UT8. Introducción a los sistemas en red. Direccionamiento IP

1. Introducción

Esta unidad es la primera que se dedica a las redes informáticas. Se comienza estudiando la clasificación y arquitectura de red basándose en los modelos OSI y TCP/IP. A continuación se ven las distintas topologías o esquemas de red existentes, para centrarse en todos los dispositivos físicos que se utilizan. También se ven los estándares de las redes inalámbricas con sus modos de conexión. Posteriormente se estudia el direccionamiento IP de las redes y subredes, para finalizar con las tablas de enrutamiento para garantizar la seguridad en los routers.

Imagen de warszawianka con licencia Creative Commons Zero 1.0, enlace

2. Redes. Características y clasificación

2.1 Características de las redes

En esta unidad se van a estudiar los conceptos teóricos de redes con sus direcciones físicas (MAC[1]) y direcciones lógicas (IP[2]), elementos físicos de

[1] **MAC.** Son las siglas inglesas de Control de Acceso al Medio, también conocida como dirección física, es un número de 48 bits, que se expresa mediante 6 parejas de números hexadecimales que se asigna de forma única a cada tarjeta o dispositivo de red en el momento de su fabricación.

[2] **IP**. Valor numérico que identifica, de manera lógica y jerárquica, la interfaz de red de un dispositivo dentro de una red que utilice el protocolo IP.

conexión y cálculos de direcciones IP. Posteriormente, en la unidad 9 se implementarán de forma práctica en Windows y en la unidad 10 en GNU-Linux.

Definimos red informática como dos o más dispositivos conectados para compartir los componentes de su red, y la información que pueda almacenarse en todos ellos.

Una definición más formal es la dada por Andrew S. Tanenbaum, una **red de computadoras**, también llamada red de ordenadores o **red informática**, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos.

Redes de ordenadores. Ventajas.

Si conectamos dos ordenadores entre sí ya tenemos una red, si conectamos más ordenadores, le agregamos impresoras, y nos conectamos a dispositivos que permitan salir a Internet, estamos consiguiendo que nuestra red sea cada vez mayor y pueda disponer de mayores recursos, ya que los recursos individuales pueden compartirse. Esta es la idea principal de las redes, a medida que conectamos más dispositivos y estos comparten sus recursos, la red será más potente.

- Las principales ventajas de las redes de ordenadores serán:
- La posibilidad de compartir recursos.
- La posibilidad de compartir información.
- Aumentar las posibilidades de colaboración.
- Facilitar la gestión centralizada.
- Reducir costes.

2.2 Clasificación de Redes. Tipos de redes

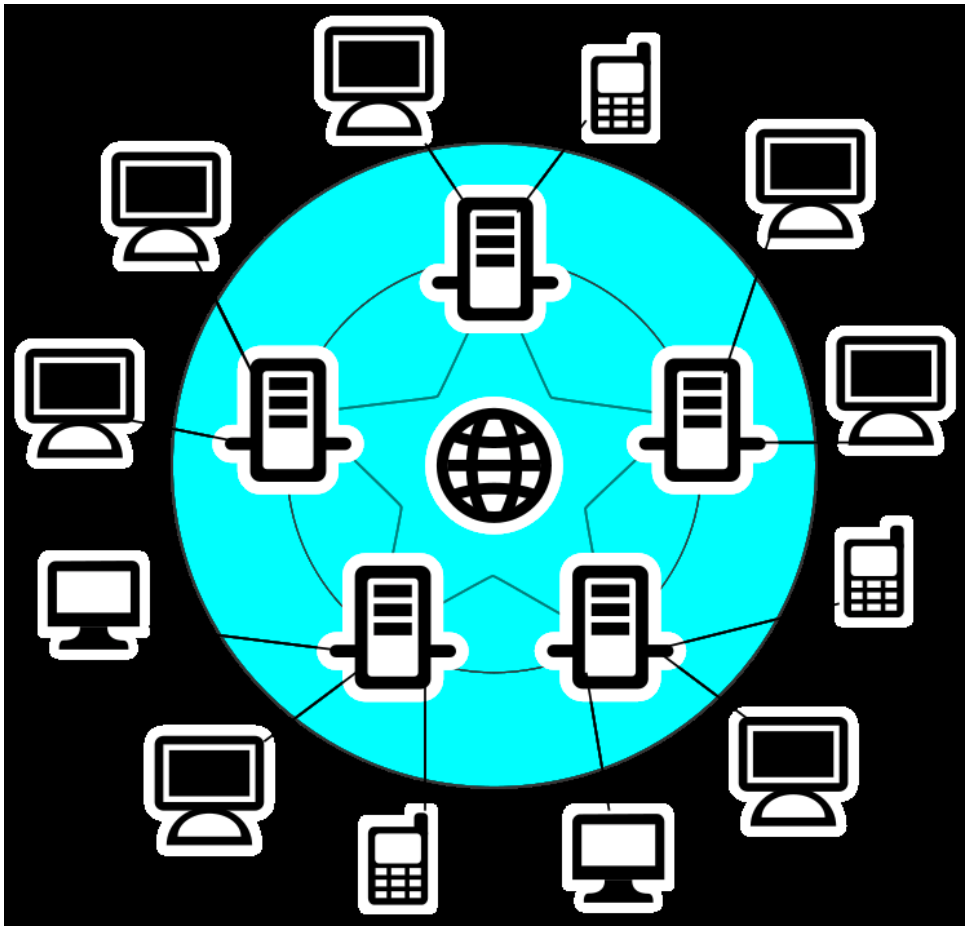


Imagen de Davide Capasso / daccap con licencia Creative Commons obtenida de:
http://www.openclipart.org/detail/131179/internet-scheme-by-daccap

Las redes se pueden clasificar según diferentes conceptos.

2.2.1 Por alcance o extensión:

- **Red de área local o LAN (local area network)** es una red que se limita a un área especial, relativamente pequeña, tal como un cuarto, un aula, un solo edificio, una nave, o un avión. Las redes de área local suelen tener mayores velocidades y la unión de ellas crearán redes más grandes.
- **Red de área metropolitana o MAN (metropolitan area network)** es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. Este concepto se utiliza para definir redes que abarcan extensiones relativamente grandes, y que necesitan recursos adicionales a los que necesitaría una red local.
- **Red de área amplia o WAN (wide area network)** son redes informáticas que se extienden sobre un área geográfica extensa. Dentro de esta clasificación

podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y el propio Internet que puede considerarse como una gigantesca red WAN.

