

TEMA 1

EXPLOTACION DE
SISTEMAS
MICROINFORMATICOS

OBJETIVOS DEL CAPITULO

- Conocer la arquitectura de los ordenadores
- Conocer lo que es un sistema informático
- Distinguir los periféricos que se pueden incorporar a un ordenador
- Conocer lo que son las herramientas de monitorización, chequeo y diagnóstico.
- Ver las normas de seguridad y prevención de riesgos laborales.

Cont.

- Conocer lo que es una red informática
- Distinguir los componentes de una red
- Conocer lo que son las topologías de red
- Conocer lo que es la transmisión de datos
- Conocer los medios de transmisión
- Conocer lo que son los protocolos y las normas IEEE
- Ver los tipos de cableado

1.LA ARQUITECTURA DE LOS ORDENADORES

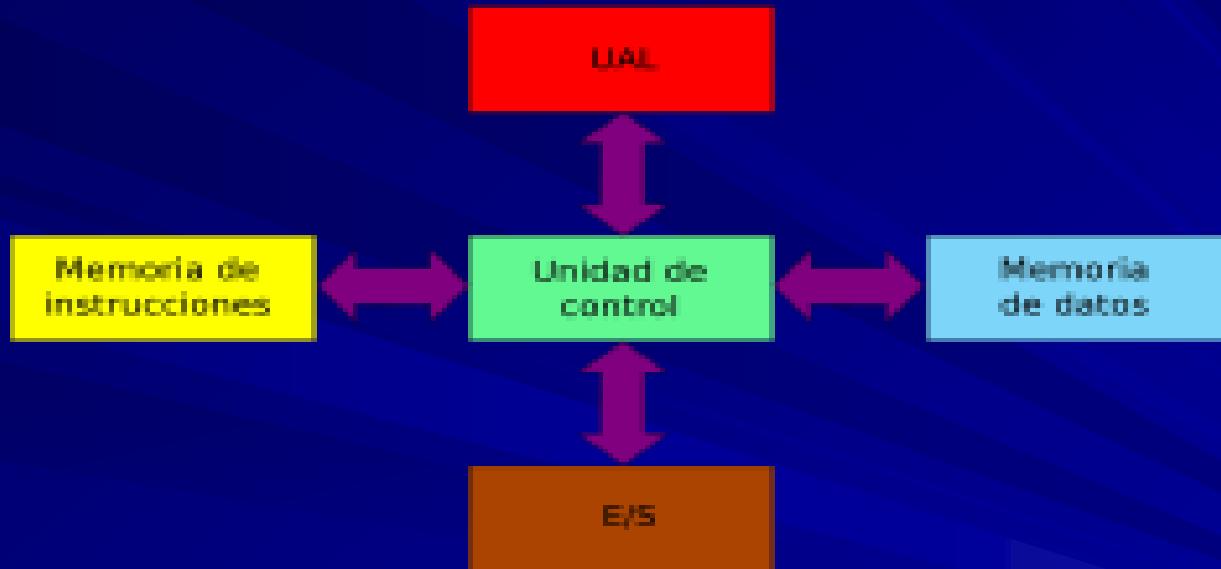
1.1 La máquina de Turing

- Alan Mathison Turing, matemático y computador científico inglés, desarrollo entre 1935 y 1945 un modelo computacional hipotético que permitía en teoría resolver cualquier problema matemático siempre y cuando se reduzca a un algoritmo.
- Es un dispositivo que manipula símbolos sobre una tira de cinta de acuerdo a una tabla de reglas. A pesar de su simplicidad, una máquina de Turing puede ser adaptada para simular la lógica de cualquier algoritmo de computador .

- No está diseñada como una tecnología de computación práctica, sino como un dispositivo hipotético que representa una máquina de computación
- Los componentes de esta maquina son:
 - La memoria: una cinta infinita dividida en celdas
 - Cabezal de lectura-escritura: Puede desplazarse a la derecha , a la izda. Escribir y leer.
 - Procesador: Se divide en : registro de estado y tabla de acción.

1.2. LA ARQUITECTURA DE HARVARD

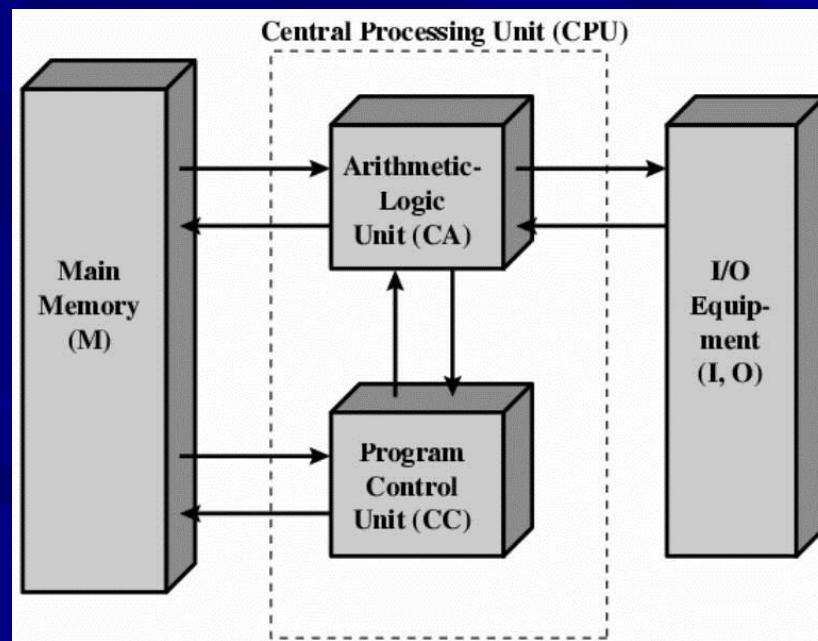
- Tiene la memoria de datos separada de la memoria del programa y estas a su vez unidas a la CPU a través de buses independientes.



- Esta arquitectura suele utilizarse en DSPs, o procesador de señal digital, usados habitualmente en productos para procesamiento de audio y video

1.3. LA ARQUITECTURA DE VON NEUMANN

- En 1944 diseño el modelo de computador con programa almacenado en memoria eléctrica (EDVAC en 1952), y es el que se utiliza en la actualidad.
- Neumann proponía que tanto el programa como los datos se almacenan en la memoria del ordenador.



- Según la arquitectura de Von Neumann un computador esta formado por:
 - Una unidad aritmético-lógica (ALU): realiza cálculos y comparaciones y toma de decisiones lógicas.
 - Una unidad de control (UC): interpreta las instrucciones del programa en lenguaje maquina y genera las señales lógicas de control para ejecutarlas.
 - La MEMORIA: Permite almacenar y recuperar la información.
 - REGISTROS: memoria donde se almacena información temporalmente
 - Los sistemas de ENTRADA/SALIDA: permite la comunicación con los dispositivos periféricos.
 - La UNIDAD CENTRAL DE PROCESO (CPU) (MICROPROCESADOR): Interpreta y ejecuta instrucciones. Se compone de la UC y la ALU y los REGISTROS. Según sea el repertorio de instrucciones del procesador, este puede ser:
 - RISC: Pocas instrucciones y poco complejas (Sparc y Alpha)
 - CISC: Muchas instrucciones y complejas (Intel)

2.- EL SISTEMA INFORMATICO

- Es un conjunto de partes interrelacionadas**
- Emplea un ordenador que usa dispositivos programables para capturar, almacenar y procesar datos.**
- Dicho ordenador, junto con la persona que lo maneja y los periféricos que lo envuelven, conforman un SISTEMA INFORMATICO.**

- Un S.I. esta compuesto por 3 elementos básicos:**
 - Hardware (componente físico)**
 - Software (componente lógico). Sistema operativo y aplicaciones.**
 - Un componente humano.**

3.- LOS COMPONENTES FISICOS DE UN SISTEMA INFORMATICO

- El chasis, caja o torre
- La fuente de alimentación
- El sistema de refrigeración
- El microprocesador
- La placa base
 - El circuito impreso
 - Zócalo del procesador (Socket)
 - Zócalos de memoria
 - Memoria caché
 - Slot de buses
 - Chipset (NorthBridge, SouthBridge)
 - BIOS: datos de configuración. Identifica los componentes principales y les proporciona acceso y control a todos ellos. Award o Ami.
 - Batería
 - Conector de alimentación
 - Jumpers
 - Conectores de pin
 - Controladores

3.1.- EL MICROPROCESADOR

- Actualmente una CPU puede estar compuesta por uno o varios microprocesadores. Núcleo (Core): porción de procesador que lleva a cabo todas las actividades de una CPU real.
- Desde el 80486 utilizan refrigeradores
- El rendimiento se puede medir de varias formas:
 - **Frecuencia de reloj:** actualmente cerca de los 4 GHz. No aumenta mas la velocidad, pero si la optimización del otros componentes.
 - **Velocidad del bus:** (FSB:Front Side Bus) comunica el procesador con el NorthBridge. Viene determinado por el ancho del mismo (64 bits) y su velocidad en MHz.
 - **Memoria Caché:** Acelera el rendimiento ya que almacena datos que prevé que mas se van a usar. Tipos:
 - Caché L1: Integrada en el procesador y muy rápida.
 - Caché L2 y L3: Conectada al micro por el bus trasero, mas rápido que el frontal. Estas son mas lentas que la L1. Velocidad de L3>L2 .

3.2.- LA MEMORIA RAM

- **Es donde el ordenador guarda los datos que está utilizando en el momento actual.**
- **Su capacidad se mide en MByte y GByte**
- **También tenemos memoria RAM en lectores ópticos, tarjetas gráficas, impresoras, etc.**
- **Según el tipo de conector que lleven se clasifican en:**
 - **SIMM: Single In-line Memory Module: 30 o 72 contactos**
 - **DIMM: Dual In-line Memory Module: 168, 184 o 240 contactos. Son los que se usan en los ordenadores de sobremesa.**
 - **SO-DIMM: Se utilizan en portátiles: 100, 144 y 200 contactos.**
 - **RIMM: Rambus In-line Memory Module: 184 contactos.**
 - **Micro-DIMM: formato más pequeño pero menos utilizado.**

■ Parámetros fundamentales en este tipo de memoria:

- **Velocidad de acceso:** Menor tiempo de acceso=mas rápida
- **Velocidad de reloj:** velocidad de reloj del bus.
- **Voltaje:** A mayor voltaje=mayor consumo=mayor temperatura
- **Tecnología soportada:**
 - **Single Memory Channel:** 1 solo canal de intercambio de información entre modulos de memoria y bus.
 - **Dual Memory Channel:** 2 canales simultáneos diferenciados de intercambio.

3.3.- MEMORIA DE VIDEO O GRAFICA

- Empleada por el controlador de la tarjeta gráfica para manejar la información visual.
- Se utilizaba hace unos años memoria DDR y ahora DDR2 y DDR3, que son convencionales.
- También se utilizan otras específicas como: GDDR3, GDDR4 y GDDR5 (Graphics Double Data Rate).

3.4. BUSES Y RANURAS DE EXPANSION

- Los buses son líneas que conectan al procesador con los distintos dispositivos del equipo.
- Tipos de Slot de expansión:
 - Bus PCI: creado en 1993 transmite datos en paralelo. Suele ser de color blanco. Reemplazó a los ISA y VESA. Esta desapareciendo, dando paso al PCI Express
 - Bus AGP: Dedicado a tarjetas de video AGP. Suele ser de color marrón.
 - Bus PCI-EXPRESS: Salió en 2006. Mayores prestaciones que los anteriores, para las nuevas demandas (puertos Gbit, nuevas tarjetas gráficas). Velocidad en torno a 2,5 o 5 Gbits/seg. Pueden ser X1 (mas rápido que el PCI normal , a X8 que es igual de rápido que la versión mas rápida de AGP). El X atiende al nº de enlace de datos.

3.5 PUERTOS Y CONECTORES

- **Los conectores de entrada/salida cumplen la norma PC99.**
- **Estos conectores pueden ser:**
 - **Puertos serie**
 - **Puertos paralelo**
 - **Puertos USB**
 - **Conector RJ-45**
 - **Conector gráfico: VGHA, HDMI, DVI**
 - **Conectores IDE, o SERIAL ATA I y II**
 - **Conectores de audio**
 - **Puertos PS2**

3.6.- UNIDADES DEL ALMACENAMIENTO SECUNDARIO

Entendidas como almacenamiento masivo y permanente. Pueden ser atendiendo a su tecnología:

- **Magnética: DD, Disquetes, Cintas magnéticas**
- **Óptica: CD, DVD, Blu-ray**
- **Magneto-óptica: Disco ZIP**
- **Flash: Tarjetas de memoria**

Características de este tipo de almacenamiento:

- **Capacidad (MB, GB, TB)**
- **Velocidad de transferencia: MB/s**
- **Tiempo medio de acceso, búsqueda y lectura/escritura: nanosegundos**

3.6.1.- DISCO DURO

Es un dispositivo no volátil que emplea un sistema de grabación digital de tecnología magnética.

Platos del disco duro:

Un disco duro está formado por varios platos en cuyas superficies se almacenan los datos.



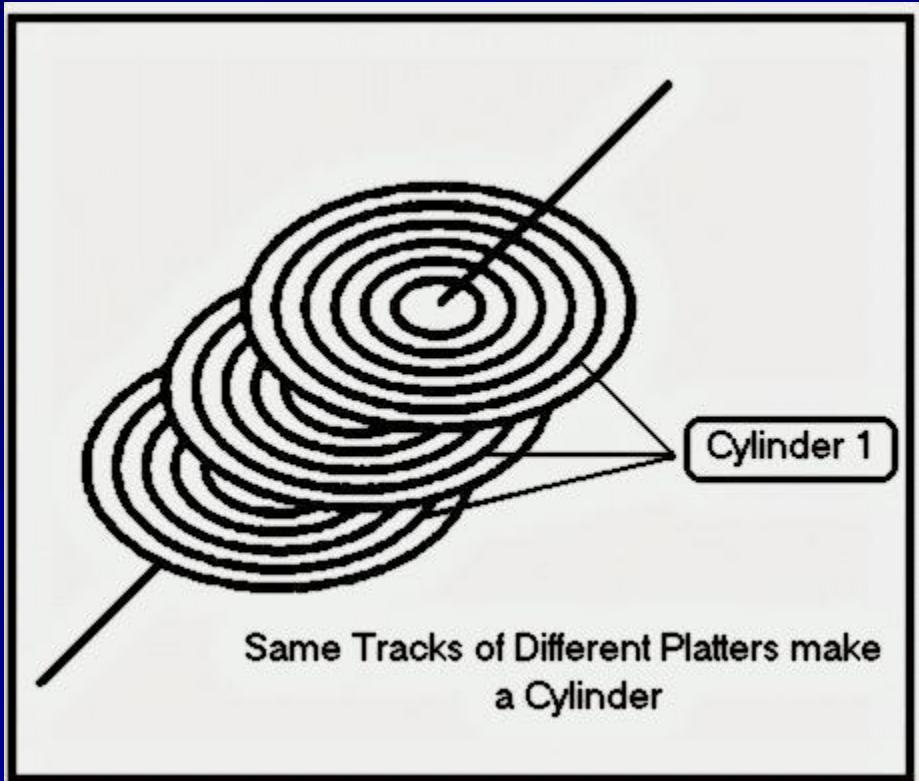
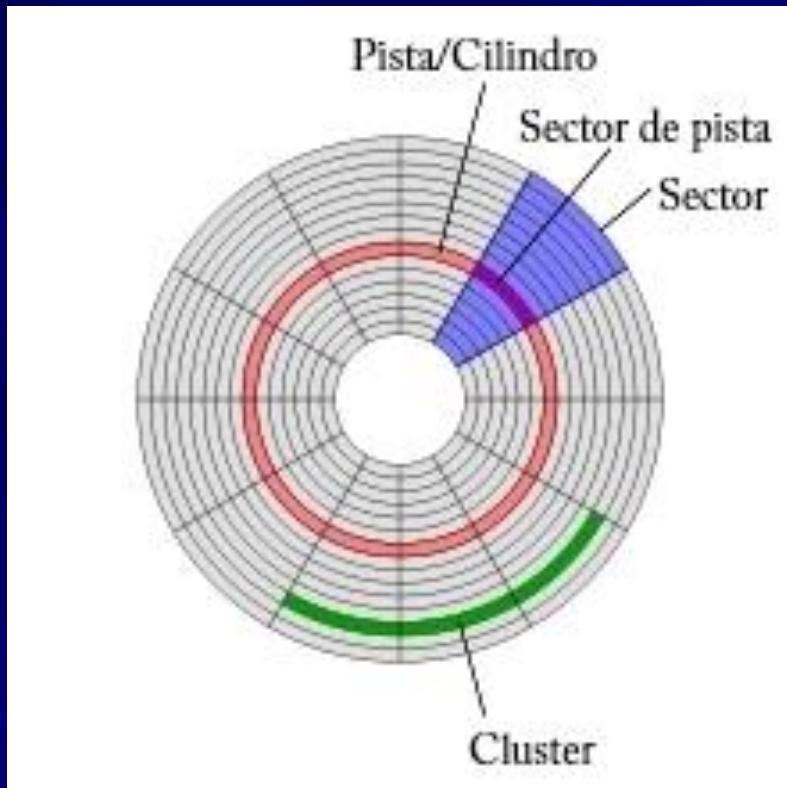
Cabeza lectora:

La cabeza lectora es solo la parte final de los brazos de acceso.

