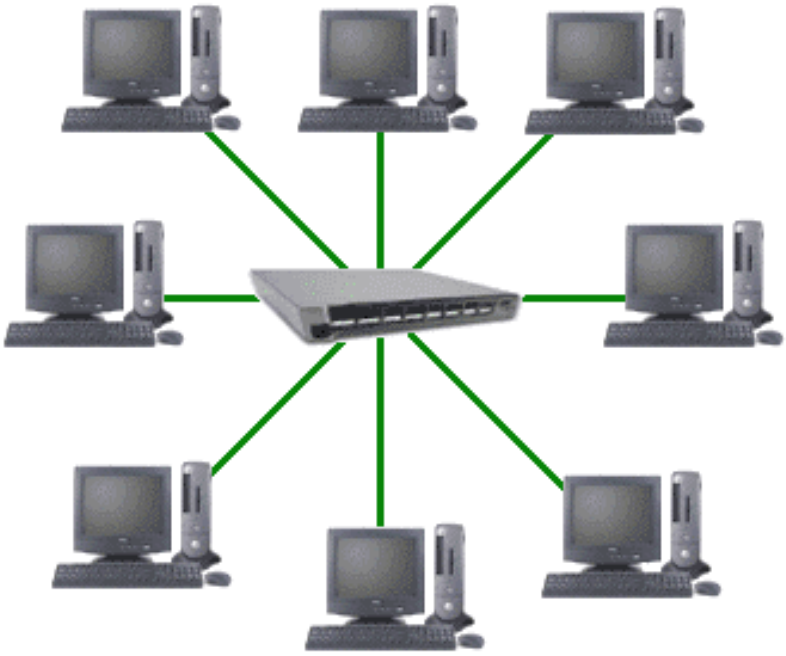
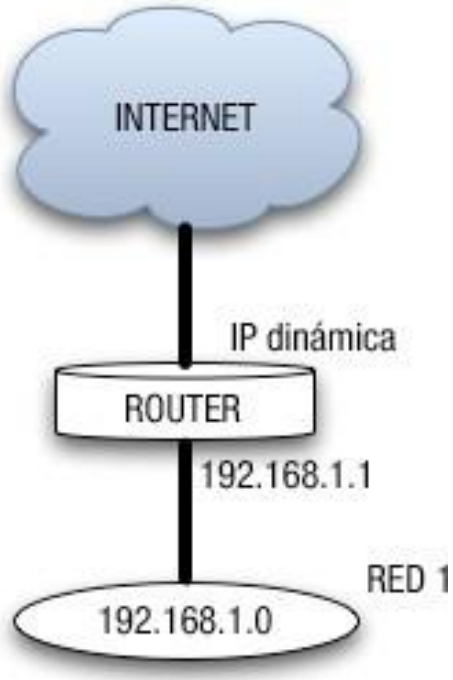
Introducción a los sistemas en red. Direccionamiento IP.





Víctor Villegas Borge

1.- Redes. Características y clasificación.

En esta unidad se van a estudiar los conceptos teóricos de redes con sus direcciones físicas (MAC) y direcciones lógicas (IP), elementos físicos de conexión y cálculos de direcciones IP.

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.

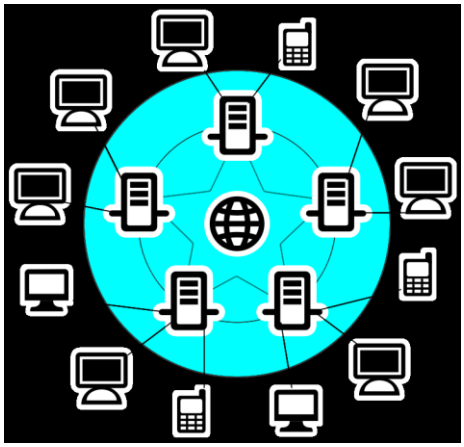
Redes de ordenadores. Ventajas.

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.

Clasificación de Redes. Tipos de redes.



Las redes se pueden clasificar según diferentes conceptos.

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.

Según las funciones de sus componentes:

- **Redes de igual a igual o ente 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.

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.

Según el grado de difusión:

- **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, 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.
- **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.

2.- Arquitectura de la red. Modelos OSI y TCP/IP.

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 importantes**:

- **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.

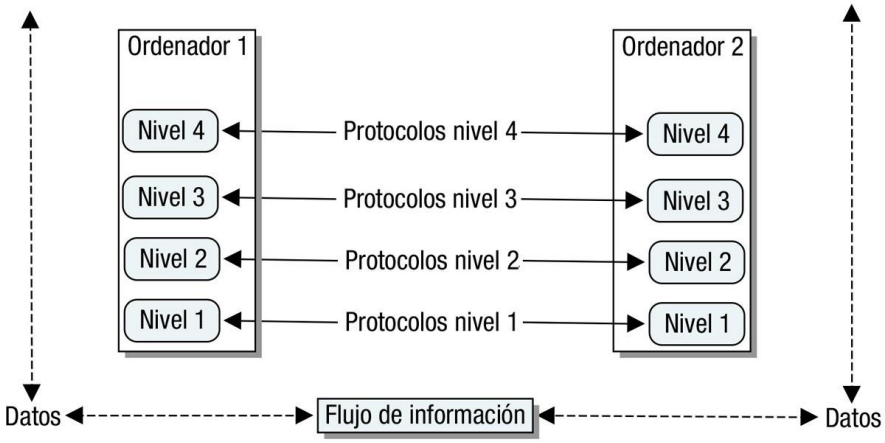
Protocolo de comunicación

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.

Modelos por capas o niveles



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.

