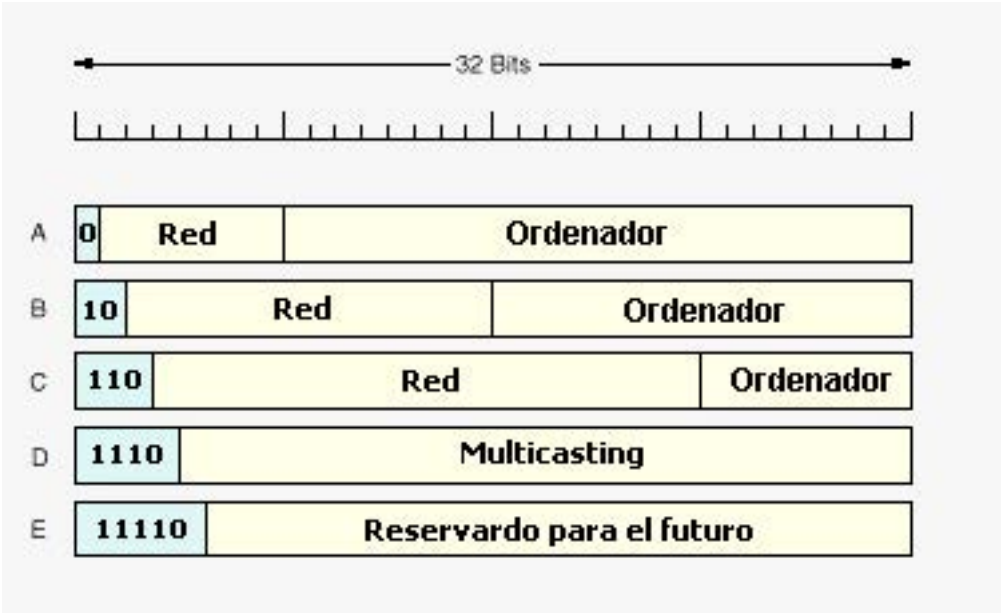
- Es **no orientado a conexión** debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.

- Es **no fiable** porque los paquetes pueden perderse, dañarse o llegar retrasados.

- Cada ordenador y cada dispositivo de interconexión (switch o router) tendrá una **dirección IP única** cuya longitud será de 32 bits, agrupados en cuatro bytes de la forma **XXXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX** de que será utilizada como dirección origen y dirección destino de la cabecera de la trama de información. Esta dirección consta de un **identificador de red** y de **un identificador de máquina**.

Es decir en la dirección IP se reservan determinados bits para identificar la red y el resto para identificar el ordenador dentro de esa red. La dirección IP -en decimal- más pequeña es la 0.0.0.0 y la mayor es 255.255.255.255.

El direccionamiento IP y la identificación de una máquina dentro de una red será objeto de una Unidad Didáctica más adelante.



PROTOCOLO IPX (INTERNET PACKET EXCHANGE)

Se trata del protocolo análogo de IP para Novell® NetWare para el intercambio de paquetes de mensajes entre redes conectadas. IPX pasa las solicitudes a los servicios de red y la red las envía a las estaciones de trabajo, servidores o dispositivos de las redes conectadas. Los datos se transmiten también en datagramas.

Este protocolo de comunicaciones NetWare se utiliza para encaminar mensajes de un nodo a otro. Los paquetes IPX incluyen, al igual que IP, direcciones de redes y pueden enviarse de una red a otra.

Ocasionalmente, un paquete IPX puede perderse cuando cruza redes, de esta manera el IPX no garantiza la entrega de un mensaje completo. La aplicación tiene que proveer ese control o debe utilizarse el protocolo SPX de NetWare.

En la actualidad debido al abrumador uso del protocolo IP en todos los ámbitos, incluyendo la Armada, IPX ha quedado cada vez más relegado, incluso Novell® NetWare en sus nuevas versiones de servidores de archivos ha implementado el protocolo IP.

16.- DIRECCIONES IP

En unidades anteriores se estableció que todo sistema informático tiene una **dirección física**, no modificable y única en el mundo dentro de una red, llamada dirección **MAC**. Esta dirección opera a nivel de enlace del modelo OSI.

Si dentro de una red se necesitan crear subredes más pequeñas por razones de administración, seguridad etc. es preciso utilizar un direccionamiento lógico o virtual, modificable que permita filtrar y administrar el acceso a determinados ordenadores a la red o a algunos contenidos dentro de un servidor de información. Este direccionamiento lógico opera a nivel de red del modelo OSI, y se conoce como **direccionamiento IP**.

Las direcciones del nivel de red en Internet pueden representarse de manera **simbólica** o **numérica**.

Una dirección simbólica es por ejemplo ***http://www.fn.mdef.es***, y su correspondiente dirección numérica se representa por cuatro bytes (8 bits) separados por puntos, como 00001010.00101010.00010000.10011100, que convertido en decimal sería **10.42.0.134**. Evidentemente estos bytes no pueden superar el valor 255 (11111111 en binario). La correspondencia entre direcciones simbólicas y numéricas las realiza el **servidor DNS** (Domain Name System).

Binario	00001010.	00101010.	00000000.	10000110
Decimal	10.	42.	0.	134.

Las máquinas sólo entienden direcciones numéricas, las direcciones simbólicas se utilizan para facilitar al usuario el acceso de forma intuitiva a los diferentes sitios dentro de la red. Por tanto para poder identificar una máquina en una red (ya sea intranet o Internet) debe de tener una dirección IP.

Según la forma de asignar las direcciones IP a las máquinas en red, aquéllas se pueden clasificar en dos tipos:

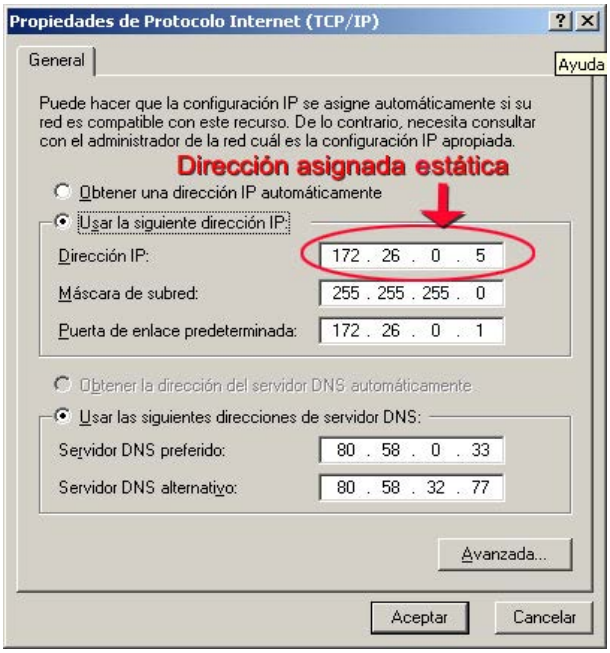
- **Direcciones IP estáticas**
- **Direcciones IP dinámicas**

DIRECCIONES IP ESTÁTICAS

Una dirección IP Estática se asigna de forma **permanente** a un equipo (por ejem. un router ADSL) de tal forma que siempre que una sesión en red se inicie desde ese equipo llevará asociada esa dirección permanente. Cuando el equipo no está conectado, esa dirección IP está **reservada**, y no se puede utilizar por ninguna otra máquina.

Este es el modo menos eficiente de asignar un recurso escaso como es la dirección IP, sin embargo es el recomendado en los casos de servidores, routers, y otros dispositivos que se necesitan tener siempre localizados dentro de la red es decir cuando ese usuario final no esté actuando sólo como usuario final sino como ***proveedor de algo*.**

No es posible técnicamente asignar direcciones estáticas a accesos conmutados de banda estrecha (acceso IP por módem a través de la Red Telefónica Básica).

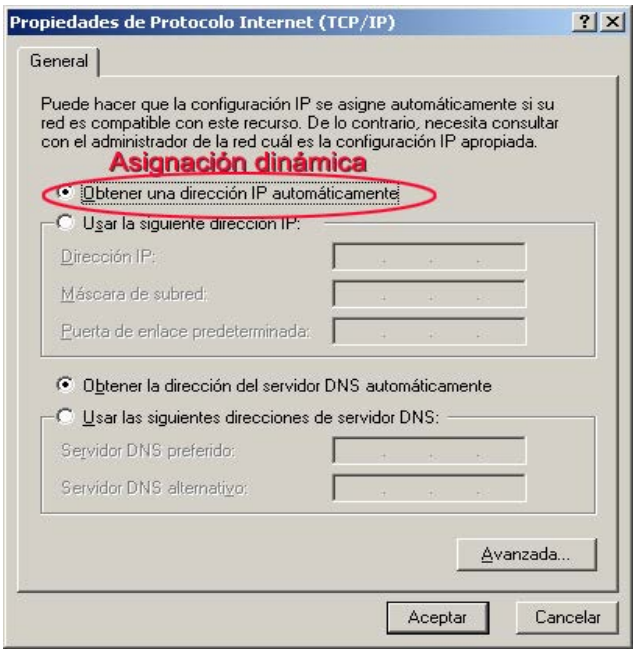


DIRECCIONES IP DINÁMICAS

Una dirección IP Dinámica se asigna de forma **aleatoria** una vez que el usuario se identifique al conectarse a su proveedor de Internet o a una intranet y se mantiene asignada mientras dure la conexión. Cuando el equipo no está conectado, la dirección se libera y puede asignarse a la comunicación de otro usuario.

Es el modo más eficiente de asignar un recurso **escaso** como es la dirección IP. Es el único posible para accesos conmutados de banda estrecha.

El dispositivo encargado de asignar las direcciones IP a las diferentes máquinas de la red se denomina ***servidor DHCP (Dynamic Host Configuration Protocol).***



CLASIFICACIÓN DE LAS DIRECCIONES IP

Atendiendo al criterio de si las direcciones IP, es si son visibles en **todo Internet**, o si, por el contrario, *sólo son visibles dentro de una* ***red privada***, se pueden clasificar en dos tipos:

- **Direcciones IP Públicas**
- **Direcciones IP Privadas**

DIRECCIONES IP PÚBLICAS

Estas direcciones son **únicas y visibles en todo Internet**, y son administradas por oficinas de registro como el **ARIN** (American Registry of Internet Numbers) o el **APNIC** (Asia Pacific Network Information Centre).

Cada oficina suministradora de **direcciones IP públicas** posee un rango de direcciones que asigna de forma dinámica a cualquier usuario que accede a Internet; una vez que ese usuario sale de Internet esa dirección queda disponible para ser usada por otro usuario.

También se asignan **direcciones estáticas públicas** a aquellos servidores o routers que necesitan ser una referencia fija dentro de Internet (Buscadores, Proveedores de servicios, routers, etc.)

DIRECCIONES IP PRIVADAS

Estas direcciones se usan en **redes privadas sin acceso a Internet**, y por tanto *pueden ser iguales a direcciones utilizadas en Internet*. Por tanto si una red no se va a comunicar con otras redes, la implementación del direccionamiento IP queda a juicio del diseñador de la red.

DIRECCIONAMIENTO DE REDES IP

En una dirección IP **una parte de los bits representa la red y el resto de los bits a la máquina (host) dentro de esa red**. Existen cinco (5) clases de direcciones IP según la manera de repartir los bits entre la dirección de red y el número de host, pero para direccionamiento de máquinas dentro de una red sólo se utilizan tres (3).

Clase	Red (bits)	Host (bits)
Clase A	8	24
Clase B	16	16
Clase C	24	8

REDES CLASE A

En una red de clase A, **se asigna el primer octeto (1 byte) para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts**, de modo que la cantidad máxima de hosts es 2^{24} (menos dos: las direcciones reservadas de broadcast (último octeto a 255) y de red (último octeto a 0), o sea, **16.777.214 hosts**.
Se acuerda que para diferenciar las redes clase A del resto, el primer bit del primer octeto se fuerza a valor 0. Por tanto en las redes clase A, los hosts u ordenadores irán **desde la dirección 1.0.0.1 hasta la 126.255.255.254**.

Las direcciones de Clase A usan **7 bits para el número de red** dando un total de 126 (128-2) posibles redes de este tipo ya que la dirección 0.0.0.0 se utiliza para reconocer la dirección de red propia y la red 127.X.X.X es la de bucle interno de la máquina.

Los restantes **24 bits son para el número de host** –quitando las que son todos los bits a 0 ó a 1 –con lo cual tenemos hasta $2^{24} – 2 = 16.777.216 - 2 = 16.777.214$ direcciones. **Son las redes 1.0.0.0 a 126.0.0.0**

El 1er bit del primer octeto se fuerza a 0

Redes clase A			
Identificación de RED	Identificación de host		
1er octeto	2º octeto	3er octeto	4º octeto
0 n n n n n n n	n n n n n n n	n n n n n n n	n n n n n n n

REDES CLASE B

En una red de clase B, **se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts de esa red**, de modo que la cantidad máxima de hosts es 2^16 (menos dos), o **65 534 hosts**.

Se ha convenido que para diferenciar las redes clase B del resto, el primer bit del primer octeto se fuerza a valor 1 y el segundo a valor 0. Por tanto en las redes clase B, los ordenadores irán **desde la dirección 128.0.0.1 hasta la 191.255.255.254**.

Las direcciones de Clase B utilizan **14 bits para la dirección de red** (16.382 posibles redes de este tipo) y **16 bits para el host** (hasta 65.534 máquinas). **Son las redes 128.0.0.0 a 191.255.0.0**

El 1er bit del primer octeto se fuerza a 1 y el segundo a 0

Redes clase B			
Identificación de RED		Identificación de host	
1er octeto	2º octeto	3er octeto	4º octeto
1 0 n n n n n n	n n n n n n n n	n n n n n n n n	n n n n n n n n

REDES CLASE C

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

Por convenio, para diferenciar las redes clase C del resto, el primer y el segundo bit del primer octeto se fuerzan a valor 1 y el tercero a valor 0. Por tanto en las redes clase C, los ordenadores irán **desde la dirección 192.0.0.1 hasta la 223.255.255.254**.

Las direcciones de clase C tienen **21 bits para la red** (2.097.150 redes) y **8 bits para el host** (254 máquinas). Son las redes 192.0.0.0 a 223.255.255.0

El 1er y el 2º bit del primer octeto se fuerza a 1 y el tercero a 0

Redes clase C			
Identificación de RED			Identificación de host
1er octeto	2º octeto	3er octeto	4º octeto
1 1 0 n n n n n	n n n n n n n n	n n n n n n n n	n n n n n n n n

DIRECCIONES CLASE D

Las direcciones de clase D están reservadas para **multicasting**, usadas por direcciones de host en áreas limitadas. **No se emplean en ningún caso para direccionamiento de hosts en las redes de área local.**

Por convenio, para diferenciar estas direcciones del resto, el primer, segundo y tercer bit del primer octeto se fuerzan a valor 1 y el cuarto a valor 0. Por tanto el rango de estas direcciones irá **desde 224.0.0.1 hasta la 239.255.255.255**.

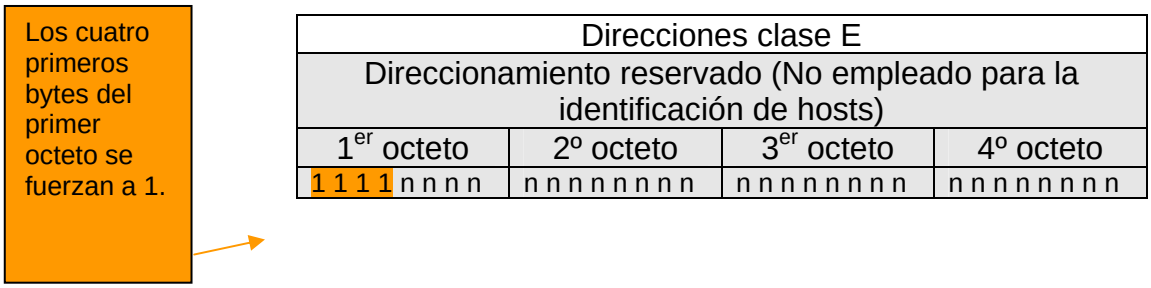
El 1er, el 2º y el 3er bit del primer octeto se fuerza a 1 y el cuarto a 0

Direcciones clase D			
Direccionamiento reservado (No empleado para la identificación de hosts)			
1er octeto	2º octeto	3er octeto	4º octeto
1 1 1 0 n n n n	n n n n n n n n	n n n n n n n n	n n n n n n n n

DIRECCIONES CLASE E

Las direcciones de clase E están **reservadas para uso futuro**. **Tampoco se emplean en ningún caso para direccionamiento de hosts en las redes de área local.**

Se acuerda que para diferenciar estas direcciones del resto, los cuatro primeros bytes primer octeto se fuerzan a valor 1. Por tanto el rango de estas direcciones irá desde **240.0.0.1 hasta la 255.255.255.255**



DIRECCIONES ESPECIALES Y RESERVADAS

Algunas direcciones de red se reservan para propósitos especiales. La **0.0.0.0** y la **127.0.0.0** son dos de estas direcciones.

La dirección 0.0.0.0 se denomina **encaminamiento por defecto** y tiene que ver con el camino por el que el IP encamina sus datagramas.

La red 127.0.0.0 está reservada para el **tráfico IP local del puesto**. Normalmente, la dirección 127.0.0.1 se asignará a una interfaz especial del puesto, (la *Interfaz loopback*), que actúa como un circuito cerrado. Es decir: cualquier paquete IP enviado a esta interfaz por TCP o UDP le será devuelto a cualquiera de ellos como si simplemente hubiese llegado desde alguna red. Esto permite desarrollar y probar el hardware de red - por ejemplo el correcto funcionamiento de la propia tarjeta de red- y el software implementado de red aunque no se esté usando una red "real".

La red loopback también permite usar software de red en un puesto solitario. Puede que esto no sea tan infrecuente como parece; por ejemplo, muchos sitios UUCP (acrónimo del inglés *Unix to Unix CoPy*, *Copiador de Unix a Unix*, -que hace generalmente referencia a una serie de programas de computadoras y protocolos que permiten la ejecución remota de comandos y transferencia de archivos, correo electrónico y Netnews entre computadoras- no tienen conectividad con IP en absoluto, pero aún pueden querer ejecutar un sistema de noticias INN **(**InterNetNews es un servidor de noticias de Usenet, acrónimo de **Use**rs **Net**work, -red de usuarios, consistente en un sistema global de discusión en Internet-). Para un funcionamiento adecuado en GNU/Linux, INN requiere la interfaz loopback.

Además, algunos rangos de direcciones de cada una de las clases de red han sido reservados y designados como rangos de direcciones "**reservadas**" o "**privadas**".

Estas direcciones están reservadas para el uso de redes privadas y no son enrutadas o utilizadas en Internet. Son usadas normalmente por organizaciones con su propia intranet como, por ejemplo, el **Ministerio de Defensa de España**; pero incluso las redes pequeñas suelen encontrarlas útiles. Las direcciones reservadas en cada clase de red son las siguientes:

Clase	Redes
A	Desde la 10.0.0.0 hasta la 10.255.255.255
B	Desde la 172.16.0.0 hasta la 172.31.0.0
C	Desde la 192.168.0.0 hasta la192.168.255.0

MÁSCARAS IP

Cuando se trabaja con una red pequeña, con pocos host conectados, el administrador de red puede fácilmente configurar el rango de direcciones IP usado para conseguir un funcionamiento óptimo del sistema. Pero conforme las redes son más grandes hace necesaria una **división en subredes** de las mismas.

En primer lugar, porque conforme se va extendiendo la red va aumentando el *dominio de colisión* -segmento físico de una red de computadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros- , llegando un momento en el que el rendimiento de la red se ve afectado seriamente. Esto se puede mitigar **segmentando la red**, dividiendo la misma en una serie de segmentos significativos, de tal forma que mediante switches podremos limitar estos dominios de colisión, enviando las tramas tan sólo al segmento en el que se encuentra el host destino.

En segundo lugar, y aunque segmentemos la red, conforme aumenta el número de host aumenta también el número de transmisiones de broadcast o multidifusión (cuando un equipo origen envía datos a todos los dispositivos de la red), llegando un momento que dicho tráfico puede congestionar toda la red fuera de los límites, al consumir un ancho de banda excesivo. Esto es así porque todos los host están enviando de forma constante peticiones de este tipo: peticiones ARP, envíos RIP, peticiones DNS, etc.

Para resolver esto es preciso dividir una red primaria en una serie de subredes, de tal forma que cada una de ellas va a funcionar luego, a nivel de envío y recepción de paquetes, como una red individual, aunque todas pertenezcan a la misma red principal (y por lo tanto, al mismo dominio).

Esto se consigue utilizando bits que en principio estarían destinados para identificar hosts dentro de una red extensa, para crear subredes dentro de esa red.

*La **máscara de red** es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una red o una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP*. En formato binario todas las máscaras de red tienen a "1" los bits que determinan la red y a "0" los bits que identifican los hosts direccionables en esa red.

Por tanto las máscaras de subred por defecto serán:

Redes clase A	Id. de red	Id. de hosts			Valor decimal
Máscara por defecto	11111111	00000000	00000000	00000000	255.0.0.0

Redes clase B	Id. de red		Id. de hosts		Valor decimal
Máscara por defecto	11111111	11111111	00000000	00000000	255.255.0.0

Redes clase C	Id. de red			Id. de hosts	Valor decimal
Máscara por defecto	11111111	11111111	11111111	00000000	255.255.255.0

Para segmentar una red utilizaremos bits que están denotando hosts para crear subredes.

Ejemplo 1

Disponemos de la dirección de red de clase B: 169.10.0.0 y necesitamos segmentarla en 14 subredes.

Resolución:

Su valor en binario será 10101001. 00001010. 00000000. 00000000

Y su máscara por defecto será: 11111111. 11111111. 00000000. 00000000 (255.255.0.0)

Ahora le quitamos 4 bits a la porción de host para crear subredes por tanto la máscara de subred será: 11111111. 11111111.1111**0000**. 00000000,
que pasada a decimal nos queda: 255.255.240.0

Este enmascaramiento nos permitirá crear 14 subredes dentro de esa red clase B, es decir 2^4 - 2, ya que dos direcciones están reservadas- a broadcast -último octeto a 255- y la de red -último octeto a 0.

Cálculo de las subredes:

Para calcular qué rango abarcan esas 14 subredes basta con aplicar un operador lógico “AND” a la dirección de red con su máscara de subred:

10101001. 00001010. 00000000. 00000000
AND
11111111. 11111111.1111**0000**. 00000000
10101001. 00001010. 00000000. 00000000

1ª subred - en decimal 169.10.0.0

Por tanto el primer host direccionable de esta subred será: 169.10.0.1
Y el último resultará de poner todos los bits destinados a direccionar hosts a “1”

10101001. 00001010. 0000**1111.11111111** pero hay que quitar la última dirección (*Broadcasting*) entonces será el 169.10.15.254

Por tanto la 1ª subred irá desde la 169.10.0.1 hasta la 169.10.15.254

La siguiente subred será la 169.10.16.0 e irá desde la 169.10.16.1 hasta la 169.10.31.254

Y así sucesivamente.

Ejemplo 2

Determinar a qué subred pertenece la siguiente dirección IP 10.42.67.112 con máscara de subred 255.255.248.0

¿Cuál es el rango de direcciones de esa subred?

¿Cuál es su dirección de *broadcasting*?

Resolución:

Sabemos que en principio es una dirección clase A (está entre 1 y 126 el primer valor)

Su máscara por defecto entonces sería 255.0.0.0

Si tiene una máscara 255.255.248.0 significa que se han utilizado 8 bits del segundo octeto y 5 bits del tercer octeto (total 13) para crear subredes.

Si “enmascaramos” nuestra dirección IP con su máscara, utilizando un operador lógico “AND”:

00001010. 00101010. 01000011. 01110000 (= 10.42.67.112)
AND
11111111. 11111111. 11111000. 00000000 (= 255.255.248.0)
00001010. 00101010. 01000000. 00000000

(= 10.42.64.0) Identificación de subred a la que pertenece.