2.2.2 Según las funciones de sus componentes

- **Redes de igual a igual o entre iguales**, también conocidas como redes peer-to-peer, son redes donde ningún ordenador está a cargo del funcionamiento de la red. Cada ordenador controla su propia información y puede funcionar como cliente o servidor según lo necesite. Los sistemas operativos más utilizados incluyen la posibilidad de trabajar de esta manera, y una de sus características más destacadas es que cada usuario controla su propia seguridad.
- **Redes cliente-servidor**, se basan en la existencia de uno o varios servidores, que darán servicio al resto de ordenadores que se consideran clientes. Este tipo de redes facilitan la gestión centralizada. Para crear redes de este tipo necesitamos sistemas operativos de tipo servidor, tales como Windows Server o GNU-Linux.

2.2.3 Según el tipo de conexión:

- **Redes cableadas**: En este tipo de redes se utilizan diferentes tipos de cables para conectar los ordenadores.
- **Redes inalámbricas**: Son las redes que no necesitan cables para comunicarse, existen diferentes tecnologías inalámbricas que se estudian más adelante.

2.2.4 Según el grado de difusión:

- **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP[3], garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Precisamente esta característica es la que ha hecho que el uso de Internet se generalice y que todas las redes funcionen utilizando protocolos TCP/IP.

[3] **TCP/IP**. Se trata de un conjunto de protocolos de red que permiten la transmisión de datos entre computadoras. A pesar de que existen más de 100 protocolos distintos, su nombre se debe a los dos más importantes por ser los más utilizados, y que además fueron los primeros en definirse: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP).

- **Intranet** es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole **de forma privada**, esto es, que no comparte sus recursos o su información con otras redes. Aunque la intranet no esté conectada a Internet, también suelen utilizar los protocolos TCP/IP. Dicho de otra forma, el funcionamiento de una intranet se basa en los mismos principios que Internet, pero sin conexión a Internet.

3. Arquitectura de la red. Modelos OSI y TCP/IP

3.1 Arquitectura

Cuando se habla de arquitectura de red se refiere a cómo está construida la red, con el **hardware y software** utilizado.

En cuanto al hardware, se definirán que **cables, equipos y conexiones** se utilizan. Aparte de decidir que equipos se van a utilizar para la conexión, **hay que definir unos protocolos** en la comunicación. Pero, ¿qué es un protocolo? Al igual que el lenguaje tiene unas normas y sintaxis para comunicarse dos personas, los **protocolos marcarán la forma de comunicarse dos dispositivos físicos**. Igual que hay distintos lenguajes, español, inglés, francés; también hay distintos protocolos.

La arquitectura de red tendrá en cuenta **tres factores im**portantes:

- **Topología**: La forma de cómo se conectan los nodos (distintos equipos) de una red.
- **Método de acceso**: El medio utilizado para la transmisión de los datos: cable, aire.
- Los **protocolos** de comunicación.

3.1.1 Protocolo de comunicación

Imagen de "Photodisc" con licencia Uso educativo no comercial para plataformas públicas de Formación Profesional a distancia, obtenida de Procedencia: CD-DVD Num. V07

Como se ha dicho un protocolo de comunicaciones es un conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación.

Se necesitan distintos protocolos para:

- Identificar el emisor y el receptor.
- Definir el medio o canal que se puede utilizar en la comunicación.
- Definir el lenguaje común a utilizar.
- Definir la forma y estructura de los mensajes.
- Establecer la velocidad y temporización de los mensajes.
- Definir la codificación y encapsulación del mensaje.

3.1.2 Modelos por capas o niveles

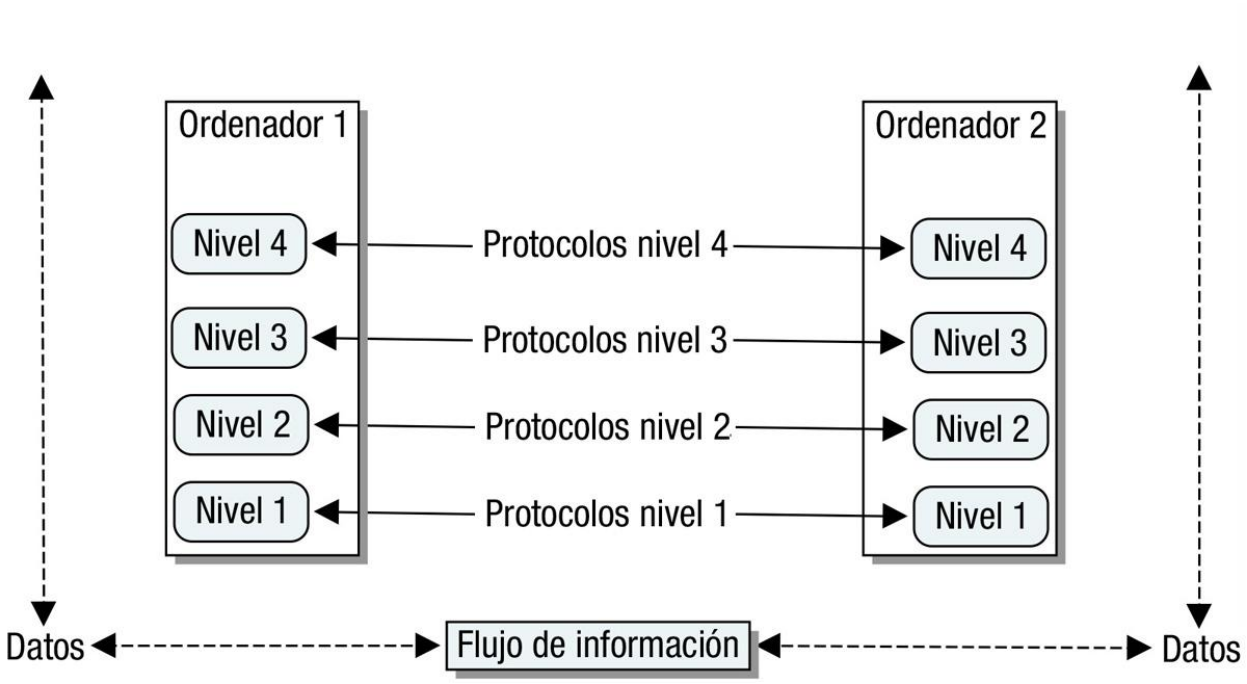


Imagen obtenida de materiales originales de FP a Distancia

La **arquitectura de red se divide en niveles o capas** para reducir la complejidad de su diseño. Las capas están jerarquizadas, cada una son sus servicios y funciones asignadas, para lo que utilizará los protocolos necesarios. Cada nivel sólo se comunica con el nivel superior o el inferior.