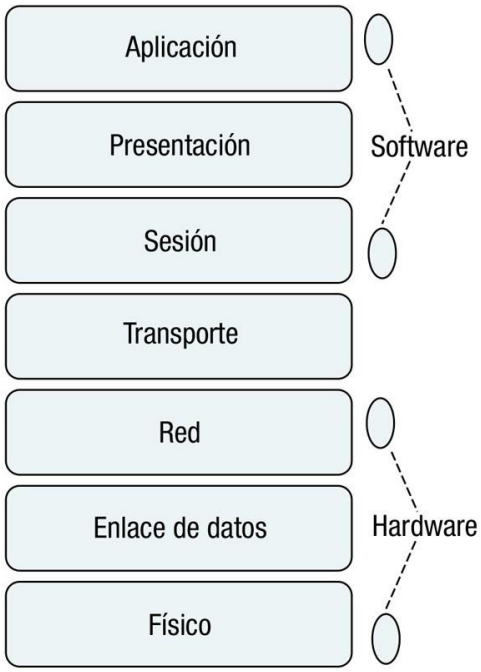
Las arquitecturas de red basadas en capas facilitan las compatibilidades, tanto de software como de hardware, pues no es necesario cambiar todas las capas cuando queremos mejorar el sistema. Bastaría modificar los protocolos afectados.

2.1.- 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.



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.

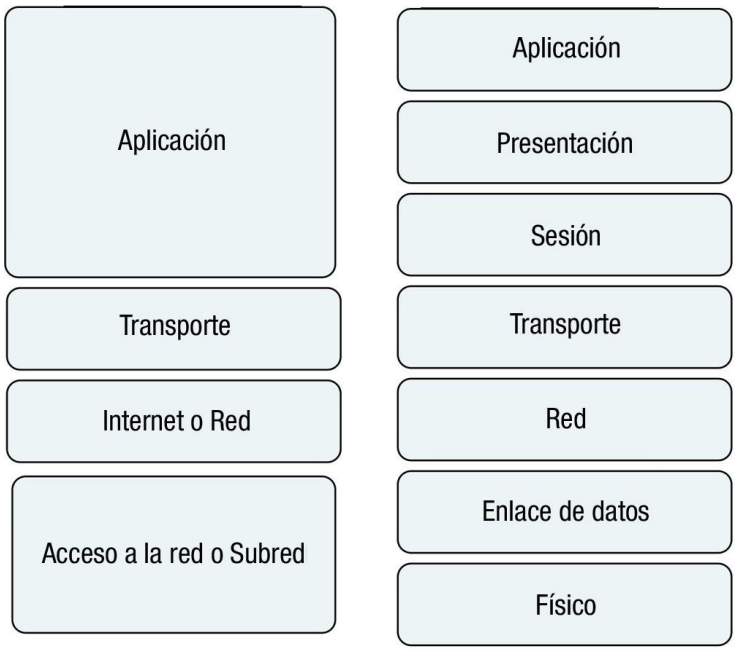
2.2.- Modelo TCP/IP.

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 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.



2.2.1.- 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.

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.

2.2.2.- 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.

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**.

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 y tracert lo utilizan** para poder funcionar.

2.2.3.- 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.

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.

2.2.4.- Nivel 4. Nivel de aplicación.

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. 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**, 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** es el protocolo simple de trasferencia de correo, basado en texto y utilizado **para el envío de mensajes** de correo. **POP** 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.

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

2.3.- Versiones de Ethernet. Estándar IEEE 802.3.

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

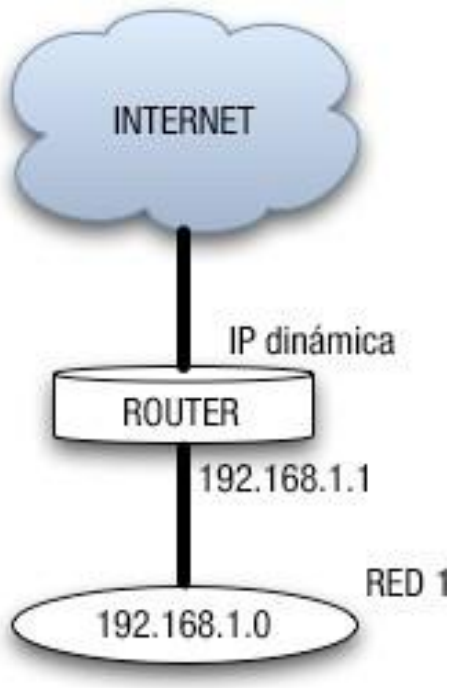
En las redes locales, las velocidades más habituales en la actualidad son Fast-Ethernet y Gigabit-Ethernet. Las instalaciones nuevas se realizan con Gigabit. Cuando incorporemos un ordenador a nuestra red, tendremos que tener en cuenta que la tarjeta sea compatible con la velocidad de nuestra LAN. Igualmente hay cableado con distintas categorías, con velocidades máximas admitidas.
Las distintas versiones IEEE 802.3 especifican que componentes se deben utilizan para esa versión.

3.- Topologías de red y modos de conexión.

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. La red se representa con un óvalo donde dentro tiene la dirección de red y fuera el nombre de la red.

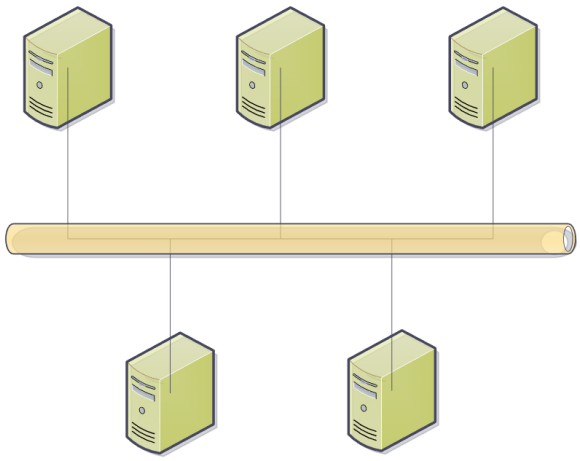


En las redes wifi o inalámbricas, se habla de **modo de conexión**. Se definen dos modos de **conexión inalámbrica**, que son **modo infraestructura** (se necesita punto de acceso) y **modo ad-hoc** (no necesita punto de acceso)
Se comienza el apartado con las topologías desde el punto de vista físico: bus, anillo y estrella.