Brazos de acceso:

Desplaza las cabezas de lectura/escritura por la superficie de los platos.

La estructura organizativa en la que se basa un DD mediante la cual se almacena la información es la siguiente:



LOS COMPONENTES DE UN DISCO DURO SON LOS SIGUIENTES:

- PLATO: Cada uno de los discos que hay dentro de un disco duro
- CARA: Cada uno de los dos lados de un plato
- CABEZA: Cada uno de los cabezales
- PISTA: Una circunferencia dentro de una cara. La 0 esta en borde exterior.
- CILINDRO: Conjunto de varias pistas alineadas verticalmente
- SECTOR: Cada una de las divisiones de una pista.

TIPOS DE CONEXIÓN DEL DISCO DURO:

- IDE: o PATA, controlan los dispositivos de almacenamiento masivo de datos. Permite la conexión de max. 4 dispositivos en master-slave.
- SCSI: DD de gran capacidad de almacenamiento. Tiempos de acceso velocidades de transmisión mayores que IDE. Un controlador SCSI puede manejar hasta 7 periféricos SCSI.
- SATA: Utiliza un bus serie para la transmisión de datos. Mas rápido y eficiente que el IDE. SATA1 de hasta 1,5 Gb/seg y SATA2 de hasta 3Gb/seg de velocidad de transferencia

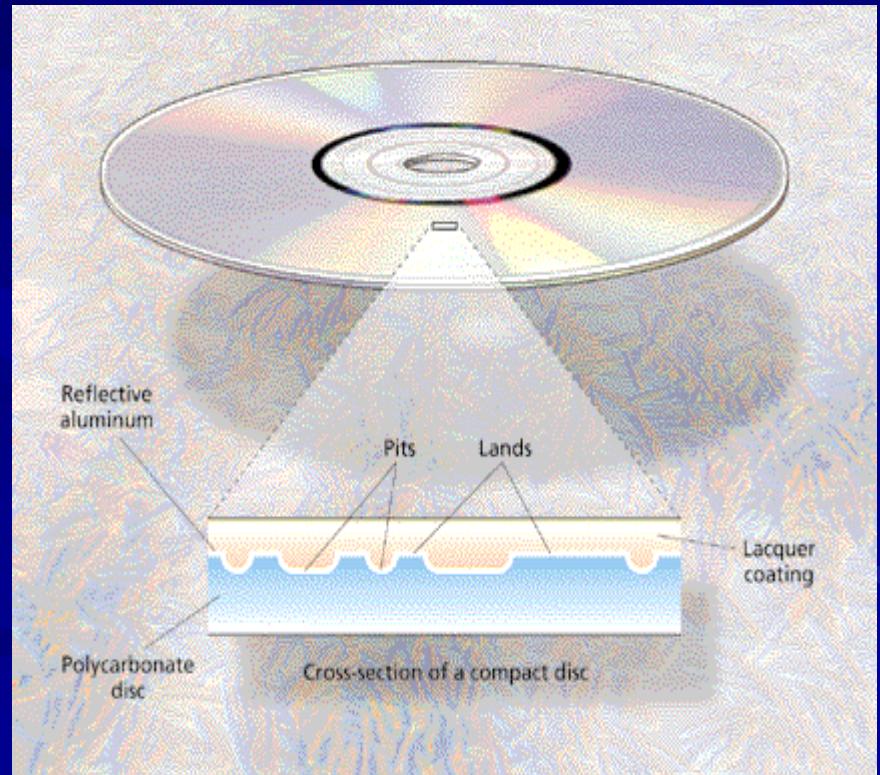
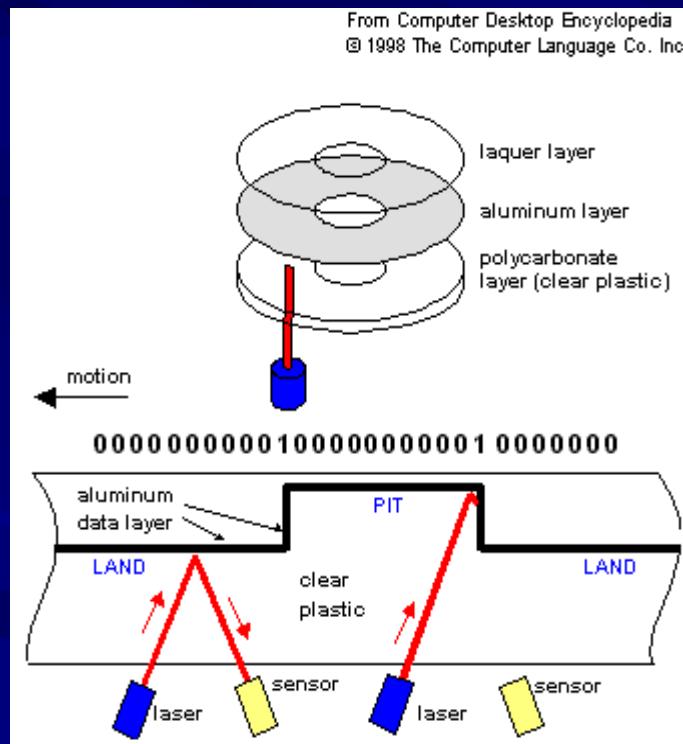
ESTRUCTURA LOGICA DEL DISCO DURO:

- SECTOR DE ARRANQUE (MBR): Es el primer sector o sector 0 y alberga el arranque del sistema operativo o para almacenar la tabla de particiones.
- LA TABLA DE PARTICIONES Y LAS PARTICIONES: Cada partición puede tener un sistema de archivos, de forma que el SO manipula a cada una como un disco físico independiente. Tipos de particiones:
 - **Primarias:** Son las divisiones primarias del disco. Solo puede haber 4 primarias o 3 primarias y una extendida.
 - **Extendida:** Actúa como partición primaria y sirve para contener múltiples unidades lógicas en su interior. Solo puede tener una por disco y solo sirve para contener unidades lógicas, por lo que no soporta ningún sistema de archivos.
 - **Lógica:** Ocupa toda o una parte de una partición extendida. Pueden tener como max 23 particiones lógicas por una partición extendida.

Los sistemas de archivos pueden ser: FAT, NTFS, EXT4, EXT3, EXT2, FAT32, etc.

3.6.2.- LECTOR-GRABADOR DE DISCO OPTICOS Y SOPORTES OPTICOS

- Un disco óptico emplea como soporte un disco circular de aluminio y policarbonato, sobre el cual la información se graba en unos surcos en espiral microscópicos continua (pits y lands) realizados con un láser, desde la pista mas interna, al exterior.

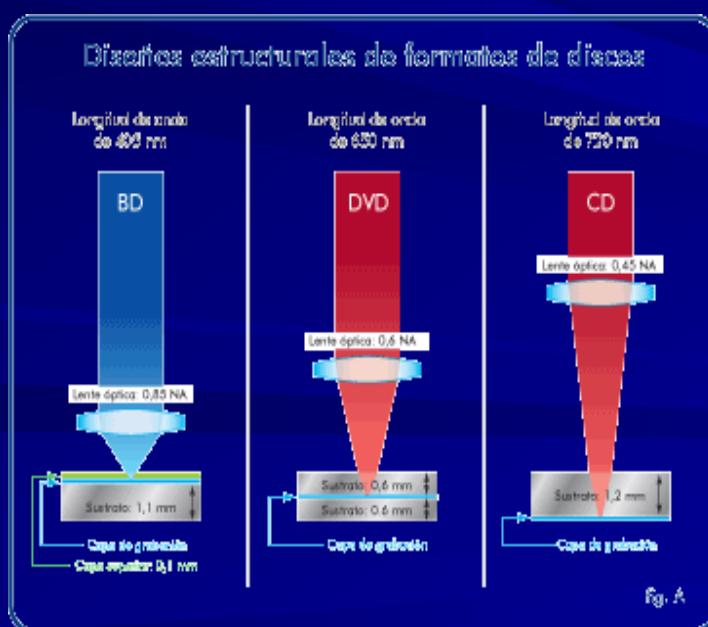


Según el tipo de grabación pueden ser:

- Solo lectura : CD-ROM
- Grabable una sola vez: CD-R
- Regrabable: CD-RW

Según la capacidad de almacenamiento:

- CD: 700 MB
- DVD: 4,7 GB
- DVD-DL: doble capa 9 GB
- BLU-RAY: 25 GB en una capa y 50 GB en doble capa



3.6.3.- TARJETAS DE MEMORIA FLASH

- Se ha ido propagando debido a la proliferación de los dispositivos electrónicos móviles.
- Los formatos más extendidos son: Compact Flash, Memory Stick, Smartmedia, SD, MiniSD y MicroSD.



3.7. TARJETAS DE EXPANSION

- Son dispositivos con diversos circuitos integrados que amplían la capacidad del ordenador.
- Estas se insertan en las ranuras de expansión: ISA (ya en desuso), PCI, AGP y PCI-Express, además de las PCMCIA y EXPRESSCARD de los portátiles.
- Cada vez se usan menos debido a la tecnología USB y a la integración en placa base de diversos componentes (video y audio, Ethernet).
- Entre las mas utilizadas son: tarjeta capturadora o sintonizadora de video y/o televisión, tarjetas de red, tarjeta de sonido, tarjeta grafica, tarjeta PCI-SCSI, tarjeta PCI-IDE, tarjeta de expansión SATA, USB, Firewire, etc.

3.7.1.- LA TARJETA GRAFICA

- Es la encargada de procesar los datos que provienen de la CPU y transformarlos en información comprensible y representable en un monitor o video-proyector.
- Esta puede estar también integrada en la placa base.
- Dada la exigencia de los videojuegos, aplicaciones 3D o programas de edición de video, necesitamos un procesador de video (GPU), para descargar de este trabajo a la CPU.
- La GPU esta especializada en procesamiento grafico y en ejecución de operaciones en coma flotante .
- Antialiasing: Es una técnica empleada en las tarjetas graficas consistente en el suavizado de los bordes de los objetos, obteniendo imágenes realzadas y mejoradas.
- Características: Velocidad del núcleo (MHz), ancho del bus (de 128 a 512 bits), velocidad de relleno de textura, pixeles procesados en un ciclo de reloj, sistema de ventilación, resolución máxima, etc.
- Los fabricantes mas importantes son: NVIDIA (Chip GeForce) y ATI (Radeon)

3.8. DISPOSITIVOS EXTERNOS DE ENTRADA/SALIDA. PERIFERICOS

- Periférico: se denomina **periféricos** a los aparatos y/o dispositivos auxiliares e independientes conectados a la unidad central de procesamiento de una computadora.
- También se les denomina dispositivo externo de entrada/salida.
- Algunos están montados dentro del chasis (DD, CD, DVD, etc.)
- Algunos requieren de unos controladores hardware que se presentan en forma de tarjetas y que incluye una potente electrónica para descargar de tareas a la CPU. Se alojan en las ranuras de expansión.
- Otros utilizan los puertos del ordenador: PS2, USB, Firewire, RJ45, puerto serie y paralelo,etc.
- DRIVER: Controlador de dispositivo que facilita la comunicación entre el periférico y el SO. Suelen venir con el dispositivo, aunque actualmente los SO suelen tenerlos.

TIPOS DE PERIFERICOS SEGÚN SU FUNCIONALIDAD

- Periféricos de entrada: Teclado, ratón, detectores ópticos, escáner, micrófono, etc.
- Periféricos de salida: monitor, impresora, altavoz.
- Periféricos de entrada/salida o mixtos: pantalla táctil, impresora multifuncional, etc.
- Periféricos de comunicación: modem, switch, router
- Periféricos de almacenamiento: DD, DD multimedia, etc.

4.- CHEQUEO Y DIAGNOSTICO

4.1.- INICIO DE LA COMPUTADORA POR PRIMERA VEZ

Si una vez montado el equipo, enchufado el monitor, ratón y teclado, se procede a encenderlo y se escucha un solo pitido es señal de que todo esta correcto.

Se comprobara que todos los leds se encienden y que los ventiladores están funcionando.

4.2.- HAY PROBLEMAS

- El ordenador no enciende
- El ordenador enciende pero no se ve nada en el monitor
- El ordenador no pita, pero parece que enciende
- El ordenador emite un pitido continuo
- El equipo pita mas de una vez: Mensaje de la BIOS

5.- HERRAMIENTAS DE MONITORIZACION Y DIAGNOSTICO

5.1.- MONITORIZACION DE LA PLACA BASE

- La BIOS ofrece funciones de monitorización del procesador, placa base y otros dispositivos.
- Se pueden monitorizar los voltajes del equipo, las RPM de los ventiladores del equipo y del procesador, la temperatura de la placa base y del micro.
- En los casos en que los errores sean aleatorios u ocurran cuando el usuario ya lleva trabajando con el equipo y después de haber descartado que el software sea el causante del mismo o la temperatura, lo mejor es pasarle una serie de pruebas exhaustivas por si la memoria tuviese celdas estropeadas, la placa base tuviese algún componente averiado o el micro no estuviese funcionando como debiera.
- Se puede optar por realizar un test de tortura u otro tipo de bechmarck o pruebas mas especificas. En estos casos siempre es mejor realizar una configuración minima con los componentes imprescindibles y testearlos a fondo para luego ir añadiendo componentes y seguir testeando.

6.- NORMAS DE SEGURIDAD Y PREVENCION DE RIESGOS LABORALES

Consejos a tener en cuenta cuando se trabaja en una oficina con sistemas informáticos:

- Cables recogidos para evitar caídas. Evitar que la instalación este en el suelo.
- Los cables de datos no deben ir junto con los de tensión
- Las instalaciones eléctricas deben de estar en buen estado
- Evitar la sobrecarga de los enchufes. Repartir la carga de los enchufes disponibles. La sobre carga produce incendios.
- Apague los equipos cuando abandone la oficina.
- Separe los equipos de la pared para evitar sobrecalentamientos
- Los enchufes deben de tener toma de tierra y diferenciales
- Se debe de disponer de un sistema contra incendios. Los extintores y salidas de incendios deben de estar señalizados y operativos.
- Climatización: Evite colocarse en las salidas del aire acondicionado, al lado de radiadores, etc. La temperatura media en invierno de 22º y en verano de 24º es la mas adecuada, con una humedad relativa entre el 30% y el 70%.

- Los ruidos dificultan la concentración. No sobrepasar los 55 Db. Habilitar una sala para los equipos mas ruidosos.
- El factor psicosocial es muy importante. Los procedimientos de trabajo deben de estar claros y la organización debe ser la adecuada. Fomentar las relaciones interpersonales y evitar el mobbing y el burnout (presencia de una respuesta prolongada de estrés provocando fatiga crónica, ineficacia) .
- Los empleados que trabajen el montaje y reparación de equipos informáticos deberán seguir las instrucciones del fabricante.
- Utilizar siempre que se pueda la luz natural. Si es artificial, no deberán producir deslumbramientos, reflejos. La intensidad de la luz deberá ser la adecuada.
- Los puestos de trabajo deberán estar cerca de las ventanas, evitando que la luz provoque reflejo en las pantallas mediante la utilización de cortinas, pantallas, etc.
- Los techos deben de ser blancos y las paredes de tonos medios.
- Las vibraciones del aire acondicionado, maquinas, impresoras, trafico, se deberán reducir o eliminarlas en lo posible.
- En oficinas con mucha carga electrostática, ésta se puede reducir aumentando la humedad en el aire.

6.1.- CONSEJOS ESPECIFICOS PARA USUARIOS DE EQUIPOS INFORMATICOS

Estos consejos son para personas que estén mucho tiempo delante del ordenador (mas de 20 h. a la semana) como administrativos, contables, escritores, delineantes, etc., ya que les pueden producir:

- Trastornos músculo esqueléticos: en espalda, cuello, hombros, manos y brazos por adoptar posturas incorrectas o estáticas durante mucho tiempo.
- Problemas visuales: Irritaciones y enrojecimiento de los ojos, visión borrosa, provocados por los esfuerzos de mirar la pantalla y a los documentos debido a la diferencia de la luminosidad entre ellos. Todo esto provoca fatiga visual.
- Fatiga mental: cuando se realizan tareas repetitivas o monótonas

Los CONSEJOS siguientes tratan de minimizar estos problemas:

- La distancia entre la pantalla y el trabajador debe de ser mayor de 40 cms.
- El trabajador debe de colocarse frente a la pantalla. El Angulo entre la línea de visión y la horizontal debe de ser menor de 60° .