Entonces, ¿cómo funciona una arquitectura basada en niveles? En la figura anterior se observan dos ordenadores conectados con una arquitectura de cuatro niveles. Supongamos que el ordenador primero quiere realizar una transferencia de datos al ordenador segundo. **En la capa superior es donde se ordena realizar esa transferencia**, pero la capa superior no se fija en los detalles (como llegar al segundo PC, su dirección, ruta para llegar, medio de transmisión a utilizar…). **Los**

detalles son las funciones de las capas inferiores. De ahí, que **hay que pasar por todas las capas desde la cuarta capa superior a la primera capa inferior**, donde cada capa realiza sus funciones de buscar el mejor camino para llegar al destino. **Desde la primera capa, se pasa la información al ordenador de destino a su primera capa. Ya en el ordenador de destino, se sigue la secuencia contraria**, se va subiendo de capa a capa, para que la capa superior solo conozca los datos recibidos, sin conocer los detalles de cómo ha llegado esa información.

Una buena analogía es mandar una carta. Como clientes de Correos se estaría en la capa superior, sin que importe al remitente y al destinatario cómo llega la carta. Esos detalles, escalas que realiza la carta, transporte utilizado (avión, tren o furgón), carteros utilizados son las funciones de las capas inferiores. Al destinatario solo le interesa que llegue la carta y sin errores.

En este tipo de arquitectura cada nivel genera su propio conjunto de datos, que se pasa con los datos originales a la siguiente capa.

Las arquitecturas de red basadas en capas facilitan las compatibilidades, tanto de software como de hardware, pues no es necesario cambiar todas las capas cuando queremos mejorar el sistema. Bastaría modificar los protocolos afectados.

3.2 Modelo OSI

El **modelo OSI** que significa Open System Interconnection "Interconexión de sistemas abiertos" es el modelo de red creado por la Organización Internacional para la Normalización (ISO) en el año 1984. OSI agrupa los procesos de comunicación en siete capas que realizan tareas diferentes. Es conveniente tener en cuenta que el modelo OSI, no es una arquitectura desarrollada en ningún sistema, sino una referencia para desarrollar arquitecturas de red, de forma que los protocolos que se desarrollen puedan ser conocidos por todos.

Los niveles o capas OSI son:

- **Capa 1, capa física**. Se encarga de las conexiones físicas, incluyendo el cableado y los componentes necesarios para transmitir la señal.
- **Capa 2, capa de enlace de datos**. Empaqueta los datos para transmitirlos a través de la capa física. En esta capa se define el direccionamiento físico utilizando las conocidas direcciones MAC. Además se encarga del acceso al medio, el control de enlace lógico y de la detección de errores de transmisión, entre otras cosas.

- **Capa 3, capa de red**. Separa los datos en paquetes, determina la ruta que tomaran los datos y define el direccionamiento.
- **Capa 4, capa de transporte**. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores.
- **Capa 5, capa de sesión**. Mantiene y controla el enlace entre los dos extremos de la comunicación.
- **Capa 6, capa de presentación**. Determina el formato de las comunicaciones así como adaptar la información al protocolo que se esté usando.
- **Capa 7, capa de aplicación**. Define los protocolos que utilizan cada una de las aplicaciones para poder ser utilizadas en red.

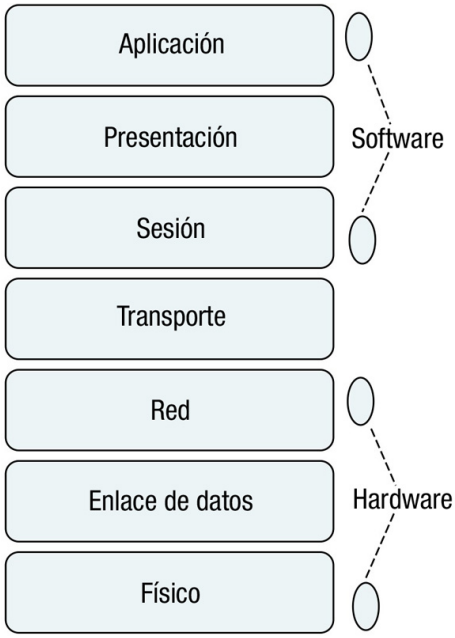


Imagen obtenida de materiales originales de FP a Distancia

En la imagen se representa los distintos niveles de OSI. **Las capas 1, 2 y 3 del modelo están relacionadas con el hardware y las capas 5, 6 y 7 están relacionadas con el software, siendo la capa 4 una capa intermedia** entre hardware y software. Lo cual quiere decir que los dispositivos y componentes de red físicos, suelen trabajar en los niveles inferiores 1 a 3, siendo los programas los que trabajan en los niveles superiores.

3.3 Modelo TCP/IP

El modelo TCP/IP es la arquitectura de redes más utilizada. Es la base de las comunicaciones de Internet y de los sistemas operativos modernos.

Cuando nos referimos a la arquitectura TCP/IP o modelo TCP/IP, nos estamos refiriendo a un conjunto de reglas generales de diseño e implementación de protocolos de red, que permiten la comunicación de los ordenadores. Su nombre se debe a que los dos protocolos más importantes que utiliza son el protocolo TCP (Protocolo de Control de Transmisión) y el protocolo IP (Protocolo de Internet)

La arquitectura TCP/IP está compuesta de cuatro capas o niveles que son:

- **Nivel de subred, nivel acceso a la red o nivel de enlace**. Se encarga del acceso al medio de transmisión, es **asimilable a los niveles 1 y 2 del modelo OSI**. Permite y define el uso de direcciones físicas utilizando las direcciones MAC.
- **Nivel de red o nivel** de Internet. Esta capa **equivale a la capa 3 del modelo OSI**, con el mismo nombre y se encarga de estructurar la información en paquetes y determinar la ruta del PC origen al destino que tomarán los paquetes.

  Los paquetes pueden viajar hasta el destino de forma independiente y desordenada. La ordenación y control de errores no será responsabilidad de esta capa. El protocolo más significativo de esta capa es el **protocolo IP**, y entre sus funciones está la de dar una dirección lógica a todos los nodos de la red.
- **Nivel de transporte**. Esta capa **equivale a la capa 4 del modelo OSI**. Se encarga de que **los paquetes** de datos **tengan una secuencia adecuada y** de **controlar los errores**. Los protocolos más importantes de esta capa son: TCP y UDP. **El protocolo TCP** es un protocolo orientado a conexión[4] y fiable, y el **protocolo UDP** es un protocolo no orientado a conexión y no fiable.
- **Nivel de aplicación**. Esta capa **engloba a las capas 5, 6 y 7 del modelo OSI**. Incluye todos los protocolos de alto nivel relacionados con las aplicaciones que se utilizan en Internet.