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.

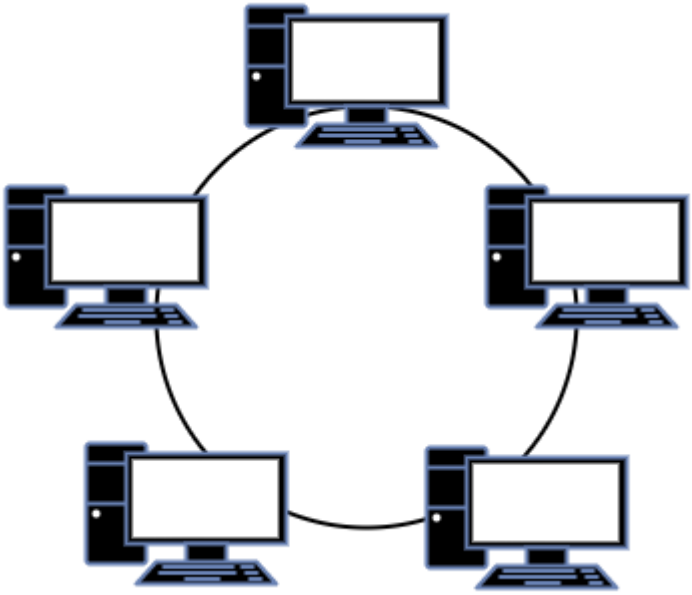


Topología en anillo

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.

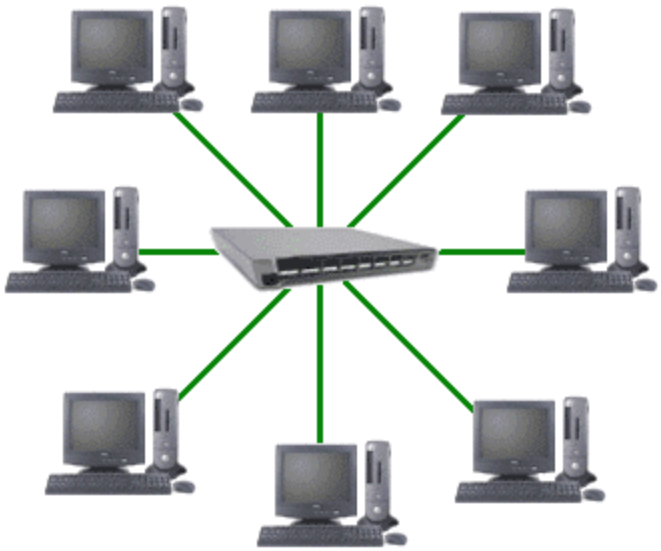
Lo habitual, es que **los datos se envíen en ambas direcciones, creando redundancia y tolerancia a fallos** (pues al contrario que en la topología en bus, con un único punto de ruptura la red sigue operativa)

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

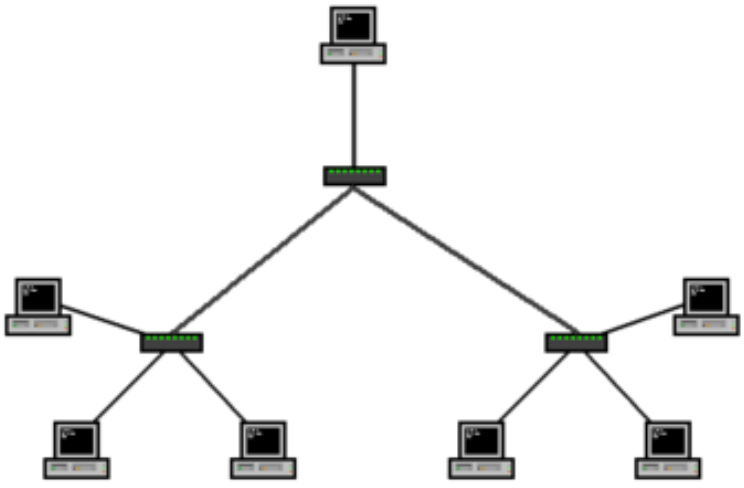


Topología en estrella

La topología en estrella conecta **todos los ordenadores a un nodo central,** llamado **equipo de interconexión**, que puede ser: un router, un conmutador o switch, 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. Además **facilita la incorporación de nuevos ordenadores** a la red siempre que el nodo central tenga conexiones libres.



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)



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.

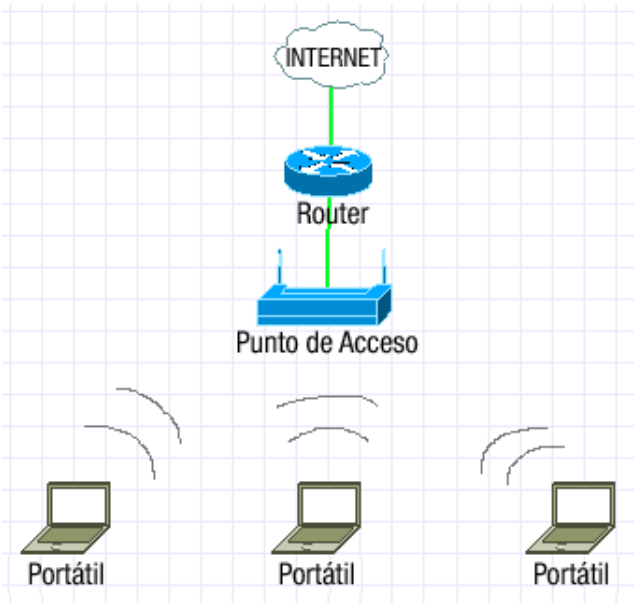
Esta topología tiene la ventaja que a partir de una única conexión a Internet podemos dar servicio a varias redes o subredes locales, con lo que se ahorran costes.