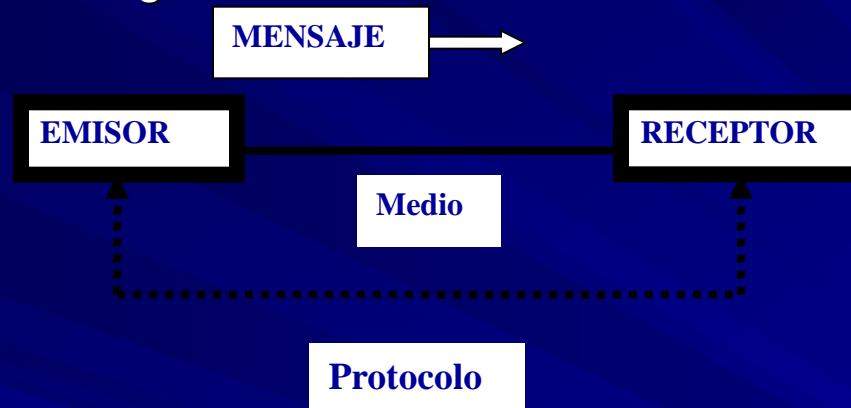


- No utilizar pantallas muy pequeñas ya que provocan fatiga visual.
- Ajustar correctamente la luminosidad y contraste de la pantalla.
- No trabajar en penumbra. Intentar que la luminosidad entre la pantalla y el resto del lugar de trabajo sea lo mas parecido posible.
- Evitar monitor CRT. Los nuevos tienen menos reflejos y mejores contrastes.
- La posición, inclinación y altura del teclado debe de ser la suficiente para que las manos estén de manera lo mas relajada posible.
- Elegir un ratón cómodo. En el caso de que el uso prolongado del ratón provoque lesiones (síndrome del túnel carpiano) utilizar un trackball.
- En la posición a adoptar frente al ordenador la columna debe permanecer recta, apoyándose en el respaldo de la silla y las demás partes del cuerpo deben de adoptar una posición relajada y lo mas natural posible.
- El mobiliario debe ser lo mas cómodo posible y ajustable.
- Las sillas deben ser ajustables, ergonómicas y cómodas.

7.- SISTEMAS DE COMUNICACIÓN

Es un conjunto de dispositivos interconectados que realizan acciones que permiten que las personas puedan comunicarse o conectarse entre si.

Los componentes generales son:



- MENSAJE: Contiene la información que se quiere transmitir.
- EMISOR: Dispositivo que genera el mensaje
- RECEPTOR: Dispositivo destino del mensaje
- MEDIO: Medio físico utilizado para llevar a cabo la transferencia de la información (guiados como cable de cobre, coaxial, fibra óptica y no guiados como el aire)
- PROTOCOLO: Es el conjunto de reglas que gobiernan la transmisión de datos

8.- QUE ES UNA RED

Una red de ordenadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello es necesario contar con los ordenadores, tarjetas de red cables de conexión, los periféricos y el software conveniente.

Según su ubicación y en función de su extensión las redes pueden ser:

- LAN: Red de área local. Ordenadores dentro del mismo edificio.
- CAN: Red de área universitaria. Edificios diferentes dentro de la misma universidad.
- MAN: Red de área metropolitana. Diferentes edificios dentro de la misma ciudad.
- WAN: Red de área amplia. Edificios en distintas localidades o países.

Según la forma en que estén conectados los ordenadores:

- REDES SIN TARJETAS: A través de los puertos serie y paralelo.
- REDES PUNTO APUNTO: Es un conjunto de medios que hace posible la comunicación entre dos ordenadores determinados de forma permanente.
- REDES ENTRE IGUALES: Todos los ordenadores conectados pueden compartir información con los demás
- REDES BASADAS EN SERVIDORES CENTRALES: Modelo básico de cliente-servidor.

8.1.- VENTAJAS DE LAS REDES

Las ventajas de utilizar una red son:

- Posibilidad de compartir periféricos e información
- Reduce la duplicidad de trabajos
- Permite utilizar el correo electrónico
- Reemplaza o complementa miniordenadores de forma eficiente.
- Establece enlace con Mainframes. Un ordenador de gran potencia actúa como servidor, haciendo que los recursos disponibles estén accesibles para cada uno de los ordenadores personales conectados.
- Permite mejorar la seguridad y control de la información que se utiliza.

8.2.- ARQUITECTURA CLIENTE-SERVIDOR

Con el paso del tiempo, los usuarios de ordenadores fueron necesitando acceder a mayor cantidad de información y de forma mas rápida, por lo que fue surgiendo la necesidad de un nuevo tipo de ordenador: el servidor.

Un servidor es un ordenador que permite compartir sus periféricos con otros ordenadores. Estos pueden ser:

- SERVIDOR DE ARCHIVOS: En subdirectorios privados y compartidos
- SERVIDOR DE APLICACIONES: Proporciona la infraestructura y servicios clave a las aplicaciones alojadas en un sistema
- SERVIDOR DE COMUNICACIONES: Enlaza diferentes redes locales o una red local con grandes ordenadores
- SERVIDOR DE CORREO ELECTRONICO: Para la red
- SERVIDOR WEB: Proporciona un lugar para guardar y administrar los documentos HTML para que sean accesibles por otros usuarios
- SERVIDOR FTP: Guarda archivos para que puedan ser descargados por otros usuarios de la red
- SERVIDOR PROXY: Monitoriza el acceso entre las redes.

Puede ocurrir que los distintos tipos de servidores residan en el mismo ordenador o se encuentren distribuidos entre aquellos que forman parte de la red.

Los servidores pueden ser:

- DEDICADOS: Solo se dedican a la gestión de la red
- NO DEDICADOS: también se utilizan como estación de trabajo. No es recomendable utilizarlo como estación de trabajo.

Cada estación de trabajo es un ordenador que funciona con su propio sistema operativo, el cual tiene una tarjeta de red y esta conectado físicamente por medio de cables con el servidor.

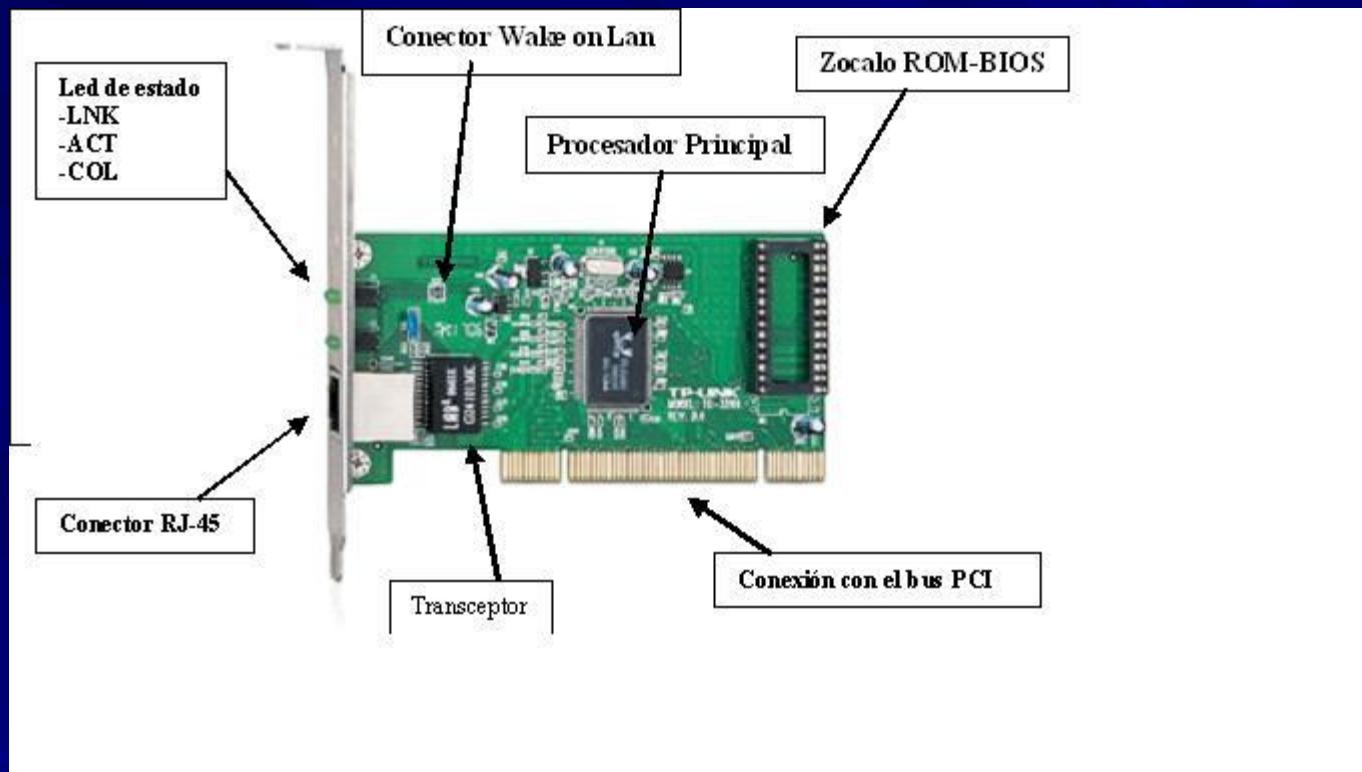
9.- COMPONENTES DE UNA RED INFORMATICA

- Esta formada por ordenadores con sus periféricos y por los elementos de conexión de los mismos.
- Los ordenadores pueden desarrollar dos funciones distintas: de servidores o de estación de trabajo.
- Se entienden como elementos de conexión a los cables y las tarjetas de red, así como los conmutadores, concentradores, puntos de acceso inalámbricos y routers.

9.1.- LA TARJETA DE RED

Actúa como interfaz física entre el ordenador y el cable de red.

Pueden estar integradas en placa base o colocadas en ranura de expansión.



- **PROCESADOR PRINCIPAL:** Realiza las operaciones de comunicación
- **CONEXIÓN CON EL BUS:** Es la vía de comunicación entre la tarjeta de red y el bus de sistema del ordenador.
- **ZOCALO ROM-BIOS:** Se utiliza para insertar una memoria ROM que permite al ordenador obtener el sistema operativo de la red y arrancar si no dispone de unidades físicas.
- **TRANSCEPTOR:** Es el dispositivo encargado de dar acceso al medio de transmisión de la red cuando el ordenador desea enviar o recibir datos.
- **CONECTOR WAKE ON LAN:** Comunica mediante un cable la tarjeta con la placa base del ordenador y permite el arranque de esa estación enviando órdenes desde otra estación diferente.
- **INDICADORES DE ESTADO:** Permite comprobar el estado actual de la comunicación. LNK (se enciende si hay conexión con la red también según el color si es naranja indica que funciona a 10 Mbps y si es verde 100 Mbps), ACT (se enciende si TX o RX datos), COL (indica si varias estaciones transmiten a la vez y se produce colisión)

Una tarjeta de red realiza las siguientes acciones:

- Prepara los datos del ordenador para su envío a la red. Los datos pasan de paralelo cuando llegan a la tarjeta a bits en serie para transmitirlos por la red.
- Envía dichos datos a la red: Indicando su dirección MAC (12 dígitos hexadecimales únicos en toda la red)
- Controla el flujo de datos entre el ordenador y el sistema cableado.
- Recibe los datos entrantes en serie del cable y los traduce en bytes en paralelo que el ordenador pueda comprender.

Antes de que la tarjeta emisora envíe los datos a la red, se establece un dialogo con la tarjeta receptora para que se pongan de acuerdo en lo siguiente:

- Tamaño máx.. Del paquete de datos
- Total de datos enviados antes de la confirmación
- Intervalo de tiempo entre cada envío de paquetes
- El tiempo a esperar antes de que sea enviada la confirmación
- Cuantos datos se pueden almacenar en la memoria de la tarjeta
- La velocidad de TX de los datos

Cada tarjeta negocia y se adapta a la otra. Después de esto empieza la TX.

9.2.- LA TRANSMISION DE DATOS

La transmisión puede realizarse en los dos sentidos. Según esta característica, existen 3 tipos de transmisión:

- **SIMPLEX:** La transmisión tiene lugar en un solo sentido y si, se desea transmitir en sentido contrario, será necesario poner otro cable.
- **SEMIDUPLEX:** La transmisión puede tener lugar en ambos sentidos, pero no simultáneamente. Se utilizan señales de control para informar si el medio esta ocupado o se puede transmitir.
- **DUPLEX INTEGRAL:** La transmisión puede tener lugar en ambos sentidos al mismo tiempo siempre sobre el mismo cable.

9.3.- LOS MEDIOS DE TRANSMISION

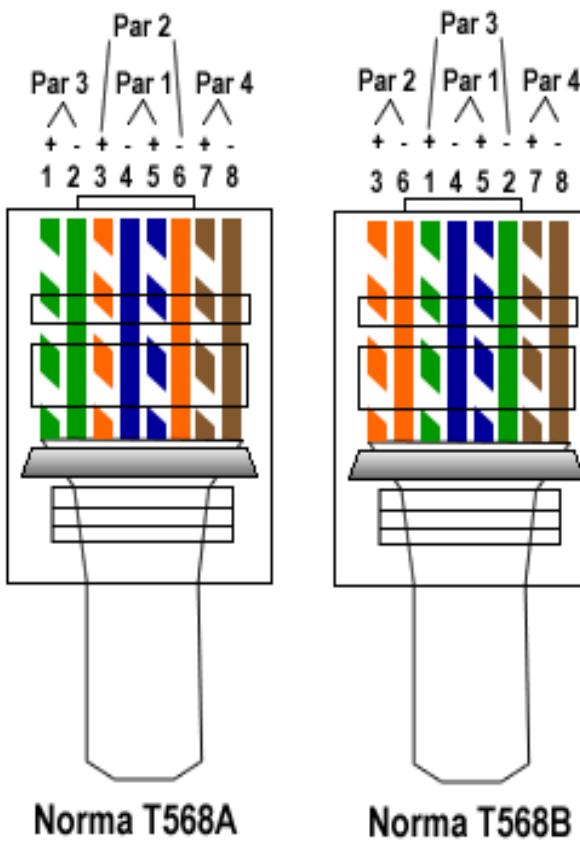
- Se clasifican en guiados y no guiados. Los guiados son aquellos que utilizan un medio sólido (un cable) para la transmisión de datos y los no guiados utilizan el aire para ello (son los medios inalámbricos).
- Los cables transmiten impulsos eléctricos o lumínicos. Los bits se transforman en la tarjeta de red y se convierten en señales eléctricas o lumínicas específicas que están determinadas por el protocolo que implemente esa red.
- La velocidad de transmisión, el alcance y la calidad son los elementos que caracterizan este tipo de medio.

9.3.1.- CABLE DE PAR SIN TRENZAR: PARALELO

- Formado por dos hilos de cobre paralelos, recubiertos de un material aislante.
- Ofrece muy poca protección frente a interferencias.
- Normalmente se utilizan como cable telefónico para transmitir voz analógica y las conexiones se realizan mediante un conector RJ-11.
- También se utiliza en tendido eléctrico, así como para transmisión de datos a poca distancia (apenas unos metros), ya que las interferencias afectan mucho a este tipo de transmisión.
- El cable paralelo en bus se utiliza comúnmente dentro del ordenador para comunicar entre si los diferentes elementos internos de el, ya que la distancia que los separa es muy corta.
- Según los estándares de cableado estructurado, a este tipo de cable también se le conoce como cable de CATEGORIA 1.

9.3.2.- CABLE DE PAR TRENZADO

- Consiste en 2 cables de cobre aislados, normalmente de 1mm de espesor, entrelazados de dos en dos de forma helicoidal
- Este trenzado se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos y a otras interferencias procedentes del exterior.
- Uno de los cables de par esta marcado con una línea longitudinal que indica que se utiliza como masa, ya que se utiliza para transmisión digital y es necesario seguir el orden en ellos cuando se engasta en el conector.
- Debido a su fácil instalación, velocidad de transmisión de hasta varios Mbps y bajo coste, los pares trenzados se utilizan ampliamente.

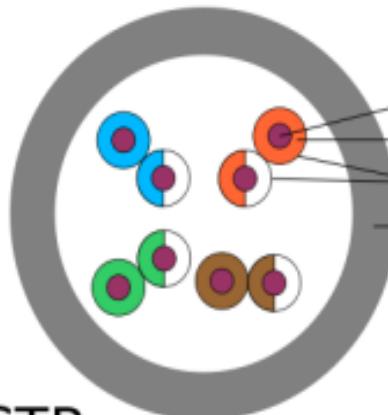


Dependiendo de la forma que se agrupan estos pares, hay varios tipos:

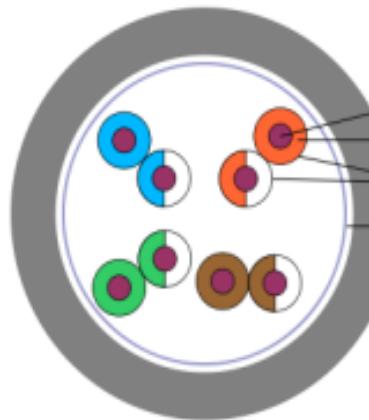
- UPT: Pares trenzados no apantallados. Son los mas simples y no tienen ningún tipo de pantalla conductora. Son muy flexibles, pero muy sensibles a las interferencias. El cable trenzado UTP de categoría 5 esta recubierto de una malla de teflón.
- STP: Pares trenzados apantallados individualmente. En este caso cada par se rodea de una malla conductora, que se conecta a las tomas de tierra de los equipos. Gran inmunidad al ruido.
- S/STP: Pares trenzados, apantallados individualmente con malla global. Igual que los anteriores, apero añadiendo una malla global a todos los cables. Son los que poseen una mayor inmunidad al ruido.
- FTP: Pares trenzados totalmente apantallados. Son unos cables de pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a los UTP, aunque son mas baratos que los STP.