La primera dirección de esta subred sería: 10.42.64.1

Si ponemos a “1” todos los bits reservados para direccionar hosts

00001010. 00101010. 01000111.11111111

excepto la última -que sería la de *broadcasting* -la última dirección utilizable de esta subred sería:

10.42.71.254

Y precisamente la de *broadcasting* sería:

10.42.71.255

Las direcciones de Internet privadas son:

Nombre	rango de direcciones IP	número de IPs	descripción de la clase	mayor bloque de CIDR	definido en
bloque de 8 bits	10.0.0.0 – 10.255.255.255	16.777.216	clase A simple	10.0.0.0/8	RFC 1597 (obsoleto), RFC 1918
bloque de 12 bits	172.16.0.0 – 172.31.255.255	1.048.576	16 clases B continuas	172.16.0.0/12	
bloque de 16 bits	192.168.0.0 – 192.168.255.255	65.536	256 clases C continuas	192.168.0.0/16	
bloque de 16 bits	169.254.0.0 – 169.254.255.255	65.536	clase B simple	169.254.0.0/16	RFC 3330, RFC 3927

El documento RFC 1597 contiene la especificación original y permanece por razones históricas, pues ha sido reemplazado por el documento RFC 1918.

18.- CÁLCULO DE SUBREDES

Antes de comenzar con la tarea se deben tener 2 datos básicos:

• Cuál es el número total de subredes que se requieren, incluyendo la consideración del posible crecimiento de la red.

• Cuál es el número de nodos que se prevén en cada subred, teniendo en cuenta también en este caso las consideraciones de expansión y crecimiento.

A partir de aquí, responda estas 6 preguntas básicas:

1. ¿Cuántas subredes?

2. ¿Cuántos nodos por subred?

3. ¿Cuáles son los números reservados de subred?

4. ¿Cuáles son las direcciones reservadas de broadcast?

5. ¿Cuál es la primera dirección de nodo válida?

6. ¿Cuál es la última dirección de nodo válida?

Con lo que debe obtener 6 respuestas.

Un ejemplo: red 192.168.1.0 máscara 255.255.255.224

(255=128+64+32+16+8+4+2+1) (255=1 1 1 1 1 1 1 1)
(224= 128+64+32+0+0+0+0+0) (224=1 1 1 0 0 0 0 0)

1. La cantidad de subredes utilizables se calcula tomando como base la cantidad de bits de la porción del nodo que se toman para generar subredes, y aplicando la fórmula siguiente:

$2^{[\text{bits de subred}]} - 2 = \text{subredes utilizables}$

Ejemplo: $2^3 - 2 = 6$

2. La cantidad de direcciones de nodo útiles que soporta cada subred, surge de la aplicación se la siguiente fórmula que toma como base la cantidad de bits que quedan para identificar los nodos:

$2^{[\text{bits de nodo}]} - 2 = \text{nodos}$

Ejemplo: $2^5 - 2 = 30$

3. La dirección reservada de la primera subred útil surge de restar a 256 el valor decimal de la porción de la máscara de subred en la que se define el límite entre subred y nodo:

256 – [máscara] = [primera subred útil y rango de nodos]

Las direcciones de las subredes siguientes surgen de seguir sumando la misma cifra.

Ejemplo: 256 – 224 = 32

_ ____ 192.168.1.0 _____ subred 0
_ ____ 192.168.1.32 ____ subred 1 - primera subred útil
+ 32 _ 192.168.1.64 ____ subred 2
+ 32 _ 192.168.1.96 ____ subred 3
+ 32 _ 192.168.1.128 ___ subred 4
+ 32 … … …

4. Las direcciones reservadas de broadcast se obtienen restando 1 a la dirección reservada de subred de la subred siguiente:

Ejemplo:

32 – 1 = 31 ___ 192.168.1.31 _____ subred 0
64 – 1 = 63 ___ 192.168.1.63 _____ subred 1
96 – 1 = 95 ___ 192.168.1.95 _____ subred 2
128 – 1 = 127 _ 192.168.1.127 ____ subred 3

… … …

5. La dirección IP del primer nodo útil de cada subred se obtiene sumando uno a la dirección reservada de subred:

reservada de subred + 1 = primer nodo utilizable

Ejemplo:
32 + 1 = 33 ___ 192.168.1.33 _____ primer nodo subred 1
64 + 1 = 65 ___ 192.168.1.65 _____ primer nodo subred 2
96 + 1 = 97 ___ 192.168.1.97 _____ primer nodo subred 3
128 + 1 = 129 _ 192.168.1.129 ____ primer nodo subred 4
… … …

6. La dirección IP del último nodo útil de cada subred se obtiene restando 1 a la dirección reservada de broadcast:

63 – 1= 62 _ __ 192.168.1.62 ____ último nodo subred 1
95 – 1 = 94 ___ 192.168.1.94 ____ último nodo subred 2
127 – 1 = 126 _ 192.168.1.126 ___ último nodo subred 3 … … …

Sintetizando:

Con esa máscara de subred se obtienen **6 subredes útiles**, cada una de ellas con una capacidad máxima de **30 nodos** (32 direcciones IP):

Subred_____ Primer nodo útil__Último nodo útil__Broadcast

0 192.168.1.0

1_ 192.168.1.32__ 192.168.1.33 ___ 192.168.1.62 __ 192.168.1.63
2_ 192.168.1.64__ 192.168.1.65 ___ 192.168.1.94 __ 192.168.1.95
3_ 192.168.1.96__ 192.168.1.97 ___ 192.168.1.126 _ 192.168.1.127
4_ 192.168.1.128_ 192.168.1.129 … … ... … …

19.- DISPOSITIVOS DE INTERCONEXIÓN DE REDES NIVEL DE RED (capa 3 OSI)

Los dispositivos de interconexión son aquellos elementos de una red LAN que permiten conectar los diferentes puestos (ordenadores, impresoras etc.) entre si. Además también son aquellos que permiten conectar diferentes redes, como por ejemplo, una red LAN interna con Internet.

Como dispositivos englobados en el **nivel de red** (**capa 3** del modelo OSI) veremos el **Router**.

ROUTER

El **enrutador** (del inglés *router)*, **direccionador**, **ruteador** o **encaminador** es un dispositivo de hardware para interconexión de red de ordenadores que opera en la **capa 3 (nivel de red)**. Un router es un *dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.*

Un Router *o* Gateway es un dispositivo conectado en la red que **une redes distintas**. Por tanto, sus funciones son:

• Adaptar la estructura de información de una red a la otra (datagramas con tamaños y estructuras distintas)

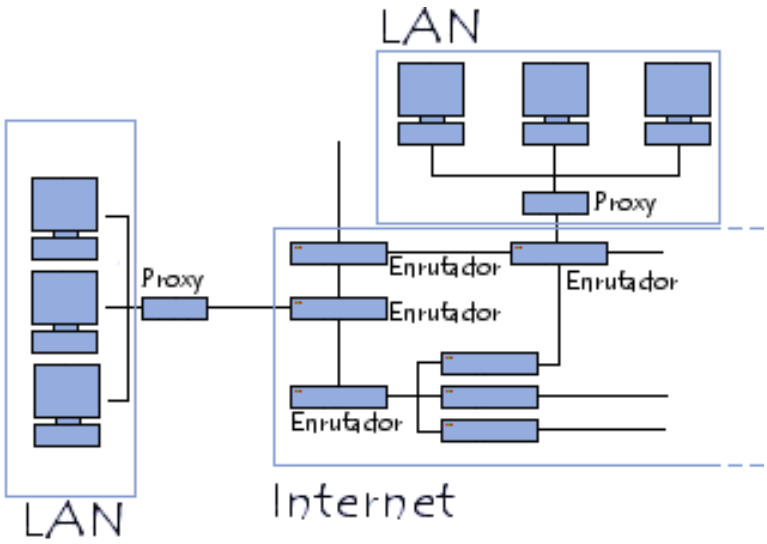
• Pasar información de un soporte físico a otro (distintas velocidades y soportes físicos)

• Encaminar información por la ruta óptima

• Reagrupar la información que viene por rutas distintas

Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica la dirección IP del equipo deseado.

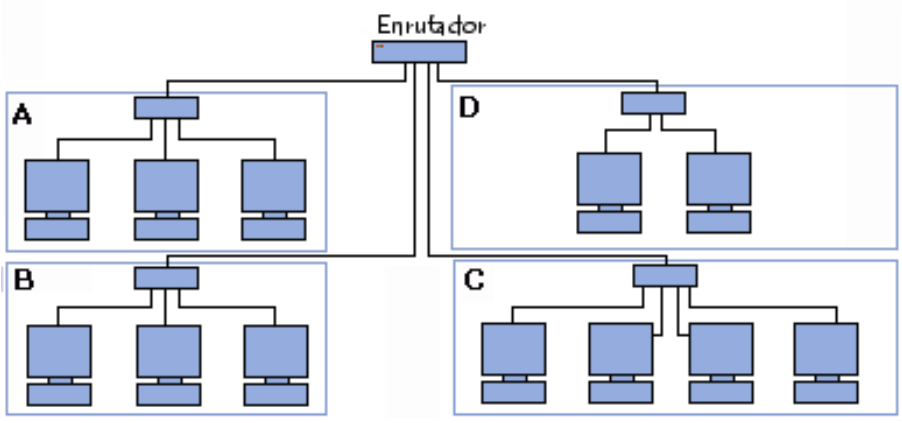
La estación de trabajo envía la solicitud al router más cercano, es decir, a la pasarela predeterminada de la red en la que se encuentra. Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible. Para hacerlo, el router cuenta con **tablas de enrutamiento** actualizadas, que son verdaderos mapas de los itinerarios que pueden seguirse para llegar a la dirección de destino. Existen numerosos protocolos dedicados a esta tarea.



Además de su función de enrutar, los routers también se utilizan para manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra. Como no todas las redes pueden manejar el mismo tamaño de paquetes de datos, los routers deben fragmentar los paquetes de datos para que puedan viajar libremente.

Diseño físico de los routers

Los primeros routers eran simplemente equipos con diversas tarjetas de red, cada una conectada a una red diferente. La mayoría de los routers actuales son hardwares dedicados a la tarea de enrutamiento.



Un router cuenta con diversas interfaces de red, cada una conectada a una red diferente. Por lo tanto, **posee tantas direcciones IP como redes conectadas.**

Router inalámbrico

Un router inalámbrico comparte el mismo principio que un router tradicional. La diferencia es que aquél permite la conexión de dispositivos inalámbricos (como estaciones WiFi) a las redes a las que el router está conectado mediante conexiones por cable (generalmente Ethernet).

Algoritmos de enrutamiento

Existen dos tipos de algoritmos de enrutamiento principales:

- Los routers del tipo **vector de distancias** generan una tabla de enrutamiento que calcula el "costo" *(en términos de número de saltos)* de cada ruta y después envían esta tabla a los routers cercanos. Para cada solicitud de conexión el router elige la ruta menos costosa.

- Los routers del tipo **estado de enlace** escuchan continuamente la red para poder identificar los diferentes elementos que la rodean. Con esta información, cada router calcula la ruta más corta *(en tiempo)* a los routers cercanos y envía esta información en forma de *paquetes de actualización*. Finalmente, cada router confecciona su tabla de enrutamiento calculando las rutas más cortas hacia otros routers (mediante el algoritmo de *Dijkstra*).

PUENTE/ROUTER

Un puente/router *es un elemento híbrido que reúne las características de un router y de un puente*. Por lo tanto, este tipo de hardware se utiliza para **transferir protocolos no enrutables de una red a otra** y para enrutar otros. Más precisamente, el puente/router actúa, en primer lugar, como un puente o en su defecto, enruta los paquetes.

Un puente/router, en algunas arquitecturas, puede ser más económico y compacto que un router y un puente.

20.- EL DATAGRAMA IP

El esquema de envío de IP es similar al que se emplea en la capa Acceso a red. En esta última se envían Tramas formadas por un Encabezado y los Datos. En el Encabezado se incluye la dirección física del origen y del destino.

En el caso de IP se envían Datagramas, estos también incluyen un Encabezado y Datos, pero las direcciones empleadas son Direcciones IP.

Encabezado	Datos

FORMATO DEL DATAGRAMA IP

Los Datagramas IP están formados por Palabras de 32 bits. Cada Datagrama tiene un mínimo (y tamaño más frecuente) de cinco palabras y un máximo de quince.

Ver	Hlen	TOS	Longitud Total	
Identificación			Flags	Desp. De Fragmento
TTL		Protocolo	Checksum	
Dirección IP de la Fuente				
Dirección IP del Destino				
Opciones IP (Opcional)				Relleno
DATOS				

• **Ver:** Versión de IP que se emplea para construir el Datagrama. Se requiere para que quien lo reciba lo interprete correctamente. La actual versión IP es la 4.
• **Hlen:** Tamaño de la cabecera en palabras.
• **TOS:** Tipo de servicio. La gran mayoría de los Host y Routers ignoran este campo. Su estructura es:

Prioridad	D	T	R	SIN USO

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes. Los tipos D, T y R solicitan un tipo de transporte dado: D =Procesamiento con retardos cortos, T = Alto Desempeño y R = Alta confiabilidad. Nótese que estos bits son solo "sugerencias", no es obligatorio para la red cumplirlo.

• **Longitud Total:** Mide en bytes la longitud de doto el Datagrama. Permite calcular el tamaño del campo de datos: Datos = Longitud Total – 4 * Hlen.

Antes de continuar con la segunda palabra del Datagrama IP, hace falta introducir conceptos relacionados con la fragmentación.

FRAGMENTACIÓN

El tamaño para un Datagrama debe ser tal que permita la encapsulación, esto es, enviar un Datagrama completo en una trama física. El problema está en que el Datagrama debe transitar por diferentes redes físicas, con diferentes tecnologías y diferentes capacidades de transferencia.

A la capacidad máxima de transferencia de datos de una red física se le llama **MTU** (el MTU de ethernet es 1500 bytes por trama, la de FDDI es 4497 bytes por trama). Cuando un Datagrama pasa de una red a otra con un MTU menor a su tamaño es necesaria la fragmentación. A las diferentes partes de un Datagrama se les llama **fragmento**. Al proceso de reconstrucción del Datagrama a partir de sus fragmentos se le llama “Reensamblado de fragmentos”.

El control de la fragmentación de un Datagrama IP se realiza con los campos de la segunda palabra de su cabecera:

• **Identificación:** Numero de 16 bits que identifica al Datagrama, que permite implementar números de secuencias y que permite reconocer los diferentes fragmentos de un mismo Datagrama, pues todos ellos comparten este número.

• **Banderas:** Un campo de tres bits donde el primero está reservado.

El segundo, llamado bit de No - Fragmentación significa:

0 = Puede fragmentarse el Datagrama
1 = No puede fragmentarse el Datagrama

El tercer bit es llamado Más – Fragmentos y significa:

0 = Único fragmento o Ultimo fragmento
1 = aun hay más fragmentos

Cuando hay un 0 en más – fragmentos, debe evaluarse el campo “Desp. De Fragmento”: si este es cero, el Datagrama no está fragmentado, si es diferente de cero, el Datagrama es un último fragmento.

• **Desp. De Fragmento**: A un trozo de datos se le llama Bloque de Fragmento. Este campo indica el tamaño del desplazamiento en bloques de fragmento con respecto al Datagrama original, empezando por el cero.

Para finalizar con el tema de fragmentación, hay que mencionar el Plazo de Reensamblado, que es un time out que el Host destino establece como máximo para esperar por todos los fragmentos de un Datagrama. Si se vence y aun no llegan TODOS, entonces se descartan los que ya han llegado y se solicita el reenvío del Datagrama completo.

• **TTL:** Tiempo de Vida del Datagrama, campo que contiene un número inicial que va disminuyendo en una unidad, a medida que el datagrama atraviesa un router, para evitar que un datagrama no aceptado circule por la red indefinidamente. El datagrama se descarta cuando el TTL llega a 0.

• **Protocolo:** Especifica que protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos de Datagrama IP. Algunos valores posibles son:

1 = ICMP, 6 = TCP, 17 = UDP, 88 = IGRP (Protocolo de Enrutamiento de Pasarela Interior de CISCO).

• **Checksum:** Es un campo de 16 bits que se calcula haciendo el complemento a uno de cada palabra de 16 bits del encabezado, sumándolas y haciendo su complemento a uno. Esta suma hay que recalcularla en cada nodo intermedio debido a cambios en el TTL o por fragmentación.

• **Dirección IP de la Fuente**

• **Dirección IP del Destino**

• **Opciones IP:** Existen hasta 40 bytes extra en la cabecera del Datagrama IP que pueden llevar una o más opciones. Su uso es bastante raro.

_ Uso de Ruta Estricta (Camino Obligatorio)
_ Ruta de Origen Desconectada (Nodos Obligatorios)
_ Crear registro de Ruta
_ Marcas de Tiempo
_ Seguridad Básica del Ministerio de Defensa Seguridad Extendida del Ministerio de Defensa

21.- SUB-PROTOCOLOS DEL PROTOCOLO DE INTERNET (IP)

PROTOCOLO ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

El Protocolo de Mensajes de Control y Error de Internet ***se utiliza para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado***. ICMP proporciona así una comunicación entre una máquina y otra. Utiliza varios comandos de consola para realizar este control:

Comando PING

Podemos realizar cómodamente solicitudes ICMP de eco mediante la consola del sistema y el comando PING. Para ello abrimos la consola de comandos y tecleamos ping x.x.x.x, donde x.x.x.x es la dirección IP del host buscado. También podemos hacer ping a una dirección directamente, con lo que obtendremos además su dirección IP correspondiente.

```
C:\>ping www.yahoo.es

Haciendo ping a homerc.europe.yahoo.con [217.12.6.17] con 32 bytes de datos:

Respuesta desde 217.12.6.17: bytes=32 tiempo=262ms TTL=235
Respuesta desde 217.12.6.17: bytes=32 tiempo=266ms TTL=235
Respuesta desde 217.12.6.17: bytes=32 tiempo=264ms TTL=235
Respuesta desde 217.12.6.17: bytes=32 tiempo=266ms TTL=235

Estadísticas de ping para 217.12.6.17:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 262ms, Máximo = 266ms, Media = 264ms

C:\>
```

Se obtienen cuatro respuestas de eco ICMP con paquetes de 32 bits, que han tardado en realizar su camino entre el servidor de destino y nuestro ordenador 262-264-266 milisegundos. También muestra las estadísticas de las solicitudes de eco, que me dicen que los cuatro paquetes han llegado bien, y que la media de tiempo de llegada ha sido de 264 milisegundos.

Por su parte, el campo TLL indica el tiempo de vida de los paquetes enviados. Un TLL=235 significa que el paquete puede atravesar 235 routers en su camino

hasta el ordenador de destino. Cada router por el que pase irá disminuyendo en una unidad el valor del campo TLL, y cuando llega a cero el paquete se descarta, enviándose al origen un mensaje ICMP del tipo “Tiempo de espera agotado”.

Esto se hace para no tener paquetes dando vueltas indefinidamente.

```
C:\>ping 172.26.0.3

Haciendo ping a 172.26.0.3 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 172.26.0.3:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\>_
```

Podemos restringir entonces el campo de fallos haciéndonos PING a nosotros mismos, para ver si es nuestro host el que falla (las direcciones 127.X.X.X siempre hacen referencia a la propia máquina)

```
Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:

Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<10ms TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 0ms, máximo =  0ms, promedio =  0ms

C:\>_
```

Se puede obtener más información sobre el comando PING escribiendo el mismo en la consola de comandos, sin ninguna dirección IP asociada y ningún parámetro: **C:\>ping**

Comando TRACERT

Este comando envía mensajes ICMP (portando datagramas UDP) de solicitud de eco con diferentes valores de TLL (tiempos de vida), indicándonos con ellos los diferentes routers y host (generalmente servidores o proxys) que atraviesa

el paquete hasta llegar al host destino. Si en el camino el paquete se queda parado podremos averiguar en qué punto (router) se ha producido el fallo.
La sintaxis general de lo orden es:

C:>tracert www.servidor.com (tracert aaa.bbb.ccc.ddd)

```
C:\>TRACERT WWW.GOOGLE.ES

Traza a la dirección www.l.google.com [66.249.87.104]
sobre un máximo de 30 saltos:

  1    16 ms    <10 ms    16 ms  192.168.0.1
  2     *        47 ms    63 ms  10.7.159.1
  3    63 ms    187 ms    94 ms  148.Red-80-58-8.pooles.rima-tde.net [80.58.8.148
]
  4     *        63 ms    62 ms  121.Red-80-58-75.pooles.rima-tde.net [80.58.75.1
21]
  5     *        63 ms    78 ms  97.Red-81-46-1.poolcs.rima-tdc.net [81.46.1.97]

  6     *        78 ms    63 ms  106.Red-80-58-72.pooles.rima-tde.net [80.58.72.1
06]
  7     *        63 ms    62 ms  18.Red-80-58-74.pooles.rima-tde.net [80.58.74.18
]
  8     *        63 ms    62 ms  GE4-0-0-0-grtmadrr1.red.telefonica-wholesale.net
 [213.140.51.9]
  9     *       110 ms   109 ms  So6-0-0-0-grtlontl1.red.telefonica-wholesale.net
 [213.140.38.26]
 10     *        94 ms   266 ms  195.66.224.125
 11   110 ms    109 ms   109 ms  66.249.87.104
```

Puede darse el caso de que el proxy o el router que nos saca a Internet tenga deshabilitado el uso de traceado a través de ellos. En estos casos obtendremos el tracert siguiente:

```
C:\>tracert www.yahoo.es

Traza a la dirección homerc.europe.yahoo.com [217.12.6.16]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  172.26.0.1
  2     *        *        *     Tiempo de espera agotado para esta solicitud.
  3     *        *        *     Tiempo de espera agotado para esta solicitud.
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5     *        *        *     Tiempo de espera agotado para esta solicitud.
  6     *        *     ^C
```

Donde podemos apreciar que los paquetes llegan hasta el router de salida, pero se quedan ahí, debido a que está configurado para no aceptar paquetes ICMP tipo 0, es decir, de respuesta de eco.

Existen numerosos programas que nos permiten realizar comandos TRACERT de forma gráfica, mostrándonos en un mapa mundial la ruta que siguen los mensajes ICMP de petición de ECO desde nuestra máquina a la de destino.

PROTOCOLO ARP (ADDRESS RESOLUTION PROTOCOL)

El protocolo de resolución de direcciones es el responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas.

ARP es el protocolo usado por IP para mapear o resolver direcciones de red IP, con las direcciones de hardware o físicas. El protocolo ARP se suele implementar como parte de los drivers de las tarjetas de red o NICs (Network Interface Cards).

En el caso de Ethernet la dirección hardware se llama MAC (Medium Access Control) y es un número de 48 bits que puede representarse mediante 12 caracteres hexadecimales. Un ejemplo de MAC es: 00-90-27-BF-AC-E9. El MAC es único en el mundo y se almacena en una memoria PROM que lleva toda tarjeta Ethernet.

```
C:\>arp -a  192.168.0.1

Interfaz: 192.168.0.11 on Interface 0x1000003
  Dirección IP          Dirección física      Tipo
  192.168.0.1           00-a0-c5-ee-8a-64     dinámico

C:\>
```

En la figura se muestra la sintaxis para ejecutar este protocolo y la resolución de una dirección física partiendo de una dirección IP.
Tecleando en la consola C:\>**ARP** podemos obtener más información de cómo funciona este protocolo.

```
C:\>ARP

Muestra y modifica las tablas de conversión de direcciones IP en direcciones
físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a            Pide los datos de protocolo actuales y muestra las
                entradas ARP actuales. Si se especifica inet_addr, sólo se
                muestran las direcciones IP y física del equipo especificado.
                Si existe más de una interfaz de red que utilice ARP, se
                muestran las entradas de cada tabla ARP.
  -g            Igual que -a.
  inet_addr     Especifica una dirección de Internet.
  -N if_addr    Muestra las entradas ARP para la interfaz de red especificada
                por if_addr.
  -d            Elimina el host especificado por inet_addr. inet_addr puede
                incluir el carácter comodín * (asterisco) para eliminar todos
                los hosts.
  -s            Agrega el host y asocia la dirección de Internet inet_addr
                con la dirección física eth_addr. La dirección física se
                indica como 6 bytes en formato hexadecimal, separados por
                guiones. La entrada es permanente.
  eth_addr      Especifica una dirección física.
  if_addr       Si está presente, especifica la dirección de Internet de la
                interfaz para la que se debe modificar la tabla de conversión
                de direcciones. Si no está presente, se utilizará la primera
                interfaz aplicable.
Ejemplo:
  > arp -s 157.55.85.212  00-aa-00-62-c6-09  .... Agrega una entrada estática
  > arp -a                                   .... Muestra la tabla arp.

C:\>
```

22.- EL PROTOCOLO TCP

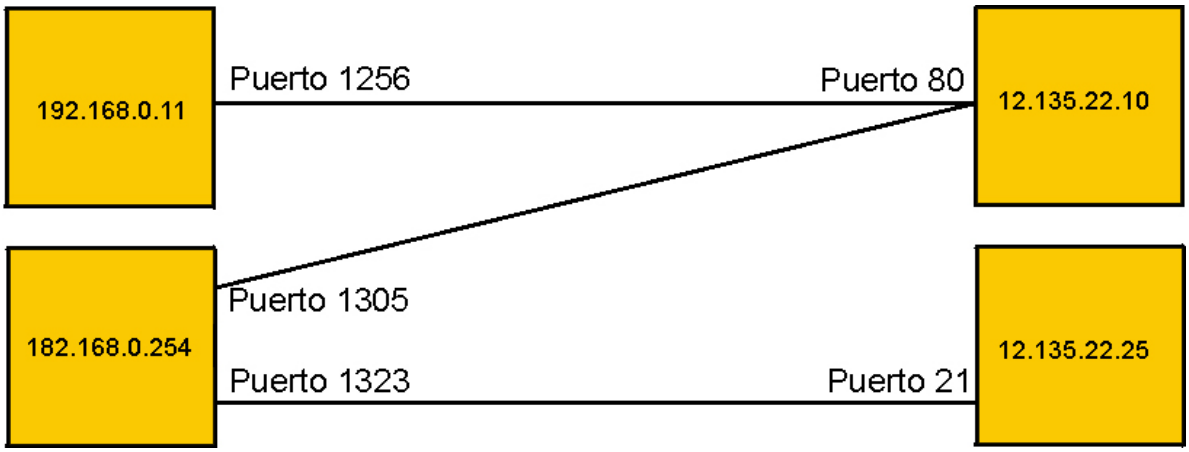
El protocolo TCP (Transmission Control Protocol, Protocolo de Control de Transmisión) está basado en IP que es no fiable y no orientado a conexión, y sin embargo es:

- **Orientado a conexión.** Es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

- **Fiable.** La información que envía el emisor llega de forma correcta al destino. El protocolo TCP permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

- **El flujo de datos entre una aplicación y otra viajan por un circuito virtual.** Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los routers intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logre la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro. Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados.