3.1.- 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**.

Modo infraestructura

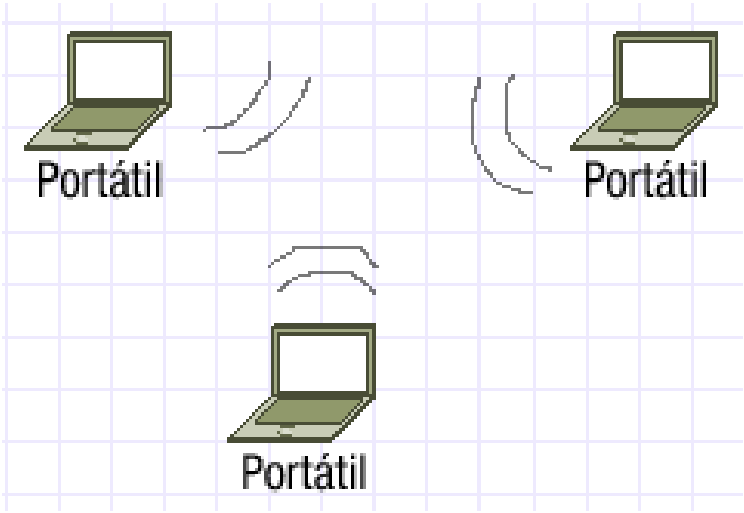
El **modo infraestructura** se suele utilizar para conectar equipos inalámbricos a una red cableada ya existente, **se utiliza un equipo de interconexión como puente entre la red inalámbrica y la cableada**. Este equipo **se denomina Punto de Acceso** y puede ser un equipoespecial que haga sólo esta 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.



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.

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


Portátil
Portátil
Portátil

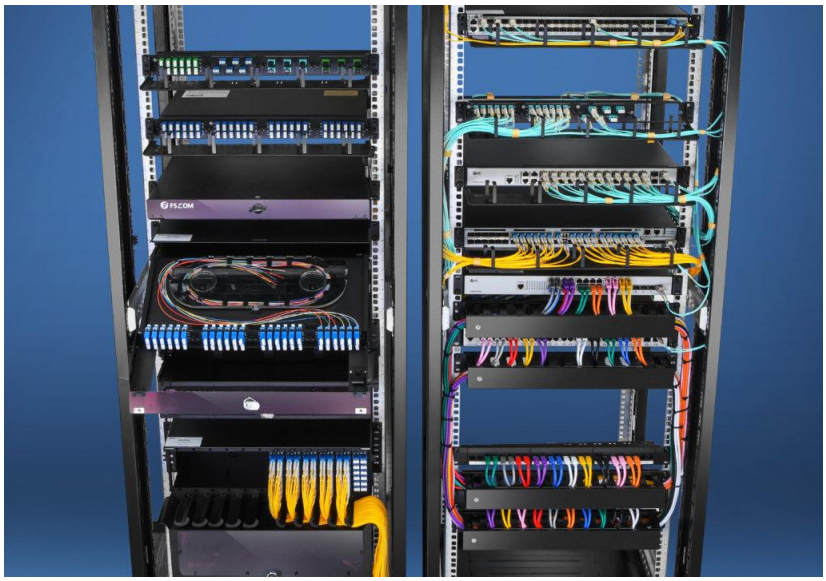
4.- Componentes físicos de las redes informáticas.

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 router**s, 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 variosswitches, routers, con conexiones de cables de par trenzado y paneles de parcheo.



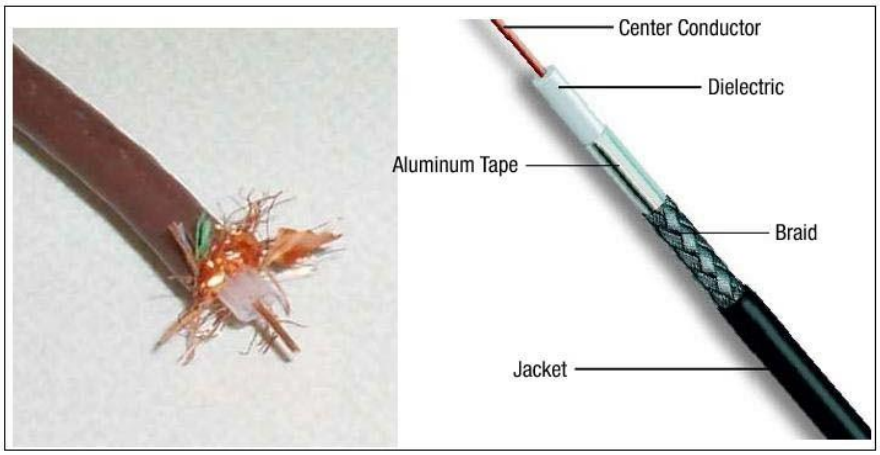
Clasificación de los medios de transmisión.

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 fibraóptica**.
- **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.

Cable coaxial



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.

Cable de par trenzado

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.

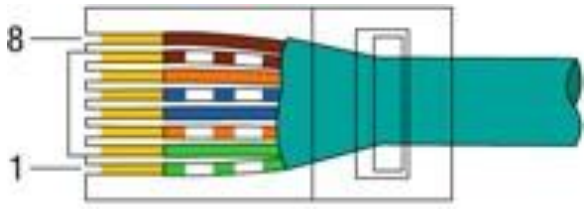
La distribución de estos colores cuando se conectan en el conector viene estandarizada, para que las conexiones de red sean fácilmente reconocibles.

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.**.