CORTE TRANSVERSAL DE DIFERENTES PARES TRENZADOS

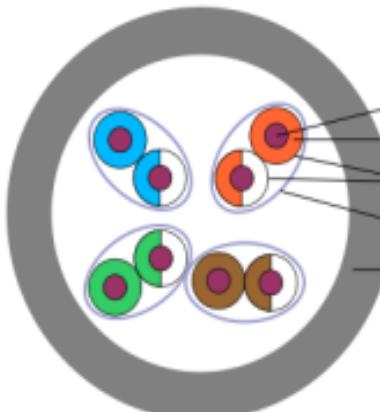
UTP



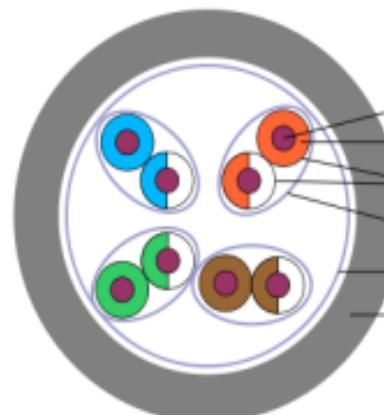
S/UTP



STP



S/STP



conductor
insulation
pair
sheath

conductor
insulation
pair
cable shield
sheath

conductor
insulation
pair
pair shield
sheath

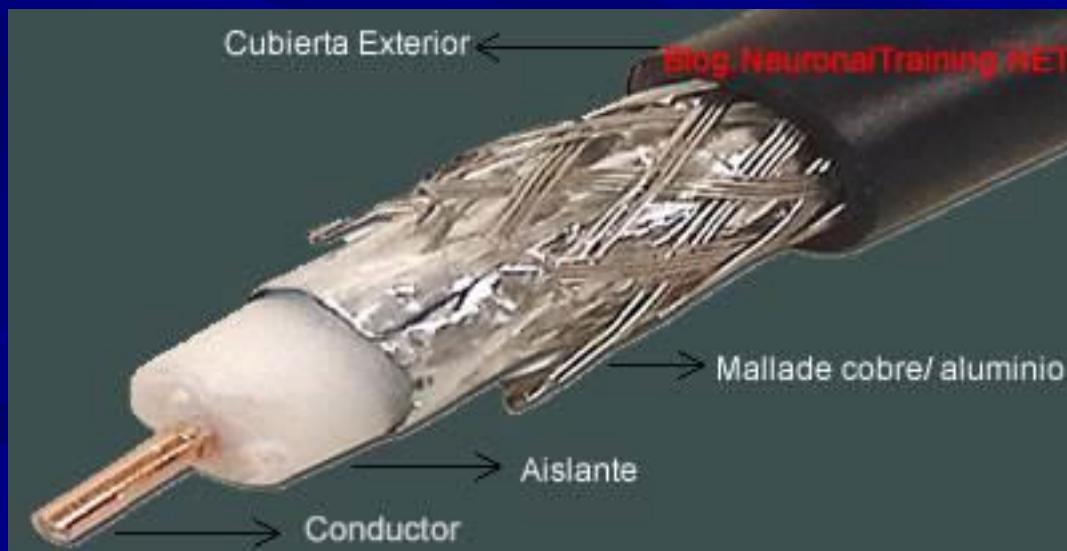
conductor
insulation
pair
pair shield
cable shield
sheath

Según el numero de pares que tenga un cable, el numero de vueltas por metro que posee su trenzado y los materiales utilizados, los estándares de cableado estructurado se clasifican en las siguientes categorías:

- CATEGORÍA 3: Se utiliza para transmitir datos hasta 10 Mbps, con longitudes de segmento hasta 100 mts. Y longitud máxima de red de 500 mts.
- CATEGORIA 4: Velocidades has 16 Mbps.
- CATEGORIA 5: Velocidades hasta 100 Mbps.
- CATEGORIA 6: Velocidades hasta 1000 Mbps.

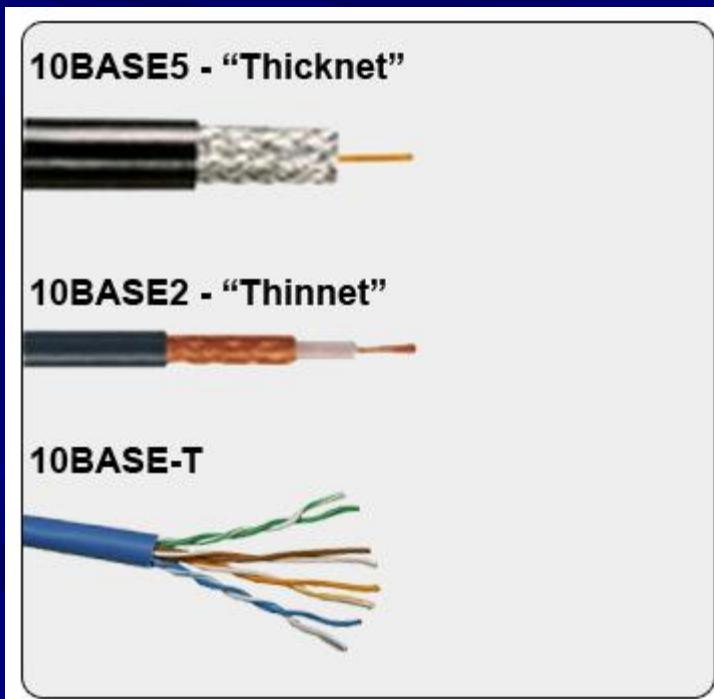
9.3.3.- CABLE COAXIAL

- Formado por un hilo conductor central rodeado de un material aislante que, a su vez, esta rodeado por una fina malla de hilos de cobre o una malla fina cilíndrica. Todo el cable esta rodeado por un aislamiento que le sirve de protección para reducir la emisiones eléctricas.
- Se usa normalmente para datos y para los sistemas de antenas de televisión.
- Transmite una sola señal a una velocidad de transmisión alta.



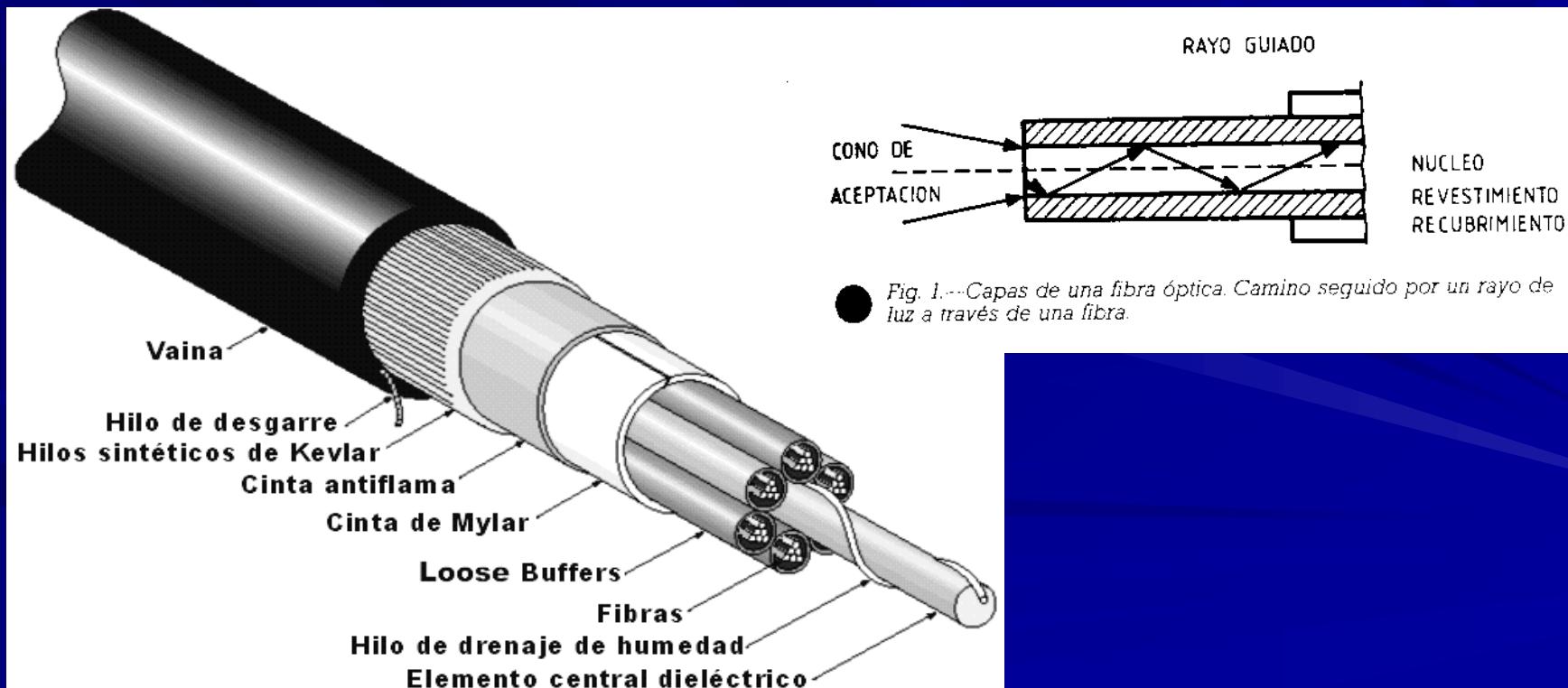
En función de sus características se clasifican en 2 categorías:

- Cable coaxial grueso: 10BASE5. (Thick Ethernet) Tiene un grosor de 0,5 pulgadas, lleva un conector tipo N. Velocidad de transmisión de 10 Mbps y una longitud máxima de 500 mts.
- Cable coaxial delgado: 10BASE2. (Thin Ethernet) Grosor de 0,25 pulgadas, lleva un conector BNC. Velocidad de transmisión de 10 Mbps y una longitud máxima de 200 mts.



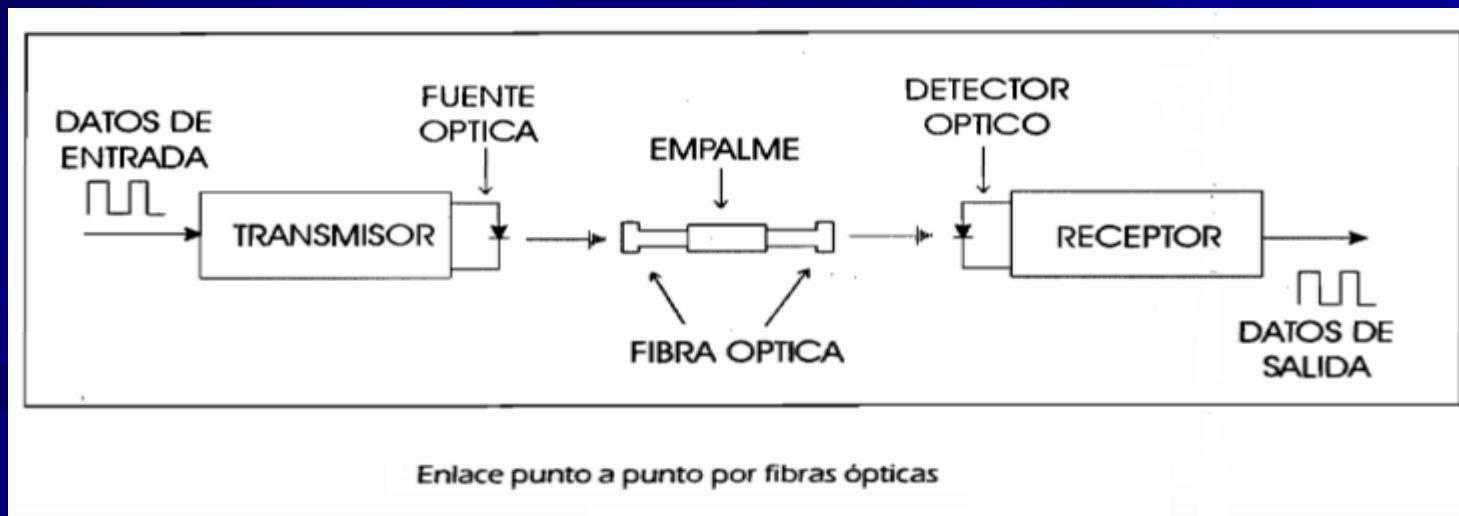
9.3.4.- CABLE DE FIBRA OPTICA

- Esta formado por un cable compuesto de fibras de vidrio.
- Cada filamento tiene un núcleo central de fibra de vidrio con un alto índice de refracción que esta rodeado de una capa de material similar pero con un índice de refracción menor. De esta manera aísla las fibras y evita que se produzcan interferencias entre filamentos contiguos a la vez que protege al núcleo.
- Todo el conjunto esta protegido por otras capas aislantes y absorbentes de luz.



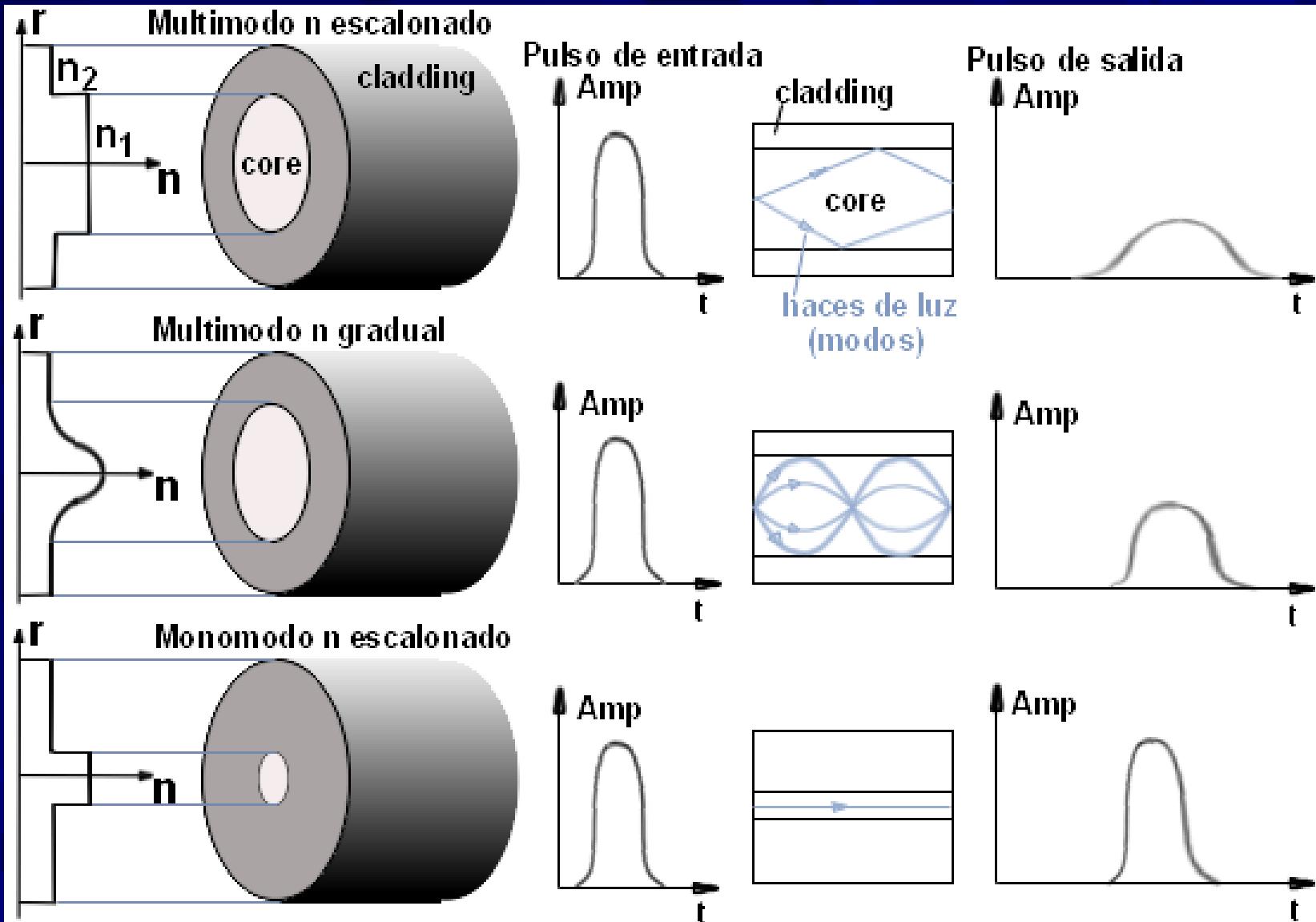
El sistema de fibra óptica esta formado por tres componentes:

- **EMISOR DE ENERGIA OPTICA:** Lleva un modulador para transformar la señal eléctrica (electrones) entrante a la frecuencia aceptada por la fuente luminosa y convertirla en señal óptica (fotones) que se emite a través de la fibra óptica.
- **FIBRA OPTICA:** Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica.
- **DETECTOR DE ENERGIA OPTICA:** Normalmente es un fotodiodo que convierte la señal óptica recibida en señal eléctrica.
- Pueden alcanzar grandes distancia sin utilizar repetidores



Los cables de fibra optica pueden transmitir la luz de tres formas diferentes:

- MONOMODO: La luz se transmite en línea recta. El núcleo tiene un diámetro de 10 μm y la cubierta de 125 μm .
- MULTIMODO: La luz se transmite por el interior del nucleo incidiendo sobre su superficie interna como si se tratara de un espejo. El núcleo tiene un diámetro de 100 μm y la cubierta de 140 μm .
- MULTIMODO DE INDICE GRADUAL: La luz se propaga por el núcleo mediante una refracción gradual. Esto es debido a que el núcleo se construye con un índice de refracción que va en aumento desde el centro a los extraemos. Suelen tener el mismo diámetro que las fibras multimodo.