En el gráfico siguiente se ve la equivalencia de los modelos OSI y TCP/IP.

[4] **Orientado a conexión**. Cuando antes de realizarse la comunicación se establece una conexión ya sea física o lógica, pero de forma permanente, lo que asegura que los datos se reciben por lo que también se suele hablar de conexiones fiables o protocolos fiables. En contraposición a este concepto esta el no orientado a conexión, que no necesita establecer una conexión para poder transmitir, esto hace a los protocolos más rápidos pero no fiables.

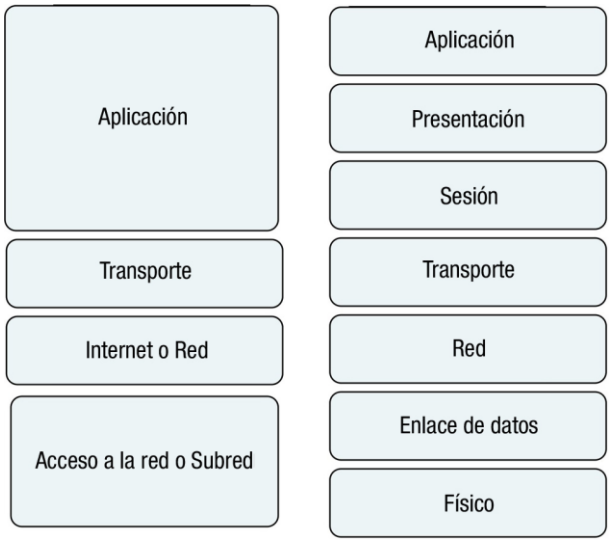


Imagen obtenida de materiales originales de FP a Distancia

Vídeos aclaratorios:

Para entender funcionamiento de capas:

https://www.youtube.com/watch?v=WnvSsQQ0z5Y

Vídeo de TCP/IP : https://www.youtube.com/watch?v=JQDCL17sARA

3.3.1 Nivel 1. Nivel de enlace o acceso

La principal función de este nivel es convertir la información suministrada por el nivel de red, en señales que puedan ser transmitidas por el medio físico al nodo de destino. La función inversa es convertir las señales que llegan por el medio físico en paquetes de información manejables para el nivel de red.

En este nivel se deben tener en cuenta las cuestiones relacionadas con las conexiones físicas, que en las redes locales vienen definidas por el estándar IEEE 802.3 que se estudia en el siguiente libro.

Un aspecto muy importante de este nivel es el **direccionamiento físico**, conocido como **control de acceso al medio**, con siglas MAC. **La dirección MAC es un identificador de 48 bits, que se representa con 12 dígitos hexadecimales**, representado habitualmente en el formato FF:FF:FF:FF:FF:FF

Al decir dígitos hexadecimales, se hace referencia a que se utiliza el sistema de numeración base 16, que significa que cada cifra puede tomar 16 valores distintos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

De esta forma, **todas las tarjetas de red tienen una dirección física o dirección MAC única en el mundo**.

De los 12 dígitos hexadecimales, los 6 primeros representan el fabricante de la tarjeta de red.

En este nivel hay dos protocolos relacionados con el direccionamiento físico: **ARP y RARP**.

ARP (Address Resolution Protocol, Protocolo de resolución de direcciones) **se encarga de relacionar la dirección física (dirección MAC) con la correspondiente dirección lógica (dirección IP)**. Mientras que la dirección física trabaja en el nivel de subred, la dirección lógica trabaja en el nivel de red. Pero se necesitan ambas para enviar mensajes de un ordenador a otro.

El protocolo **RARP** (**Reverse ARP**, Protocolo de resolución de nombres inverso) realiza la función contraria.

Estos dos protocolos también trabajan en el siguiente nivel, por ser el que trabaja con las direcciones IP.

De esta forma, la información a enviar al ordenador de destino, será la recibida de la capa superior (capa de red), junto con la dirección MAC del equipo origen y la dirección MAC del equipo destino. A esta información se le llama trama.

3.3.2 Nivel 2. Nivel de red

El objetivo principal del nivel de red será **encaminar los paquetes desde el nodo origen hasta el nodo destino, aunque estén en distinta red**. La información se divide en paquetes, que viajan de forma independiente, atravesando distintas redes y sin orden. **La capa de red no se preocupa de las tareas de ordenación de los paquetes cuando llegan a su destino**. Esto es lo que se conoce como servicio no orientado a conexión. Cada paquete recibe el nombre de datagrama[5].

Las **funciones** más importantes de la **capa de red** son:

- **El direccionamiento lógico**: Permite identificar de forma única cada nodo de una red. **Las direcciones lógicas reciben el nombre de IP**. En este nivel se habla de direccionamiento lógico, para distinguirlo del direccionamiento físico visto en el nivel de subred.
- **El enrutamiento**: También llamado **encaminamiento**, los protocolos de esta capa deben ser capaces de encontrar el **mejor camino entre dos nodos**.

[5] **Datagrama**. Técnica de conmutación de paquetes, donde cada paquete se trata de forma independiente, conteniendo cada uno la dirección de destino.

Para realizar estas funciones el nivel de red utiliza como **protocolos** más destacados **de este nivel**:

- **IP: Internet Protocol, o Protocolo de Internet** proporciona un enrutamiento de paquetes no orientado a conexión y es usado tanto por el origen como por el destino para la comunicación de datos.

  El protocolo IP, también **proporciona las direcciones IP**. La dirección IP es la dirección lógica que identifica dentro de una red a un nodo o tarjeta de red. Coexisten en la actualidad dos versiones de IP, IPv4 (versión 4) e IPv6 (versión 6). Se diferencian en el número de bits que utiliza cada dirección, **IPv4 utiliza direcciones de 32 bits e IPv6 6 utiliza direcciones de 128 bits**.

  Ejemplos de direcciones IP son:

  IP versión 4: 192.168.1.11 (Utilizando valores en decimal).

  IP versión 6: 2001:0DB8:0000:0000:0000:0000:1428:57AB (Utilizando valores en hexadecimal y puede simplificarse como: 2001:0DB8::1428:57AB)

- **ARP y RARP**: También se utilizan en la capa de subred de datos y sirven para relacionar direcciones IP con direcciones MAC y viceversa.