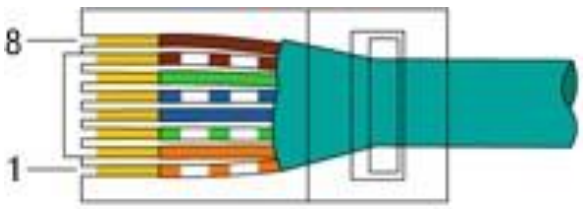
- Los de **categoría 5 admiten solo transferencias de 100 Megabit/seg. Válidos para redes Fast-Ethernet.**
- Los de **categoría 5e, 6 y 7 alcanzan ya los 1000 Megabit/seg = 1 Gigabit/seg. Obligatorio para redes Gigabit-Ethernet**

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**.



EIA/TIA-568A



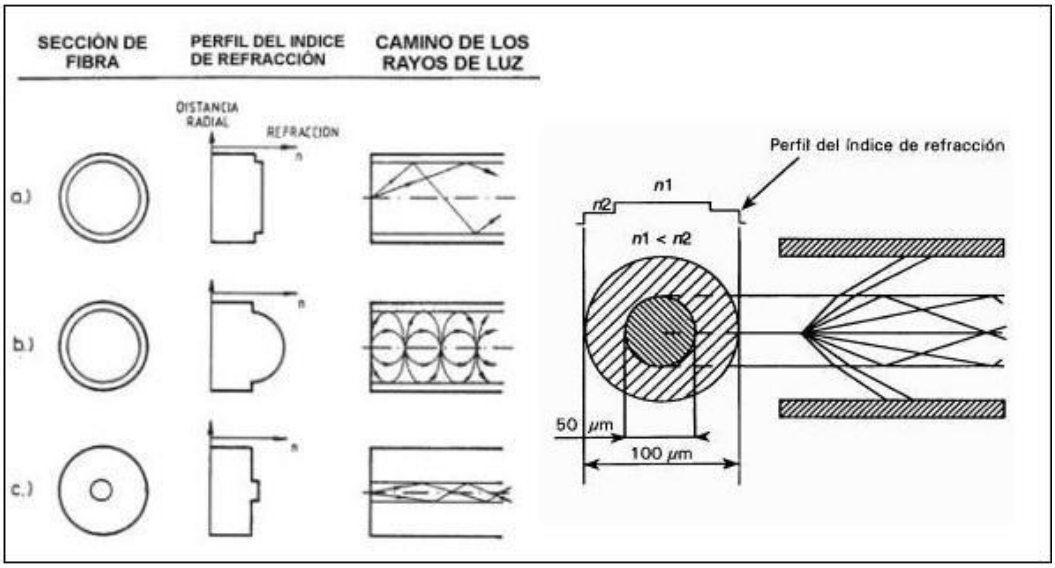
EIA/TIA-568B

Lo **habitual es utilizar cables directos**. Los **cables cruzados se usan para conectar dos**

equipos del mismo tipo (que no es lo habitual), por ejemplo, ordenador con ordenador, router con router. Al final del libro, una vez vistos los dispositivos de interconexión, se aclara cuando se utilizan cables directos y cables cruzados.
Tabla de estándar 568A y 568B:

Pin	568-A	568-B
1	Blanco-verde	Blanco-naranja
2	Verde	Naranja
3	Blanco-naranja	Blanco-verde
4	Azul	Azul
5	Blanco-azul	Blanco-azul
6	Naranja	Verde
7	Blanco-marrón	Blanco-marrón
8	Marrón	Marrón

Fibra óptica



La fibra óptica es **un hilo muy fino de material transparente, vidrio** o materiales plásticos, por el que se envían pulsos de luz. **La fuente de luz puede ser láser o un led** y es inmune a las interferencias electromagnéticas, por lo que es muy fiable. Además permite transmitir **gran**

cantidad de datos a una gran distancia y a una gran velocidad.
Existen dos tipos de fibra óptica, la multimodo y la monomodo. Los **conectores** que se utilizan son **FC y FDDI**.

Cableado estructurado

Se llama cableado estructurado a la infraestructura de telecomunicaciones necesaria para conectar un edificio o un conjunto de edificios. En esta infraestructura se incluyen cables, conducciones, regletas, armarios, dispositivos, espacios específicos, etc.

Elementos incluidos en el cableado estructurado son:

- Armarios de distribución, donde confluyen los cables y donde se montan los equipos de interconexión, utilizando rack y paneles de parcheo.
- Cableado horizontal, el cableado de planta.
- Cableado troncal o vertical de distribución entre plantas.
- Sala de equipamiento, sala donde se distribuyen todas las conexiones del edificio, para los distintos armarios de distribución.
- Entrada del edificio, por donde se conectan los cables exteriores con los interiores.
- Cableado de interconexión de edificios.

Los estándares de cableado estructurado especifican cómo organizar la instalación del cableado, tipo de cable, conectores, longitudes máximas de los tramos, etc. Por ejemplo, en el cableado horizontal se recomienda un máximo de 100 metros desde el armario de distribución o rack hasta el área de trabajo

4.1.- Elementos de interconexión.

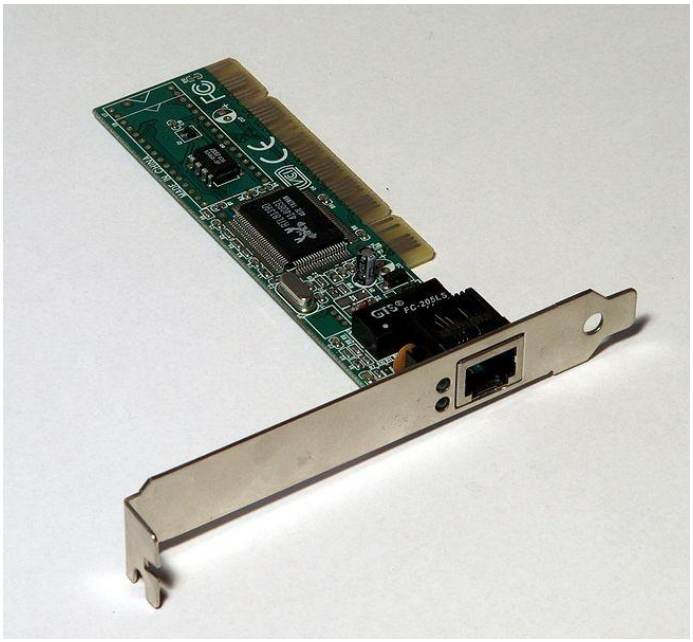
Los elementos de interconexión se refieren a los equipos que permiten conectar equipos en una red local o red extensa. Una forma de clasificar a los equipos de interconexión es teniendo en cuenta el nivel en el que trabajan tomando como referencia el modelo OSI.