La unidad de datos del protocolo es el **byte**, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes. Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un **segmento** y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.



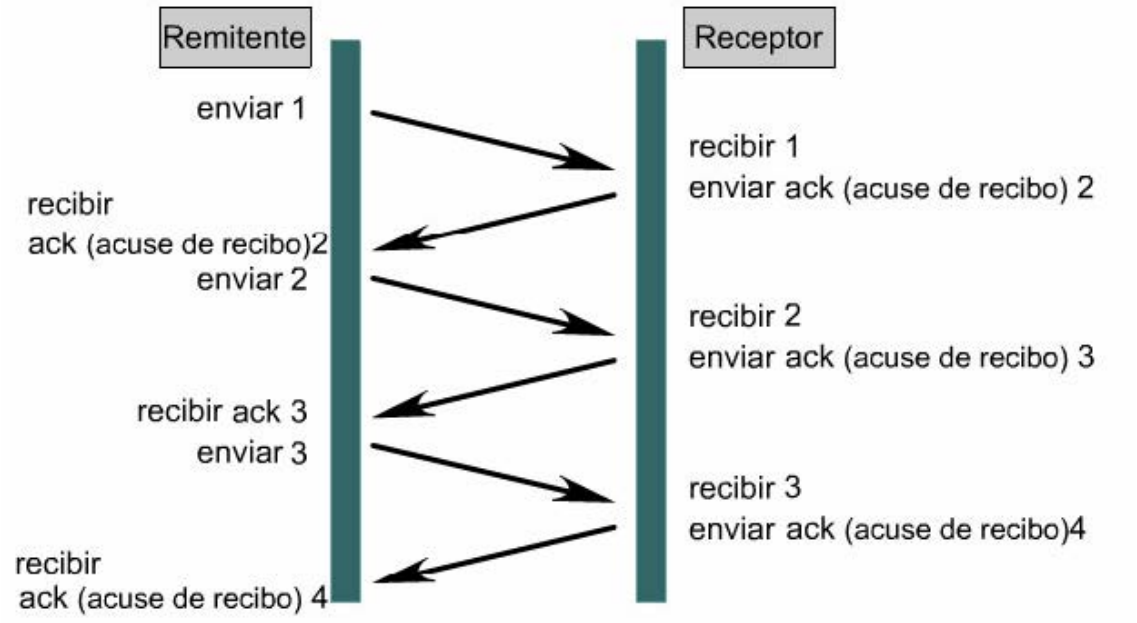
El protocolo TCP envía un flujo de información no estructurado. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando. **Las conexiones que abre una aplicación de una máquina para comunicarse con otra aplicación de otra máquina se denominan puertos.**

Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-duplex.

En los servidores Novell® NetWare la función de TCP la hace el protocolo SPX, de análogo funcionamiento.

Las direcciones IP permiten el enrutamiento de los paquetes entre las redes. Sin embargo, IP no garantiza la entrega. La capa de transporte es responsable del transporte confiable y de la regulación del flujo de datos desde el origen hacia el destino. Esto se logra utilizando ventanas deslizantes y números de secuencia junto con un proceso de sincronización que garantiza que cada host se encuentra listo y desea comunicarse.

Para comprender la confiabilidad y el control de flujo, piense en un estudiante que ha estudiado un idioma extranjero durante un año. Ahora imagine que este estudiante visita un país donde se habla ese idioma. Durante las conversaciones, deberá pedirle a la gente que repita lo que ha dicho (para confiabilidad) y que hable despacio, para que pueda entender las palabras (control de flujo). La capa de transporte, la Capa 4 del modelo OSI, provee estos servicios a la capa 5 por medio de TCP.



TCP es un protocolo **orientado a conexión**. Antes de transmitir datos, los dos clientes que desean comunicarse deben llevar a cabo un proceso de sincronización para establecer una conexión virtual para cada sesión entre ellos. Este proceso de sincronización asegura que ambas partes están listas para la transmisión y permite que los dispositivos determinen los números de la secuencia inicial de dicha sesión.

Este proceso se llama saludo de tres vías, es un proceso de tres pasos para establecer una conexión virtual entre dos dispositivos. Es muy importante saber que este proceso lo inicia un cliente. Para establecer la sesión TCP, el cliente usa un puerto conocido del servicio que desea contactar.

A menudo, la cantidad de datos que se necesita transmitir es demasiado grande como para ser enviada en un solo segmento de datos. En este caso, los datos deben dividirse en porciones de menor tamaño para permitir su correcta transmisión. TCP tiene la responsabilidad de dividir los datos en segmentos. Esto se puede comparar con la forma en que son alimentados los niños pequeños. Su comida se corta en pedazos más pequeños que sus bocas pueden acomodar.

Además, es posible que las máquinas receptoras no sean capaces de recibir datos con la rapidez que el origen los envía, tal vez, porque el dispositivo receptor está ocupado con otras tareas o porque el transmisor simplemente es un dispositivo más robusto.

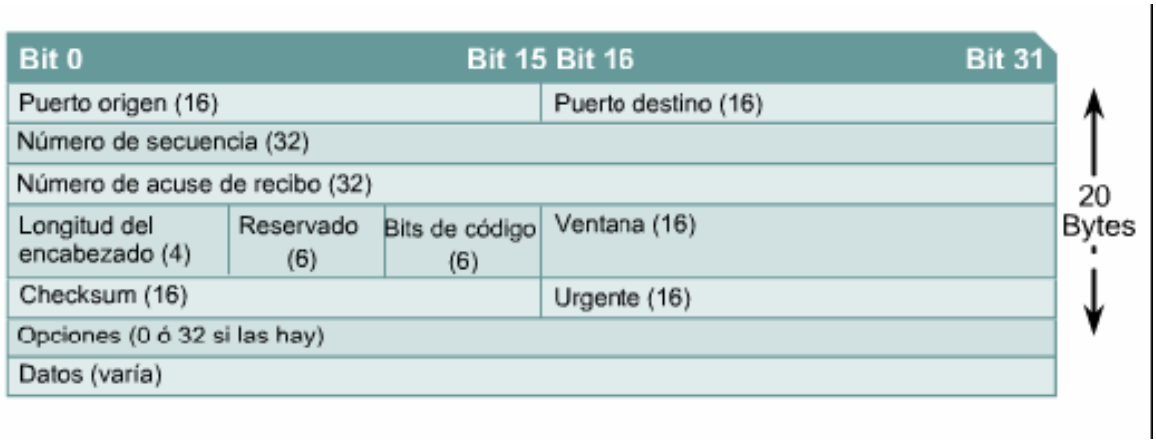
Una vez segmentados los datos, deben transmitirse hacia el dispositivo destino. Uno de los servicios que provee TCP es el **control de flujo** que regula la cantidad de datos enviada durante un período de transmisión dado. Este proceso de control de flujo se conoce como **uso de ventanas.**

El **tamaño de la ventana** *determina la cantidad de datos que se pueden transmitir simultáneamente antes que el destino responda con un Acuse de recibo (ACK).* Después que un host transmita el tamaño de ventana en bytes, el host debe recibir un ACK indicando que la información se recibió antes de poder enviar más información. Por ejemplo, si la ventana es de 1, se debe generar un ACK por cada byte antes de enviar el siguiente.

TCP usa las ventanas para determinar de forma dinámica el tamaño de la transmisión. Los dispositivos negocian el tamaño de la ventana a un número específico de bytes para transmitir antes del ACK.

Este proceso de variación dinámica del tamaño de la ventana incrementa la confiabilidad. El tamaño de la ventana se puede basar en los ACKs.

23.- EL SEGMENTO TCP



El Protocolo para el control de la transmisión (TCP) es un protocolo de Capa 4 orientado a conexión que suministra una transmisión de datos full-duplex confiable. TCP forma parte de la pila del protocolo TCP/IP. En un entorno orientado a conexión, se establece una conexión entre ambos extremos antes de que se pueda iniciar la transferencia de información.

TCP es responsable por la división de los mensajes en segmentos, reensamblándolos en la estación destino, reenviando cualquier mensaje que no se haya recibido y reensamblando mensajes a partir de los segmentos. TCP suministra un circuito virtual entre las aplicaciones del usuario final.

Los protocolos que usan TCP incluyen:

- FTP (Protocolo de transferencia de archivos)
- HTTP (Protocolo de transferencia de hipertexto)
- SMTP (Protocolo simple de transferencia de correo)
- Telnet

Las siguientes son las definiciones de los campos de un segmento TCP:

- **Puerto origen:** El número del puerto que realiza la llamada.
- **Puerto destino:** El número del puerto al que se realiza la llamada.

• **Número de secuencia:** El número que se usa para asegurar el secuenciamiento correcto de los datos entrantes.

• **Número de acuse de recibo:** Siguiente octeto TCP esperado.

• **HLEN:** La cantidad de palabras de 32 bits del encabezado.

• **Reservado:** Establecido en cero.

• **Bits de código:** Funciones de control, como configuración y terminación de una sesión.

• **Ventana:** La cantidad de octetos que el emisor está dispuesto a aceptar.

• **Checksum (suma de comprobación):** Suma de comprobación calculada a partir de los campos del encabezado y de los datos.

• **Indicador de mensaje urgente:** Indica el final de la transmisión de datos urgentes.

• **Opción:** Una opción definida actualmente, tamaño máximo del segmento TCP.

• **Datos:** Datos de protocolo de capa superior.

24.- EL PROTOCOLO UDP

La pila del protocolo TCP/IP contiene muchos protocolos diferentes, cada uno diseñado para realizar una tarea determinada. IP provee transporte de Capa 3 no orientado a conexión a través de una internetwork. TCP permite la transmisión confiable, orientada a conexión de los paquetes en la Capa 4 del modelo OSI. **UDP proporciona la transmisión de paquetes no orientado a conexión y no confiable de los paquetes en la Capa 4 del modelo OSI.**

Tanto TCP como UDP utilizan IP como protocolo subyacente de Capa 3. Además, distintos protocolos de capa de aplicación utilizan TCP y UDP.

El protocolo UDP (User Datagram Protocol,Protocolo de Datagrama de Usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. Al igual que el protocolo IP, UDP es:

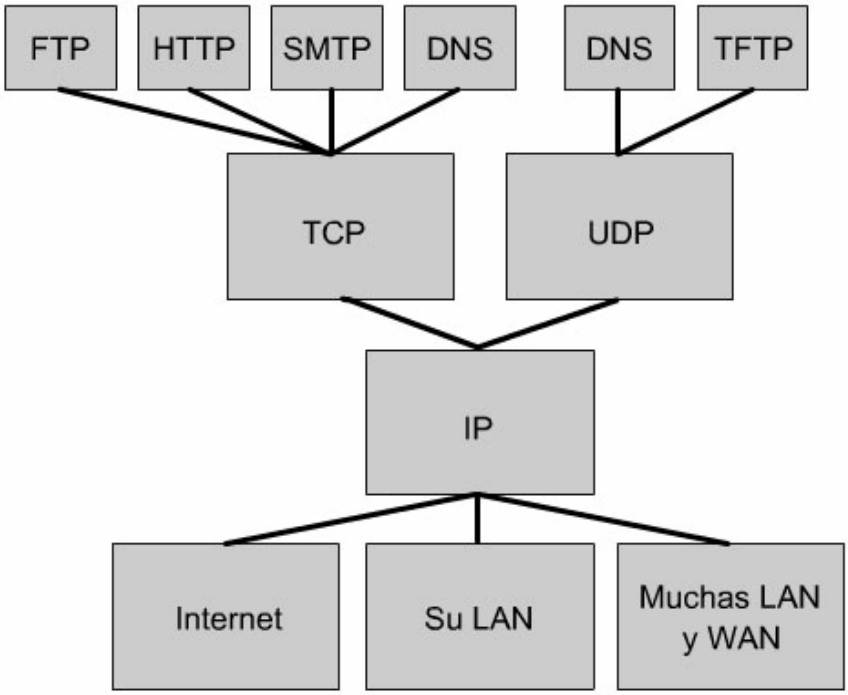
- **No orientado a conexión**. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino.

- **No fiable.** Los mensajes UDP se pueden perder o llegar dañados.

- **UDP utiliza el protocolo IP para transportar sus mensajes.** Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos (conexiones entre aplicaciones) origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.

TCP provee servicios para aplicaciones tales como FTP, HTTP, SMTP y DNS.

UDP es el protocolo de capa de transporte utilizado por DNS, TFTP, SNMP y DHCP.



TCP debe utilizarse cuando las aplicaciones requieren la garantía de que un paquete llegue intacto, en secuencia y sin duplicar. El encabezado que se asocia con garantizar la entrega del paquete, a veces, se convierte en un problema al utilizar TCP. No todas las aplicaciones necesitan garantizar la entrega del paquete de datos, por lo tanto, utilizan un mecanismo de entrega no orientado a conexión, más rápido, que aporta el UDP. El estándar del protocolo UDP, que se describe en RFC 768, es un protocolo simple que intercambia segmentos sin acuses de recibo ni entrega garantizada.

UDP no hace uso de ventanas ni acuses de recibo de modo que los protocolos de capa de aplicación deben brindar la detección de errores.

Número de Bits	16	16	16	16	16
	Puerto origen	Puerto destino	Longitud	Checksum	Datos...

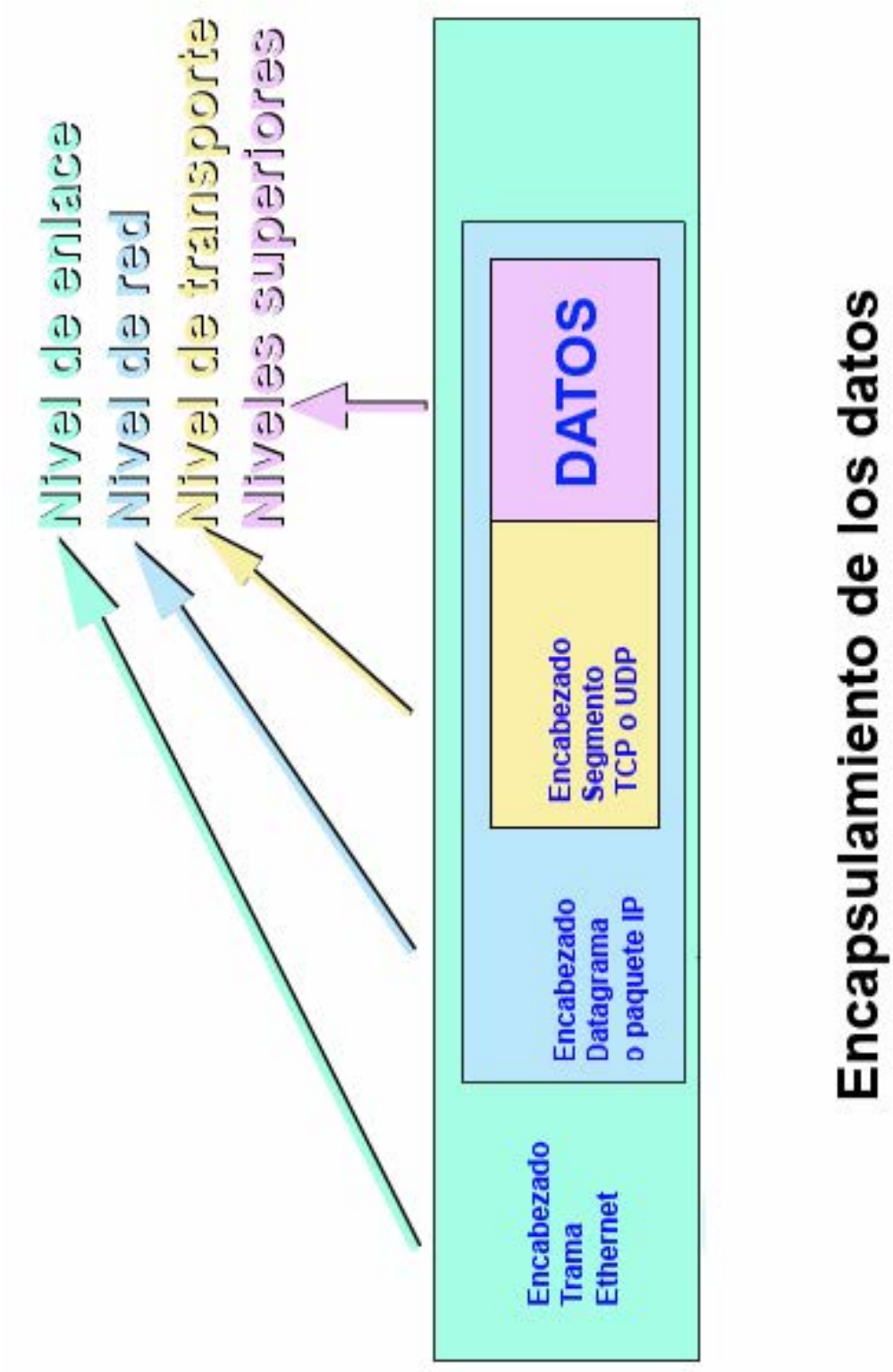
• **Puerto de origen:** es un campo optativo que sólo se utiliza si la información debe regresar al host transmisor. Cuando un router destino recibe una actualización de enrutamiento, el router origen no solicita nada, de modo que nada debe regresar a la fuente. No existe intercambio de información o datos alguno.

• **Puerto de destino:** especifica la aplicación a la que UDP necesita pasar el protocolo. Una petición DNS proveniente de un host hacia un servidor DNS suele tener un campo Puerto destino de 53, el número de puerto de UDP para DNS.

• **Longitud:** identifica el número de octetos de un segmento UDP.

• **Checksum:** es optativo pero debería utilizarse para garantizar que no se han dañado los datos durante la transmisión. Para el transporte a través de la red, UDP se encapsula en el paquete IP.

Una vez que el segmento UDP llega a la dirección IP destino, debe haber un mecanismo que permita que el host receptor determine la exacta aplicación en destino. Para este fin se utilizan los puertos destino. Si un host provee servicios de TFTP y DNS, debe ser capaz de determinar cuál es el servicio que necesitan los segmentos UDP que llegan. El campo del Puerto destino del encabezado UDP determina la aplicación hacia la que se enviará el segmento UDP.



Encapsulamiento de los datos

26.- PUERTO DE RED

Un **puerto de red** es una interfaz para comunicarse con un programa a través de una red. Un puerto suele estar numerado. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite a una máquina establecer simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes.

Los números de puerto se indican mediante una palabra, **2 bytes (16 bits), por lo que existen 65535**. Aunque podemos usar cualquiera de ellos para cualquier protocolo, existe una entidad, la IANA, encargada de su asignación, la cual creó tres categorías:

1. Los puertos **inferiores al 1024** son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos". Si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.

2. Los **comprendidos entre 1024 y 49151** (0400 y BFFF en hexadecimal) son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista pública en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos.

3. Los **comprendidos entre los números 49152 y 65535** (C000 y FFFF en hexadecimal) son denominados dinámicos o privados, porque son los usados por el sistema operativo cuando una aplicación tiene que conectarse a un servidor y por tanto necesita un puerto por donde salir.

Un ejemplo fácil de comprender, lo tenemos en cuando nuestro navegador solicita una página a un servidor web. Nuestro navegador al solicitar dicha petición, le envía al servidor web remoto, una solicitud – señal a través del puerto 80 del PC remoto. Una vez recibida esta solicitud el servidor remoto, enviar la información solicitada.

La responsabilidad para la asignación de los puertos públicos (servicios más utilizados como FTP, WWW, Telnet, …) la tiene la Autoridad de asignación de numero de Internet (**IANA Internet Assigned Numbers Authority**). La relación entre identificadores de puertos (número de puertos) y el tipo de servicio que hacen uso (servicio) quedó establecido en el **RFC Assgined Numbers**.

No todos los puertos se utilizan para dar un determinado tipo de servicio de transferencia de información. **Ciertos puertos son utilizados para proporcionar pruebas de comunicación, depuración o mediciones**. Tal es el caso del servicio “echo” que tiene el puerto 7 como identificador predefinido. El servicio “Echo” se encarga de chequear el estado de una conexión devolviendo cualquiera de los datagramas que se le envía.

Deshabilitar los puertos que no utilicemos

Es muy importante **deshabilitar aquellos puertos que no vayamos a utilizar o que no deseemos que sean utilizados por aplicaciones innecesarias**. El cortafuegos a menudo nos avisa de si queremos utilizar un puerto antes de establecer una comunicación, pero otras veces los deberemos de deshabilitar a mano.

Algunos de los puertos a los que nos debemos cuidar de que permanezcan cerrados son:

Puertos, 137, 138, 139.
Identifican servicios del protocolo NetBios de Windows. NetBios es un protocolo de red, que se encarga de permitir compartir archivos e impresoras conectados a una red. No es necesario tener habilitado y escuchando a NetBios ni nuestro equipo no pertenece a una determinada red en la que compartamos archivos o donde mandemos a imprimir documentos en una impresora compartida.

Para cerrar estos puertos deberemos seguir el siguiente procedimiento:

1. Abrimos las propiedades de nuestra conexión de red. Panel de control – Conexiones de red – Botón derecho sobre la conexión de área local que utilicemos

2. En propiedades del protocolo TCP / IP, abrimos la pestaña “Opciones avanzadas”

3. En esta última pestaña, seleccionamos a su vez la pestaña WINS

4. Por último, seleccionaremos la opción “Deshabilitar NetBios” en la zona de “Configuración de NetBios”

Una vez hecho esto, Windows nos pedirá reiniciar para establecer los nuevos cambios.

Es necesario mantener cerrados los puertos que se utilicen puesto que existen muchas “vulnerabilidades” ó fallos de seguridad en los programas que hacen uso de la red. Estos fallos de seguridad pueden y son utilizados por otras personas para tomar control de un PC remoto o para obtener, modificar o introducir archivos ó información privada ó maliciosa.

Por lo tanto, lo mas recomendable, es mantener sólo abiertos aquellos servicios que nos resulten imprescindibles y utilicemos a menudo, como por ejemplo el navegador.

Los estados de un puerto de red

Un puerto de red puede adoptar los siguientes estados:

- **Abierto.** El puerto puede recibir conexiones. Un pequeño programa, conocido como "servidor", se encuentra continuamente escuchando a la espera de recibir peticiones para establecer una comunicación e intercambiar datos con otro PC remoto.

- **Cerrado.** Las conexiones se rechazan. En este caso es probable que no exista ninguna aplicación escuchando por ese puerto o no se permite el acceso por algún motivo concreto. A este estado se le considera como el comportamiento normal del sistema operativo.

- **Bloqueado o sigilosos.** En este estado no es posible saber si el ordenador esta conectado. Se le considera como el estado ideal. A menudo este estado se debe a la existencia de un cortafuegos o simplemente a que el ordenador se encuentra apagado.