- **ICMP: Protocolo de mensajes de control en Internet**, suministra capacidades de control y envío de mensajes. **También se considera protocolo del nivel de transporte, y herramientas tales como ping[6] y tracert[7] lo utilizan** para poder funcionar (estas herramientas las estudiaremos en la unidad 9 y 10)

3.3.3 Nivel 3. Nivel de Transporte

Cumple la función de establecer las reglas necesarias para establecer una conexión entre dos dispositivos remotos. Como la capa de red en la arquitectura TCP/IP no se preocupa del orden de los paquetes ni de los errores, es en esta capa donde se cuidan estos detalles.

Este nivel es el encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén conectados en la misma red.

---

[6] **Ping**. Es un comando que se utiliza para comprobar el estado de la conexión en una red de ordenadores utilizando paquetes ICMP de solicitud y de respuesta

[7] **Tracert**. En sistemas Windows, y traceroute en sistemas GNU/Linux, permite seguir la pista de los paquetes desde un ordenador de origen a otro de destino, algo así como saber la ruta que siguen los paquetes desde un origen hasta su destino.

Al igual que las capas anteriores, la información que maneja esta capa tiene su propio nombre y se llama segmento. Por tanto, la capa de transporte se debe de encargar de unir múltiples segmentos del mismo flujo de datos.

Los dos protocolos más importantes que trabajan en este nivel son el TCP y el UDP.

TCP es un protocolo orientado a conexión y fiable, **se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo** a través de redes no fiables. Por eso es tan útil en Internet, ya que las redes que configuran Internet podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete, etc. Pero TCP tiene un diseño que se adapta de manera dinámica a las propiedades de estas redes y permite la conexión en muchos tipos de situaciones.

UDP es un protocolo no orientado a conexión y no fiable, este protocolo proporciona todo lo necesario para que las aplicaciones envíen datagramas IP encapsulados sin tener una conexión establecida. Uno de sus usos es en la **transmisión de audio y vídeo en tiempo real**, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

3.3.4 Nivel 4. Nivel de Aplicación

Imagen de "ufo_web_factory" con licencia Creative Commons dominio público, obtenida de http://www.openclipart.org/detail/16603/world-wide-web-by-ufo_web_factory

El **nivel aplicación contiene los programas de usuario (aplicaciones)** que hace que nuestro ordenador pueda crear textos, chatear, leer correo, visitar páginas web, etc. En este nivel se incluyen todos los protocolos de alto nivel que utilizan los programas o servicios para comunicarse.

Algunos de los protocolos de la capa de aplicación son:

- **HTTP**: Protocolo de transferencia de hipertexto, es el protocolo utilizado en las **páginas web**. De ahí que una página web, siempre se pone previamente **http://** que significa que se está utilizando el protocolo **http**[8]. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Tiene una **versión segura que es el HTTPS**.
- **FTP**: Protocolo utilizado en la **transferencia de ficheros** entre un ordenador y otro.
- **DNS**: **Servicio de nombres de dominio**[9], es el sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones de red. Gracias a este servicio, al navegar por páginas web se utilizan nombres del dominio (ejemplo, **www.mipagina.es**) en vez de direcciones IP, más difíciles de memorizar.
- **SMTP y POP**: Protocolos **para el correo electrónico**. **SMTP**[10] es el protocolo simple de trasferencia de correo, basado en texto y utilizado **para el envío de mensajes** de correo. **POP**[11] es el protocolo de oficina de correo, y se utiliza en los clientes de correo **para obtener los mensajes de correo almacenados** en un servidor.
- **SNMP**: Protocolo de administración de redes, permite monitorizar y controlar los dispositivos de red y de administrar configuraciones y seguridad.

---

[8] **Http**. Hypertext Transfer Protocol, en español, Protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción de la World Wide Web (WWW). HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. El cliente efectúa la petición al servidor web por medio de un navegador, de un recurso que viene identificado por un localizador uniforme de recursos (URL). Los recursos pueden ser archivos html, imágenes, multimedia, una consulta a una base de datos, la ejecución de un script, etc. El número de puerto utilizado es el 80.

[9] **Dominio**. Un dominio es un conjunto de equipos que forman parte de una misma red y comparten una base de datos de seguridad común que reside en servidores de dicha red (servidores controladores de dominio). Esta base de datos contiene también cuentas de usuario (que son del dominio, no cuentas locales) y que son gestionadas por el controlador del dominio. Esta estructura permite gestionar el acceso a los recursos de los servidores de la red (almacenamiento, impresoras de red) y establecer directivas de seguridad centralizadas.

[10] **SMTP**. Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo, es un protocolo de red para el intercambio de mensajes de correo electrónico entre ordenadores u otros dispositivos (PDA's, teléfonos móviles, etc.). Utiliza normalmente el puerto 25.

[11] **POP** (Post Office Protocol). Protocolo para la recepción de correo electrónico.

Puerto y socket

A cada aplicación se le asigna una dirección de transporte, llamado **puerto**.

Por ejemplo la aplicación o protocolo HTTP utiliza el puerto 80. De esa forma, **en un servidor de páginas web, siempre está abierto o escuchando el puerto 80**, que significa que está esperando peticiones de páginas web por dicho puerto desde cualquier otro ordenador del mundo para atenderla.

El concepto de puerto es similar, a decir que en una casa existan varias puertas (principal, jardín, lateral). Cada servicio utiliza distintos puertos.

- HTTP utiliza el puerto 80, mientras que HTTPS utiliza el puerto 443.
- El servicio FTP utiliza los puertos 20 y 21.
- El servicio DNS utiliza el puerto 53.

Un socket es una conexión única, que está formada por la unión de la dirección IP más el puerto. Si en un navegador web escribimos http://www.empresa.es , y supongamos que el servidor web que atiende http://www.empresa.es corresponde a la dirección IP 192.168.1.11, es equivalente a escribir en el navegador 192.168.1.11:80

Se profundizará en estos conceptos y servicios, configurando algunos de ellos en las unidades 9 y 10.

3.4 Versiones de Ethernet. Estándar IEEE 802.3

En los siguientes libros se va a estudiar cómo se conectan los ordenadores en la red (topología de red) y qué dispositivos físicos se utilizan para su conexión.

Antes de ello, se dedica este apartado para el estándar IEEE 802.3 que regulas las redes cableadas, llamadas redes Ehternet.

Desde los años 80, se han estandarizado muchas versiones, para ver las distintas versiones visitar https://es.wikipedia.org/wiki/IEEE_802.3

Aquí, simplemente se va a reseñar las velocidades alcanzadas más importantes y los nombres denominados comercialmente.