- En el **nivel 1 o nivel físico** tenemos:
  Tarjetas de red: cableadas o inalámbricas. Permiten conectar los equipos a la red.
  Concentradores o hubs: Son un dispositivo que permiten conectar varios ordenadores, pero lo realiza de forma no inteligente, pues envía la información a todos los ordenadores, sin regular el tráfico. Como analogía, es como si un cartero no supiera localizar a un destinatario, y enviara una copia de la carta a todo el mundo, siendo labor del destinatario, ver si esa carta era para él o no.
  La mayor eficiencia de los switches y su bajo coste, ha hecho desaparecer la venta de hubs.
  Repetidores: pueden ser locales o remotos, y su función es repetir la señal para regenerarla y/o amplificarla.
- En el **nivel 2 o nivel de enlace de datos** tenemos:
  Conmutadores o switches: Son un dispositivo que permiten conectar varios ordenadores, pero de forma inteligente (al contrario que un hub), ya que sólo se envía la información al ordenador que la necesita. De esta forma el tráfico es mucho más rápido que con un hub. También se dice que conectan segmentos y ordenadores de la misma red.
  Puentes o bridges: conectan subredes, transmitiendo de una a otra el tráfico generado no local.
  Puntos de acceso: se encargan de conectar elementos inalámbricos entre sí, y de permitir el acceso de dispositivos inalámbricos a redes cableadas.
- En el **nivel 3 o nivel de red**:
  Enrutadores o routers: se encargan de **conectar redes diferentes**. Su principal uso está en la conexión a Internet, ya que permite que redes de área local puedan conectarse a Internet. Como une redes diferentes, necesita al menos dos direcciones IP, una para cada red. Por ejemplo, los **router que nos ofrecen las compañías telefónicas, trabajan con dos IP**, **una** de ellas está **en la red del operador telefónico, que llamamos** nuestra **IP externa**, porque es la dirección con la que nos ven desde fuera, **y la otra está en la red interna** en nuestras casas, **llamada IP interna.**
- En los **niveles superiores**:
  Pasarelas: suele denominarse pasarelas a los **equipos de interconexión que trabajan en los niveles superiores del modelo OSI.** Existen **diferentes tipos** de pasarelas, podemos tener las que se encargan de **conectar redes con tecnologías diferentes**, las que facilitan el control de acceso a una red, la que controlan los acceso no autorizados. Según su función pueden también ser **servidores**, **cortafuegos**, etc.

Se va a profundizar en los elementos más utilizados: tarjeta de red, switch y router.

2.1. Tarjetas de red y direccionamiento MAC

Una tarjeta de red o adaptador de red **trabaja en nivel 1 de OSI o nivel físico**. A las tarjetas de red también se les llama NIC (Network interface card, “Tarjeta de interfaz de red”)
La función principal de una tarjeta de red es la de permitir la conexión del ordenador a la red. Todas las tarjetas de red tienen la **dirección MAC** compuesta de **48 bits o 12 cifras hexadecimales** y se le conoce como **dirección física** y **es única** en el mundo.



Las tarjetas de red pueden conectarse al equipo utilizando alguna ranura de expansión como el PCI-Express, utilizando el USB o estar integradas en la placa base.

Las tarjetas de red tienen una velocidad de transferencia máxima, siendo las actuales de 100 Megabit/seg (Fast Ethernet) o 1000 Megabit /seg = 1Gigabit /seg (Gigabit-ethEthernet) Estas velocidades coinciden con las velocidades de los cables de par trenzado de categoría 5 y categoría 5e respectivamente.

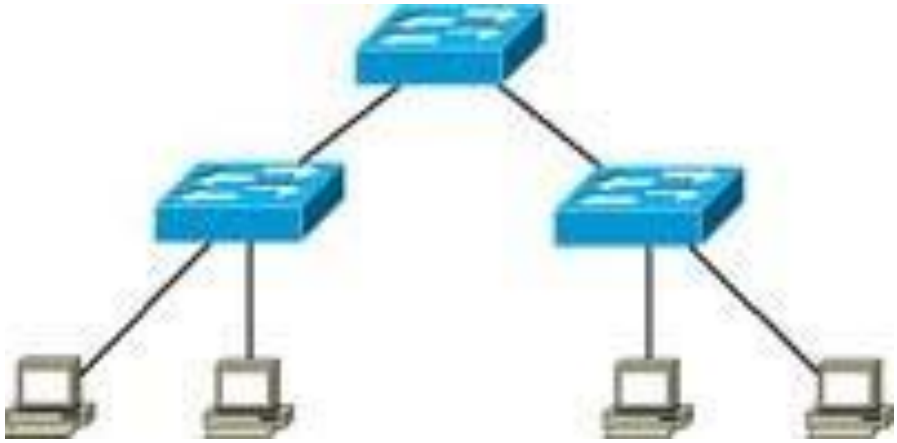
La instalación y configuración de la tarjeta dependerá del sistema operativo, pero en general, necesitaremos que tenga configurada una dirección IP, una máscara de red y una puerta de enlace. Estos conceptos se estudiarán en los últimos libros de esta unidad.