Ejemplos de puertos y los servicios que utilizan

Vamos a señalar los servicios más significativos y su relación numérica que es utilizada para el establecimiento de una comunicación remota.

- Echo. 7. Utilizado como ya se ha comentado para pruebas. Este puerto también puede ser utilizado por usuarios maliciosos. Se recomienda bloquearlo.

- Svstat 11. Proporciona información del sistema PC así como conexiones, procesos activos, carga del sistema, … Recomendado su cierre.

- Chargen. 19. También utilizado para pruebas. Puede ser utilizado para provocar problemas al PC afectado. Cerrar

- FTP. 20. Permite subir o descargar archivos de un servidor FTP.

- Telnet. 23. Permite establecer conexiones con ordenadores remotos y utilizar su sistema y linea de comandos. Es una forma de utilizar un PC remoto, utilizandolo como si estuvieramos sentados delante de él y utlizando su línea de comandos.

- Smtp. 25. .Se recomienda "filtrar" este puerto y mantener siempre la última versión de cualquier programa de correo, especialmente si

trabajamos con sendmail, servicio que ha sido muy explotado para acceder a información sensible de PCs remotos.

- Time. 37. Permite conocer la hora de un sistema remoto.

Elementos para conocer el estado y las características de un puerto de red

Existen una serie de aplicaciones de diverso tipo y características que nos van a permitir conocer el estado de los puertos. Con su uso se nos va a dar a conocer si nuestro sistema es vulnerable a ataques remotos a través de puertos abiertos o si alguna aplicación maliciosa como un caballo de Troya esta utilizando nuestros servicios sin que nosotros tengamos noticia de ello.

Por último, se proporciona una dirección donde conocer diferentes tipos de escaneadores de puertos que te permitirán establecer el estado de los mismos en tu PC. La URL es :

http://www.adslayuda.com/test-scan.html

27.- anexo. SERVICIO_PUERTO_PROTOCOLO

C:\WINDOWS\system32\drivers\etc\services

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Este archivo contiene números de puerto para los servicios más conocidos
# tal y como están definidos por RFC 1700 (Assigned Numbers).
#
#
# Formato:
#
# <nombre de servicio> <número de puerto>/<protocolo> [alias...] [#<comentario>]
#

echo                 7/tcp
echo                 7/udp
discard              9/tcp    sink null
discard              9/udp    sink null
systat              11/tcp    users                 #Usuarios activos
systat              11/tcp    users                 #Usuarios activos
daytime             13/tcp
daytime             13/udp
qotd                17/tcp    quote                 #Cuota del día
qotd                17/udp    quote                 #Cuota del día
chargen             19/tcp    ttytst source         #Generador del carácter
chargen             19/udp    ttytst source         #Generador del carácter
ftp-data            20/tcp                          #FTP, datos
ftp                 21/tcp                          #FTP. control
telnet              23/tcp
smtp                25/tcp    mail                  #Protocolo simple de
                                                     transferencia de correo (SMTP)
time                37/tcp    timserver
time                37/udp    timserver
rlp                 39/udp    resource              #Protocolo de ubicación del
                                                     recurso
nameserver          42/tcp    name                  #Servidor del nombre host
nameserver          42/udp    name                  #Servidor del nombre host
nicname             43/tcp    whois
domain              53/tcp                          #Servidor de nombre-dominio
domain              53/udp                          #Servidor de nombre-dominio
bootps              67/udp    dhcps                 #Servidor del protocolo de
                                                     inicio del sistema
bootpc              68/udp    dhcpc                 #Servidor del protocolo de
                                                     inicio del sistema
tftp                69/udp                          #Transferencia de archivos
                                                     trivial
gopher              70/tcp
finger              79/tcp
http                80/tcp    www www-http          #World Wide Web
kerberos-sec        88/tcp    krb5                  #Kerberos
```

```
kerberos-sec     88/udp    krb5                 #Kerberos
hostname        101/tcp    hostnames            #Servidor del nombre host NIC
iso-tsap        102/tcp                         #ISO-TSAP Clase 0
rtelnet         107/tcp                         #Servicio Telnet remoto
pop2            109/tcp    postoffice           #Protocolo de oficina de
                                                 correos: versión 2
pop3            110/tcp                         #Protocolo de oficina de
                                                 correos: versión 3

sunrpc          111/tcp    rpcbind portmap      #Llamada de procedimiento remoto
                                                 SUN
sunrpc          111/udp    rpcbind portmap      #Llamada de procedimiento remoto
                                                 SUN
auth            113/tcp    ident tap            #Protocolo de identificación
uucp-path       117/tcp
nntp            119/tcp    usenet               #Protocolo de transferencia de
                                                 noticias a través de la red
ntp             123/udp                         #Protocolo de tiempo de red
epmap           135/tcp    loc-srv              #Resolución del extremo DCE
epmap           135/udp    loc-srv              #Resolución del extremo DCE
netbios-ns      137/tcp    nbname               #Servicio de nombre NETBIOS
netbios-ns      137/udp    nbname               #Servicio de nombre NETBIOS
netbios-dgm     138/udp    nbdatagram           #Servicio de datagramas NETBIOS
netbios-ssn     139/tcp    nbsession            #Servicio de sesión NETBIOS
imap            143/tcp    imap4                #Protocolo de acceso de mensajes
                                                 de Internet
pcmail-srv      158/tcp                         #Servidor PCMail
snmp            161/udp                         #SNMP
snmptrap        162/udp    snmp-trap            #Captura SNMP
print-srv       170/tcp                         #Red PostScript
bgp             179/tcp                         #Protocolo de puerta de enlace
                                                 de borde
irc             194/tcp                         #Protocolo IRC (Internet Relay
                                                 Chat)
ipx             213/udp                         #IPX para IP
ldap            389/tcp                         #Protocolo de acceso al
                                                 directorio de peso ligero
https           443/tcp    MCom
https           443/udp    MCom
microsoft-ds    445/tcp
microsoft-ds    445/udp
#? kpasswd      464/tcp                         # Kerberos (v5)
#? kpasswd      464/udp                         # Kerberos (v5)
isakmp          500/udp    ike                  #Intercambio de claves de
                                                 Internet
exec            512/tcp                         #Ejecución del proceso remoto
biff            512/udp    comsat
login           513/tcp                         #Inicio de sesión remoto
who             513/udp    whod
cmd             514/tcp    shell
syslog          514/udp
printer         515/tcp    spooler
talk            517/udp
ntalk           518/udp
efs             520/tcp                         #Servidor de nombres de archivos
                                                 extendido
router          520/udp    route routed
timed           525/udp    timeserver
tempo           526/tcp    newdate
courier         530/tcp    rpc
conference      531/tcp    chat
```