- Ethernet: velocidad de 10 Megabit/seg
- Fast-Ethernet: velocidad de 100 Megabit/seg
- Gigabit-Ethernet: velocidad de 1 Gigabit/seg
- 10 Gigabit-Ethernet: velocidad de 10 Gigabit/seg

En las redes locales, las velocidades más habituales en la actualidad son Fast-Ethernet y Gigabit-Ethernet. Las instalaciones nuevas se realizan con Gigabit. Cuando incorporemos un ordenador a nuestra red, tendremos que tener en cuenta que la tarjeta sea compatible con la velocidad de nuestra LAN. Igualmente hay cableado con distintas categorías, con velocidades máximas admitidas.

Las distintas versiones IEEE 802.3 especifican que componentes se deben utilizan para esa versión.

4. Topologías de red y modos de conexión

4.1 Topologías de red

La **topología de red desde el punto de vista físico**, se considera la forma en que se conectan los ordenadores de una red. Las topologías de conexión principales son **bus, anillo y estrella**.

Cuando se hace una instalación de red se realiza un esquema de red donde se muestre la ubicación de cada ordenador, cada equipo de interconexión y el cableado utilizado. Se realiza utilizando los planos del edificio y es una herramienta útil a la hora del mantenimiento y actualización.

La **topología desde el punto de vista lógico** o esquema lógico, nos muestra el uso de la red, el nombre de los ordenadores, las direcciones, las aplicaciones, etc. Como ejemplo en la figura siguiente se muestra un esquema lógico de una red de ordenadores que tendrá conexión a Internet gracias a un router[12]. La red se representa con un óvalo donde dentro tiene la dirección de red y fuera el nombre de la red.

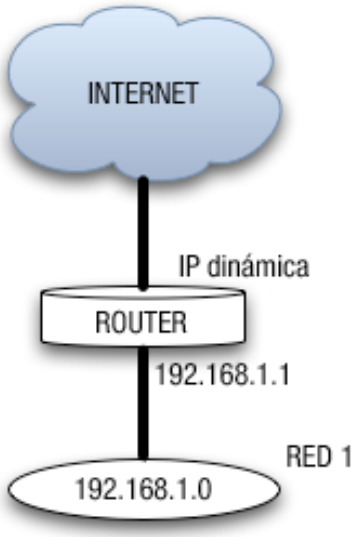


Imagen obtenida de materiales originales de FP a Distancia

En las redes wifi[13] o inalámbricas, se habla de **modo de conexión**. Se definen dos modos de **conexión inalámbrica**, que son **modo infraestructura** (se necesita punto de acceso[14]) y **modo ad-hoc**[15] (no necesita punto de acceso).

---

[12] **Router**. Dispositivo hardware o software que permite comunicar varias redes.

[13] **Wifi**. Es un sistema de radio para la conexión de dispositivos electrónicos de forma inalámbrica.

Se comienza el apartado con las topologías desde el punto de vista físico: bus, anillo y estrella.

4.1.1 Topología en bus

La topología en bus utiliza **un único cable troncal con terminaciones en los extremos**, de tal forma que los ordenadores de la red se conectan directamente a la red troncal. Las primeras redes Ethernet utilizaban está topología usando cable coaxial (igual que el cable de televisión).

Actualmente se emplean variantes de la topología en bus en las redes de televisión por cable y en equipamientos industriales.

Se dejó de utilizar por su poca flexibilidad ante fallos. Al observar la figura es fácil darse cuenta de que la rotura de un punto de la red, deja toda la red inutilizable.

Imagen de "Lmbuga" con licencia Domino público, obtenida de
http://meta.wikimedia.org/wiki/File:Topolox%C3%ADa_en_bus.png

4.1.2 Topología en anillo

La topología en anillo **conecta cada ordenador o nodo con el siguiente y el último con el primero**, creando un anillo físico de conexión. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación. En este tipo de red la comunicación se da por el paso de un testigo, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. Las redes locales Token-ring emplean una topología en anillo aunque la conexión física sea en estrella.

---

[14] **Punto de acceso**. Dispositivo que permite crear una red inalámbrica e interconectarla con una red cableada.

[15] **Ad-hoc**. Del latín, para esto, en redes inalámbrica se suele utilizar para nombrar las conexiones que se realizan para un propósito específico.

Lo habitual, es que **los datos se envíen en ambas direcciones, creando redundancia y tolerancia a fallos** (pues al contrario que en la topología en bus, con un único punto de ruptura la red sigue operativa).

Esta topología **se utiliza actualmente en las redes FDDI** (Fiber Distributed Data Interface, Interfaz[16] de datos distribuidos por fibra) como parte de una **red troncal** que distribuye datos por **fibra óptica**.

Imagen de "Lmbuga" con licencia Domino público, obtenida de
http://meta.wikimedia.org/wiki/File:Topolox%C3%ADa_en_anel.png

4.1.3 Topología en estrella

La topología en estrella conecta **todos los ordenadores a un nodo central,** llamado **equipo de interconexión**, que puede ser: un router[17], un conmutador o switch[18], o, un concentrador o hub. Las **redes de área local modernas** basadas en el **estándar IEEE 802.3 utilizan esta topología**.

El **equipo de interconexión** central canaliza toda la información y por el pasan todos los paquetes de usuarios, este nodo central realizará funciones de distribución, conmutación y control. Este equipo **debe estar siempre activo**, ya que si falla toda la red queda sin servicio.

Entre las ventajas de utilizar esta topología tenemos que **esta topología es tolerante a fallos** ya que la ruptura de un cable, solo deja inoperativo un nodo.

---

[16] **Interfaz**. Una interfaz hardware es una conexión física, entre dos aparatos o sistemas independientes, que funciona a través de un protocolo común a ambos. Existen diferentes interfaces estándares como el USB o el SATA, etc., definidas con unas especificaciones técnicas concretas, que deben ser comunes en todos los dispositivos con la misma interfaz, para que puedan conectarse y comunicarse entre ellos.

[17] **Router**. Dispositivo hardware o software que permite comunicar varias redes.

[18] **Switch**. Dispositivo que permite interconectar ordenadores de una misma red.

Además **facilita la incorporación de nuevos ordenadores** a la red siempre que el nodo central tenga conexiones libres.

Imagen de "Lmbuga" con licencia Domino público, obtenida de
http://meta.wikimedia.org/wiki/File:Topolox%C3%ADa_en_estrela.png

Lo habitual en un edificio es que se utilice una **estrella extendida o árbol**, donde las redes en estrella se conectan entre sí con switch (conmutadores).

Imagen de "Lmbuga" con licencia Domino público, obtenida de
http://meta.wikimedia.org/wiki/File:Topolox%C3%ADa_en_%C3%A1rbore.png

La estrella extendida habitualmente es una **estrella jerárquica** donde un nodo marca el inicio de la estructura. Es habitual que ese nodo inicial sea un router que sirve para la comunicación con el exterior con internet, y a partir de ese router se crea una red de área local que permite dar servicios a redes de área locales más pequeñas.