9.3.5.- MEDIOS NO GUIADOS

- Se basan en la propagación de ondas electromagnéticas por el espacio. El comportamiento de una radiación electromagnética dependerá de sus características ondulatorias y especialmente de la longitud de onda.
- Las ondas electromagnéticas pueden ser:
 - Ondas de radio: λ superior a 30 cms. Recorre grandes distancias y pueden atravesar paredes. Son ondas multidireccionales. El mayor problema son las interferencias entre usuarios. Se emplean en Wifi, bluetoooh.
 - Micro-ondas: λ entre 30 cms y 1 mm.. Viajan en línea recta, por lo que el emisor y el receptor deben estar perfectamente alineados. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra la distancia entre dos repetidores no puede ser superior a 80 Kms.
 - Infrarrojos: Son ondas electromagnéticas direccionales incapaces de atravesar objetos sólidos. Están indicadas para transmisiones a corta distancia. No se consiguen altas velocidades de transmisión.
 - Ondas de luz láser: Son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos.

9.4.- LOS DISPOSITIVOS DE INTERCONEXION

Entre los dispositivos que se utilizan para llevar a cabo una transmisión de datos entre distintos equipos se encuentran: el modem RTC, el cablemódem, el modem ADSL, los puntos de acceso inalámbrico, el concentrador (hub), el conmutador (switch), el puente (bridge), el encaminador (router), la pasarela (gateway) y el cortafuegos (Firewalls).

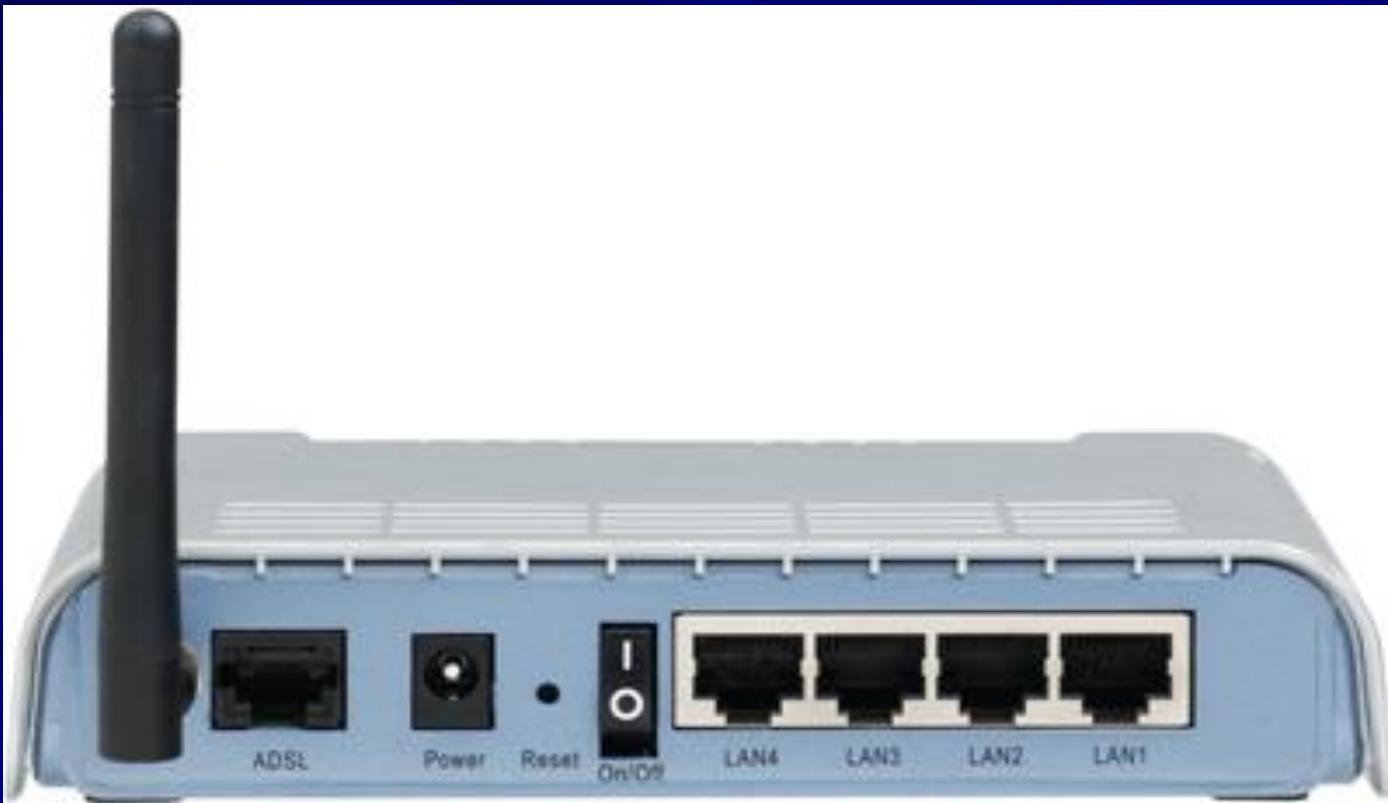
- MODEM RTC: Convierte las señales digitales del ordenador en analógicas (modulación) y cuando llega al otro ordenador las vuelve a pasar a digitales (desmodulación). Permite conectar equipos que están muy separados físicamente o para acceder a Internet a través de la línea telefónica comutada. Actualmente en desuso.



- MODEM DE CABLE O CABLEMODEM: permite la provisión de servicio de datos de banda ancha a través de las redes de los operadores de televisión por cable. La red de cable utiliza un medio compartido en el que los usuarios no tienen un ancho de banda fijo en recepción que permite reducir los costes de mantenimiento y operación frente a tecnologías como la RDSL o el ADLS en las que por cada usuario debe existir una línea física entre el usuario y la central local. El inconveniente en que el ancho de banda se divide entre el número de usuarios conectados.



- MODEM ADSL: La tecnología ADSL se utiliza para aprovechar todo el ancho de banda que ofrece el bucle local de abonado y multiplexar las señales de voz y datos. Su uso depende de la longitud del bucle de abonado, no pudiendo llegar a mas de 5 Km. de la central local. La velocidad de transmisión depende de la distancia a la central. Tecnologías como ADSL 2+ alcanzan mayores distancias.



- PUNTOS DE ACCESO INALAMBRICOS: Los nuevos estándares IEEE 802.11g y n permiten velocidades de transmisión muy elevadas. En una red inalámbrica existen 2 tipos de dispositivos:
 - Tarjetas de red inalámbricas: son los dispositivos que comunican las estaciones con la red a través de tarjetas ISA, PCI, PCMCIA o USB con una antena instalada.
 - Puntos de acceso: Son dispositivos que realizan la misma función que un concentrador de cableado, centralizando las conexiones de red. Sin embargo estos dispositivos funcionan sobre una red sin cables.

Las redes inalámbricas pueden ser de dos tipos:

- Infraestructura: requieren un punto de acceso inalámbrico que gestione todas las comunicaciones
- Ad-hoc: En este caso son los propios ordenadores que llevan instalados adaptadores inalámbricos realizan esta función.



Existen muchos tipos de puntos de acceso dependiendo del tipo de red sobre el que funcionan. Una antena de telefonía móvil también es un punto de acceso al que se conectan todos los usuarios que se encuentran dentro de un radio de acción.

Para que una red inalámbrica extienda su radio de acción, es necesario que cada punto de acceso tenga una cobertura suficiente para llegar a todos los equipos. En el caso de que no se alcancen todos los equipos, es posible instalar nuevos puntos de acceso, que deberán conectarse unos con otros utilizando la propia señal inalámbrica o a través de un cableado ethernet. Las antenas de telefonía móvil se comunican unas con otras a través de enlaces de microondas o a través de cables.

Las antenas pueden ser omnidireccionales o direccionales.

CONCENTRADOS (HUB): Es un equipo que permite compartir el uso de una línea entre varios ordenadores, pero no de forma simultanea. El concentrador simplemente regenera y transmite la señal que recibe, pero no es capaz de identificar hacia donde va la trama de datos y en función de ello, filtrar el trafico. Todos los equipos de la red se conectan mediante un cable al hub. Cuando un equipo envía un mensaje, los datos llegan al hub, este los regenera y los retransmite a todos los equipos conectados al él. Esto hace que el trafico se multiplique por el numero de equipos conectados y se haga mas lenta la transmisión.



CONMUTADOR (SWITCH): Es un dispositivo similar al hub, pero los paquetes los envía solamente al destinatario, y no a todos los equipos. Su función consiste en tomar la dirección MAC destino de una trama de datos y en función de ella enviar los datos por el puerto correspondiente. Actúa de una forma mas inteligente que el hub ya que filtra el trafico y se obtienen mejores velocidades.

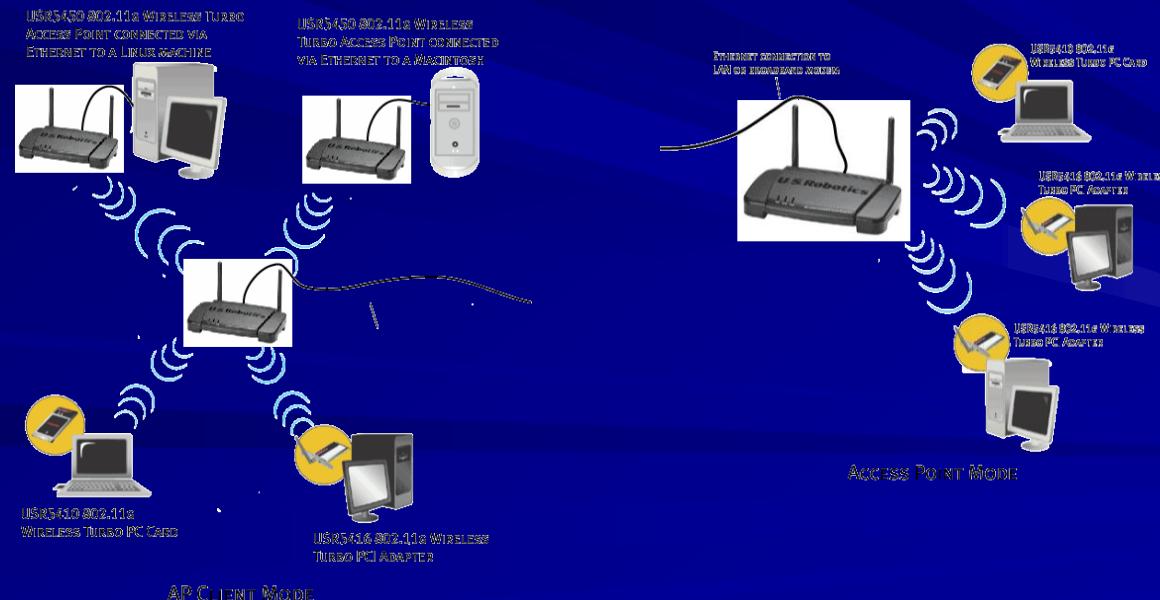


Las principales diferencias entre un hub y un switch son:

- El hub es pasivo y el switch es activo
- El hub repite la señal que recibe a través de un puerto al resto de los puertos, mientras que el switch toma la dirección MAC destino de una trama de datos y, en función de ella, envía la información por el puerto correspondiente.
- En el hub hay mas colisiones que en el switch
- La velocidad de transmisión de un hub siempre es la correspondiente al dispositivo mas lento conectado, mientras que en el switch negocia con cada uno de los dispositivos que se conectan a él, la velocidad de funcionamiento, así como si van a funcionar en full-duplex o half-duplex
- El hub no es configurable mientras que el switch si y además permite la creación de Vlans.
- El hub es mas barato.

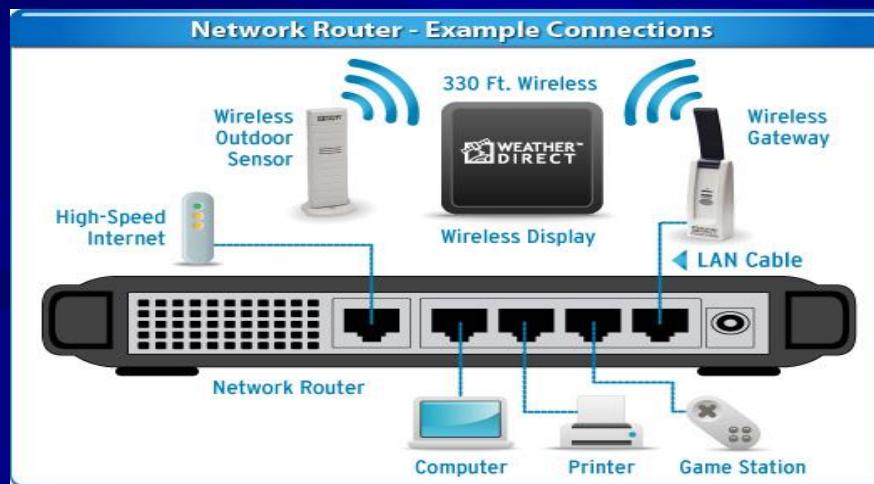
9.4.7 PUENTE (BRIDGE)

- Es un sistema formado por hardware y software que permite conectar dos redes entre si
- Ambas redes deben de usar el mismo protocolo de comunicaciones.
- Sus funciones básicas son las de autoaprendizaje, filtrado y reenvío.
- Si desea reenviar un paquete de datos a una dirección de red que no esta incluida en su tabla de destinos, examina los campos de dirección del paquete (filtrado) y las dirige a la dirección que ha localizado (reenvío). A continuación, la añade a su tabla de destinos (autoaprendizaje).



9.4.8. ENCAMINADOR (ROUTER)

- Un router, no solo incorpora función de filtrado, características de los bridge, sino que además determina la ruta hacia su destino.
- Se utiliza tanto en LAN como en WAN.
- Permite la comunicación entre un equipo individual e Internet, entre una red e Internet o entre redes.
- Las funciones del router son:
 - Interconectar redes físicas o lógicas
 - Recibir los paquetes de datos y almacenarlos para distribuirlos progresivamente en función de la situación de la red.
 - Averiguar las direcciones IP de las redes y equipos que están conectados para realizar un envío óptimo de los paquetes.
 - Evitar la congestión de las redes.



- Un router posee dos direcciones IP, una publica para acceder a internet y otra privada para la red interna.
- Se basan en la utilización de un sistema de direccionamiento jerárquico (tabla de rutas) que distinguen entre la dirección del dispositivo dentro de la red y la dirección de la red.

Enrutador - NAT

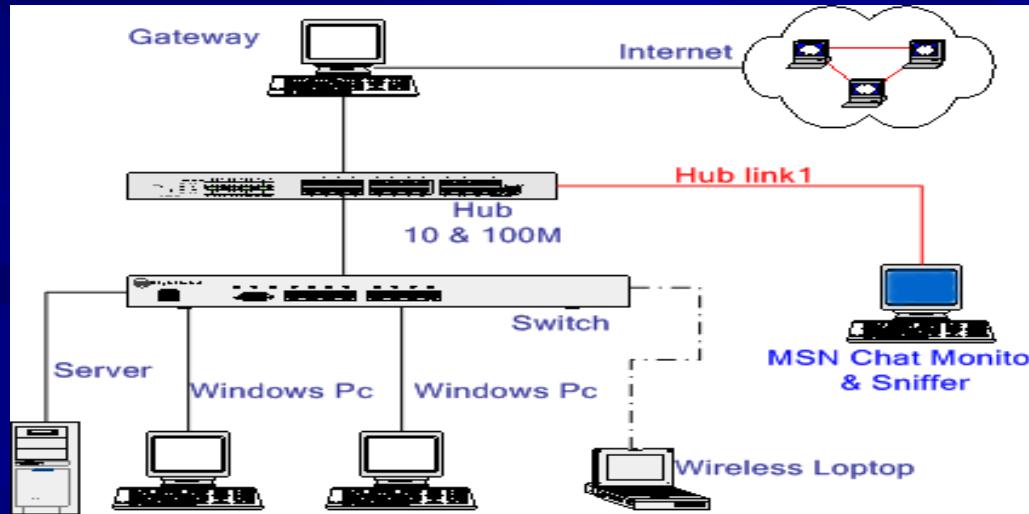
Configuración del redireccionamiento de puerto para utilizar ciertas aplicaciones o para acceder al ordenador desde Internet.