```
netnews          532/tcp    readnews
netwall          533/udp                        #Para emisiones de emergencia
uucp             540/tcp    uucpd
klogin           543/tcp                        #Kerberos
kshell           544/tcp    krcmd               #Kerberos shell remoto
new-rwho         550/udp    new-who
remotefs         556/tcp    rfs rfs_server
rmonitor         560/udp    rmonitord
monitor          561/udp
ldaps            636/tcp    sldap               #LDAP para TLS/SSL
doom             666/tcp                        #Software del Id. Doom
doom             666/udp                        #Software del Id. Doom
kerberos-adm     749/tcp                        #Administración Kerberos
kerberos-adm     749/udp                        #Administración Kerberos
kpop            1109/tcp                        #Kerberos POP
phone           1167/udp                        #Llamada de conferencia
ms-sql-s        1433/tcp                        #Microsoft-SQL-Server
ms-sql-s        1433/udp                        #Microsoft-SQL-Server
ms-sql-m        1434/tcp                        #Microsoft-SQL-Monitor
ms-sql-m        1434/udp                        #Microsoft-SQL-Monitor
wins            1512/tcp                        #Servicios de nombres Internet
                                                 de Microsoft Windows (WINS)
wins            1512/udp                        #Servicios de nombres Internet
                                                 de Microsoft Windows (WINS)
ingreslock      1524/tcp    ingres
l2tp            1701/udp                        #Protocolo de túnel capa 2
pptp            1723/tcp                        #Protocolo de túnel punto a
                                                 punto
radius          1812/udp                        #Protocolo  de autenticación
                                                 RADIUS
radacct         1813/udp                        #Protocolo de gestión de cuentas
                                                 RADIUS
nfsd            2049/udp    nfs                 #Servidor NFS
knetd           2053/tcp                        #Desmultiplexor Kerberos
ttcp            5001/tcp                        #TTCP
ttcp            5001/udp                        #TTCP
man             9535/tcp                        #Servidor remoto MAN
```

28.- PROTOCOLO RPC

Una de las funciones del Nivel de Sesión es controlar los diálogos entre dos entidades que se estén comunicando, y definir los mecanismos para hacer las Llamadas a Procedimientos Remotos (RPC).

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el trasporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

El RPC (del inglés Remote Procedure Call, Llamada a Procedimiento Remoto) es un protocolo que ***permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.***

El protocolo fue propuesto inicialmente por Sun Microsystems como un gran avance sobre los sockets usados hasta el momento. De esta manera el programador no tenía que estar pendiente de las comunicaciones, estando éstas encapsuladas dentro de las RPC.

Las RPC son muy utilizadas dentro del sistema cliente-servidor. Siendo el cliente el que inicia el proceso solicitando al servidor que ejecute cierto procedimiento o función y enviando éste de vuelta el resultado de dicha operación al cliente.

29.- PROTOCOLOS DE APLICACIÓN

PROTOCOLO HTTP (Hypertext Transfer Protocol)

El Protocolo de Transferencia de Hipertexto *(Hypertext Transfer Protocol)* es un sencillo protocolo cliente-servidor que ***articula los intercambios de información entre los clientes Web y los servidores HTTP***. La especificación completa del protocolo HTTP 1/0 está recogida en el RFC 1945. Fue propuesto por Tim Berners-Lee, atendiendo a las necesidades de un sistema global de distribución de información como el World Wide Web.

Desde el punto de vista de las comunicaciones, está soportado sobre los servicios de conexión **TCP/IP**, y funciona de la misma forma que el resto de los servicios comunes de los entornos UNIX: un proceso servidor escucha en un puerto de comunicaciones TCP (por defecto, el 80), y espera las solicitudes de conexión de los clientes Web. Una vez que se establece la conexión, el protocolo TCP se encarga de mantener la comunicación y garantizar un intercambio de datos libre de errores.

HTTP se basa en sencillas operaciones de solicitud/respuesta. Un cliente establece una conexión con un servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que contiene el estado de la operación y su posible resultado. Todas las operaciones pueden adjuntar un **objeto o recurso** sobre el que actúan; cada objeto Web (documento HTML, fichero multimedia o aplicación).

Etapas de una transacción HTTP

Cada vez que un cliente realiza una petición a un servidor, se ejecutan los siguientes pasos:

a) Un usuario accede a una URL, seleccionando un enlace de un documento HTML o introduciéndola directamente en el campo *Dirección* del cliente Web.

b) El cliente Web descodifica la URL, separando sus diferentes partes. Así identifica el protocolo de acceso, la dirección DNS o IP del servidor, el posible puerto opcional (el valor por defecto es 80) y el objeto requerido del servidor.

c) Se abre una conexión TCP/IP con el servidor, llamando al puerto TCP correspondiente.

d) Se realiza la petición. Para ello, se envía la dirección del objeto requerido (el contenido de la URL que sigue a la dirección del servidor), la versión del protocolo HTTP empleada (casi siempre HTTP/1.0) y un conjunto variable de información, que incluye datos sobre las capacidades del navegador datos opcionales para el servidor etc.

e) El servidor devuelve la respuesta al cliente. Consiste en un código de estado y el tipo de dato MIME de la información de retorno, seguido de la propia información.

f) Se cierra la conexión TCP.

Este proceso se repite en cada acceso al servidor HTTP. Por ejemplo, si se recoge un documento HTML en cuyo interior están insertadas cuatro imágenes, el proceso anterior se repite cinco veces, una para el documento HTML y cuatro para las imágenes.

En la actualidad se ha mejorado este procedimiento, permitiendo que una misma conexión se mantenga activa durante un cierto periodo de tiempo, de forma que sea utilizada en sucesivas transacciones. Este mecanismo, denominado *HTTP Keep Alive,* es empleado por la mayoría de los clientes y servidores modernos. Esta mejora es imprescindible en una Internet saturada, en la que el establecimiento de cada nueva conexión es un proceso lento y costoso.

PROTOCOLO FTP (File Transfer Protocol)

Una de las alternativas más importantes que nos permite Internet es la ***transferencia de archivos de un ordenador a otro*** desde cualquier parte del mundo. Para ello utilizamos el protocolo de transferencia de archivos o FTP (file transfer protocol).

Mediante FTP podemos compartir (recibir y enviar) nuestros ficheros con otros ordenadores, siempre que el administrador de estos últimos nos lo permita.
La copia de ficheros de una máquina a otra es una de las operaciones más frecuentes. La transferencia de datos entre cliente y servidor puede producirse en cualquier dirección. El cliente puede enviar o pedir un fichero al servidor.

Para acceder a ficheros remotos, el usuario debe identificarse al servidor. En este punto el servidor es responsable de autentificar al cliente antes de permitir la transferencia de ficheros.

Desde el punto de vista de un usuario de FTP, el enlace está orientado a conexión. En otras palabras, es necesario que ambos hosts estén activos y ejecutando TCP/IP para establecer una transferencia de ficheros.

Descripción de FTP

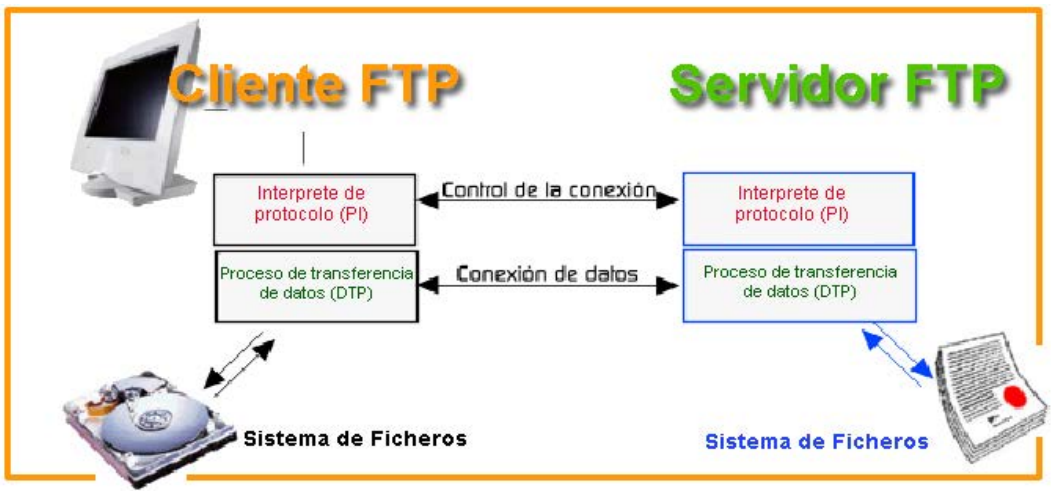
FTP usa **TCP** como protocolo de transporte para proporcionar conexiones fiables entre los extremos. Se emplean dos conexiones:

la *primera* es para el *login* y sigue el protocolo TELNET

la *segunda* es para gestionar la transferencia de datos

Como es necesario hacer un login en el host remoto, el usuario debe tener un nombre de usuario y un password para acceder a ficheros y a directorios. El usuario que inicia la conexión asume la función de cliente, mientras que el host remoto adopta la función de servidor.

En ambos extremos del enlace, la aplicación FTP se construye con intérprete de protocolo (PI), un proceso de transferencia de datos, y una interfaz de usuario.

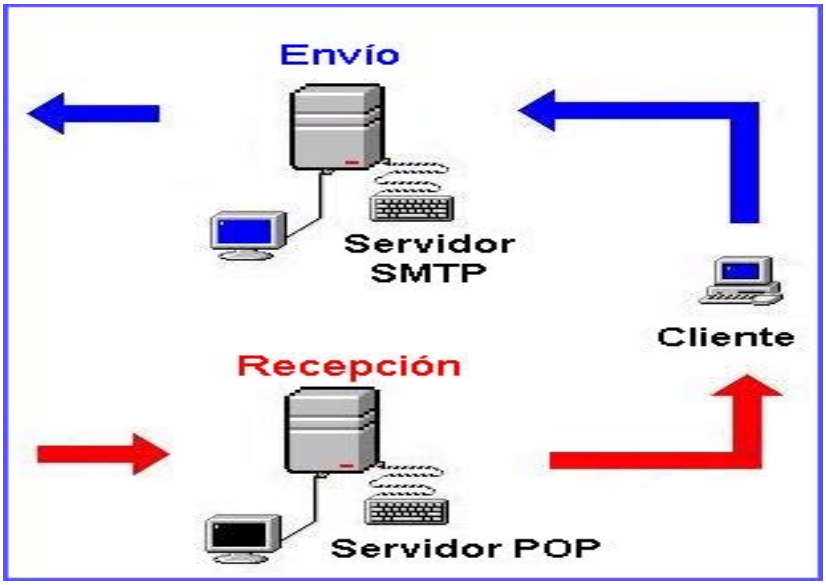


La interfaz de usuario se comunica con el PI, que está a cargo del control de la conexión. Este intérprete de protocolo ha de comunicar la información necesaria a su propio sistema de archivos.

En el otro extremo de la conexión, el PI ha de iniciar la conexión de datos. Durante la transferencia de ficheros, los DTPs se ocupan de gestionar la transferencia de datos. Una vez que la operación del usuario se ha completado, el PI ha de cerrar la conexión de control.

PROTOCOLO POP (Post Office Protocol)

El protocolo POP (Protocolo de oficina de correo) permite a los clientes de correo electrónico ***recuperar los mensajes de los servidores remotos y guardarlos en las máquinas locales***. La mayoría de los clientes de correo que utilizan el protocolo POP se configuran automáticamente para eliminar el mensaje del servidor de correo después de transferirlo correctamente al sistema del cliente, aunque esto se puede cambiar.



Para establecer una conexión a un servidor POP, *el cliente de correo abre una conexión TCP en el puerto **110** del servidor*. Cuando la conexión se ha establecido, el servidor POP envía al cliente POP una invitación y después las dos máquinas se envían entre sí otros comandos y respuestas que se especifican en el protocolo.

Como parte de esta comunicación, al cliente POP se le pide que se autentifique en lo que se denomina autenticación, donde el nombre de usuario y la contraseña del usuario se envían al servidor POP. Si la autenticación es correcta, el cliente POP pasa al estado de transacción, fase en la que se pueden mostrar, descargar y eliminar.

PROTOCOLO SMTP (Simple Mail Transfer Protocol)

Mientras que el protocolo POP permite que un usuario reciba y lea el correo electrónico, el protocolo SMTP (Protocolo simple de transferencia de correo) ***sirve para enviar correo electrónico***. Los mensajes salientes utilizan SMTP para pasar de la máquina del cliente al servidor, lugar desde el que se trasladan hasta el destino final. También dos servidores de correo que intentan transferir entre sí un mensaje utilizan SMTP para comunicarse, incluso si utilizan plataformas totalmente distintas.

SMTP *usa el puerto **25** del servidor* para establecer la comunicación. A continuación, el sistema conectado comunica las direcciones de correo electrónico para recibir el mensaje del sistema receptor, seguido de un mensaje que notifica al sistema receptor que la siguiente parte de la comunicación será el cuerpo real del mensaje de correo electrónico. Cuando el sistema conectado finaliza de enviar el mensaje de correo electrónico, coloca un punto sencillo (.) en una línea. A partir de ese momento, se considera que el mensaje se ha enviado.

El protocolo SMTP también permite gestionar el reenvío de mensajes entre sistemas si el sistema receptor sabe el destino al que tiene que enviar el mensaje. El protocolo puede verificar si determinados usuarios utilizan realmente un servidor de correo concreto o ampliar una lista de distribución de correo. También se puede retrasar el envío de correo electrónico entre dos servidores SMTP si en los dos sistemas se permite realizar esta actividad.

A diferencia del protocolo POP, el protocolo SMTP no requiere autenticación en su forma más básica. Esto ha provocado mucho correo basura o *spam*, ya que un usuario no local puede utilizar el sistema de otro para enviar o transmitir el correo a listas completas de destinatarios con los recursos y ancho de banda del sistema.
Las aplicaciones SMTP modernas han progresado enormemente al minimizar este comportamiento y restringir las transmisiones de modo que sólo los hosts conocidos puedan enviar correo.

PROTOCOLO TELNET

TELNET es el ***protocolo básico de conexión de uno a otro ordenador***, de hecho la mayoría de los servicios anteriores, se basan en TELNET (pe. FTP, HTTP). Haciendo TELNET a una máquina, se ejecutan programas en ella, recibiendo en la propia máquina la entrada/salida de los datos.

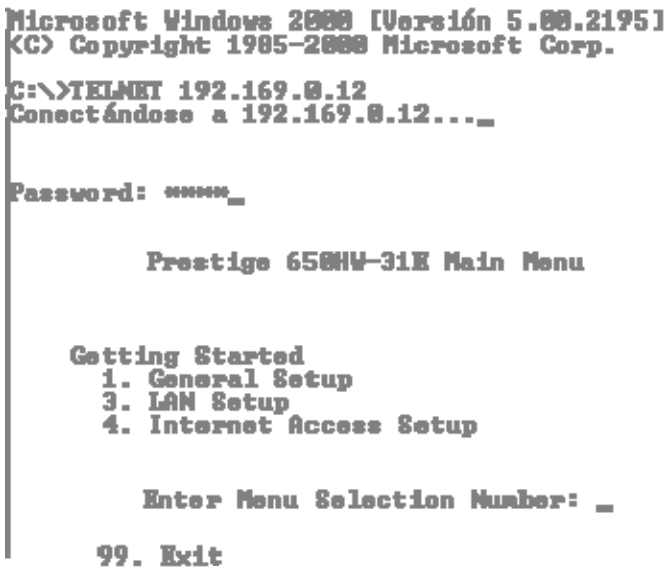
Es una herramienta basada en texto de llamada que hace conexión con otra máquina mediante nombre de dominio o dirección IP, y *el puerto que utiliza es el **23**.* Por TELNET se pueden utilizar TODO tipo de servicios, haciendo TELNET a la máquina y puerto correspondientes según cada caso.

Por ejemplo si queremos utilizar el servicio POP para ver el correo que tenemos, haremos TELNET a la maquina POP por el puerto de este protocolo, el 110. También podemos consultar grandes bases de datos e incluso acceder a servicios WWW, muy útil si no tenemos acceso a estos servicios por la vía normal de HTTP.

El cliente de TELNET, prácticamente cualquier sistema operativo lo lleva incluido de serie. Por lo tanto si nos proporcionan la dirección tecleamos en la línea de comandos "TELNET maquina.remota.es " y ya iniciamos una conexión.

En algunos casos podremos conectar a la maquina remota sin contraseña, pero en la mayoría de las veces deberemos saber el *login* antes de conectarnos.

El siguiente paso es configurar la emulación de terminal, es decir, decirle al sitio remoto como queremos que nos muestre los datos en nuestra pantalla. La configuración más común es la VT100, que es la estándar para las comunicaciones basadas en terminales (algunos clientes TELNET configuran ellos solos la emulación).



30.- SERVIDORES Y SERVICIOS

EL SERVIDOR

Antes empezar, es conveniente precisar que la elección de un servidor depende en gran medida del tipo y la cantidad de tráfico que tenga que gestionar. Otro factor determinante es la sistema operativo utilizado: Windows 2003 Server ®, Linux etc.

Para elegir un buen hardware, hay que considerar seis factores:

Memoria RAM: nunca como en este caso conviene no escatimar y evitar ahorros contraproducentes. En el caso de Linux es posible mantener el sistema con una memoria RAM básica (128 MB o 256 MB), dadas las escasas pretensiones del sistema, pero en servidores Windows Server® es absolutamente necesario montar por lo menos 1GB, si queremos que el sistema funcione con fluidez y sin congestiones.

Procesador: absolutamente aconsejable orientarse hacia procesadores de gran potencia como Intel ® Xeon o AMD Opteron. Naturalmente, si las exigencias de tráfico son muy limitadas o las aplicaciones instaladas son pocas, puede bastar también un procesador menos potente. En las redes LAN, no es muy frecuente pero puede ser necesario tener más de un procesador instalado en cada servidor.

Discos Duros: La tecnología **SCSI** ofrece más prestaciones, porque se libera casi del todo al procesador de cálculos que interesan a los discos. También en este caso cuanto más rápidos son, mejor responde el servidor a los problemas de tráfico elevado. Además, se hace en muchos casos imprescindible, que los discos duros soporten la tecnología **RAID** (Redundant Array of Independent Disks), que es un método de combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante, y por tanto permita, en caso de avería, la sustitución de un disco "en caliente" sin detener el servidor, y, por tanto, sin interrumpir el servicio.


Disco duro SCSI (abierto)

Tarjeta vídeo: Sin embargo la tarjeta puede ser de baja calidad es perfecta puesto que un servidor nunca es una estación de trabajo y no requiere como norma general que haya un operador trabajando permanente en él. El uso que se hace de esta tarjeta se limita a conectar un monitor, casi siempre apagado.

Protección del enfriamiento interno: Un servidor es una máquina que está en servicio 365 días al año y por tanto debe estar bien refrigerada y no debe tener nunca problemas térmicos.

Fuente de alimentación: debe estar probada y por duplicado; cuando se avería una, automáticamente se pone en funcionamiento la otra con la posibilidad de cambiar la averiada sin apagar. Además debe de tener un Sistema de Alimentación Ininterrumpido (SAI) mediante baterías.

SERVICIOS

Servicio WEB

Un servidor WEB, es una *máquina destinada a alojar uno o varios sitios que contienen paginas WEB*. El servicio WEB implementa el ***protocolo HTTP*** (Hypertext transfer protocol). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas Web o páginas HTML (Hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Un servidor Web se encarga de mantenerse a la espera de peticiones HTTP llevada a cabo por un cliente HTTP que solemos conocer como **navegador**. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al teclear *http://www.mde.es* en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla. Como vemos con este ejemplo, *el cliente es el encargado de interpretar el código HTML*, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Sobre el servicio Web clásico podemos disponer de *aplicaciones Web*. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

Aplicaciones en el lado del cliente: el cliente Web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo **Java** o **Javascript:** el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones.

Aplicaciones en el lado del servidor: el servidor Web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones Web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional, como sí ocurre en el caso de querer ejecutar aplicaciones javascript o java. Así pues, cualquier cliente dotado de un navegador Web básico puede utilizar este tipo de aplicaciones.

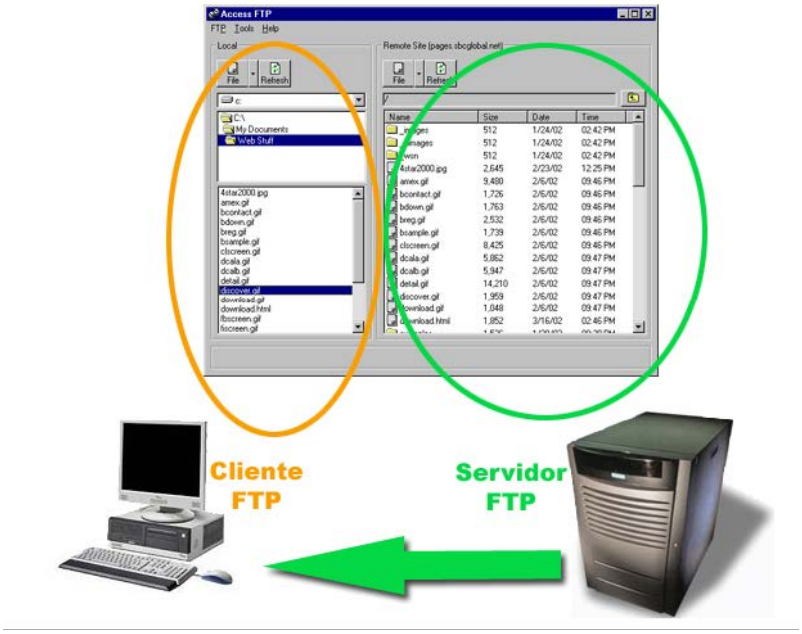
Servicio FTP

El servicio FTP (File Transfer protocol) permite realizar la *transferencia de ficheros entre ordenadores*, es decir, que hace posible que un usuario copie en su ordenador los ficheros que están almacenados en otro. Los programas y protocolos diseñados para llevar a cabo esta función se conocen con el nombre de FTP. Los ficheros a transferir pueden ser documentos, textos, imágenes, sonidos, programas, etc.

El procedimiento mediante el cual se accede a un ordenador para copiar ficheros en forma libre y sin restricciones se conoce como **FTP anónimo** y en este caso por tanto no se necesita de un password *(contraseña)* para entrar en el ordenador remoto. La aplicación FTP funciona de forma muy similar en todos los sistemas, los distintos comandos que pueden ejecutarse tienen, en su mayoría, el mismo formato.

Significa esto, que cada vez que descargamos una información de la red estamos usando el servicio FTP. En la mayoría de los casos es la propia aplicación quien solicita el servicio, no requiriendo del usuario intervención alguna.

En otros casos el usuario se tiene que autentificar mediante una contraseña, para poder acceder al servicio.



Servicio SERVIDOR DE FICHEROS

Los servidores de ficheros tienen como función el *almacenamiento e intercambio de documentos e información*. Permiten el acceso desde cualquier ordenador conectado a la red. Son accesibles tanto desde entornos Windows como de otras plataformas.

Sus misiones fundamentales son:

- Proporcionar a los usuarios un espacio de almacenamiento de información seguro y eficaz.
- Facilitar la distribución del software corporativo licenciado por la organización, a todos los miembros de la red.
- Establecer un espacio de información corporativo al alcance de todos los Usuarios.

Principalmente en la Armada se han usado dos sistemas operativos para servidores de ficheros: Novell Netware® y Windows® 2000 y actualmente se usa Windows® 2003 Server que migrará en un futuro a Windows® 2008 Server.

Novell NetWare ®

La Armada utilizó este sistema operativo para servidores de ficheros *hasta 2002* en fecha en que empezó a imponerse Windows® 2000 Server.

La *principal característica* de esta plataforma es que, originalmente, en las versiones 2.x, 3.x y 4.x, implementaba el direccionamiento **IPX/SPX** (y no TCP/IP). Este protocolo, propietario por Novell, ha demostrado sobradamente su valía en redes de área local, es rápido, fácil de configurar y requiere pocas atenciones.

El *principal inconveniente* que presentaba para redes medianas y grandes es que **no se puede enrutar** o sea que no puede pasar de una subred a otra si entre ambas hay un router, por lo que no puede usarse en redes WAN como la intranet de una institución o Internet. Otro inconveniente que presenta en redes con un cierto número de equipos es que puede llegar a saturar la red con los broadcast que lanzan los equipos para anunciarse en la red. Por estas razones ha ido poco a poco dejando dejándose de utilizar, en beneficio de las plataformas Windows® Server.

A partir de la versión 5, Novell Netware® comenzó a utilizar el protocolo TCP/IP, pero, para ese momento, en la Armada ya se había impuesto Windows® Server.

Windows Server ®

Posteriormente en la Armada se impuso el sistema operativo Windows® Server en su versión 2000 y recientemente en su versión 2003. Esta plataforma implementa de origen direccionamiento IP, y presenta numerosas ventajas:

- Permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros sistemas operativos.
- Buena gestión de almacenamiento, backups, etc.
- Gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de caché para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitan.
- Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware
- Gestión centralizada la seguridad de una red corporativa a nivel local.
- Implementa servicio DNS con registro de IP's dinámicamente.
- Incluye servicio DHCP.
- Rápida y fácil gestión de políticas de usuarios y de seguridad.

En la Armada, hoy en día, prácticamente, todos los servicios de red se instalan sobre máquinas Windows® Server: Correo, Ficheros, DNS, DHCP etc.

Servicio de IMPRESIÓN

El servidor de impresión, *es un equipo destinado a gestionar los trabajos de impresión enviados por los usuarios de una red a la impresora*. Su misión fundamental es administrar las demandas de servicios de impresora realizadas por los puestos trabajo de una red. Además permite la gestión de diferentes impresoras (láser, inyección de tinta, *plotters*, etc) dentro de la red, de tal forma que los usuarios pueden seleccionar una impresora u otra según sus necesidades.

Generalmente todos los sistemas operativos de red incluyen un software de servidor de impresión, y es poco usual encontrarse con un ordenador dedicado sólo a esta tarea, normalmente lo comparte con el servicio de ficheros.

Debido a que un servidor de impresión típico suele administrar una gran cantidad de impresoras, debe tener *suficiente memoria de acceso aleatorio (RAM) para procesar los documentos*. Si un servidor de impresión no dispone de suficiente RAM para su carga de trabajo, se puede reducir el rendimiento de impresión.

El servidor de impresión también debe tener suficiente espacio en disco para almacenar todos los documentos enviados hasta que pueda enviarlos al dispositivo de impresión. Los documentos para los que el servidor no tiene espacio permanecen en el equipo cliente hasta que el servidor tenga espacio suficiente. Este proceso reduce el rendimiento en el equipo cliente.

Por último es necesario destacar que, como norma general, las colas de impresión de un servidor dan prioridad de salida a la impresora según el orden de llegada de las peticiones; aunque se puede configurar para dar prioridad a determinadas estaciones de la red.

Servicio de CORREO

Un servidor de correo es una *máquina que nos permite enviar mensajes (correos) de unos usuarios a otros con independencia de la red que dichos usuarios estén utilizando.*

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

- **SMTP:** (Simple Mail Transport Protocol) Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes, también conocido como servicio de correo saliente.

- **POP:** (Post Office Protocol) Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario, se conoce también como servicio de correo entrante.

- **IMAP:** (Internet Message Access Protocol) Su finalidad es la misma que la de POP, pero el funcionamiento es diferente.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Microsoft Outlook) y son servicios en general de pago. Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario; es el caso de los clientes vía Web, (como Hotmail, Gmail, etc). Suelen ser gratuitos.

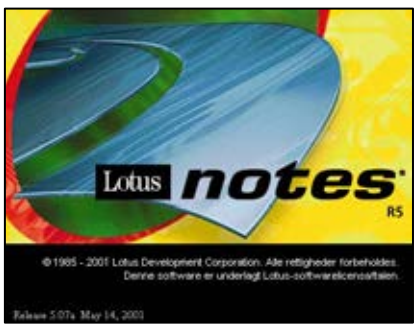
En cualquier caso, los protocolos SMTP/POP/IMAP son inseguros en cuanto a que los mensajes viajan en claro por la red, es decir, es fácil obtener nuestros mensajes y contraseñas. Para ello se suele añadir una capa **SSL**, es decir, un método de encriptación que puedan implementar tanto el servidor como el cliente.

Existen multitud de aplicaciones de servicio de correo. En el Ministerio de Defensa se ha optado por **Lotus Notes® de IBM®** que implementa seguridades adicionales como el uso de fichero de identificación personal (fichero ID) y la firma electrónica.

Otra aplicación de servicio de correo muy utilizada en la actualidad es Microsoft Exchange®.

Lotus Notes ®

Lotus Notes® es la aplicación de correo utilizada en la red del Ministerio de defensa con un uso similar a cualquier tipo de cliente de correo convencional.



Tiene algunas peculiaridades con respecto a las aplicaciones de correo al uso:

- Utiliza su propio tipo de bases de datos, de tipo documental, no relacional.

- Incluye un navegador en el software de cliente.

- Utiliza el fichero de identificación personal (**fichero ID**), para implementar más seguridad, ya que si no se está en posesión de éste, y validado por el servidor, no se puede acceder al correo.

- Los usuarios tienen su *buzón* en el servidor, de tal forma que pueden acceder a él, desde cualquier ordenador, sin configurar nada, siempre que estén en posesión de su fichero ID.

- Permite una gestión y administración, sencilla y rápida.

Microsoft Exchange ®

Microsoft Exchange ® es una aplicación de correo desarrollada por Microsoft, y que presta servicios de *e-mail* en combinación con el célebre cliente de correo Microsoft Outlook ®.

Microsoft Exchange® ofrece la posibilidad de acceso móvil, remoto y de escritorio al correo electrónico con avanzada seguridad y privacidad; alta fiabilidad y gran rendimiento; fácil actualización, implementación y administración.

El funcionamiento es parecido al de Lotus Notes® con la particularidad de que no implementa el fichero de identificación personal, es decir el usuario se identifica con un nombre y una contraseña y basta con que tenga una cuenta creada en el servidor.

Sus características principales son:

- Listas de distribución restringida a usuarios autentificados.

- Soporta listas en tiempo real de Seguridad y Bloqueo.

- Filtra correo no deseado

- Incluye un antivirus.

- Protege la privacidad en Outlook y Outlook Web Access.

- Permite el acceso a carpetas públicas a usuarios desconocidos.

- Implementa servicios de mensajería instantánea.

Servicio de BACKUP

Un servidor de copia de seguridad, de respaldo o simplemente **backup** consiste en *una máquina que guarda automáticamente la información sensible referida a un sistema*. Normalmente estos servidores tienen conectado un medio de almacenamiento **extraíble** en el que el servidor – programado a una hora determinada - graba todos los trabajos realizados durante el día por los usuarios de la red. Este medio puede ser un disco duro externo, un CD-ROM grabable, cintas de datos (DAT), discos ZIP o magneto-ópticos.

Las copias de seguridad en un sistema informático tienen por objetivo el mantener cierta capacidad de recuperación de la información ante posibles pérdidas. Esta capacidad puede llegar a ser algo muy importante, incluso crítico, para las empresas.

Típicamente las copias de seguridad se suelen hacer en cintas magnéticas, si bien dependiendo de lo que se trate podrán usarse disquetes o CDs o pueden realizarse a un centro de servidores de respaldo remoto (actualmente esta es la tendencia). Todo dependerá de la escala a la que se trabaje, ya sea un PC doméstico o un enorme sistema centralizado de una gran empresa o un organismo público.

La copia de seguridad puede realizarse de los datos (bases de datos, correo electrónico, carpetas compartidas en un servidor de archivos) pero también de archivos que formen parte del sistema operativo.