2.2. Conmutadores o switches

El conmutador o switch es un elemento de interconexión que **trabaja en capa 2** o nivel de enlace de datos, **permite conectar dos o más segmentos de red**. El conmutador nos permite conectar

diferentes ordenadores para que puedan conectarse entre sí, y que éstos tengan acceso a otros segmentos de red.
El conmutador funciona almacenando las direcciones MAC de los ordenadores que están conectados a él y de los dispositivos que se encuentran en cada segmento. Gracias a ello **es capaz de conectar un ordenador con otro de forma eficiente, sin necesidad de enviar la información a toda la red** (al contrario que el hub, justo por eso el hub es de nivel 1, mientras que el switch es de nivel 2)
Esta característica es la que hace que el switch sea el elemento principal de interconexión en las redes de área local con topología en estrella.

En la imagen, se puede ver un switch central, al que se conectan otros 2 switch, y a cada uno de ellos dos equipos.



Existen algunos conmutadores o switch que permiten definir redes de área local virtuales o VLAN. Las VLAN son redes lógicamente independientes dentro de una misma red física.

2.3. Enrutadores o routers

El enrutador o router **trabaja en la capa 3**, capa de red del modelo OSI. Es el equipo de interconexión que **se encarga de conectar dos o más redes diferentes**. En la imagen se ve el icono con el que se representa un router.

Los routers dirigen el tráfico de red, buscando el mejor camino para llegar al destino.

Cada interfaz del router se conectará a una red diferente. Necesitan una **configuración inicial, para guardar la dirección IP de cada interfaz o puerto, y su máscara de red.** También se pueden configurar servidores DNS y si se admiten direcciones IP dinámicas (protocolo DHCP). Todos estos aspectos se verán con más profundidad en próximos libros y unidades 9 y 10.

La mayor parte de las veces utilizaremos un router para conectarnos a Internet, ya sea por ADSL o por cable. En los domicilios particulares los routers suelen venir configurados por los proveedores de servicios de Internet.

Para realizar sus funciones un router guarda información de las redes a las que puede acceder, esto lo hace a través de la tabla de enrutamiento, que no es más que una tabla donde se guarda cómo se llega de una red a otra y que servicios se permiten.

En este apartado es importante **diferenciar un router profesional,** por ejemplo **de** la marca Cisco, a **los router que facilitan los operadores telefónicos**.

Un router profesional, si tiene 10 tomas RJ45 es para unir 10 redes diferentes.

Los routers que tenemos en las casas, facilitados por los **operadores telefónicos sólo pueden unir dos redes:** La red externa, por la que estamos conectados a Internet (la toma de teléfono o fibra óptica) y la red interna. Para la red interna, suele tener conexión inalámbrica y **varios puertos RJ45**; en este tipo de routers, estos puertos RJ45 **son un switch**, pues todos los equipos que se conecten a ellos, están en la red interna (unen nodos de la misma red, pero no de redes distintas). Además, **si** el router **es inalámbrico, también realiza la función de punto de acceso**. Por tanto, **estos routers son básicos, pero sin embargo es un dispositivo de varias capas OSI a la vez: la 3 o capa de red (router), la 2 o capa de enlace (switch) y la 1 ocapa física (punto de acceso).**

Cable directo o cable cruzado entre equipos de interconexión

En anterior libro se ha hablado de cable directo y cable cruzado. Lo habitual es realizarconexiones entre dispositivos de un nivel y otro de nivel inmediato. Por ejemplo, los ordenadorescon sus tarjetas de red (nivel 1) se unen con los switch (nivel 2) que a su vez se unen con el router (nivel 3). En estos casos se utiliza un cable directo.

¿Cuándo se utiliza un cable cruzado?, entre dispositivos del mismo nivel, o cuando hay 2 niveles de diferencia, por ejemplo si se conectan dos ordenadores directamente, la conexión se realiza con un cable cruzado entre ambas tarjetas de red (dos dispositivos de nivel 1). O si se conecta un ordenador (nivel 1) a un router (nivel 3) directamente, por habernos saltado un nivel.

Este concepto es teórico, pues los dispositivos en venta hoy día, suelen tener la inteligencia necesaria para que si no funciona de una forma determinar automáticamente si se ha conectado con el cable equivocado.

5.- Redes inalámbricas.

Las redes inalámbricas WLAN (Wifi Lan) **basan su funcionamiento en el estándar IEEE 802.11.** El funcionamiento de una red Wi-Fi es similar al funcionamiento de una red de área local cableada, ya que el estándar define el formato de trama ligeramente diferente al de las redes cableadas, uso de la MAC, la forma de acceder al medio, etc.

Las **redes ad-hoc permiten conectarse entre sí, pero a velocidades bajas y con una seguridad mínima. El modo infraestructura**, donde se utiliza un punto de acceso para que actúe como canalizador de todas las conexiones **mejora la velocidad y la seguridad**.
Es usual que **el punto de acceso se conecte a una red de área local a través de un cable**, con la idea de poder dar acceso a Internet. O que, tal como se acaba de comentar en anterior apartado **el router incorpore un punto de acceso Wifi.**

Algunas ventajas de las redes Wi-Fi son:

- Movilidad: se pueden conectar dispositivos estáticos y móviles.
- Escalabilidad: fáciles de ampliar.
- Flexibilidad: se puede conseguir un alto grado de conectividad.
- Menor tiempo de instalación: instalando un punto de acceso se consigue conectividad rápida.

Las mayores desventajas son:

- La seguridad: es difícil conseguir un alto grado de seguridad.
- Interferencias: al trabajar en rangos de frecuencias compartidos por otros dispositivos se pueden tener muchas interferencias.