En la imagen se muestra un router, al que se conectan dos switch y 3 PC conectados a cada switch.

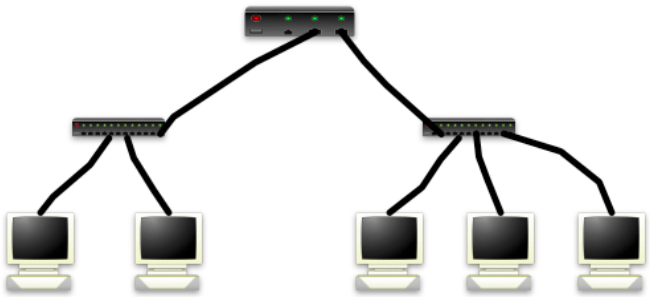


Imagen obtenida de materiales originales de FP a Distancia

Esta topología tiene la ventaja que a partir de una única conexión a Internet podemos dar servicio a varias redes o subredes locales, con lo que se ahorran costes.

Todos estos elementos se entenderán mejor en el próximo libro donse se estudian los elementos de interconexión.

4.2 Redes inalámbricas. Modo de conexión: infraestructura y ad-hoc.

En **redes inalámbricas o redes Wifi**, que siguen el **estándar IEEE 802.11,** se introduce un concepto diferente al de topología, que es el de **modo de conexión**. Se especifican dos modos de conexión, que son el **modo infraestructura y el modo ad-hoc**.

4.2.1 Modo infraestructura

El **modo infraestructura** se suele utilizar para conectar equipos inalámbricos a una red cableada ya existente, **se utiliza un equipo de interconexión como puente entre la red inalámbrica y la cableada**. Este equipo **se denomina Punto de Acceso** y puede ser un equipo especial que haga sólo esta función, o el mismo router (el que suele instalar la compañía de telecomunicaciones) que a su vez haga de punto de acceso.

En la imagen aparece un router, conectado al punto de acceso, donde tres portátiles se conectan a la red a través del punto de acceso.

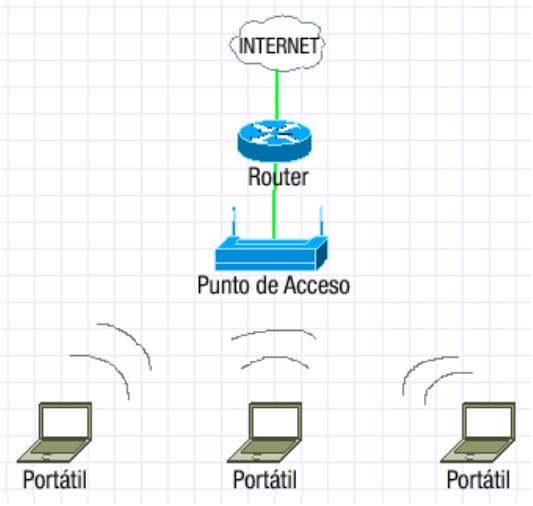


Imagen obtenida de materiales originales de FP a Distancia

4.2.2 Modo ad-hoc

El **modo ad-hoc permite conectar dispositivos inalámbricos** entre sí, **sin necesidad de utilizar ningún equipo como punto de acceso.** De esta forma cada dispositivo de la red forma parte de una red de igual a igual (Peer to Peer). Este tipo de conexión permite compartir información entre equipos de forma puntual y a poca velocidad, estando dirigidas para redes inalámbricas personales. Un ejemplo de modo ad-hoc son las conexiones a través de Bluetooth[19]. Más información sobre ad-hoc: http://redesad-hoc.blogspot.com/

En la imagen se ven tres equipos portátiles conectados entre ellos sin ningún elemento más.

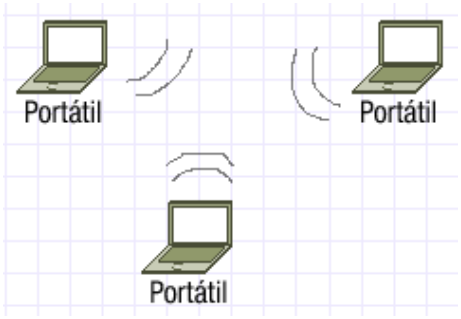


Imagen obtenida de materiales originales de FP a Distancia

[19] **Bluetooth**. Es un tipo de red inalámbrica de área personal, de pequeño alcance, con la que se puede transmitir voz y datos entre dispositivos de diferentes tipos. Permite crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales como teléfonos móviles, dispositivos de mano, ordenadores, impresoras, cámaras digitales, etc.

5. Componentes físicos de las redes informáticas.

5.1 Componentes. Medios de transmisión

Se puede considerar componentes de la red a los propios ordenadores con sus sistemas operativos y a todo el hardware y software que ayuda a que la red funcione. Este punto se va a centrar en los componentes hardware.

Algunos de estos componentes son:

- El **cableado de red y sus conectores**, que permite la transmisión de la señal.
- **El rack o armario de conexiones**, destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- Los patch panel, **paneles de parcheo** que sirven para organizar el cableado en el rack.
- Las **tarjetas de red**, que permiten la conexión física del ordenador, bien por cable o de forma inalámbrica.
- Los **conmutadores o switches**, que **permiten la conexión** de diferentes ordenadores entre sí y **de segmentos de la misma red** entre sí.
- Los **enrutadores o routers**, también conocidos como encaminadores, que **permiten conectar redes diferentes**, como por ejemplo una red de área local con Internet.
- Los **puntos de acceso**, que **permiten la interconexión de dispositivos inalámbricos** entre sí, y/o la conexión de dispositivos cableados con los inalámbricos.
- Los cortafuegos, que pueden ser dispositivos hardware con un software específico para bloquear accesos no autorizados a la red, o software específico que se instale en los servidores para evitar los accesos no autorizados.
- Los servidores, que no son más que ordenadores pero con software de servidor.
- Los **nodos de red**, donde se hace referencia a las estaciones de trabajo, que son los ordenadores que trabajarán en red, así como cualquier periférico conectado a un equipo o directamente a la red, por ejemplo impresoras o discos duros de red.

En la imagen se puede visualizar un armario de distribución donde se encuentran varios switches, routers, con conexiones de cables de par trenzado y paneles de parcheo.