Las **copias de seguridad del sistema** tienen por objeto el mantener la capacidad poder rearrancar el sistema informático tras un desastre. Esta contendrá la copia de los ficheros del software de base y del software de aplicación.

Las **copias de seguridad de los datos**, las más importantes al fin y al cabo, tienen por objeto mantener la capacidad de recuperar los datos perdidos tras un incidente de seguridad.

Servicio de DHCP

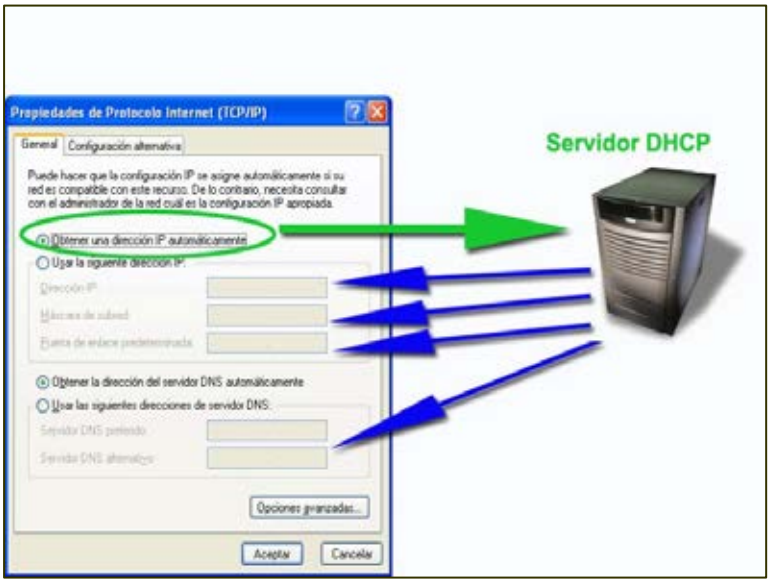
DHCP son las iniciales de Dynamic Host Configuration Protocol, un protocolo que instalado en un servidor de una red local, *permite la configuración automática del protocolo TCP/IP de todos los clientes de dicha red*. Permite configurar automáticamente el protocolo TCP/IP a una máquina que inicia una nueva sesión en la red.

Por tanto cuando una máquina cliente inicia una sesión en red DHCP automáticamente le suministra:

- Una dirección IP
- Una máscara de subred
- Una puerta de enlace o *gateway*
- Una dirección del servidor o servidores DNS
- Una dirección del servidor WINS

DHCP permite además modificar la configuración de todos los equipos de la red con sólo modificar los datos del servidor.

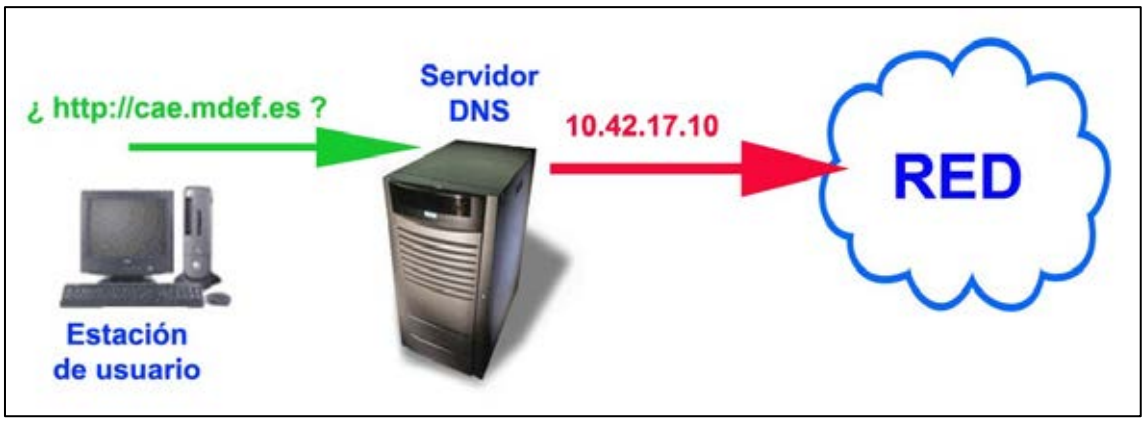
Es importante resaltar que en una red **sólo debe haber un servidor DHCP funcionando**, ya que más de uno realizando la misma función, entrarían en conflicto, y provocarían configuraciones ambiguas.



Servicio de DNS

El servicio DNS (Domain Names Service) es un servicio que *traduce los nombres de los diferentes sitios de una Intranet o de Internet* (direcciones por nombre, p. ej. *http://cae.mdef.es/uvicoa*) *en direcciones IP* (direcciones numéricas, p. Ej. 193.144.238.1) y viceversa. Este servicio es imprescindible para poder iniciar cualquier comunicación con otro ordenador accediendo al mismo por su nombre.

En definitiva un servidor DNS contiene una **base de datos** que relaciona el nombre de un sitio - o un ordenador - de una red, con su dirección IP, teniendo el cuenta que el sistema de búsqueda en la red sólo utiliza direcciones IP.



GLOSARIO DE TÉRMINOS

REDES LAN

A

ACCESO CONMUTADO: Conexión de red la cual se puede crear y desechar según se requiera. Los enlaces de marcado por línea telefónica son la forma más sencilla de conexiones con acceso conmutado. Los protocolos utilizados generalmente en este tipo de conexiones son SLIP y PPP.

ACTIVE X: Una tecnología de Microsoft que facilita el uso de información compartida entre aplicaciones. Se utiliza principalmente para desarrollar *aplicaciones interactivas* y *contenido de Web*. ActiveX se ha construido sobre la tecnología OLE que se utilizó durante algún tiempo, pero expande el alcance de los objetos compartidos desde el escritorio a todo Internet. Debido a que la tecnología ActiveX es modular en cuanto al diseño, los programas pueden escribirse como aplicaciones independientes, como "objetos inteligentes" incrustados dentro de programas Visual Basic o páginas Web, o como objetos OLE tradicionales dentro de los documentos. Actualmente *sólo* es soportado por el navegador Microsoft Internet Explorer.

ADDRESS (DIRECCIÓN): Este término se puede referir a la dirección IP (*ip address*), o a una dirección de correo electrónico, (*e-mail address*).

***ADJUNTO (ANEXO, ATTACHMENT)*:** archivo que se adjunta a un mensaje de correo electrónico para su envío por esa vía de transmisión.

ADMINISTRADOR DE FICHEROS: Aplicación que permite realizar funciones como la gestión de archivos y la impresión. Con el administrador de ficheros de Windows se pueden crear, copiar, buscar o borrar directorios o ficheros, etc.

ADSL (LÍNEA DE SUBSCRIPCIÓN ASIMÉTRICA DIGITAL ASYMMETRIC DIGITAL SUBSCRIBER LINE): Se refiere a una tecnología para mejorar el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

Se define como Línea Digital Asimétrica de Abonado. Sistema asimétrico de transmisión de datos sobre líneas telefónicas convencionales (utiliza el clásico cable de cobre telefónico). Existen algunas que alcanzan velocidades de 8 Megabits por segundo al bajar información de Internet y entre 16 y 576 Kilobits en sentido contrario.

AGENTE DE USUARIO*: (Ing.: user agent)* Se llama así al programa cliente que inicia una demanda a un servidor de red. Normalmente, se trata de programas que son visualizadores, editores, (robots de navegación de Web), u otras herramientas de usuario final.

ALIAS: Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre usualmente largo y difícil de recordar. Ver Nick.

ANCHO DE BANDA: *(bandwidth)* Cantidad de bits que pueden viajar por el medio físico (cable coaxial, par trenzado, fibra óptica, etc.) en un determinado momento. Cuanto mayor es el ancho de banda con más rapidez se transfiere la información. Se mide normalmente en bits por segundo (bps), o en alguno de sus múltiplos, dependiendo del tipo de conexión, (Kbps: ~1.000 bps, Mbps: ~1.000.000 bps, etc.).
Por ejemplo:
-un módem rápido puede trabajar a una velocidad de hasta 56 Kbps.
-sobre una línea telefónica normal.
-en redes locales se manejan anchos de banda de entre 10Mbps y 10^6 Mpbs.
-sobre fibra óptica y con técnicas especiales (Sonet o Jerarquía Digital Síncrona) se pueden conseguir anchos de banda aún mayores.

ANCLA: *(Ing.: anchor)* marcador que se inserta en una página Web de tal manera que, colocando el puntero sobre ella, ésta se refiere a una URL particular.

ANSI (AMERICAN NATIONAL STANDARDS INSTITUTE): Organismo de normalización USA.

API: *("Application Program Interface")* Conjunto de reglas de programación que determinan cómo una aplicación debe acceder a un servicio.

APLICACIÓN: Software que realiza una función útil. Los programas que se utilizan para realizar alguna función (como correo electrónico, FTP, etc.) son las aplicaciones cliente.

APPLET: Aplicación realizada en Java para ser ejecutada en el sistema cliente.

APACHE: Servidor HTTP de dominio público el cual está basado en el sistema operativo Linux. Fue desarrollado en 1995 y actualmente es uno de los servidores HTTP más utilizados en la red. http://www.apache.org

ARCHIE: Sistema para la localización de archivos que están disponibles públicamente por FTP anónimo. Es necesario conocer el nombre del archivo o una subcadena del mismo para utilizar archie. Basado en la arquitectura Cliente/Servidor, archie da nombre a ambos.
Existen muchos clientes archie: archie, xarchie (X Windows), e incluso una pasarela archie desde WWW. En España, el servidor archie: archie.rediris.es, es gestionado por Rediris.

ARPANET: Este término proviene de "*Advanced Research Project Agency Network*" (Red de Proyectos de Investigación Avanzados), el precursor de la red Internet. Fue desarrollado a finales de los años 60 y a comienzos de los 70 por el Departamento de Defensa americano, como un experimento en redes mundiales que sobreviviera una guerra nuclear.

ASCII: Acrónimo del código estándar americano para el intercambio de información ("*American Standard Code for Information Interchange*"). Es el código estándar de conjunto de caracteres que cualquier ordenador puede entender, usado para representar las letras latinas, en mayúsculas, minúsculas, números, puntuación, etc. Hay *128 códigos* estándar ASCII, cada uno de los cuales puede representarse por un número binario de 7 dígitos.
Sin embargo, otros conjuntos de caracteres como Latin-1 están comenzando a usarse. Los documentos HTML no se limitan a ASCII.

ASP (PÁGINA DE SERVIDOR ACTIVO): Las páginas ASP, son un tipo de HTML que además de contener los códigos y etiquetas tradicionales, cuenta con programas (o scripts) que se ejecutan en un servidor Microsoft Internet Information Server antes de que se desplieguen en la pantalla del usuario. Por lo general este tipo de programas realizan consultas a bases de datos, siendo los resultados de éstas los que el usuario final obtiene. La extensión de estos archivos es ".asp."

ATM: (*"Asyncronous Transmision Mode"*). Modo de Transmisión Asíncrona. Sistema de transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea. Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1,2 Gbps.

AUTENTICACIÓN: *(Ing.: authentification)* Este término se refiere a la acción de verificar la identidad de una persona o de un proceso, en general, con la ayuda de una firma electrónica.

B

BACKUP: Copia de seguridad de los ficheros o programas del disco duro que se duplican en otro soporte de almacenamiento.

BACKBONE: (Espina dorsal). Línea o serie de conexiones de alta velocidad que forman una vía con gran ancho de banda. Un backbone conecta dos puntos o redes distanciados geográficamente, a altas velocidades.

BASES DE DATOS DISTRIBUIDAS: Bases de datos que se pueden encontrar en distintas localizaciones geográficas y que se presentan ante el usuario como una base de datos única.
Un ejemplo de ello es el DNS (*"Domain Name Service"*) en que se basa Internet, donde las direcciones de las computadoras se encuentran en diversas computadoras (cada una encargada de un dominio), y que se presentan ante el usuario como una base de datos única con todos los dominios del planeta.

BAUDIO: Unidad de medida. Número de cambios de estado de una señal por segundo, generalmente equiparable a un bit por segundo. Cuando se transmiten datos, un baudio es el número de veces que cambia el "estado" del medio de transmisión en un segundo. Por ejemplo, un módem de 14.400 baudios cambia 14.400 veces por segundo la señal que envía por la línea telefónica. Como cada cambio de estado puede afectar a más de un bit de datos, la tasa de bits de datos transferidos (por ejemplo, medida en bits por segundo) puede ser superior a la correspondiente tasa de baudios.

BBS: ("*Bulletin Board System*") Servicio que proporcionaban desde grandes compañías (Compuserve, America On Line, etc) hasta pequeños proveedores, que consistía en intercambiar información con otros usuarios, descargar archivos etc., sin estar conectados a Internet, por lo que actualmente han caído en desuso. Las BBS se contaban por miles en el mundo, corriendo desde una simple PC con una o dos líneas telefónicas. La tendencia fue que las BBS se convirtieron en proveedores de servicio de Internet.

BETA: Versión de prueba de un programa, previa a su lanzamiento comercial.

BINARIO: Código básico de la informática que reduce todo tipo de información a cadenas de ceros y unos.

BITNET: ("*Because It's time NETwork*") red de puntos educación separados de Internet, pero cuyo correo electrónico está en intercambio entre BITNET e Internet.

BLUETOOTH: Conexión inalámbrica de corto alcance, que se va imponiendo para la conexión de los periféricos. teclado, ratón... Es un sistema de radiofrecuencia que permite transferir texto, voz e imagen. Alcance: unos 10 metros.
Estándar de transmisión de datos inalámbrico vía radiofrecuencia de corto alcance (unos 10 metros). Entre otras muchas aplicaciones, permite la comunicación entre videocámaras, móviles y ordenadores dotados con este protocolo para el intercambio de datos digitalizados (vídeo, audio, texto, etc.).

BPS: Acrónimo de bits por segundo (*"Bits-Per-Second"*). Es la medida estándar de la velocidad de transmisión de datos a través de un módem.

BRIDGE (puente): Mecanismo que conecta redes locales separadas y que permite que los datos se transfieran entre ellas.

BROWSER: (Examinador, navegador) Programa cliente que se utiliza para buscar diferentes recursos de Internet. Se trata de una herramienta de navegación sin la cual no se podría acceder a los recursos de Internet. Los browsers más usados son Netscape Navigator y Microsoft Internet Explorer.

BTW: Acrónimo de "*By The Way"* (por cierto...), una abreviatura usada junto a un comentario escrito en un forum *on line*.

BUFFER: Espacio de almacenamiento temporal donde se guardan determinados datos antes de ser transmitidos. Constituye una memoria intermedia que se utiliza en distintos periféricos (teclado, impresoras...) para aumentar su rapidez y rendimiento, compensando las velocidades entre la recepción de datos (más lento) y su rápido proceso.

BYTE: Serie de ocho bits con los que se representa cualquier carácter. 1.024 bytes son un Kbyte, y 1.024 Kbytes hacen un Mbyte. El código ASCII (American Standard Code for Information Interchange) establece una equivalencia entre cada carácter que podemos usar y una serie de 7 o 8 bits. Por ejemplo:
carácter.....byte equivalente
A.....0100 0001
B.....0100 0010
C.....0100 0011
D.....0100 0100

C

CABECERA: *(header)* Este término se refiere a la información acerca de un documento Web o un mensaje de correo que se encuentra al principio del documento o mensaje.
La información que contiene una cabecera puede hacer referencia al autor, o el generador del texto. No se debe confundir este término con el de encabezamiento.

CABLE COAXIAL: Núcleo de cobre, aislado por plástico de un recubrimiento metálico y este a su vez envuelto en otra capa de plástico. Suelen emplearse dos tipos de cable coaxial para las redes locales: cable de 50 Ohms, para señales *digitales*, y cable de 75 Ohms, para señales *analógicas* y para señales de alta velocidad. Es un medio físico por medio del cual se pueden conectar varias computadoras.

CABLE DE FIBRA ÓPTICA: Soporte para el transporte de datos que se utiliza en las comunicaciones de alta velocidad en Internet. Ofrece velocidades similares al ADSL, pero puede llegar a10 Mbps. Las compañías que ofrecen servicios de acceso a Internet a través de cable, incluyen también opcionalmente servicios de telefonía y televisión.

CABLE MODEM: Un cable módem es un dispositivo que permite conectar el PC a una línea local de TV por cable a aproximadamente 1.5 Mbps. Esta tasa de datos excede con mucho la de los módems telefónicos de 28.8 y 56 Kbps. Además de la mayor velocidad de transferencia de datos, una ventaja de Internet por cable sobre la que se provee por teléfono es que se trata de una conexión continua.

CABLEADO: Columna vertebral de una red que utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), que lleva la información de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

CACHÉ: Almacenamiento local y temporal de un programa, de los mensajes de respuesta y el subsistema que controla el almacenamiento, la recuperación y eliminación de sus mensajes. Un caché, almacena respuestas para reducir el tiempo de respuesta y el consumo de ancho de banda de red en demandas equivalentes futuras.

CACHÉ DE DISCO: Espacio que se reserva en el disco duro para guardar archivos temporalmente (por ejemplo, imágenes y documentos Html visitados por el navegador).

CADENA: *(string)* Secuencia de caracteres. Cada palabra es una cadena. Una búsqueda preguntará por una cadena de búsqueda, refiriéndose no sólo a palabras, sino a una secuencia de caracteres, formen éstos una palabra una frase, o ninguna de las dos posibilidades.

CARPETA DE CORREO: Área de almacenamiento en la que se colocan documentos que tienen un carácter común, por ejemplo: todos han sido enviados, o todos han sido recibidos...

CERN*: "Conseil Européenne pour la Recherche Nucléaire"*, el Laboratorio europeo de física de partículas de Génova (Suiza) donde, en la década de 1980, un equipo de ingenieros pioneros bajo la dirección de Timothy Berners-Lee desarrolló la tecnología World Wide Web, buscando construir un sistema de hipertexto.

CGI: *("Common Gateway Interface")* es una interface para que programas externos (pasarelas) puedan rodar bajo un servidor de información. Actualmente, los servidores de información soportados son servidores HTTP (*"Hypertext Transfer Protocol"*).

Las pasarelas pueden usarse para muchos propósitos, algunos de ellos:
• Manejo de formas y cuestionarios.
• Conversión de las main pages del sistema a páginas html y presentación del resultado por parte del cliente WWW.
• Interface con bases de datos WAIS y Archie, y presentación de los resultados en formato html por parte de clientes WWW.
• Mensajería electrónica (comunicación con los administradores WWW) .

CHAT: Término utilizado para describir la comunicación de usuarios en tiempo real. Un programa de software de red que permite a varios usuarios mantener "conversaciones" en tiempo real con los demás, escribiendo mensajes en sus equipos y enviándolos a través de una red de área local o de Internet.

CIBERESPACIO: *(cyberspace)* Este término fue acuñado por primera vez por el escritor William Gibson en 1984 que lo definió como "una representación gráfica de los datos abstraídos de los bancos de memoria de todos los equipos de un sistema humano". Actualmente es ampliamente usado para describir los recursos de información disponibles a través de Internet.

CLIENTE: *(client)* Programa que se usa para contactar y obtener datos de un programa de servidor localizado en otro ordenador, a menudo a gran distancia. Cada programa cliente está diseñado para trabajar con uno o más tipos de programas servidores específicos, y cada servidor requiere un tipo especial de cliente.

CLIENTE/SERVIDOR: Sistema que se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor). De esta manera los clientes son los elementos que necesitan servicios del recurso y el servidor es la entidad que lo posee. Los clientes, sin embargo, no dependen totalmente del servidor debido a que pueden realizar los procesamientos para desplegar la información (por ejemplo en forma gráfica). El servidor los provee únicamente de la información sin hacerse cargo de otros procesos de forma que el tráfico en la red se ve aligerado y las comunicaciones entre las computadoras se realizan más rápido.

CÓDIGO MÁQUINA*:* También llamado Lenguaje Máquina. Lenguaje de Programación que trabaja directamente con los registros de memoria y los comandos del microprocesador. Es diferente para cada familia de microprocesadores y puede cambiar con la arquitectura del ordenador.

CONEXIÓN: *(connection)* Circuito virtual de transporte que se establece entre dos programas de aplicación con fines comunicativos.

CONEXIÓN DIRECTA A INTERNET: Forma de conectarse directamente a Internet para que el ordenador forme parte de la Red cuando se conecte. Los dos protocolos que gestionan la conexión directa a Internet vía módem son SUP y PPP.

CONEXIÓN "EN CALIENTE": Conexión de un periférico a la unidad central que no requiere apagar o reinicializar el equipo (por ejemplo, generalmente la conexión de periféricos por el puerto USB se realiza en caliente)

CONEXIÓN REMOTA: Operación realizada en un ordenador remoto a través de una red de computadoras, como si se tratase de una conexión local.

CONEXIONES A INTERNET: Hay diversos sistemas: módem convencional y línea telefónica (permite velocidades de hasta 56 Kbps.), RDSI con módem digital (128 Kbps), ADSL con módem específico (actualmente 256 Kbps en sentido red-usuario y 12 Kbps en sentido contrario, pero puede alcanzar hasta 8 Mbps), cable de fibra óptica (ofrece velocidades similares al ADSL, pero podría llegar a10 Mbps), PLC a través de las líneas eléctricas (entre 2 Mbps y 25 Mbps)

CONMUTACIÓN DE PAQUETES: Método empleado para transferir los datos a través de Internet. Estos se dividen en pequeños paquetes que contienen la dirección de origen y la de destino. Los paquetes viajan, a veces por distintas vías, a su destino, donde se reunifican. Paradigma de comunicaciones mediante el cual cada paquete de un mensaje recorre una ruta entre sistemas anfitriones (hosts), sin que esa ruta (path) esté previamente definida.

CONTRASEÑA: *(password)* Palabra o cadena de caracteres, normalmente secreta, para acceder a través de una barrera. Se usa como herramienta de seguridad para identificar usuarios de una aplicación, archivo, o red. Puede tener la forma de una palabra o frase de carácter alfanumérico, y se usa para prevenir accesos no autorizados a información confidencial.

COOKIE: Procedimiento ejecutado normalmente en un servidor Web que consiste en guardar información acerca del cliente para sus posterior recuperación. En la práctica la información es proporcionada por el navegador o visualizador al servidor de Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro de un usuario a un servicio determinado.

CORREO ELECTRÓNICO: *(Electronic Mail, o e-mail)*. Los mensajes, normalmente en forma de texto, enviados de una persona a otra sobre un tema en concreto a través del ordenador. El correo electrónico puede enviarse automáticamente a un gran número de direcciones a través de una lista de correo (mailing list).

CORTAFUEGOS: Ver Firewall.

CPI: Centro Proveedor de Información. Nombre genérico de las empresas y/o instituciones que ofrecen servicios de acceso a Internet.

CRACKER: Persona que se dedica a entrar en redes de forma no autorizada e ilegal, para conseguir información o reventar redes, con fines *destructivos*. No hay que confundir este término con el de hackers.

CU-SEEMEE: (Te veo-me ves) Programa de videoconferencia, de libre distribución, desarrollado por la Universidad de Cornell (EE.UU). Permite a cualquiera que tenga dispositivos de audio y vídeo (y una conexión a Internet de un cierto ancho de banda), realizar una videoconferencia con alguien que tenga esos mismos dispositivos. Permite también la multivideoconferencia.

D

DATO: Unidad mínima que compone cualquier información.

DATOS ANALÓGICOS: Representación de la información (textos, sonidos, imágenes) mediante una señal eléctrica que varia de frecuencia y amplitud. Los datos analógicos pueden transmitirse a través de las líneas telefónicas convencionales.

DATOS BINARIOS: Representación de la información (textos, sonidos, imágenes) mediante una serie de unos y ceros (bits) que se manifiestan en el ordenador por a presencia o la ausencia de señal eléctrica. Los sistemas informáticos convierten los datos analógicos en binarios para procesarlos.

DATOS: Entendemos por DATOS la información que introducimos en el ordenador para ser procesada. POr ejemplo los nombres y las direcciones de los socios de un club, con las que elaboramos un fichero informatizado que nos facilitará la gestión de las cuotas anuales y la emisión de listados.

DIRECCIÓN ELECTRÓNICA: *(address).* Dirección de un usuario en Internet. Por medio de ella es posible enviar correo electrónico a un usuario. Esta es única para cada usuario y se compone por el identificativo (login) de un usuario, el símbolo arroba, @, y el nombre del servidor de correo electrónico o dominio al que pertenece ese usuario, por ejemplo: *usuario@computadora.dominio.com* o *usuario@dominio.com*

DIRECCIÓN IP: *(IP address)*. Es la dirección numérica de una computadora en Internet. Cada dirección IP se asigna a una computadora conectada a Internet y por lo tanto es única. Consiste en un número de 32 bits que suele representarse como cuatro octetos separados por un punto, como 150.214.90.66. En la actualidad hay una escasez real de direcciones IP libres, por lo que se ha definido un nuevo sistema de direccionamiento IP mucho más amplio y compatible con el actual (IP Versión 6) que se irá implantando a medio/largo plazo a medida que crezca Internet.

DIRECCIÓN IP DINÁMICA: Dirección IP que los proveedores de acceso a Internet asignan generalmente a sus clientes. Es distinta cada vez que estos se conectan a Internet.

DIRECCIÓN IP ESTÁTICA: Dirección IP fija que los proveedores de acceso a Internet asignan a algunos de sus clientes.

DNS: Acrónimo de *"Domain Name System"* (Sistema de Nombres de Dominio). Sistema para traducir los nombres de los ordenadores en direcciones IP numéricas, (y viceversa).

DOMINIO: "Nombre que permite identificar un ordenador o un grupo de ellos. Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Los más comunes son .com, .edu, .net, .org y .gov; la mayoría de los países tienen su propio dominio, y en la actualidad se están ofreciendo muchos dominios nuevos debido a la saturación de los dominios .com (utilizados muchas por empresas)."

DOWNLOAD: Término prestado del inglés, cuya traducción literal significa "descargar". Se refiere a la acción de importar archivos de un ordenador remoto a otro local por medio de una conexión, como se puede realizar a través de un FTP. En el argot de Internet, se usa para describir esta acción, la frase "bajar de la red" o, simplemente "traerse" un archivo o un programa.

DRIVERS: Programas que controlan el funcionamiento de los dispositivos hardware (módem, impresora, etc.). Están estrechamente ligados con el sistema operativo que controla el hardware, de tal forma que un mismo hardware necesita distintos drivers para distintos sistemas operativos.

DUPLEX: Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/transmitir.
Existen dos modalidades; HALF-DUPLEX: Cuando puede recibir y transmitir alternativamente y FULL-DUPLEX: cuando puede hacer ambas cosas simultáneamente.

DVD: *"Digital Video Disk"*. Nuevo estándar en dispositivos de almacenamiento masivo con formato de *CD* pero que llega a 17 GB de capacidad (una cara/dos caras, capa simple/capa doble)

E

E-MAIL: (*Electronic Mail*). Ver correo electrónico.

ENCABEZAMIENTO: *(heading)* Este término describe el tipo y tamaño de letra que deben tener los títulos en las páginas Web. Este último término es una marca de HTML, representada por <h#> y </h#>, donde # describe un número del 1 al 6 en orden decreciente de tamaño e importancia. No se debe confundir este término con el de cabecera.

ENLACE: *(link)*. Conexión a otro documento Web, por medio de la dirección URL. Los enlaces aparecen en el texto de un documento Web en forma de texto subrayado y de distinto color. Permiten al usuario presionar el botón del ratón sobre dicho texto y automáticamente saltar a otro documento, o a otro servidor, o enlazar a otra parte del mismo documento.

ENTIDAD: *(entity)* Representación particular de recursos de datos, o respuesta a un recurso de servicio que puede estar incluido en un mensaje de petición o respuesta. Una entidad consiste en "meta-información" en forma de cabeceras de entidad, y el contenido en forma de cuerpo de entidad.

ENRUTADO INTERDOMINIOS SIN CLASES (CIDR): Método de asignar y especificar direcciones Internet utilizados en enrutadores interdominios (interdomain routers) el cual presenta mayor flexibilidad con respecto al sistema original de clases de direcciones del protocolo Internet. Como resultado se ha ampliado en gran medida el número de direcciones Internet disponibles.

EQUIPO TERMINAL DE DATOS: Se refiere por ejemplo al ordenador conectado a un módem que recibe datos de éste.

ETHERNET: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment, que se ha convertido en un estándar. Es compatible con distintos medios físicos (cable coaxial, par trenzado, fibra óptica) y con distintas topologías de red (bus, estrella).
El ancho de banda ha evolucionado desde los 10 Mbps originales hasta 100 Mbps (Fast Ethernet) y 1000 Mbps (Gigabit Ethernet), incluyendo compatibilidad hacia atrás.

EUDORA: Una de las aplicaciones cliente de *correo electrónico* más extendidas, que funciona además, sobre distintas plataformas (Windows y Macintosh). Existen dos versiones: la comercial y la versión Freeware.

EXTRANET (extrarred): Interconexión entre dos o más organizaciones a través de sistemas basados en la tecnología Internet. Web privada accesible externamente mediante claves de acceso.

F

FAQ: Acrónimo de "*Frequently Asked Questions"* (Preguntas más frecuentes). Documento que contiene las preguntas de interés general más usuales acerca de un tema, con sus respuestas. Hay miles de FAQs sobre temas tan diversos como la Criptografía o el cuidado de los animales domésticos, sin olvidar, por supuesto aspectos de la red Internet, que son los más usuales.

FDDI: Acrónimo de *"Fiber Distributed Data Interface"* (interface de datos distribuidos por fibra) Un estándar para transmitir *datos por cable de fibra óptica* a la velocidad de alrededor 100 millones de bits por segundo (10 veces más rápido que Ethernet).

FIBRA ÓPTICA: Medio físico formado por la combinación de vidrio y materiales plásticos. A diferencia del cable coaxial y del par trenzado no se apoya en los impulsos eléctricos, sino que transmite por medio de *impulsos luminosos* (técnicas optoeléctricas). Se caracteriza por una gran velocidad de transmisión, un elevado ancho de banda y poca perdida de señal.
Su uso es cada vez más generalizado, debido al continuo abaratamiento de los costes y al gran ancho de banda que es capaz de conseguir.