Dirección IP de su ordenador: 192.168.1.100

Servicio	Protocolo	Puerto externo	Puerto interno	Dirección IP del servidor	Eliminar
emule_TCP	TCP	4662	4662	192.168.1.100	<input type="checkbox"/>
emule_UDP	UDP	4672	4672	192.168.1.100	<input type="checkbox"/>
TELNET_TCP	TCP	23	23	192.168.1.100	<input type="checkbox"/>
TELNET_UDP	UDP	23	23	192.168.1.100	<input type="checkbox"/>
HTTPS	TCP	443	443	192.168.1.102	<input type="checkbox"/>
SSH	TCP	22	22	192.168.1.102	<input type="checkbox"/>
ServerHTTP	TCP	5555	80	192.168.1.102	<input type="checkbox"/>
ServerFTP	TCP	5556	21	192.168.1.102	<input type="checkbox"/>
HTTP	TCP	80	80	192.168.1.102	<input type="checkbox"/>

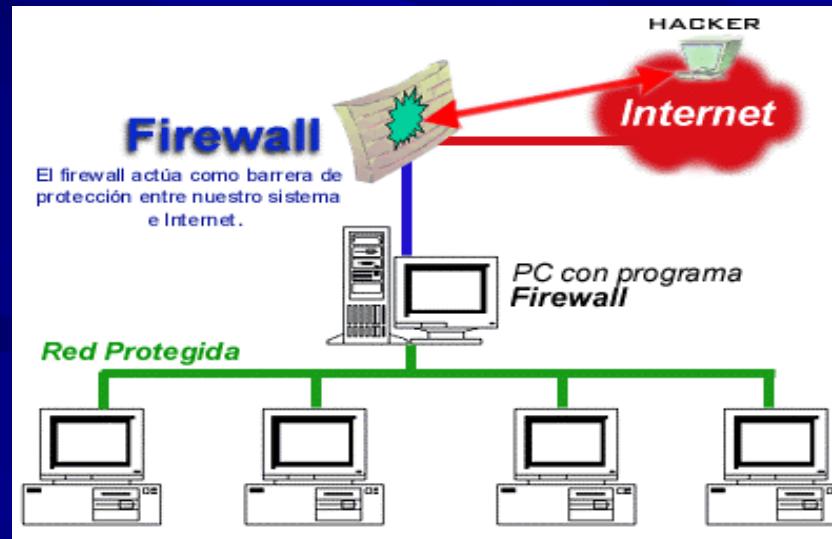
Agregar **Eliminar**

- 9.4.9. PASARELA (GATEWAY)
- Es un sistema formado por hardware y software que permite las comunicaciones entre la red local y un gran ordenador, o un mini ordenador.
- Se suele colocar en el servidor de comunicaciones.
- El Gateway realiza la traducción completa entre las familias de protocolos, proporcionando una conectividad completa entre redes de distinta naturaleza.
- Se encarga del encaminamiento de la información y la interconexión de redes diferentes
- El retraso de propagación de un paquete que atraviesa una pasarela es mucho mayor que el experimentado en otros dispositivos.



9.9.10. CORTAFUEGOS (FIREWALLS)

- Su función es filtrar los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre ellos.
- Este puede ser configurado para permitir que solo determinadas direcciones, origen y destino, puedan acceder a su red o desde ella.
- Las funciones de cortafuegos se pueden realizar por:
 - Ordenadores dedicados (servidor proxy)
 - Routers configurados para esta tarea.
 - Software para distintos sistemas operativos
 - Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.



Beneficios de utilizar cortafuegos:

- Acceso controlado a la red
- Detección de intrusos
- Protección para servicios de Internet que sean vulnerables
- Administración de seguridad centralizada
- Estadísticas de conexiones a la red.
- Filtrado sofisticado de paquetes.

Posibles razones para no utilizar cortafuegos:

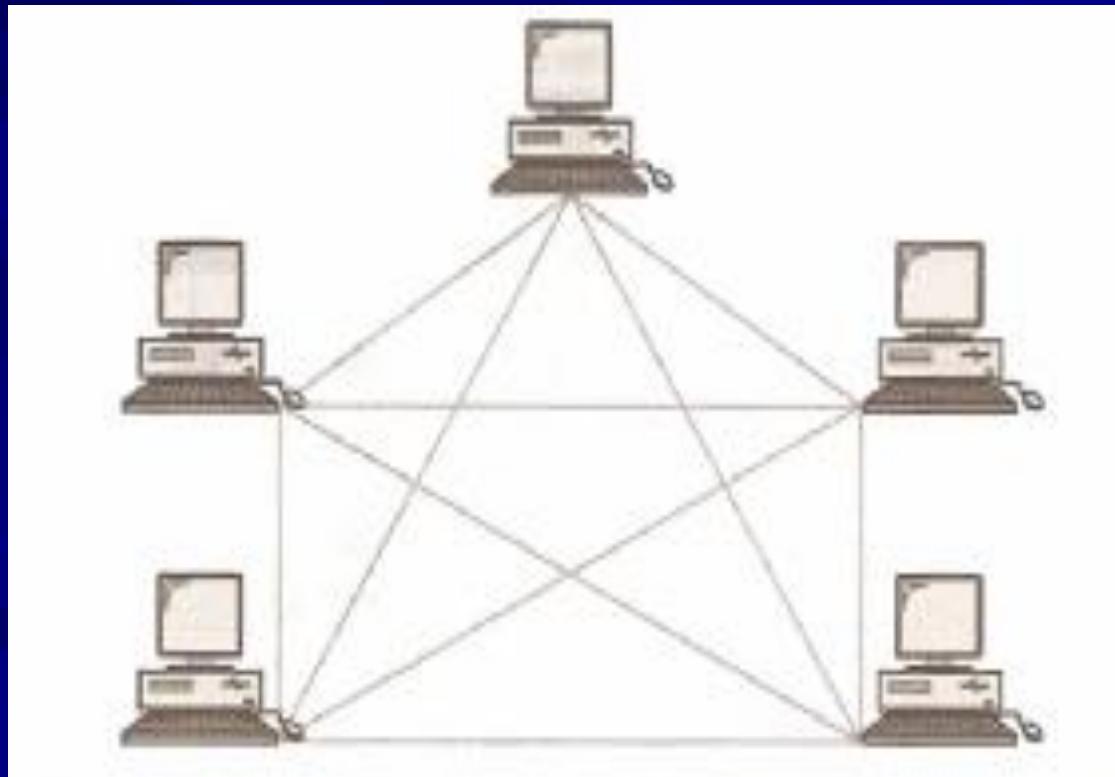
- El acceso a los servicios deseados puede llegar a ser mas complejo de lo normal.
- El peligro de acceso por una puerta trasera a la red se incrementa si no se tiene prevista su inutilización.
- Es necesaria una administración suplementaria de la red
- El coste es mayor
- La configuración se hace demasiado compleja para realizarla de forma adecuada.

10. TOPOLOGIAS DE RED

- Se denomina topología a la forma geométrica en que están distribuidos los diferentes nodos y los cables que las conectan.
- Los nodos de una red se intercomunican entre si mediante una conexión física, y el objeto de la topología es buscar la forma mas económica y eficaz de conectarlas para, al mismo tiempo:
 - Facilitar la fiabilidad del sistema,
 - Evitar los tiempos de espera en la transmisión de los datos,
 - Permitir un mejor control de la red
 - Permitir de forma eficiente el aumento de las estaciones de trabajo.

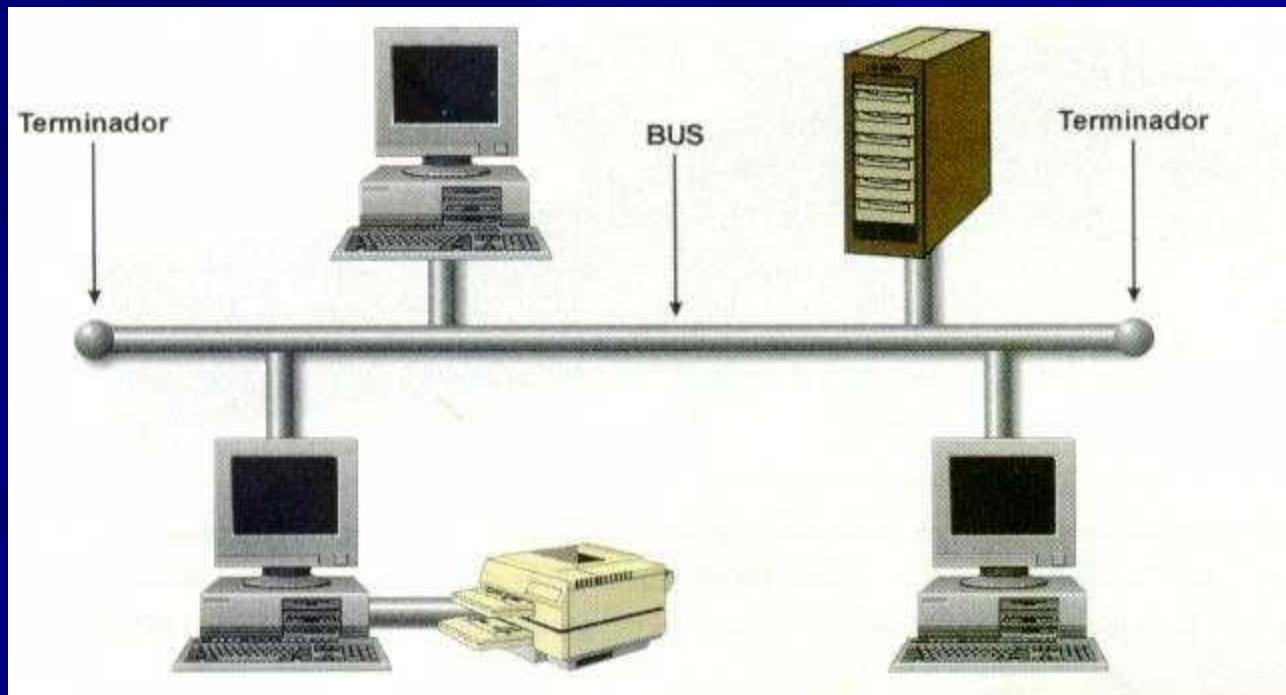
10.1. TOPOLOGIA EN MALLA

- Cada dispositivo tiene un enlace dedicado y exclusivo por cada otro dispositivo que forme parte de la red.
- Es la mas eficiente en cuanto rendimiento
- Es prácticamente inviable en la mayor parte de los casos ya que es muy cara de implementar y muy compleja de mantener o ampliar.



10.2. TOPOLOGIA EN BUS

- Es una topología multipunto donde un mismo enlace físico actúa como red troncal que une todos los dispositivos a la red.
- Es facil de instalar
- La cantidad de cable a utilizar es mínima
- Tiene gran flexibilidad (aumento o disminución de estaciones)
- Un fallo de una estación no repercuten en la red
- La ruptura de un cable la dejara totalmente inutilizada



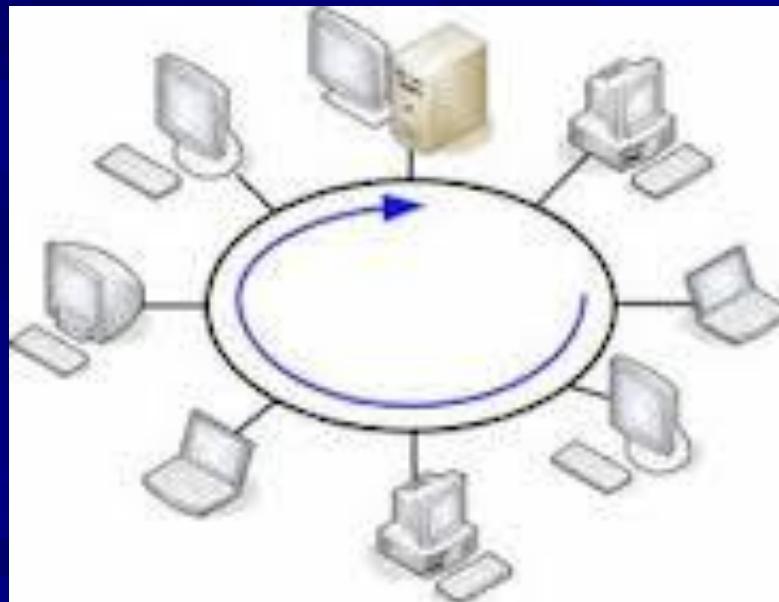
10.3. TOPOLOGIA EN ESTRELLA

- En esta configuración todos los equipos están conectados directamente al conmutador y las comunicaciones se hacen necesariamente a través de él.
- Permite incrementar y disminuir fácilmente el numero de estaciones
- Si se produce el fallo en una de ellas no repercutirá en el funcionamiento general de la red.
- Si se produce un fallo en el conmutador, toda la red se vendrá abajo.
- Es la topología mas utilizada actualmente



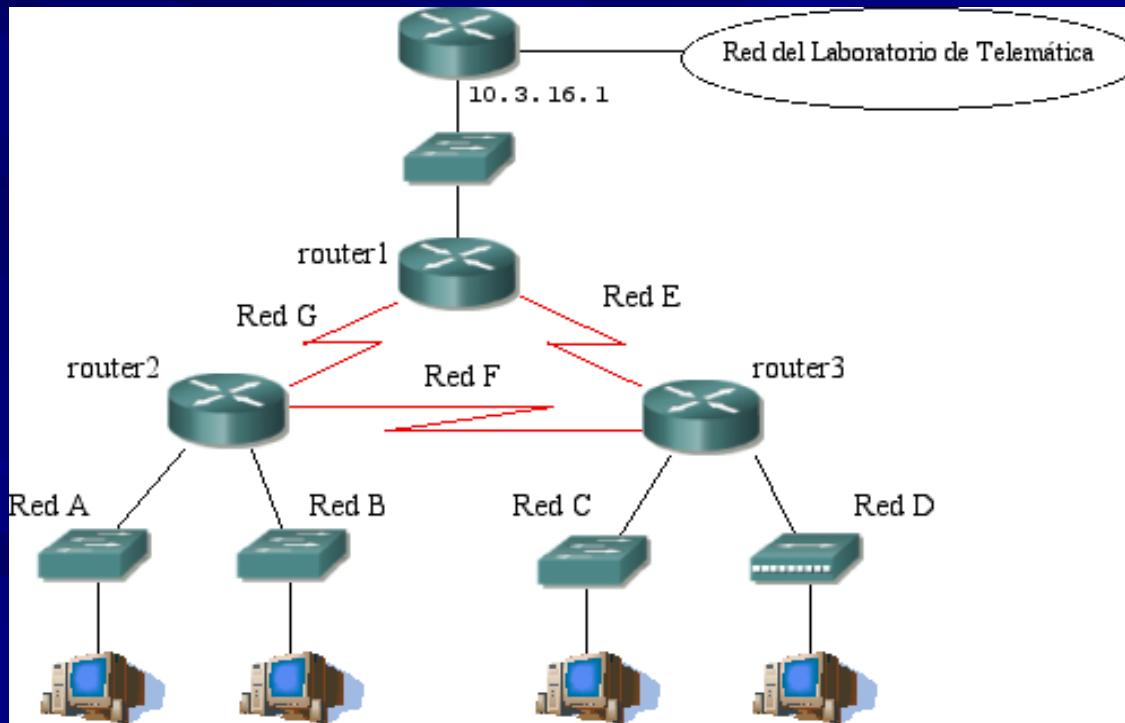
10.4. TOPOLOGIA EN ANILLO

- Cada dispositivo tiene una línea de conexión dedicada y exclusiva solamente con los dos dispositivos mas cercanos.
- Permite aumentar y disminuir el numero de estaciones sin dificultad
- A medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red.



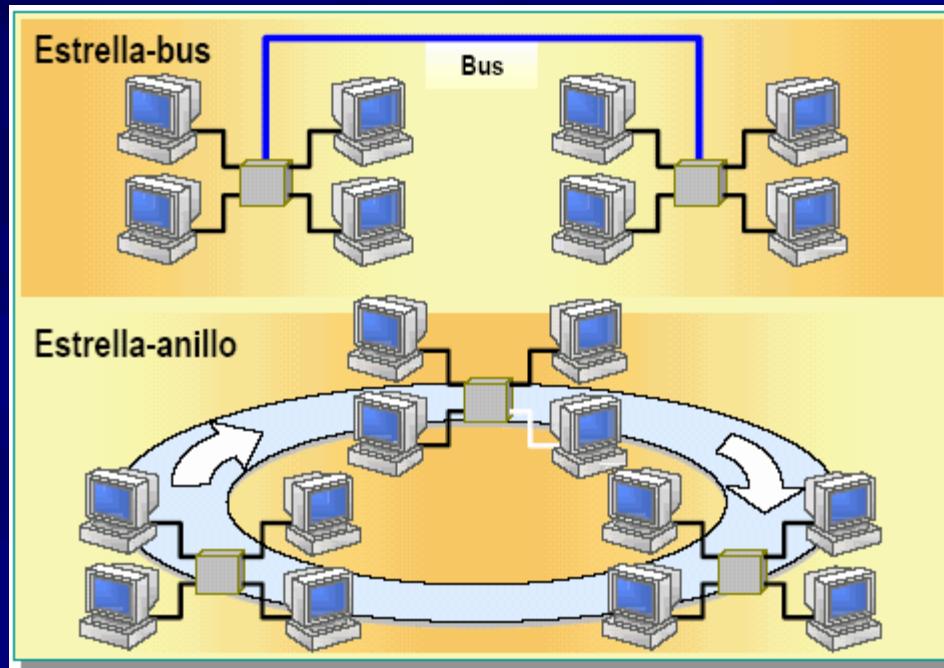
10.5. TOPOLOGIA EN ARBOL

- Es una variante de la topología en estrella
- Es una forma de conectar los nodos como una estructura jerarquizada.
- Es la menos utilizada, ya que el fallo de un nodo o un enlace deja conjuntos de nodos incomunicados entre si
- Se utiliza ampliamente en redes de telefonía, donde los enlaces intermedios son centralitas locales y regionales.