Imagen obtenida de materiales originales de FP a Distancia

5.2 Clasificación de los medios de transmisión

El medio de transmisión en las redes de ordenadores serán los canales que transmiten la información entre los nodos de la red, **las transmisiones se realizan habitualmente empleando ondas electromagnéticas**. Las ondas electromagnéticas son susceptibles de ser transmitidas por el vacío. Por ese motivo podemos clasificar los medios de transmisión como:

- **Medios guiados**: conducen las ondas electromagnéticas a través de un camino físico. Entre los tipos de cables más utilizados encontramos el **par trenzado, el coaxial y la fibra óptica**.
- **Medios no guiados**: proporcionan un soporte para que las ondas se transmitan, pero no las dirigen. Las ondas se transmiten **a través del aire o del vacío**.

Se ven a continuación los distintos tipos de cables utilizados.

5.2.1 Cable coaxial

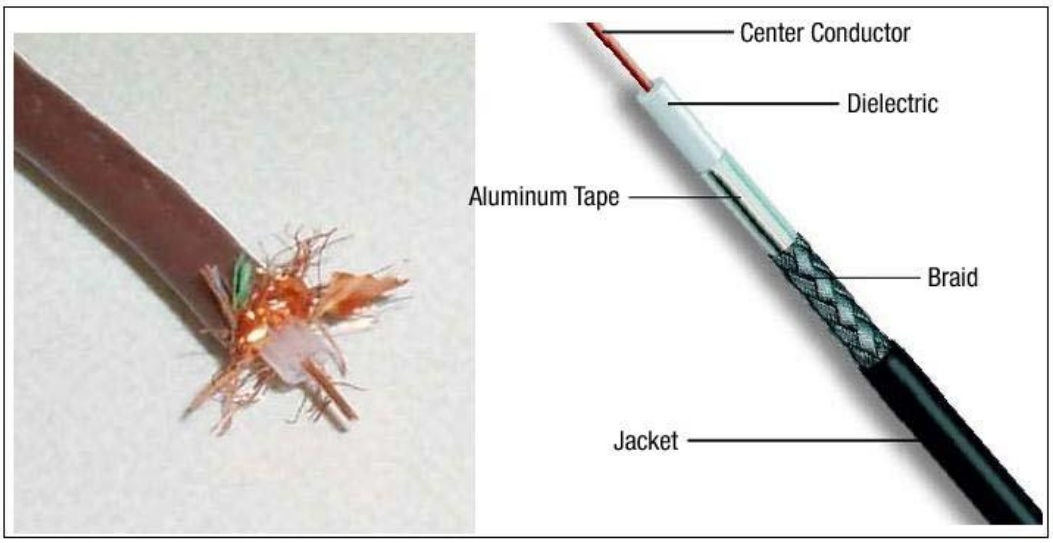


Imagen de "RONALD" con licencia Creative commons, atribución, igualmente compartido, obtenida de http://commons.wikimedia.org/wiki/File:CABLE_IX.JPG

El **cable coaxial**, está compuesto de un hilo conductor llamado núcleo y de un mallazo externo separados por un dieléctrico o aislante.

Los **conectores** que se suelen utilizar son el **BNC y el tipo N**. **Actualmente el cable coaxial no se utiliza para** montar redes de **ordenadores**, **si no** para la distribución de las señales de **televisión, internet por cable**, etc.

5.2.2 Cable de par trenzado

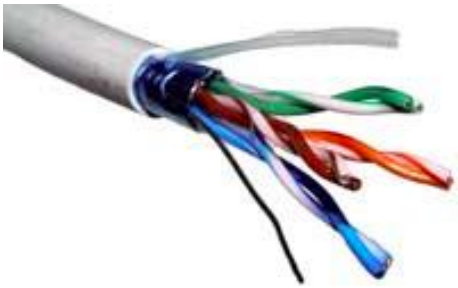


Imagen de "Baran Ivo" con licencia Dominio público, obtenida de http://es.wikipedia.org/wiki/Archivo:FTP_cable3.jpg

El **cable más utilizado** en redes de área local, es el **par trenzado de ocho hilos.** Consta de ocho hilos con colores diferentes y se utiliza en redes de ordenadores bajo el estándar IEEE 802.3 (Ethernet). Se dice par trenzado, porque van de 2 en 2 hilos trenzados.

Los colores son: blanco-naranja, naranja, blanco-verde, verde, blanco-azul, azul, blanco-marrón y marrón. Cuando se habla de color blanco-naranja se está hablando

de un hilo naranja, con una línea blanca pintada, de forma que el par de hilos trenzado lo forman el naranja con el blanco-naranja.

La distribución de estos colores cuando se conectan en el conector viene estandarizada, para que las conexiones de red sean fácilmente reconocibles.

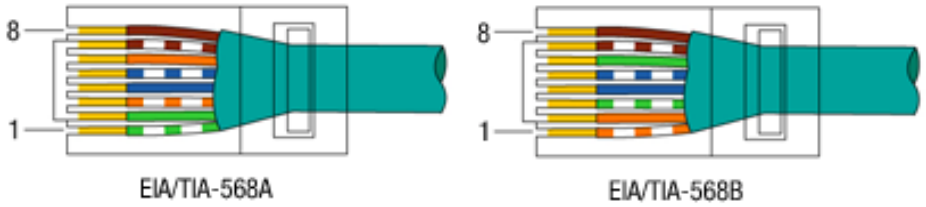
En el mercado se encuentran cables de par trenzado de distintas categorías. Para las redes actuales Ethernet se utilizan **cables de categoría 5, 5e, 6, 7**.

- Los de **categoría 5 admiten solo transferencias de 100 Megabit/seg. Válidos para redes Fast-Ethernet.**
- Los de **categoría 5e, 6 y 7 alcanzan ya los 1000 Megabit/seg = 1 Gigabit/seg. Obligatorio para redes Gigabit-Ethernet**

El **conector** que se utiliza con este cableado es el **RJ-45**. Para realizar el cable, se conectan 2 conectores RJ-45 machos a las puntas del cable con una herramienta específica, llamada crimpadora. Este cable una vez terminado, se podrá conectar a las conexiones hembras habituales en las tarjetas de red, router y switch.

Para la conexión de los 8 hilos al conector RJ-45 se realiza según los **estándares** ANSI/EIA/TIA **568 A y B**.

- En las conexiones de red usaremos **cables directos, que significa que los** dos **extremos utilizarán el mismo estándar**, se recomienda usar la 568B.
- En caso de querer hacer un **cable cruzado, se usará la norma 568A en un extremo y la norma 568B en el otro**.



Imágenes de "Lp" con licencia: Dominio público y obtenidas de http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568A_Left.png y http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568B_Left.png