FINGER: Programa de Internet que sirve para localizar personas en otros servidores de Internet. También se puede usar para acceder a información no personal. Su uso más generalizado es para determinar si una persona tiene una cuenta de Internet.

FIREWALL: Cortafuegos. Una combinación de hardware y software que separa una red de área local (LAN) en dos o más segmentos con propósitos de seguridad. Su misión es proteger una red de intrusiones no autorizadas.
El sistema Firewall se coloca normalmente entre la red local (Intranet) e Internet. La regla básica de un Firewall es asegurar que todas las comunicaciones entre la Intranet e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Además, estos sistemas conllevan características de privacidad, autentificación, etc.

FREENET (redes libres): Sistema comunitario de comunicación Internet con sitios web, correo electrónico, servicios de información, comunicaciones interactivas y conferencias. Las "redes libres" son financiadas y gestionadas a menudo por voluntarios. En Estados Unidos forman parte de la NPTN (National Public Telecomputing Network, Red Nacional Publica de Telecomputación), organización dedicada a conseguir que las telecomunicaciones a través de ordenador y los servicios de redes sean gratuitos como las bibliotecas públicas.

FREEWARE: Se llama así al software de *dominio público*, es decir, el que no es comercial y puede distribuirse gratuitamente, aunque no se puede modificar, pues el autor mantiene los derechos de copyright. Ver también shareware.

FORMULARIO: Documento HTML con campos donde el usuario puede escribir o casillas que pueden ser marcadas. Los datos resultantes se pasan a un programa CGI o se envían a través de e-mail.

FTP: Acrónimo de *"File Transfer Protocol"* (Protocolo de transferencia de archivos). También designa la aplicación cliente que permite *transferir archivos* utilizando el protocolo de transferencia de archivos. Los servidores de FTP más difundidos son los de FTP anónimo, (FTP Anonymous), que permiten descargar archivos públicos sin necesidad de una identificación personal por parte del usuario.

FYI: Acrónimo de "*For Your Information"* (para su información), usado en mensajes de correo electrónico a través de los grupos de noticias (Usenet) y listas de correo.

G

GATEWAY: (Pasarela, Puente) Sistema hardware/software que transfiere información entre sistemas o redes incompatibles. Este término también se aplica a los sistemas que actúan como "routers" o "encaminadores", cuando el protocolo usado es TCP/IP.

GMT: *"Greenwich Mean Time"*. Hora de Referencia de Greenwich. Equivalente a *UTC.*

GNU: Fundación para el Software Libre (FSF – *"Free Software Foundation"*) está dedicada a eliminar las restricciones de uso, copia, modificación y distribución del software. Promueve el desarrollo y uso del software libre en todas las áreas de la computación. Específicamente, la Fundación pone a disposición de todo el mundo un completo e integrado sistema de software llamado GNU. La mayor parte de este sistema está ya siendo utilizado y distribuido.
Según la FSF, se puede o no se puede pagar para obtener el software de GNU, pero al menos se tienen dos libertades una vez que se tiene el software: la primera, la libertad de copiar el programa y darlo a amigos y colaboradores, y la segunda, la libertad para cambiar el programa y adaptarlo a las necesidades propias (por acceso a todas las fuentes).

GOPHER: Herramienta de búsqueda que presenta información en un sistema de menús jerárquicos parecidos a un índice. Se trata de un método de hacer menús de material disponible a través de Internet. El Gopher es un programa de estilo Cliente-Servidor, que requiere que el usuario tenga un programa cliente Gopher. Aunque Gopher se extendió rápidamente por todo el mundo, ha sido sustituido en los últimos años por el Hipertexto., también conocido como WWW (World Wide Web), todavía hay miles de usuarios servidores de Gopher en la Internet.

La información contenida en gopher es similar a la contenida en la WWW, sólo que organizada de manera distinta.

GSM (Global System for Mobile Communications): Sistema Global para Comunicaciones Móviles. Segunda generación de teléfonos móviles que facilita el acceso WAP a determinados formatos de páginas web de Internet. La velocidad de acceso a Internet es muy baja (unos 10 Kbits/seg).
Originalmente desarrollado como estándar europeo para la telefonía móvil digital, GSM se ha convertido en el sistema móvil de uso más difundido en el mundo. Se usa en las frecuencias de 900 y 1800 MHz en Europa, Asia y Australia y en la frecuencia de 1900 MHz en Norteamérica y Latinoamérica.

GRUPOS DE DISCUSIÓN: Ver Grupos de noticias.

GRUPOS DE NOTICIAS (NEWS): Área de mensajes automatizada, operada normalmente a través de USENET, en la que los suscriptores dejan mensajes a todo el grupo sobre temas específicos.

GUI: Acrónimo de "*Graphical User Interface"* (Interface Gráfico de Usuario). Colección gráfica de iconos, carpetas, escritorio, cajas de diálogo, etc. que se activan o desactivan por medio del ratón. En definitiva, se llama así a todo programa o aplicación que se ejecuta en un entorno gráfico, y cuyo interface es gráfico.

H

HACKER: Persona que tiene muchos conocimientos del mundo de las redes. Normalmente se dedican a comprobar la seguridad de las redes, intentando acceder a ellas de forma no autorizada, para examinar los fallos de seguridad y corregirlos. No se les debe confundir con los crackers, cuyas intenciones no son tan buenas.

HAYES AT: Lenguaje de mandatos de control de modems. Entre sus muchos mandatos se hallan los que sirven para inicializarlos, para ordenarles que marquen un número o que cuelguen.

HANDSHAKING: Método para controlar el flujo de datos entre dos dispositivos.

HEADER: Ver cabecera.

HEADING: Ver encabezamiento.

HERZIO (HZ)**:** Unidad con la que se mide la frecuencia de las vibraciones de las ondas eléctricas, y que representa 1 ciclo/segundo. Se utiliza para medir la velocidad de trabajo de los microprocesadores, la frecuencia de refresco de la información que se visualiza a través de los monitores...

HIPERMEDIA: Combinación de texto y multimedia. Actualmente es un recurso ampliamente explotado en el World Wide Web.

HIPERTEXTO: *(hypertext)* Cualquier texto que contiene enlaces a otros documentos. Determinadas palabras o frases en el documento, (que están unidas a otro documento o parte del mismo mediante un enlace), al ser activadas (normalmente mediante un clic del ratón), provocan la recuperación y posterior visualización del documento enlazado.

HOME PAGE: Ver Página de inicio.

HOP (salto): Término utilizado para denominar cada uno de los pasos que es preciso dar en orden de llegar de un punto de origen a otro de destino a lo largo de una red a través de enrutadores.

HOST: Anfitrión. En una red local, ordenador que realiza todas las funciones de mantenimiento centralizadas, y pone a disposición de otros usuarios los programas y proporciona otros servicios.
En Internet, se llama así a un ordenador conectado a la red, que tiene su propio número IP y nombre de dominio, y que sirve información a través de WWW.

HREF: Marca de enlace usada en HTML, para designar la dirección de destino del enlace. Permite especificar una dirección de enlace dentro de un documento HTML.

HTML: Acrónimo de "*HiperText Markup Language"* (Lenguaje de Marcas de Hipertexto). Es el lenguaje con que se escriben los documentos en el World Wide Web.
HTML sigue un modelo de desarrollo abierto. Cuando una nueva característica es propuesta, es implementada en algunos clientes y probada en algunas aplicaciones. Si la demanda para esta nueva característica es suficiente, otras implementaciones son animadas a seguir esta nueva demanda, y la nueva característica llega a ser ampliamente empleada. En este proceso, el diseño es revisado y quizás modificado o potenciado. Finalmente, cuando existe suficiente experiencia con esta nueva característica, llega a ser parte del conjunto estándar de HTML. La versión más extendida actualmente es la 3.2, aunque ya está disponible la 4.0.

HTTP: Acrónimo de "*HyperText Transport Protocol"* (Protocolo de Transporte de Hipertexto). Protocolo para mover archivos de hipertexto a través de la Internet. Requiere un programa cliente HTTP en un extremo y un programa servidor de HTTP en el otro. HTTP es el protocolo más importante usado en el WWW y se ha usado desde sus inicios en 1990.

HTTPS: Creado por Netscape Communications Corporation para designar documentos que llegan desde un servidor WWW seguro. Esta seguridad es dada por el protocolo SSL (Secure Sockets Layer) basado en la tecnología de encryptación y autentificación desarrollada por la RSA Data Security Inc.

HYPERTERMINAL: Programa de comunicaciones para módem incluido en el sistema operativo Windows.

I

IEEE (Institute of Electrical and Electronic Engineers): Asociación internacional que regula los estándares informáticos y electrónicos.

IMAP: Protocolo de Acceso a Mensajes de Internet (*"Internet Message Access Protocol"*). Protocolo diseñado para permitir la manipulación de buzones remotos como si fueran locales.
IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el buzón y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el buzón hasta que el usuario confirma su eliminación.

IMG: Abreviatura de "image". Se usa para designar un enlace con un archivo gráfico. Sólo se pueden visualizar con browsers gráficos, que en ocasiones permiten desactivar el proceso de las imágenes, si va a ocupar mucho tiempo**.**

INFOVÍA PLUS: Servicio creado y promovido por Telefónica para universalizar el acceso de los ciudadanos a las llamadas Autopistas de la Información, sucesor de la desaparecida Infovía. Aunque utilizaba la tecnología Internet (protocolos, WWW, ..) Infovía Plus no era Internet, si bien los usuarios de Infovía Plus podían conectarse a dicha red a través de proveedores Internet conectados a su vez con esta red (Basada en la Red UNO).

INTERFERENCIA: Fluctuaciones no deseadas de un sistema eléctrico que distorsionan o alteran las señales.

INTERNET: La gran colección de redes interconectadas que usan protocolo TCP/IP y que evolucionó de ARPANET a finales de los 60 y principios de los 70. Internet conecta hoy por hoy a 60.000 redes independientes dentro de la red mundial global.
Es la red de redes. Nacida como experimento del ministerio de defensa americano, conoce su difusión más amplia en el ámbito científico-universitario. Embrión de las 'superautopistas de la información'. Para convertirse en ellas faltan aún mayores infraestructuras y anchos de banda.

Desde el punto de vista técnico, Internet es un gran conjunto de redes de ordenadores interconectadas (la mayor red mundial). Desde otro punto de vista, Internet es un fenómeno sociocultural: un usuario desde su ordenador, tiene acceso a la mayor fuente de información que existe.
En cuanto a funcionamiento interno, Internet no se ajusta a ningún tipo de ordenador, tipo de red, tecnología de conexión y medios físicos empleados. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión. La familia de protocolos *TCP/IP* es la encargada de aglutinar esta diversidad de redes.
A principios de 1.992 fue creada la "Internet Society" (ISOC). Se trata de una sociedad profesional sin ánimo de lucro, formada por organizaciones e individuos de todos los sectores involucrados de una u otra forma en la construcción de Internet (usuarios, proveedores, fabricantes de equipos, administradores, etc.). El principal objetivo es fomentar el crecimiento de la Internet en todos sus aspectos (número de usuarios, nuevas aplicaciones, infraestructuras, etc.)

INTRANET: Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo *TCP/IP* y servicios similares como *WWW*.
Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

IP: *(Internet Protocol)* Protocolo de Internet. Es la parte del protocolo TCP/IP encargada del direccionamiento, (identificación del origen y destino). Ver Dirección IP. Protocolo que gestiona la forma en la que los ordenadores conectados a Internet se comunican e intercambian información. Se gestiona asignando a cada ordenador conectado a Internet un identificador IP formado por cuatro números separados por puntos. La asignación y coordinación de estos números lo realiza la sociedad INTERNIC.

IPX: *"Internet Packet Exchange"*. Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware**.**

ISDN: Acrónimo de "*Integrated Services Data Network"*. Ver RDSI.

IrDA (Infrared Data Association): Sistema para la transmisión de información mediante infrarrojos.

IRC: Acrónimo de "*Internet Relay Chat"* (Grupo de discusión de Internet). Se trata de una gran área de discusión multi-ususario. Hay una gran cantidad de servidores de IRC a lo largo del mundo, que están interconectados entre ellos. En un canal de participación, las personas pueden "hablar" en tiempo real, tecleando sus opiniones, que pueden ser leídas al tiempo que se escriben por todas las personas del grupo de discusión.

IRC trabaja en arquitectura Cliente/Servidor. El usuario rueda un programa cliente llamado 'irc', el cual conecta vía red con otro programa servidor. La misión del servidor es pasar los mensajes de usuario a usuario a través de la red irc.

ISO (International Standarization Organitation): "Organización Internacional para la Estandarización -- Organización que ha definido un conjunto de protocolos diferentes, llamados protocolos ISO; y es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática, las ecológicas y las comunicaciones. Está formada por las organizaciones de normalización de sus 89 países miembros."

ISP (Internet Service Provider): Empresas o instituciones proveedoras de acceso a Internet para los particulares y las empresas. Organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc.). Los factores que se deben considerar para elegir un proveedor de Internet son: a) Ancho de Banda (velocidad ofrecida por el proveedor para transmitir datos). b) Tipo de conexión (directa o conmutada). c) Costo por hora, mes o año (tanto de la conexión como del registro del correo electrónico en un servidor). d) Numero de usuarios por línea disponible. e) Seguridad (Confianza en la ética del proveedor para respetar los datos de los usuarios).

J

JAVA: Lenguaje de programación orientado a objetos, diseñado por Sun Microsystems para el desarrollo de aplicaciones multiplataforma y para la WWW. Se puede describir como una versión simplificada de C++. Además, Java implementa muchas características de seguridad en tiempo de compilación y de ejecución, para asegurar la aplicación que se ejecuta. Pero la novedad de este lenguaje es que es independiente de la plataforma cliente, y las applets se ejecutan en el sistema cliente.
Java es un lenguaje orientado a objetos. Comparte similitudes con *C*, *C++* y *Objetive C*. Basándose en otros lenguajes orientados al objeto, Java recoge lo mejor de todos ellos y elimina sus puntos más conflictivos.
El principal objetivo de JAVA fue hacer un lenguaje que fuera capaz de ser ejecutado de una forma segura a través de Internet (aunque el código fuera escrito de forma maliciosa). Esta característica requiere la eliminación de muchas construcciones y usos de C y C++. El más importante, es que no existen punteros. Java no puede acceder arbitrariamente a direcciones de memoria.
Java es un lenguaje compilado en un código llamado *"código-byte" (byte-code)*. Este código es interpretado *"en vuelo"* por el interprete Java.

Java fue diseñado también para escribir código libre de *bugs*, esto se consigue en gran parte, eliminando las operaciones de localización y desalocalización de memoria del lenguaje C.
Java no es un lenguaje para ser usado solo en el WWW, pero su despegue y utilización se debe al World Wide Web. Hoy día casi todos los browser interpretan código Java.

JAVASCRIPT: Lenguaje interpretado desarrollado por Netscape para dotar de mayor interactividad a las páginas Web. En contra de lo que pudiera parecer JavaScript no está relacionado directamente con Java, su nombre se debe únicamente a cuestiones de "Marketing".

JPEG: Acrónimo de *Joint Photographic Experts Group* (Grupo de expertos fotógrafos) Es, como gif, un formato para archivos gráficos, y un estándar para imágenes en Web. Los archivos de este formato tienen extensión ".jpg". Lo que diferencia a los formatos gif y jpeg es cómo se comprimen los datos (con pérdidas en jpeg, y sin pérdidas en gif) y la profundidad de bits (8 bits para gif, y 24 bits para jpeg). Su algoritmo de compresión es especialmente eficiente con imágenes de tono continuo como fotos de personas, paisajes, etc.

K

KILOBYTE: Mil bytes. Actualmente es usado como 1024 (dos elevado a la 10) bytes.

KBPS (Kilobits por segundo): Unidad para medir la velocidad de transmisión de los datos que equivale a 1.024 bits por segundo.

L

LAN: Acrónimo de *Local Area Network* (Red de Área Local). Red de ordenadores limitada a un área inmediata, que es normalmente el mismo edificio o piso de un edificio, pero que puede llegar a extenderse hasta varios kilómetros. Para distancias mayores se suele emplear mejor el término MAN.

LATIN-1: Se conoce también este código como ISO 8879. Se trata de un conjunto de caracteres de 8 bits que contiene, por lo tanto, 256 caracteres, de los cuales, los primeros 32 son caracteres no imprimibles como el tabulador o salto de línea. Incluye los caracteres marcados diacríticamente usados en lenguas europeas como el francés y el alemán (aunque no incluye la L polaca, la r y s checas, o la i sin puntuación turca).

LÁSER: Haz de luz muy preciso y potente, con diversas aplicaciones (tanto en informática como en general): sistemas de medición, dispositivos de control, lectores y grabadoras de CD-ROM, impresoras láser, sistemas de almacenamiento óptico, etc.

LENGUAJE INTERPRETADO: Lenguaje cuyos programas se traducen a código máquina sobre la marcha en el momento de su ejecución; tiene la ventaja de ser independiente de la máquina en que se ejecuta. Su inconveniente es la lentitud, dado que al tiempo de ejecución hay que añadir el de traducción a lenguaje máquina.

LÍNEA CONMUTADA (dial up): "Conexión temporal que se establece usando un emulador de terminal y un módem; en oposición a conexión dedicada o permanente, la cual es establecida entre ordenadores por línea telefónica normal y realiza una conexión de datos a través de una línea telefónica."

LÍNEA DEDICADA: Línea privada que se utiliza para conectar redes de área local de tamaño moderado a un proveedor de servicios de Internet y se caracteriza por ser una conexión permanente.

LÍNEA DIGITAL DE ABONADO DE ALTA VELOCIDAD (HDSL): Sistema de transmisión de datos de alta velocidad que utiliza dos pares trenzados.

LÍNEA DIGITAL SIMÉTRICA DE ABONADO (SDSL): Sistema de transferencia de datos de alta velocidad en líneas telefónicas normales.

LÍNEAS DE SUBSCRIPCIÓN DIGITAL (XDSL): Tecnología de transmisión que permite que los hilos telefónicos de cobre convencionales transporten hasta 16 Mbps mediante técnicas de compresión. Hay diversas modalidades de esta tecnología, tales como ADSL, HDSL y RADSL, siendo la Línea de Suscripción Asimétrica Digital (ADSL) la más utilizada actualmente.

LINK: Enlace, hiperenlace. Ver HREF, TELNET, FTP, GOPHER, HTTP.

LINUX: Linux es una implementación independiente del sistema operativo UNIX. Tiene extensiones System V y BSD, y ha sido escrito completamente a base de aportaciones desinteresadas, por eso su código es libre y gratuito. Funciona sobre distintas plataformas y con distintas arquitecturas (ISA, EISA), y requiere un procesador 386 o superior.
El kernel de Linux fue escrito por *Linux Torvalds (Torvalds@kruuna.helsinki.fi)*, desde Finlandia y otros voluntarios de otras partes del mundo. La mayoría de los programas que ruedan bajo linux son freeware, y muchos de ellos del *Proyecto GNU*.
Linux tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitarea real, memoria virtual, librerías compartidas, dirección y manejo propio de memoria y TCP/IP. Usa las características hardware de la familia de procesadores 386 para implementar las capacidades anteriores.

LUCAS: LinUx CAStellano.

LOGIN: Clave de acceso que se le asigna a un usuario para que pueda utilizar los recursos de una computadora. También define la acción de entrar en un sistema de ordenadores.

M

MACINTOSH*:* Serie de ordenadores de Apple Computer. Poseen un sistema operativo basado en una interfaz gráfica de usuario similar al de MS Windows, aunque cronológicamente los Macintosh fueron los pioneros.

MAIL: Programa cliente para la edición, lectura y respuesta de correo electrónico en entornos UNIX. El correo electrónico es el servicio más básico, antiguo, y más utilizado dentro de Internet.
La mensajería electrónica es el medio más eficaz y más rápido de comunicación, permite intercambiar además de mensajes, programas, audio, vídeo e imágenes. Cada usuario dentro de un sistema posee una dirección de correo formada por: nombre de usuario, @ y nombre de ordenador o dominio al que pertenece el usuario, por ejemplo:

usuario@ordenador.dominio.subdominio

MAILING LIST: Listas de correo o listas de distribución, establecen foros de discusión privados a través de correo electrónico.
Las listas de correo están formadas por direcciones e-mail de los usuarios que la componen. Cuando uno de los participantes envía un mensaje a la lista, ésta reenvía una copia del mismo al resto de usuarios de la lista (inscritos en ella).
Las listas pueden ser:
• abiertas: cualquier persona puede subscribirse y participar en ella.
• cerradas: Existe un dueño y moderador de la lista, que decide quien puede entrar en ella.
El fichero ftp://usc.edu/net-resources/interest-groups es la lista de todas las listas.

MAN: Red de área metropolitana (*Metropolitan Area Network*). Red que no va más allá de los 100 km.

MARCADOR: Se utiliza este término para designar la característica que tienen algunos navegadores de archivar la dirección URL de una página Web, como si de una agenda se tratara. De esta manera, cuando queremos acceder a dicha página, basta con utilizar esta función, y nos conectaremos su dirección. Una colección de marcadores se denomina lista de marcadores.

MEGABITS POR SEGUNDO (MBPS): Unidad de medida de la capacidad de transmisión por una línea de telecomunicación donde cada megabit está formado por 1.048.576 bits.

MEGAHERTZIO (MHz): Un millón de Hertzios. Unidad de frecuencia que se utiliza para medir la velocidad de proceso de los microprocesadores.

***MENSAJE**: (message)* La unidad básica de la comunicación HTTP, consistente en una secuencia estructurada de octetos que se ajustan a la sintaxis y transmitidos por medio de la conexión.

MIME: Acrónimo de *Multipurpose Internet Mail Extensions* (Extensiones de Correo de Internet Multifunción). Estándar para adjuntar archivos a mensajes de correo de Internet, por ejemplo archivos que no son de texto, como gráficos, documentos de procesadores de texto formateados, archivos de sonido, etc. Cuando un programa cliente de correo electrónico envía archivos de no texto, usando el estándar MIME, se convierten (codifican) a texto, aunque, en realidad, el texto resultante no se puede leer (no es legible). El estándar MIME es una manera de especificar tanto el tipo de archivo que se envía como el método que se debería usar para devolverle su formato original. Además de software de correo electrónico, el estándar MIME se usa para identificar los archivos que se envían a clientes Web, nuevos formatos de ficheros se pueden acomodar simplemente actualizando la lista de browsers de pares de tipos MIME y el software apropiado para manejar cada tipo.

MIRROR: Término usado en Internet para hacer referencia a un FTP, WEB o cualquier otro recurso que es espejo de otro. Estos mirrors se realizan automáticamente y en una frecuencia determinada, y pretenden tener una copia exacta del lugar del que hacen mirror.

MÓDEM: Palabra que provienen de la fusión de las palabras modulador/demodulador. El módem pone en comunicación un ordenador con la línea telefónica, permitiéndole acceder a redes telemáticas y comunicarse con otros ordenadores.
Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados (ISDN), mediante un procesos denominados modulación (para transmitir información) y demodulación (para recibir información). La velocidad máxima que puede alcanzar un módem para línea telefónica es de 33 kBps, sin embargo los más comerciales actualmente son los de 28 kBps. Un módem debe cumplir con los estándares de MNP5 y V42.bis para considerar su adquisición. Los módems pueden ser en internos (los que se colocan en una ranura de la computadora) y en externos (que se conectan a un puerto serial de la computadora).

MODULACIÓN DE SEÑAL: Proceso mediante el cual se transforma una señal original para adaptarla al canal a través del cual se va a transmitir (este proceso se realiza sobre una señal que servirá de soporte llamada "señal portadora"). Por ejemplo, un módem modula la señal digital del ordenador para poder transmitirla a través de las líneas telefónicas analógicas.

MOSAIC: El primer visualizador (*browser*) de WWW disponible para Macintosh, Windows y UNIX con el mismo dispositivo. "Mosaic" comenzó la popularidad del Web. El código fuente de Mosaic ha sido tomado por varias empresas.

MS-DOS: *Microsoft Disk Operating System*. Sistema Operativo en Disco de Microsoft. Sistema operativo muy extendido en PC del tipo de línea de comandos.

MULTICASTING*:* Técnica de transmisión de datos a través de Internet que consiste en el envío de paquetes de información desde un punto a varios destinatarios simultáneamente.

MULTIDIFUSIÓN: Método de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y, por lo tanto, por múltiples usuarios.

N

NCSA: Abreviatura de National Center for Supercomputing Applications de la Universidad de Illinois de Urbana-Champaign, un instituto de investigación avanzada cuyos científicos e ingenieros desarrollaron gran parte de la tecnología que es el fundamento de World Wide Web. NCSA desarrolló el primer explorador capaz de mostrar gráficos, llamado *Mosaic*.

NetBEUI: Este término proviene de NetBIOS Extended User Interface. Se trata de un controlador de dispositivo de red. Es el controlador de transporte proporcionado con LAN Manager (Administrador de Red Local de Microsoft), y es el protocolo de comunicación entre redes LAN.

NETIQUETTE: Combinación de *net y etiquette*, un código tácito de reglas para preservar las buenas maneras y la eficiencia en el uso de Internet.

NETSCAPE*:* Es un browser WWW y el nombre de una empresa. Esta herramienta de navegación estaba basada, en un principio, en el programa Mosaic, desarrollado por la NCSA. Netscape ha crecido en sus características rápidamente y hoy es uno de los dos grandes navegadores de la Web.

NETWORK: Red de trabajo entre varios ordenadores. Máquina de computación cuyo objetivo exclusivo es el de conectarse a la red y que por tanto incorpora únicamente los recursos hardware y software necesarios para tal fin. Es capaz de sintonizar canales de TV e Internet a través de un módem y utilizando el WWW. Se espera que su utilización se extienda más en el futuro conforme vayan aumentando las prestaciones y se reduzca su precio. También es llamada NET PC, Web PC y Web TV.

NETWORKING: Término utilizado para referirse a las redes de telecomunicaciones en general.

NEWS: Es el tablón de anuncios electrónico. Permite al usuario participar en grupos de discusión, mediante el envío de mensajes, o bien sólo acceder a estos grupos para obtener información.

Los mensajes están clasificados por temas y se integran por grupos (*newsgroups*). News es un conjunto de Newsgroups distribuidos electrónicamente en todo el mundo. Los grupos pueden estar moderados o no, en el primer caso, el moderador decide que mensajes aparecerán.
Servicio de mucha actividad. La distribución de los mensajes utiliza el método de transporte NNTP, esta forma de transmisión está basada en el código de identificación de la cabecera del mensaje. Cuando un NNTP local ofrece un artículo a una máquina vecina, le indica también el código de identificación, si esta máquina no lo tiene, le pide que se lo envíe.

NICK: Nombre o pseudónimo que utiliza un usuario de *IRC.* Ver alias.

NODO: Cualquier ordenador conectado a una red.

NODO DE INTERNET: Cualquiera de los servidores que están permanentemente conectados en Internet.