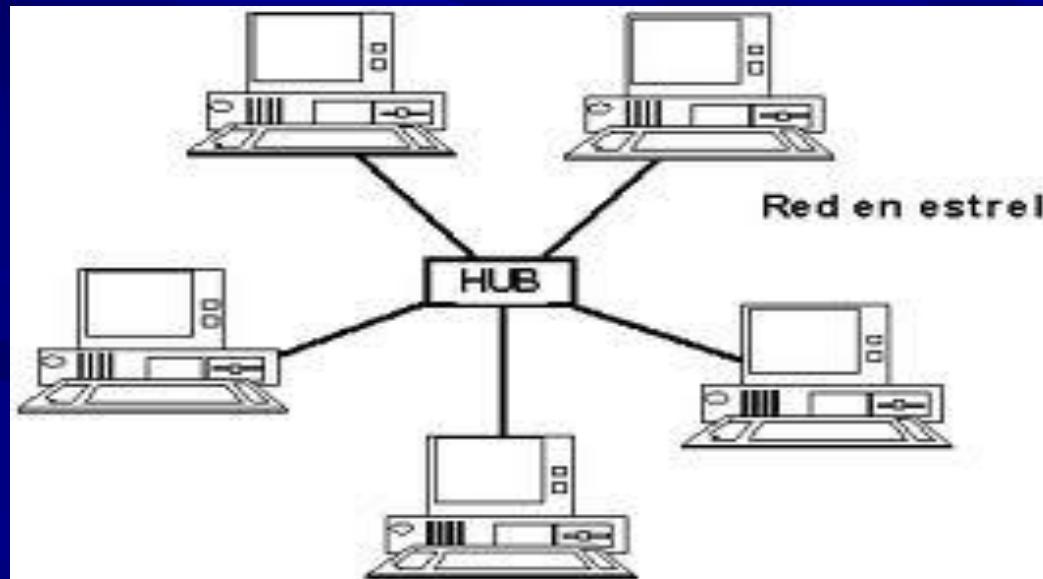
10.6. TOPOLOGIA HIBRIDA

- Es la combinación de varias topologías



10.7. TOPOLOGIA FISICA Y LOGICA

- Hasta ahora todo lo que se ha visto son topologías físicas
- Cada red designa una topología lógica que describe la red desde la perspectiva de las señales que viajan a través de ella.
- Por ejemplo si tenemos una topología de estrella con un hub, cada estación envía y recibe señales por el mismo cable. En el hub se mezclan las señales de todas las estaciones y son trasmisidas a todas ellas (como si estuviesen en bus).
- Por lo tanto es una topología física en estrella que funciona como una topología lógica en bus.



11. LOS PROTOCOLOS

- Son las reglas y procedimientos utilizados por los ordenadores para comunicarse entre ellos a través de una red.
- Existen diferentes niveles de protocolos:
 - De alto nivel: definen como se comunican las aplicaciones
 - De bajo nivel: definen como se transmiten las señales por el cable.Entre estos existen otros protocolos intermedios que realizan funciones como establecer y mantener sesiones de comunicaciones y controlar las transmisiones para detectar errores.

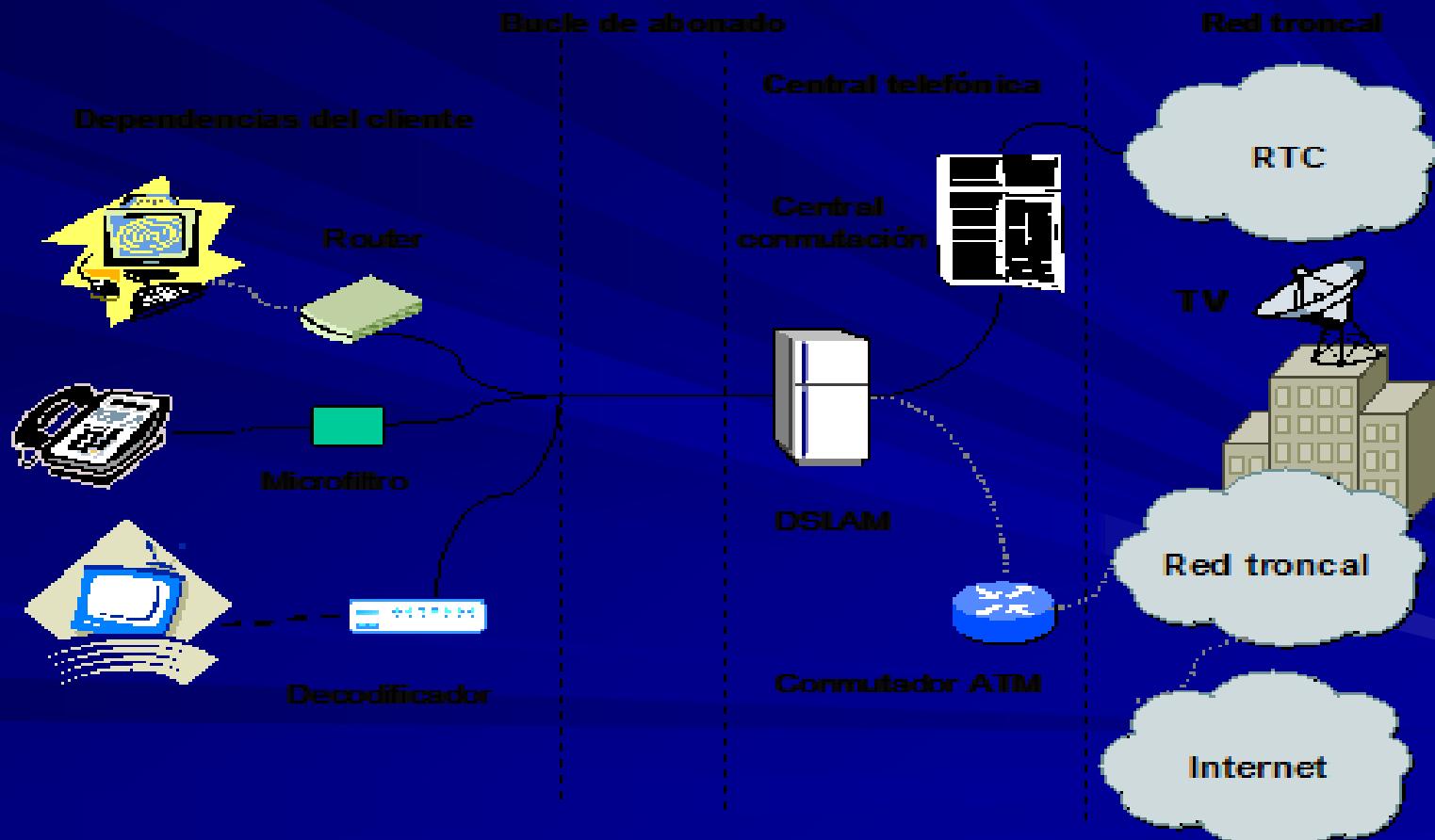
Nivel	Nombre	Categoría
Capa 7	<u>Nivel de aplicación</u>	Aplicación
Capa 6	<u>Nivel de presentación</u>	
Capa 5	<u>Nivel de sesión</u>	
Capa 4	<u>Nivel de transporte</u>	
Capa 3	<u>Nivel de red</u>	Transporte de datos
Capa 2	<u>Nivel de enlace de datos</u>	
Capa 1	<u>Nivel físico</u>	

12. LAS NORMAS IEEE

- El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) es un organismo que ha normalizado la comunicación entre ordenadores.
- Para ello propuso la norma 802, que indica que una red local es un sistema de comunicaciones que permite a varios dispositivos comunicarse entre sí.
- Adicionalmente, el subcomité IEEE 802.1 elabora documentos relativos a la arquitectura de red, interoperación y gestión de red.
- Entre las distintas especificaciones de la norma 802 se encuentran:
 - IEEE 802.1 (1990): Se encarga de la gestión de la red, mensajería, etc.
 - IEEE 802.2 (1990): Normalización para el control del enlace lógico.
 - IEEE 802.3 (1990): Desarrollo del protocolo del acceso múltiple con detección de portadora y detección de colisión.
 - IEEE 802.4 (1990): Desarrollo del bus de paso de testigo.
 - IEEE 802.5 (1989-1991): Especificaciones para una configuración en anillo con paso de testigo (Token Ring)
 - IEEE 802.6 (1990): Especificaciones para una red de área metropolitana (MAN)
 - IEEE 802.7 : Redes locales de banda ancha
 - IEEE 802.8 : Fibra óptica
 - IEEE 802.9 : Estándar para la definición de voz y datos en las redes locales
 - IEEE 802.10: Seguridad en las redes locales
 - IEEE 802.11: Redes locales inalámbricas

13. LA ARQUITECTURA DE RED

Hay muchos tipos distintos de redes, por lo que se pueden realizar múltiples combinaciones distintas al seleccionar el tipo de cableado, la topología, el tipo de transmisión e, incluso, los protocolos utilizados. Estos factores van a determinar la arquitectura de la red.



13.1. ETHERNET

- Fue desarrollada por Xerox
- En un principio se creó para ser utilizada con cable coaxial de banda base, aunque actualmente se pueden utilizar otros tipos de cables y es la que está más extendida.
- El IEEE publicó en 1990 la implementación 10BASE-T, basado en un elemento central donde se implementa un bus lógico pero utilizando una topología física en estrella.
- Las uniones entre cada estación y el elemento central se realizan utilizando cable de par trenzado de categoría 3.
- Esta implementación es la más barata y la más fácil de mantener.
- Paralelamente a esto se desarrolla el cableado estructurado para edificios comerciales.
- Los datos se transmiten a 10 Mbps a una distancia máxima de 2 Km.
- El tamaño del bloque de datos oscila entre 72 a 1526 bytes.
- Todas las estaciones tienen asignada una dirección para la tarjeta de red, que permite que, cuando se cambia de lugar una estación, no haya posibilidad de conflictos y, por tanto, se puede reconfigurar completamente la red local con unos mínimos cambios en el sistema operativo.

13.2. FAST ETHERNET

- Basada en la tecnología Ethernet pero a una velocidad de transmisión de 100 Mbps debido a las siguientes variaciones:
 - Esta construida con hub/switch distribuidos
 - Los cables utilizados son: 100BASE-TX, 100BASE-FX y 100BASE-T4
 - Utiliza tarjetas de red de 100 Mbps

13.3. GIGABIT ETHERNET

- Entre los años 1998 y 1999 el IEEE amplió el estándar a un nuevo tipo de redes, el Gigabit Ethernet en base a dos especificaciones:
 - La 1000BASE-X que utiliza fibra óptica y
 - La 1000BASE-T que utiliza el cable de cobre de par trenzado UTP de cat. 5, 5e o 6 con una longitud max. De 100 mts.
 - La velocidad de tx es de 1000 Mbps o 1Gbps

13.4. 10-GIGABIT ETHERNET

- En 2002 se publico el estándar del 10-Gigabit-Ethernet sobre fibra optica.
- 10GBASE-SR para distancias hasta 300 mts.
- 10GBASE-LR que utiliza fibra óptica monomodo y distancias de hasta 20 Kms.
- 10GBASE-LX4 que utiliza multiplexacion por división de onda (WDM)
- La ultima implementación es del 2006 es 10GBASE-LRM que utiliza fibra óptica multimodo.
- La especificación de la tecnología 10 Gigabit Ethernet sobre cable UTP se publica en 2006 (IEEE 802.3an) . Utiliza cable cat. 6 con una distancia máx.. De 100 mts.

13.5. TOKEN RING

- Creada por IBM en 1985 emplea una topología en anillo con protocolo de paso de testigo y se puede utilizar cable de par trenzado, cable coaxial o fibra óptica.
- Velocidad de 4 Mbps, pudiéndose conectar hasta 8 equipos y una distancia máx., de 350 mts. Con cable coaxial y hasta 16 Mbps si es fibra óptica.

Equivalencias binario/octal/hex/dec

- http://www.sitiosargentina.com.ar/categorias/internet/formatos/tabla_conversion.htm
- Necesitamos conocer estas equivalencias ya que vamos a operar en binario y decimal para las direcciones IP, y binario/hexadecimal para las direcciones MAC.
- De cualquier forma los números que manejamos en este tipo de direcciones siempre están entre 0 y 255 (decimal).

Dirección MAC

- Identifica a una interfaz de red (cableada o inalámbrica) de un equipo o dispositivo en la red local (LAN).
- Se compone de 6 cifras de 8 bits (48 bits total), separadas por “：“, y se suelen representar con 2 dígitos hexadecimales cada una (4+4 bits)
- Ejemplo → E1:AC:30:00:6F:A7
- Las 3 primeras cifras (24 bits) identifican al fabricante del dispositivo, mientras que las 3 últimas identifican de forma ÚNICA al dispositivo.

Dirección IP

- Sirve para identificar un dispositivo de red en redes que usen el protocolo TCP/IP (Internet por ejemplo)
- En una red local (LAN) sirve también para identificar a los equipos y dispositivos, aunque para comunicarse dentro de este tipo de red se utiliza realmente la MAC.
- Se compone de 4 cifras de 8 bits, que se suelen representar en decimal.
- Ejemplo → 192.168.2.12 → En binario:
1100000.10101000.00000010.00001100

Protocolo ARP

- En las comunicaciones dentro de la LAN se utiliza la dirección MAC, sin embargo la dirección que se configura es una dirección IP.
- El protocolo ARP consiste en:
 - Un ordenador A se quiere comunicar con otro B (sabe únicamente su IP)
 - A envía un mensaje ARP a TODOS (broadcast) los ordenadores de la red preguntando por la MAC del que tiene esa dirección IP
 - (A envía su propia MAC también)
 - El ordenador B recibe ese mensaje y contesta a A, indicándole su dirección MAC
 - A apunta la IP y la MAC de B en una tabla ARP, y B hace lo mismo.

Protocolo ARP (II)

- Si B no responde en un determinado tiempo de espera, A deja de esperar (no lo encuentra).
- Cada cierto tiempo las entradas de la tabla ARP se van borrando (se puede cambiar una tarjeta de red de un equipo o la IP) y hay que volver a preguntar
- Se pueden crear entradas estáticas
- Comandos para ver la tabla ARP
 - Linux → **arp -n**
 - Windows → **arp -a**

Interface 220.0.0.80

Internet Address	Physical Address	Type
220.0.0.160	00-50-04-62-F7-23	static
192.128.0.3	00-54-0A-14-AC-13	dynamic

Máscara de Red

- Parte de una dirección IP se utiliza para identificar a la red, mientras que otra parte identifica al dispositivo.
- Para delimitar ambas partes se utiliza la máscara de red.
- La máscara es una dirección del mismo tamaño que una IP. Se representa en decimal, pero hay que pasarla a binario para entender cómo funciona.
- Los bits de la máscara empezarán con una cantidad de unos seguidos y el resto serán ceros.
- Los bits que están a 1, indican los bits de la IP que identifican a la red.
- Los que están a 0 indican qué bits identifican a los equipos de la red.

Máscara de Red (II)

- Tipos de red local según bits de la máscara a 1:
 - Tipo A → 8 bits → 255.0.0.0
 - Tipo B → 16 bits → 255.255.0.0
 - Tipo C → 24 bits → 255.255.255.0
 - Se pueden usar otros tamaños de máscara
- Tendremos que traducir la máscara y la IP a binario para saber identificar la parte que corresponde a la red y cual a los equipos en la IP.
 - IP → 192.168.2.12 Máscara → 255.255.255.0 (C)
 - IP → 11000000.10101000.00000010.00001100
 - Máscara → 11111111.11111111.11111111.00000000
 - Los bits a 1 identifican la red (192.168.2)
 - Los bits a 0 identifican al equipo (12)

Máscara de Red (II)

- Si tenemos n bits para identificar equipos dispondremos de $(2^n - 2)$ direcciones disponibles.
- Hay 2 direcciones que no podremos usar para identificar equipos:
 - Todos los bits de equipo puestos a 0 → Es la dirección que identifica a la red (y nunca a un equipo)
 - Todos los bits de equipo puestos a 1 → Es la dirección de difusión o broadcast. Sirve para enviar un mensaje a todos los equipos de la red.
 - Ejemplo → Si queremos una red de 7 equipos necesitaremos como **mínimo** 4 bits para los equipos → $2^4 - 2 = 14$, mientras que con 3 no es suficiente → $2^3 - 2 = 6$ equipos.