NOMBRE DE DOMINIO: *(domain name)* Nombre que identifica el punto de Internet. Los nombres de dominio tienen dos o más partes, separadas por puntos. La parte de la izquierda es la más específica, mientras que la de la derecha es la más general. Un ordenador puede tener más de un nombre de dominio, pero un determinado nombre de dominio sólo se refiere a una máquina. Normalmente, todos los ordenadores de una red tendrán el mismo nombre que la parte derecha de sus nombres de dominio. Es posible que un nombre de dominio exista pero no esté conectado a un ordenador. Esto ocurre a menudo, de tal modo que un grupo o empresa puede tener una dirección de correo electrónico sin tener que establecer un punto real en Internet.

NOMBRE DE USUARIO: *(userid, username)* El nombre que utiliza el usuario cuando accede a otro ordenador.

O

OPERADORES LÓGICOS: *(logic operators)*. También llamados operadores booleanos (del álgebra de Bool), se usan en los buscadores para restringir una búsqueda y eliminar resultados no deseados. Son los operadores AND (y), para añadir un término; NOT (no) para excluirlo, y OR (o) para hacer una elección.

OSI: Acrónimo de *Open System Interconnection* (Interconexión de sistemas abiertos). Conjunto de protocolos diseñados por comités ISO con el objetivo de convertirlos en estándares internacionales de arquitectura de redes de ordenadores. El modelo de referencia OSI proporciona la base para el desarrollo de estándares relativos a las redes. Este modelo enumera siete capas que definen las actividades que deben tener lugar cuando se comunican los dispositivos a través de una red. Estas siete capas (de arriba a abajo) son: aplicación, presentación, sesión, transporte, red, enlace y física.

El modelo representa las relaciones entre una red y los servicios que puede soportar como una jerarquía de capas de protocolos. Cada capa usa los servicios ofrecidos por capas más bajas además de sus propios servicios para crear otros nuevos que estén disponibles para capas superiores.
En resumen, cada una de las siete capas del modelo de referencia OSI realiza tareas únicas y específicas, conoce las capas inmediatamente adyacentes, usa los servicios de la capa que está por debajo, y realiza funciones y proporciona servicios para las capas superiores.

P

PÁGINA DE INICIO: (home page) También llamada página principal, es la primera página que aparece cuando se accede a un servidor de páginas Web, y es desde donde se puede explorar dicho servidor.

PÁGINA WEB: *(Web page)* No se trata de una página en el sentido literal, sino un documento completo editado en la World Wide Web. La página principal (en inglés home page) es la primera página que aparece cuando se entra en un puesto de Web al que se ha llamado.

PAR TRENZADO: Dispositivo parecido al cable telefónico el cual contiene una mayor cantidad de cables. Es el medio físico por el cual pueden conectarse varias computadoras.

PERIFÉRICO: Cualquier componente que se le incorpora a un ordenador para ampliar sus capacidades.

PERL: Perl es un lenguaje para manipular textos, ficheros y procesos. Perl proporciona una forma fácil y legible para realizar trabajos que normalmente se realizarían en C o en alguna Shells. Podría decirse que Perl está a caballo entre un lenguaje de alto nivel (tipo C) y una "*Commands shell*. Perl rueda en varios sistemas operativos y permite portar los fuentes a diferentes plataformas. No obstante, donde nació y donde más se ha difundido es bajo el sistema operativo UNIX.
Perl fue desarrollado por Larry Wall (lwall@netlabs.com), y está distribuido libremente bajo licencia de GNU.

PETABYTE (PB): Unidad de medida de la capacidad de memoria y de dispositivos de almacenamiento informático (disquete, disco duro, CD-ROM, DVD, etc.). Un PB corresponde a 1.024 billones (2^50) de bytes. Todavía no se han desarrollado memorias ni dispositivos de almacenamiento de esta capacidad.

PING (Packet Internet groper): Sin lugar a dudas en una red el comando que más se puede llegar a utilizar es ping. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa.

Su función más habitual es simplemente verificar si una máquina está encendida. Lo que se está haciendo en realidad es mandar paquetes del tipo ``echo request'', y para los que se devuelven son del tipo ``echo reply''

POP: Acrónimo de *Post Office Protocol* (Protocolo de Oficina de Correo). Protocolo para almacenar y recibir correo electrónico. Algunos programas de correo electrónico usan este protocolo, como Eudora.

PORTADORA: Señal que transporta determinada información mediante la modulación de su amplitud, frecuencia o fase.

PPP: Acrónimo de *Point to Point Protocol* (Protocolo de Punto por Punto). Es más conocido como el protocolo que permite que un ordenador use una línea telefónica regular y un módem para realizar conexiones TCP/IP.

PROVEEDOR DE SERVICIO: *(provider)* Empresa que proporciona acceso a Internet, o a servicios de correo electrónico, FTP, Gopher, etc., por medio de una tarifa mensual. Ver CPI.

PROTOCOLO: *(protocol)* Sistema de reglas o estándares para comunicarse a través de una red, en especial a través de Internet. Los equipos y las redes interactuan de acuerdo con los protocolos que determinan el comportamiento que cada lado espera del otro en la transferencia de información.

PROTOCOLO DE ACCESO A MENSAJES DE INTERNET (IMAP): Protocolo diseñado con el fin de permitir la manipulación de buzones remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el buzón y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el buzón hasta que el usuario confirma su eliminación. Un programa característico es Pine.

PROTOCOLO DE AUTENTIFICACIÓN POR CONTRASEÑA (PAP): Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante una contraseña.

PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP): Forma de comunicación básica de Internet la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

PROTOCOLO DE DATAGRAMAS DE USUARIO (UDP): Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda y como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada debido a que un paquete perdido no afecta la

calidad del sonido. Entre las aplicaciones que utilizan este protocolo encontramos a Real Audio.

PROTOCOLO DE LÍNEA SERIAL COMPRIMIDA (CSLIP): "Versión mejorada del SLIP desarrollada por Van Jacobson la cual, principalmente, trata; en lugar de enviar las cabeceras completas de los paquetes; enviar solo las diferencias."

PROTOCOLO DE LÍNEAS SERIALES DE INTERNET (SLIP): Protocolo utilizado para gestionar el protocolo Internet (IP) en líneas seriales tales como circuitos telefónicos o cables RS-232, interconectando dos sistemas SLIP está definido en RFC 1055 pero no es un estándar oficial de Internet y está siendo reemplazado por el protocolo PPP. Esta implementación de TCP/IP por líneas seriales permite conectar un módem a Internet mediante un protocolo SLIP o PPP.

PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN DE RETORNO (RARP): Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

PROTOCOLO DE TIEMPO REAL (RTP): Protocolo utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una videoconferencia.

PROXY: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red.
Al mismo tiempo contiene mecanismos de seguridad (cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada. Los servidores proxy implementan el rendimiento del servidor, al servir las páginas de manera local en una "caché".

PUENTE (BRIDGE): Dispositivos que tienen usos definidos como interconectar segmentos de red a través de medios físicos diferentes (es usual ver puentes entre un cable coaxial y otro de fibra óptica). Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI).

PUERTO: *(port)* Se llama así a un lugar donde la información entra o sale de un ordenador o ambas cosas. Por ejemplo, el "puerto serie" de un ordenador es donde se conectaría un módem. En Internet, puerto también se refiere a menudo a un número que es parte del URL, apareciendo tras el signo ":", justo después del nombre de dominio.

R

RAS: *Remote Access Server*. Servidor de Acceso Remoto.

RASTREADOR DE PAQUETES INTERNET: Programa utilizado para comprobar si un Host está disponible debido a que envía paquetes de control para comprobar si dicho host está activo y los devuelve.

RASTREADOR DE SEGURIDAD DE INTERNET (ISS): Programa que busca puntos vulnerables de la red con relación a la seguridad.

RDSI (ISDN): Acrónimo de *Red digital de servicios integrados*, (ISDN: *Integrated Services Data Network*). Una red que actúa como un servicio de conexión digital para los teléfonos y otros dispositivos de comunicación.
Una conexión RDSI puede proporcionar una velocidad de acceso a Internet relativamente alta (hasta 128000 bits por segundo, usando las líneas telefónicas existentes, (o sea, un par de hilos de cobre).

RECURSO: *(resource)* Objeto de datos de red o servicio que puede identificarse por un URI. Se llama así a la información que se encuentra en Internet, ofrecida por los servidores.

RED: *(network)*. Grupo de ordenadores y otros dispositivos periféricos conectados unos a otros para comunicarse y transmitir datos entre ellos.

RED AISLADA (stub network): "Red que distribuye paquetes desde y hacia sistemas locales; e inclusive, aunque tenga definidas rutas a alguna otra red, no le transmite mensajes. "

RED DE ACCESO: Conjunto de elementos que permiten conectar a cada abonado con la central local de la que es dependiente.

RED DE ÁREA DOMÉSTICA (HAN): Conjunto de dispositivos de todo tipo, informáticos (PCs y sus periféricos) o no (electrodomésticos) instalados en un hogar y conectados entre sí. Todos ellos pueden incluso ser operados a distancia mediante Internet.

RED DE ÁREA LOCAL (LAN): Red cuyas dimensiones no exceden 10 km. como computadoras conectadas en una oficina, en un edificio o en varios. Por ende, pueden optimizarse los protocolos de señal de la red hasta alcanzar velocidades de transmisión de 100 Mbps .

RED DE ÁREA METROPOLITANA (MAN): Red que no va más allá de los 100 km. Comprende los equipos de computo y sus periféricos conectados en una ciudad o en varias.

RED DE ÁREA MUNDIAL (WAN): "Red de computadoras conectados entre sí en un área geográfica relativamente extensa. Este tipo de redes suelen ser públicas, es decir, compartidas por muchos usuarios; y pueden extenderse a todo un país o a muchos a través del mundo"

RED INALÁMBRICA: Red que no utiliza como medio físico el cableado sino el aire y generalmente utiliza microondas o rayos infrarrojos.

RED PRIVADA VIRTUAL: Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

RED TELEFÓNICA CONMUTADA (RTC): Red de teléfono diseñada primordialmente para la transmisión de voz, aunque pueda también transportar datos, como es el caso de la conexión a Internet a través de la red conmutada.

RedIRIS: Red pública dependiente del C.S.I.C. (Centro Superior de Investigaciones Científicas) que proporciona servicios Internet a la comunidad académica y científica española. Es también el NIC local, es decir, el organismo que se encarga de la asignación de direcciones Internet en España.

RENDER: Proceso mediante el que un ordenador crea una imagen partiendo de la descripción de las características de los objetos que contiene (geometría, color, textura, posición de la luz, etc.).

RF (Radio Frequency): Tecnología utilizada en radio, televisión y redes de banda ancha para transmitir la información. Utiliza señales portadoras del rango de megahercios (MHz)

RFC: Acrónimo de *Request for Comments* (Petición de Comentarios). Resultado y proceso de creación de un estándar en Internet. Los nuevos estándares se proponen y publican en Internet, como RFC. El grupo de trabajo de ingeniería de Internet (IETF) es un cuerpo de opinión que admite discusión a través de comentarios, en los que se establece un nuevo estándar.

RJ-11: Conector telefónico estándar muy utilizado en USA. Es parecido a RJ-14, pero éste último es doble

RJ-45: Conector para cable de Par Trenzado

RTC o RTB: Red Telefónica Conmutada o Red Telefónica Básica. Red Telefónica para la transmisión de voz.

ROUTER: Encaminador. Ordenador con fines especiales (o paquete de software) que maneja la conexión entre dos o más redes. Los routers usan su tiempo mirando las direcciones de destino de los paquetes, pasando a través de ellas y decidiendo qué ruta enviarles.

Dispositivo que distribuye trafico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento.

S

SCSI: Acrónimo de *Small Computer System Interface*. Es una interfaz del estándar ANSI (*American National Standards Institute*), para la comunicación en alta velocidad de datos paralelos entre ordenadores y sus dispositivos periféricos. La velocidad que proporciona la interfaz SCSI es un elemento importante que permite conectar hasta siete dispositivos SCSI diferentes en una conexión. Se lee "escasi".

SEARCH ENGINE: Motor de búsqueda. Herramienta que realiza búsquedas en sus propias bases de datos desde el ordenador cliente. También llamados buscadores, estas aplicaciones son muy útiles para navegar por Internet, pues nos indican dónde encontrar la información necesaria, pudiendo ir a ese lugar mediante un enlace.

SEÑALES ANALÓGICAS: Una SEÑAL ANALÓGICA Es una señal que puede variar de manera continua. Entre dos valores próximos siempre se pueden considerar valores intermedios. La temperatura que registra un termómetro de mercurio proporciona señales analógicas.

SEÑALES DIGITALES: Una SEÑAL DIGITAL Es una señal que sólo puede variar de manera discreta. Entre dos valores consecutivos no puede haber ningún valor intermedio. Un reloj digital proporciona señales digitales.

SGML: Acrónimo de *Standard Generalized Markup Language* (Lenguaje Estándar de Marcas Generalizado). Conjunto de estándares usados para unir los elementos de un documento electrónico, para facilitar su producción en distintos medios. Este lenguaje es el padre del HTML, con el que se construyen los documentos en hipertexto.

SHAREWARE: Software protegido por leyes de copyright, que se encuentra disponible gratuitamente durante cierto tiempo para su evaluación por el usuario. Tras pasar dicho tiempo, el programa expira y no podrá volver a ser utilizado, a no ser que el usuario registre el programa por un precio.
Frecuentemente, el shareware es desarrollado por pequeñas compañías o programadores individuales que se disponen a resolver un problema específico de los equipos o que desarrollan una aplicación novedosa. En algunos casos, cuando se envía el pago, se recibe posteriormente documentación junto con el software. Comparar con freeware.

SÍNCRONO: Método de comunicación serie en el que los datos se envían como un flujo continuo de bits.

SIGNATURE: Firma. Mensaje de tres o cuatro líneas situado al final de un mensaje de correo electrónico o de un articulo de Usenet que identifica a su autor. Las firmas con mas de cinco líneas suelen estar muy mal vistas.

SLIP: Acrónimo de *Serial Line Internet Protocol* (Protocolo de Internet de Línea en serie). Es un estándar para usar una línea telefónica y un módem para hacer de un ordenador un servidor de Internet. Este protocolo ha sido casi completamente reemplazado por PPP.
Junto con PPP (Point-to-Point Protocol) son estándares para transmisión de paquetes IP (Internet Protocol) sobre líneas serie (líneas telefónicas). La información de Internet es empaquetada y transmitida en paquetes IP.
Un proveedor de servicio de acceso a Internet puede ofrecer SLIP, PPP o ambos. El ordenador debe usar un software de conexión (normalmente suministrado por el proveedor) que marca el protocolo de conexión con el servidor. PPP es un protocolo más reciente y robusto que SLIP.

SLIP dinámico: Cuando se usa SLIP para conectarse a Internet, el servidor del proveedor de acceso a Internet, identifica al ordenador proporcionándole una dirección IP (por ejemplo 150.214.110.8). Mediante SLIP dinámico, ésta dirección es asignada dinámicamente por el servidor de entre un conjunto de direcciones. Esta dirección es temporal, y dura lo que dure la conexión.

***SLIP estático*:** Cuando se usa SLIP estático, el servidor del proveedor de acceso a Internet asigna una dirección permanente al ordenador para su uso en todas las sesiones.

SMILEYS: Son los gestos del lenguaje corporal a través de la red, simbolizados en simpáticas caritas que expresan el sentimiento del autor. Por ejemplo, moviendo la cabeza hacia abajo y girándola 90º a la izquierda, se puede ver una carita sonriente en :-) . Ver Emoticon.

SMTP: *Acrónimo* de *Simple Mail Transfer Protocol*; protocolo que se utiliza para el envío de mensajes de correo electrónico.
Protocolo utilizado para transferir mensajes de correo electrónico entre ordenadores.
Dicho protocolo es definido en STD 10, RFC 821, y se usa para la transferencia de correo electrónico entre computadoras. Es un protocolo de servidor a servidor, de forma que para poder leer los mensajes se deben utilizar otros protocolos.

SNMP: Acrónimo de Simple Network Management Protocol. Protocolo estándar para la administración de red en Internet. Prácticamente todos los sistemas operativos, routers, switches, módems cable o ADSL módem, firewalls, etc. se ofrecen con este servicio.

SOCKET: Número de identificación compuesto por dos números: la dirección IP y el número de puerto TCP. En la misma red, el número IP es el mismo, mientras que el número de puerto es el que cambia.

En máquinas de distintas redes, pueden tener el mismo número de puerto sin llevar a confusión, pues el número IP las distingue.

SPAM: Se llama así al "bombardeo" con correo electrónico, es decir, mandar grandes cantidades de correo o mensajes muy largos indiscriminadamente a listas de usuarios para hacer publicidad o difundir información que los usuarios no han solicitado.

SPAMMEr: El que realiza *spam*.

SSL: Acrónimo de *Secure Socket Layer* (Capa de toma de corriente segura) Protocolo de bajo nivel utilizado para encriptar transacciones en un protocolo de mayor nivel como el HTTP, FTP y NNTP, entre clientes y servidores.

T

TCP/IP: Acrónimo de *Transmission Control Protocol*/Internet Protocol (Protocolo de Internet/Protocolo de Control de Transmisión).
Es el tipo de protocolos que define la Internet. Diseñado originalmente por el sistema operativo UNIX, el software TCP/IP está disponible para la mayor parte de los sistemas operativos. Para acceder a Internet, el ordenador debe tener software TCP/IP.

TDMA: Acceso múltiple por división de tiempo. Se trata de compartir el tiempo de acceso entre múltiples usuarios de un sistema.

TELNET: Programa de emulación de terminal que permite iniciar una sesión en un sistema remoto, (tradicionalmente en entornos Unix). Por ejemplo, se puede usar telnet para iniciar una sesión en un catálogo del servidor de una biblioteca, obteniendo así acceso a los archivos que constituyen los registros de la biblioteca.

TERABYTE (TB): Unidad de medida de la capacidad de memoria y de dispositivos de almacenamiento informático (disquete, disco duro, CD-ROM, etc.) equivalente a algo más de mil billones de bytes, concretamente 1,024 (2^40). Se destaca que todavía no se han desarrollado memorias de esta capacidad aunque sí dispositivos de almacenamiento.

TERMINAL: *(terminal)* Dispositivo que permite enviar comandos a un ordenador que se encuentra en otro lugar. Esto significa una ventana de visualización y un teclado. Normalmente, se usa software de terminal en un ordenador personal, el software pretende "emular" a un terminal físico y permite teclear comandos para otro ordenador.

TOKEN RING: Red en anillo. Una red en anillo es un tipo de LAN con nodos cableados en anillo. Cada nodo pasa constantemente un mensaje de control ("token") al siguiente, de tal forma que cualquier nodo que tiene un "token" puede enviar un mensaje.

TOPOLOGÍA DE ANILLO: Topología en donde las estaciones de trabajo se conectan físicamente en un anillo, terminando el cable en la misma estación de donde se originó.

TOPOLOGÍA DE BUS: Topología en donde todas las estaciones se conectan a un cable central llamado "bus". Este tipo de topología es fácil de instalar y requiere menos cable que la topología de estrella.

TOPOLOGÍA DE ESTRELLA: Topología en donde cada estación se conecta con su propio cable a un dispositivo de conexión central, ya sea a un servidor de archivo o a un concentrador o repetidor.

TOPOLOGÍA DE RED: Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Existen tres topologías principales de red anillo, bus y estrella.

TUNNELING: Término que se aplica al uso de la Red como parte de una red privada segura. Transporte de paquetes Multicast a través de dispositivos y ROUTERS UNICAST.
Los paquetes multicast se encuentran encapsulados como paquetes normales de esta manera pueden viajar por Internet a través de dispositivos que solo soportan protocolos unicast.

U

UART: Es el chip del Puerto Serie del ordenador. El modelo UART 16550 trabaja a una velocidad máxima de 115.200 bps, su predecesor el modelo UART 8650 sólo alcanza 19.200 bps.

UDP: Acrónimo de *User Datagram Protocol* (Protocolo de datagrama a nivel de usuario), perteneciente a la familia de protocolos TCP/IP. Este protocolo no es tan fiable como TCP, pues se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar el éxito de la transferencia, UDP hace que la máquina de destino envía un mensaje de vuelta. Si no es así, el mensaje se envía de nuevo. Con este protocolo no se establece una conexión entre las dos máquinas.

UNIDAD MÁXIMA DE RECEPCIÓN (MRU): Se refiere al máximo tamaño del paquete de datos para algunos protocolos de Internet.

UNIDAD MÁXIMA DE TRANSMISIÓN (MTU): Máximo tamaño del paquete de datos en protocolos IP como el SLIP.

UNIX: Sistema operativo multiusuario y multitarea que soporta TCP/IP nativo. Es el sistema operativo más común para servidores en Internet.
Sus características más importantes son:
• Redireccionamiento de Entradas/Salidas.
• Sistema jerárquico de ficheros. Estructura de árbol invertido (File System).
• Interface simple e interactiva con el usuario.
• Alta portabilidad al estar escrito en C. Es casi independiente del hardware.
• Creación de utilidades fácilmente.

UPLOAD*:* Enviar un archivo al servidor. En Internet, proceso de transferir información desde un ordenador personal a un servidor de información, por tanto, inverso a Download.

URI: Acrónimo de *Uniform Resource Identifier* (Identificador de Recursos Uniforme). Se refiere a las direcciones de Internet, y define la sintaxis de direccionamiento.

URL: Acrónimo de *Uniform Resource Locator* (Localizador de Recursos Uniforme). Es el modo estándar de proporcionar la dirección de cualquier recurso en Internet, que es parte de la WWW. Las URLs pueden ser absolutas o relativas.
Una URL absoluta consiste en un prefijo que denota un método ("http" para servidores Web, "gopher" para gophers, "ftp" para transferencia de ficheros, etc.), seguido por dos puntos y dos barras (://), una dirección, que consiste en un nombre de dominio, seguido por una barra, un nombre de vía, y un ancla opcional (precedido por un símbolo * que apunta a un lugar dentro de una página Web).
Una URL relativa designa un elemento relativo en el que la designación se hace. Es similar a dar el número de teléfono sin el prefijo de provincia para llamar desde la misma ciudad.
Utilizado para especificar un objeto en Internet. Puede ser un fichero, grupo de news, gopher, etc.

USENET: Sistema mundial de grupos de discusión con comentarios que pasan entre cientos de miles de ordenadores. No todos los ordenadores Usenet están en Internet, ya que Usenet está completamente descentralizada, con más de 10.000 áreas de discusión, llamadas newsgroups.

USERID: Identificación de usuario. Ver nombre de usuario.

USERNAME: Ver nombre de usuario.

V

V.90: Estándard actual para el sistema de comunicación entre los módems.

VERONICA: Acrónimo de *Very Easy Rodent Oriented Net-wide Index to Computerized Activities* (Índice de actividades informatizadas orientado a un fácil uso mediante ratón), desarrollado en la Universidad de Nevada, Veronica es una base de datos que se pone al día continuamente con los nombres de casi todos los elementos de menú de miles de servidores Gopher.
La base de datos Veronica puede buscarse desde la mayoría de menús Gopher.

VIDEOCONFERENCIA: Sistema de comunicación que permite conversar y ver en vídeo al otro interlocutor.

VÍNCULO: Abreviatura de hipervínculo, un vínculo hace referencia a una zona activa de un documento Web y se suele resaltar con un color diferente al del texto que lo rodea. Es posible hacer clic en los vínculos para abrir un objeto de la misma base de datos o de otra diferente, de un documento diferente o de una página HTML de Web o de una intranet local.

VIRUS: Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

VRML: Acrónimo de *Virtual Reality Modeling Language* (Lenguaje de Modelado de la Realidad Virtual). Se trata de un lenguaje para la construcción de mundos virtuales en la red. Aunque todavía está en desarrollo, puede que en un futuro no muy lejano, todas las páginas Web se vean en tres dimensiones, con enlaces a nuevos mundos.

W

WAN: Acrónimo de *Wide Area Network* (Red de Área Extendida). Una red que cubre un área más grande un sólo edificio.

WAIS: Acrónimo de *Wide Area Information Servers* (Servidores de Información de Área Extendida) Paquete de software comercial que permite indizar grandes cantidades de información y hacer que esos índices puedan buscarse a través de Internet. Una característica primordial de WAIS es que los resultados de búsqueda están medidos de acuerdo a lo relevantes que son, y otras búsquedas subsiguientes.

WAP (Wireless Application Protocol - Protocolo de Aplicación de Telefonía Inalámbrica): Protocolo que permite a los usuarios de teléfonos móviles el acceso a servidores web especializados, visualizando la información en el visor del teléfono.

WAREZ: Software pirata que ha sido desprotegido.

WEB: Abreviatura de World Wide Web.

WEBCAM: Cámara conectada a una página WEB a través de la cual los visitantes pueden ver imágenes, normalmente en directo.

WEBMASTER: Persona encargada del mantenimiento de un conjunto de páginas Web o de todo un servidor.

WI-FI (Wireless Infranet): Red inalámbrica por microondas, que tiene un alcance de unos 400 metros.

WORM: Gusano. Programa que se envía a través de una red y se infiltra en los controladores de dispositivos, y se reduplica hasta que llena el controlador, usa toda la memoria y acaba con el ordenador, pudiendo acabar con toda una red.

WWW: Acrónimo de *World Wide Web* (tela de araña mundial). Se denomina así al gran universo de recursos a los que se puede acceder usando Gopher, FTP, HTTP, Telnet, Usenet, WAIS y otras herramientas. Es el universo de servidores HTTP que permiten mezclar texto, gráficos, archivos de sonido, etc. juntos.

WYSIWIG: *What You See is What You Get*, "lo que ves es lo que obtienes", con esta expresión se indica que lo que se ve en pantalla es lo que se obtendrá cuando se imprima.

X

X.400: Estándares de CCITT e ISO para correo electrónico. Utilizados principalmente en Europa y Canadá, se han ido integrando progresivamente en Internet.

X25: Protocolo de transmisión de datos muy usado en Iberpac. Establece circuitos virtuales, enlaces y canales.

X.500: El directorio X.500 es una base de datos distribuida que permite la consulta de datos sobre objetos del mundo real. A través de X.500 se puede buscar información sobre personas, departamentos y organizaciones de todo el mundo. Puede proporcionar direcciones de mensajería electrónica, direcciones postales, teléfonos y números de Fax.

XMODEM: Protocolo utilizado para transferir archivos de un servidor a una computadora conectada vía modem, el cual es principalmente usado para extraer archivos de un BBS.

Z

ZIP: Sistema de compresión de archivos que se ha popularizado en Internet debido, entre otros motivos, a sus elevadas prestaciones. La mayoría de los archivos disponibles para su descarga en los servidores FTP anónimos se encuentra en este formato, principalmente archivos para entornos de PC. La manipulación (compresión y descompresión) de estos ficheros requiere de programas especializados, como por ejemplo: pkzip para entorno MS-DOS y winzip para entorno Windows. Se distinguen fácilmente por su extensión: .zip en PC, .gz en Unix, etc. Ver Shareware, Freeware, Download.