Servidor DNS

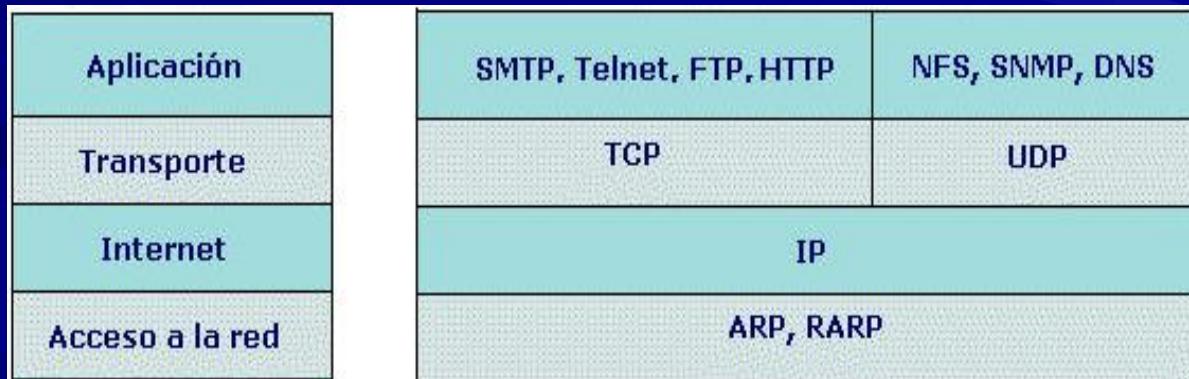
- Cuando nos comunicamos con un ordenador que está en internet, a menudo usamos el nombre del dominio (gmail.com, youtube.es,...) en lugar de directamente usar la dirección IP.
- Los servidores DNS (que configuramos en los equipos) son servidores en internet que se encargan de traducir estos nombres de dominio a sus respectivas IP y viceversa.
 - Con el comando “**arp nombre_dominio**” podremos ver la ip, por ejemplo. Otra opción es mandarle un ping a esa dirección → “**ping nombre_dominio**”

Servidor DHCP

- Cuando no necesitamos tener una dirección IP fija en un equipo, la opción más sencilla es que se le asigne de forma automática.
- Para ello un equipo, normalmente el router, debe tener instalado un servidor DHCP.
- El servidor DHCP se encargará de suministrar una ip automática (dentro de un rango definido) a los equipos que se lo pidan, también envía la configuración de los servidores DNS y la puerta de enlace (router que da salida fuera de la red)
- De forma temporal, el servidor DHCP guarda a que equipo (MAC) le ha asignado IP. Muchas veces esta IP asociada caduca (leasing time) y se le proporciona otra nueva.

Modelo TCP/IP

- Es el modelo usado para las comunicaciones a través de internet.
- Las capas de arriba hacen uso de los servicios que le ofrecen las capas de abajo.
- Ejemplo: El protocolo IP (internet), necesita del protocolo ARP (Acceso a la red) para poder llegar a su destino dentro de una red local.



Tablas de rutas (encaminamiento)

- Todos los equipos, y routers sobre todo, tienen una tabla interna donde aparecen las redes a las que pueden acceder, y a qué dirección IP (puerta de enlace) deben dirigir el paquete para que llegue a esa red.
 - Comandos “**route -n**” o “**netstat -n -r**” en linux. “**route print**” en Windows.
- La red 127.0.0.0/8 representa a una red interna del equipo (físicamente no existe), para mandarse mensajes a sí mismo.
- Las direcciones que empiezan por 169.x.x.x también están reservadas para cuando una interfaz no tiene una IP válida sea asignada automáticamente, es una dirección falsa, que no sirve, sino que se utiliza porque “debemos de tener alguna IP asignada aunque no sea válida”.

Tablas de rutas (encaminamiento) (II)

- Ejemplo de tabla de rutas en Windows

Dirección de red	Máscara de red	Puerta de enlace	Interfaz
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.33
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
192.168.1.0	255.255.255.0	192.168.1.33	192.168.1.33
192.168.1.255	255.255.255.255	192.168.1.33	192.168.1.33

- Ejemplo de tabla de rutas en Linux

Destino	Pasarela	Genmask	Indic	Métric	Ref	Uso	Interfaz
0.0.0.0	192.168.2.1	0.0.0.0	UG	0	0	0	eth0
192.168.2.0	0.0.0.0	255.255.255.0	U	1	0	0	eth0

Tablas de rutas (encaminamiento) (III)

- Método para construir una tabla:
 - Primero ponemos la red (o redes) a las que esté conectado directamente el equipo. La puerta de enlace a esas redes será la ip que tenga asignada el equipo en esa tarjeta de red.
 - También podemos poner “directo” en ese apartado.
 - Añadimos el resto de redes de nuestra organización, y como puerta de enlace ponemos el router al que le tenemos que enviar el paquete para que llegue.
 - La última dirección (si queremos tener salida a internet por ejemplo) es la de por defecto (0.0.0.0) que implica todas las demás redes. Aquí la puerta de enlace es el router que nos dará acceso a internet. En el equipo está la primera, pero como la tabla se suele recorrer en orden, nosotros la

Capa de transporte

- La capa de red (o capa de enlace) se encarga de transportar datos a través de las redes locales, y la capa de internet, de transportarlos por medio de routers a otra red diferente.
- La capa de transporte se encarga, entre otras cosas, del control de errores en la comunicación, control de congestión, direccionamiento de aplicaciones (números de puerto).
- Hay 2 protocolos de transporte → TCP y UDP
- Por ejemplo el protocolo TCP se encarga de verificar:
 - Los datos llegan en orden (los ordena)
 - Los datos no tienen errores (si no, pide un reenvío)
 - Descarta los datos duplicados (reenvío por error)
 - Controla la congestión del tráfico

Capa de transporte (II)

- El protocolo UDP sin embargo, no controla ninguna de estas cosas. Se utiliza para aplicaciones donde es importante que lleguen los datos lo más rápido posible sin importar que se pierdan algunos (audio y vídeo en tiempo real por ejemplo, donde no importa si en un momento fijo se han perdido unos cuantos píxeles o baja la calidad de sonido).
- Las aplicaciones que reciben comunicaciones de datos “**escuchan**” los puertos (16 bits → hasta el 65535) para recibir datos.
- Cada aplicación tiene su puerto asignado. Hasta el 1024 son puertos estándar reservados por el sistema, y a partir de ahí, los puede usar cualquier aplicación.
- http://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puerto

PAT/NAT

- El PAT (Port Address Translation) o NAT (Network Address Translation) de una única dirección, lo utilizan los router para que un equipo de la red externa pueda enviar a otro de la red interna.
- Cuando un ordenador de la red interna establece una conexión con otro exterior, el router le asigna automáticamente un puerto (mayor de 1024) a esa conexión.
- El equipo externo sólo verá la IP externa de nuestro router, pero también reciben el puerto al que deben responder.
- Cuando el equipo manda la respuesta a nuestro router en el puerto asignado a la conexión, el router nos la redirige automáticamente a nosotros.

PAT/NAT (II)

- Lo que hace el router es hacer una traducción para que un paquete que vaya hacia un equipo de la red interna (dirección privada) pueda llegar a su destino.
- Cuando un equipo envía un paquete además de la IP de destino también tiene un puerto de destino.
- El equipo establece un puerto de origen, para que la respuesta la envíen a ese puerto.
- Cuando se establece una conexión desde un equipo de la red interna hacia el exterior, el router guarda, mientras dure la conexión un puerto

PAT/NAT (III)

- Para que pueda establecer conexión un equipo de fuera con uno interno, se debe establecer la traducción de forma manual (NAT estático).
- Ejemplo: Si tengo un servidor web en mi red interna (el servicio web escucha en el puerto 80) y quiero que desde el exterior se puedan hacer peticiones a mi servidor (establecer conexión), debo hacer la siguiente equivalencia:
 - $\text{IP_EXTERNA_ROUTER:80} \rightarrow \text{IP_MAQUINA:80}$
- De esta forma los equipos de fuera harán las peticiones al puerto 80 de la IP externa del router (IP pública) y este se encargará de redirigirlas al equipo interno.

IPv6

- Para solventar el problema de la escasez de direcciones IPv4, entre otros, hace años que existe el nuevo estándar IPv6, aunque aún no se utiliza casi en la práctica.
- Las direcciones IPv6 se representan con 128bits, separados en 8 grupos de 16bits, cada grupo representado con 8 caracteres hexadecimales.
 - Ejemplo: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
- Cuando hay grupos donde los 16 bits están a 0 consecutivos se pueden omitir, pero sólo se puede hacer en una parte de la dirección.
 - 2001:0DB8:0000:0000:0000:1428:57ab
 - 2001:0DB8::1428:57ab
- Los ceros iniciales se pueden omitir.

Pv6 (II)

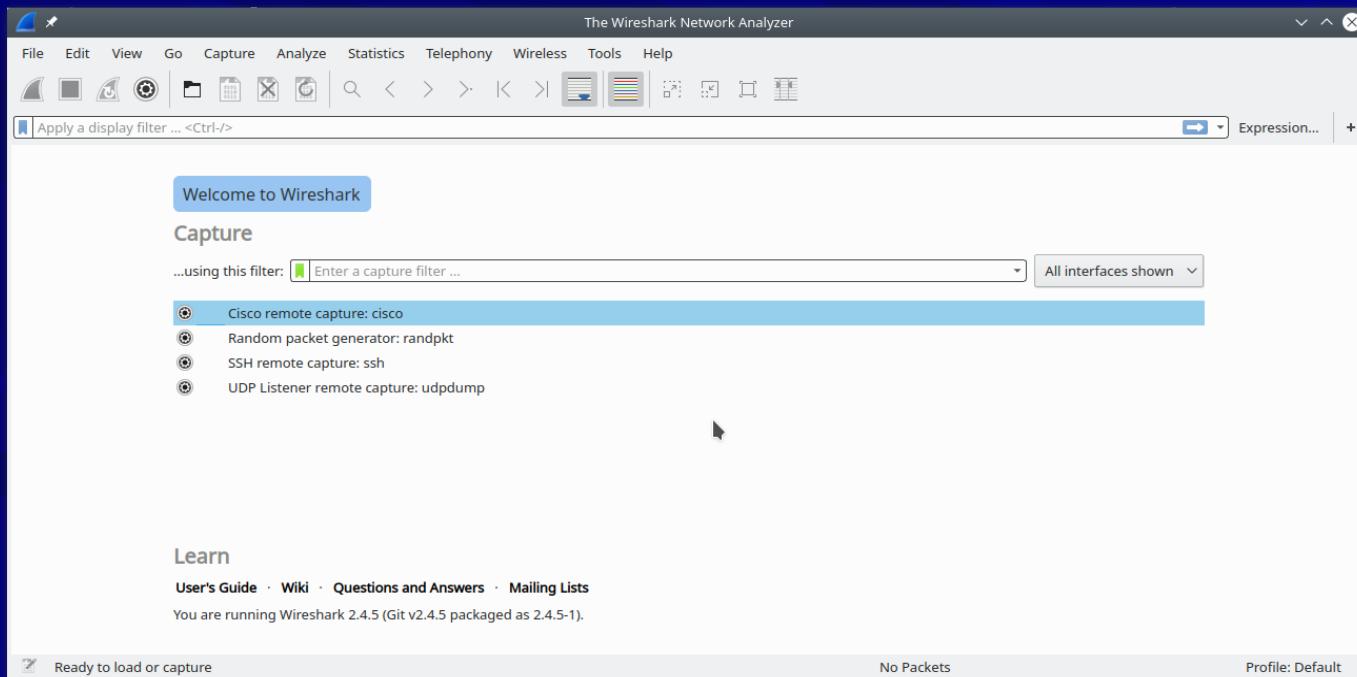
- Si se tiene una dirección IPv6 con un campo de ceros no consecutivo, sólo se puede representar la dirección de la siguiente forma:

1319:0000:0000:7344
0000:7344

- La razón es que no podemos saber cuantos bloques faltan en cada sitio.
- Para representar una dirección IPv4 en formato IPv6 y así tener sistemas híbridos, pasamos la dirección IPv4 a hexadecimal y los representamos como los últimos 32 bits, precedidos de un bloque FFFF.
 - 192.168.12.4 → 11000000.10101000.00001100.00000100
 - ::FFFF:C0A8:0C04

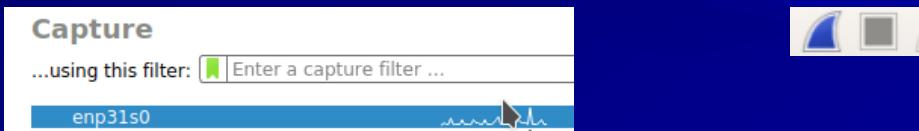
Monitorización de la red - Wireshark

- El software Wireshark permite capturar y analizar paquetes que recibe y envía un equipo de la red local.
 - Podemos filtrar y analizar estos paquetes, obteniendo



Monitorización de la red – Wireshark (II)

- Primero debemos seleccionar la interfaz de la red donde queremos escuchar.
 - Posteriormente, haciendo clic en el botón de captura, el programa escucha todos los paquetes que pasan por la interfaz y los va capturando hasta que lo paremos.
- Una vez capturados los paquetes, podemos inspeccionarlos y filtrarlos:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	AsrockIn_3e:f5:57	Broadcast	ARP	42	Who has 192.168.1.170? Tell 192.168.1.205
2	0.033065578	Apple_f0:3d:03	AsrockIn_3e:f5:57	ARP	64	192.168.1.170 is at d0:a6:37:f0:3d:03 [ETHERNET FRAME CHECK SEQUENCE]
3	0.033085816	192.168.1.205	192.168.1.170	ICMP	98	Echo (ping) request id=0x7bc1, seq=1/256, ttl=64 (reply in 4)
4	0.035603446	192.168.1.170	192.168.1.205	ICMP	98	Echo (ping) reply id=0x7bc1, seq=1/256, ttl=64 (request in 3)
5	0.717478081	192.168.1.205	91.189.91.157	NTP	90	NTP Version 4, client
6	0.835608252	91.189.91.157	192.168.1.205	NTP	90	NTP Version 4, server
7	1.001696937	192.168.1.205	192.168.1.170	ICMP	98	Echo (ping) request id=0x7bc1, seq=2/512, ttl=64 (reply in 8)
8	1.003096852	192.168.1.170	192.168.1.205	ICMP	98	Echo (ping) reply id=0x7bc1, seq=2/512, ttl=64 (request in 7)

Monitorización de la red – Wireshark (III)

- Al seleccionar un paquete, podemos ver más abajo información del mismo en las diferentes capas de red, así como del protocolo usado.
- Ejemplo: Envío de paquete ARP para preguntar por la IP 192.168.1.170

```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface "VirtualBox Host-Only Network", link-layer type Ethernet II (Ethernet), timestamp {0, 0}, length 42 (104 bytes on wire (336 bits), 42 bytes captured (336 bits))  
└─ Ethernet II, Src: AsrockIn_3e:f5:57 (70:85:c2:3e:f5:57), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
    └─ Address Resolution Protocol (request)  
        Hardware type: Ethernet (1)  
        Protocol type: IPv4 (0x0800)  
        Hardware size: 6  
        Protocol size: 4  
        Opcode: request (1)  
        Sender MAC address: AsrockIn_3e:f5:57 (70:85:c2:3e:f5:57)  
        Sender IP address: 192.168.1.205  
        Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)  
        Target IP address: 192.168.1.170
```

Monitorización de la red – Wireshark (IV)

- Ejemplo: Paquete de respuesta de ping (protocolo ICMP)

```
▶ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) o
└ Ethernet II, Src: Apple_f0:3d:03 (d0:a6:37:f0:3d:03), Dst: AsrockIn_
  └ Destination: AsrockIn_3e:f5:57 (70:85:c2:3e:f5:57)
  └ Source: Apple_f0:3d:03 (d0:a6:37:f0:3d:03)
    Type: IPv4 (0x0800)
└ Internet Protocol Version 4, Src: 192.168.1.170, Dst: 192.168.1.205
  └ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
```

Monitorización de la red – Wireshark (V)

- Ejemplo: Paquete de respuesta de un servidor DNS con la IP del dominio iessanvicente.com.

```
▶ Frame 151: 104 bytes on wire (832 bits), 104 bytes captured (8
▼ Ethernet II, Src: CompalBr_20:71:77 (dc:53:7c:20:71:77), Dst:
  ▶ Destination: AsrockIn_3e:f5:57 (70:85:c2:3e:f5:57)
  ▶ Source: CompalBr_20:71:77 (dc:53:7c:20:71:77)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 62.81.16.213, Dst: 192.168.1
▶ User Datagram Protocol, Src Port: 53, Dst Port: 57890
▼ Domain Name System (response)
  [Request In: 79]
  [Time: 0.219801918 seconds]
  Transaction ID: 0x1cd3
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 1
  ▼ Queries
    ▶ iessanvicente.com: type A, class IN
  ▼ Answers
    ▶ iessanvicente.com: type A, class IN, addr 176.31.241.20
```

Monitorización de la red – Wireshark (VI)

- Se pueden filtrar los paquetes capturados en base a ciertos criterios. Se pueden ver algunos ejemplos de filtros en el menú **Analyze** → **Display Filters**.
 - Dichos filtros pueden combinarse con los operadores **||**, **&&** y **!** (negación), o los equivalentes **and**, **or** y **not**

Name	Filter
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}