1. Tipos de redes 802.11. Características.

El **estándar IEEE 802.11** define diferentes **versiones**:

- **IEEE 802.11a**: opera en la **banda de 5 Ghz** con una **velocidad máxima de 54 Mbps.**
- **IEEE 802.11b**: opera en la **banda de 2,4 Ghz** con una **velocidad máxima de 11 Mbps.** No puede interoperar con equipos del estándar 802.11ª por operar en otra banda.
- **IEEE 802.11g**: opera en la **banda de 2,4 Ghz** por lo que es compatible con la versión b, pero ofrece las mismas tasas de transferencia que la versión a, por tanto puede alcanzar una **velocidad máxima de 54 Mbps.** Hay que resaltar que aunque la versión b y la g son compatibles se recomienda usar versión g, ya que si un dispositivo versión b se conecta a punto de acceso g, baja la velocidad de toda el área de cobertura, perjudicando a los otros dispositivos.
- **IEEE 802.11n**: **opera simultáneamente en las bandas de 5 Ghz y en la de 2,4 Ghz**, gracias a esto la versión n es compatible con las otras versiones. Además es útil que trabaje en la banda de 5 Ghz ya que está menos congestionada y sufre menos interferencias de otros dispositivos. **Tiene una velocidad máxima de 600 Mbps.** Al igual que la versión g si los dispositivos que se conectan son de versiones anteriores, las velocidades y coberturas bajan.
- **IEEE 802.11ac**: opera en la **banda de 5 Ghz** con una **velocidad máxima de 1,3 Gbps,** doblando la velocidad del estándar IEEE 802.11n.

Es importante reseñar que las velocidades aquí indicadas son máximas, pero las velocidades reales obtenidas son bastante menores, por lo que las **versiones más utilizadas en la actualidad son las versiones g, n y ac** por sus altas velocidades.

Asimismo, indicar que la **banda de 5Ghz incorpora mayor calidad**, pues tiene menor ruido por

no interferir con otras tecnologías. **Pero tiene menor alcance (un 10%) y es más sensible a**

los muros de los edificios. Esto se ha corregido en los router ac inalámbricos que alcanzan mayores distancias.

2. El SSID de una red 802.11.

El SSID (Identificador de conjunto de servicio) **es una cadena alfanumérica de 32 caracteres de longitud, donde se distinguen las mayúsculas de las minúsculas, y sirve para identificar a la red.** Cuando alguien se conecta con un móvil a una red WiFi, tiene queseleccionar a que red se conecta, los nombres que aparecen son los SSID de las distintas redesWLAN.
Es necesario que todos los dispositivos inalámbricos de la misma red se configuren con el mismo SSID.
En una red tipo infraestructura el SSID se configura en el punto de acceso (en el router si es inalámbrico). Si la red es tipo ad-hoc el SSID se configura en cada ordenador.
Cada punto de acceso que su área de cobertura se solape con el área de un punto de acceso cercano deberá utilizar canales diferentes, que en el caso del estándar IEEE 802.11b/g, implica utilizar canales con una diferencia de 5.

Si el punto de acceso no consigue la cobertura necesaria, se pueden conectar varios puntos de acceso entre sí, preferiblemente con cable. Cada punto de acceso utilizará un canal diferente, pero el SSID será el mismo.

3.- Seguridad en 802.11.

Las redes WiFi son muy vulnerables a la interceptación de paquetes y a usuarios no autorizados que aprovechen la conexión, por tanto es conveniente implementar medidas de seguridad que prevengan un uso indebido de la red.

3.1. Tipos de cifrado

Las medidas habituales son **encriptar o codificar la información de la red.** Para ello se usan distintos **tipos de cifrado**:

- **WEP** (Privacidad equivalente a cableado): es un método débil pues es fácilmente descifrable, por lo que es recomendable utilizarlo.
- **WPA** (Acceso Wi-Fi protegido): se considera un método relativamente seguro por su cifrado.
- **WPA2**: versión WPA mejorada. Se recomienda utilizar WPA2 con el algoritmo AES. Esta es la versión más segura hoy día.

3.2. Ocultar SSID

Una medida que no proporciona ningún tipo de seguridad, pero dificulta a los clientes el conectarse, es **ocultar el SSID**. Desde los puntos de acceso se difunde el SSID, si esa función se desactiva los ordenadores deben configurar manualmente el SSID. Esto es fácilmente salvable ya que existen herramientas que detectan el SSID oculto, pero es un primer paso.

3.3. Deshabilitar WPS

Para la seguridad inalámbrica, es importante hablar de WPS (WiFi Protected Setup, Instalación a Wifi protegida) que trata de la posibilidad de conectar dispositivos a la red inalámbrica sin utilizar contraseña. Esta utilidad incluida en muchos router inalámbricos, facilitan la conexión de distintos dispositivos, pero a cambio se compromete la seguridad de la conexión, por lo que si queremos tener una red segura es conveniente deshabilitar WPS en el router inalámbrico o punto de acceso.

3.4. Filtrado de direcciones MAC

El **filtrado de direcciones MAC** es una buena medida de seguridad adicional y se recomienda utilizarla como complemento de algunos de los métodos de encriptación**. Consiste en configurar el punto de acceso o router de tal forma que tenga un listado de direcciones MAC de los equipos autorizados a conectarse** a la red inalámbrica, para que aquellos equiposque no estén en la lista no puedan conectarse.
En el ejemplo de una casa, se trataría de averiguar las direcciones MAC de todos los ordenadores, móviles, impresora de red, Smart-tv y configurar en el router inalámbrico la lista dedirecciones MAC permitidas.
Filtrar por direcciones MAC es una buena medida de seguridad.

6.- Sistema binario. Conversión decimal - binario.

Sistema binario. El bit y el byte.

Sistema binario

En el libro siguiente se van a estudiar las direcciones lógicas de una red, es decir las direcciones IP. Para entender sus cálculos es necesario conocer el binario. De ahí, que este libro se va a utilizar para aprender binario y su conversión de binario a decimal y viceversa.
En nuestro lenguaje utilizamos cifras y letras. En los números utilizamos el **sistema decimal**, llamado así porque **utiliza 10 cifras distintas: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9**.
El **sistema binario utiliza dos cifras distintas: 0. 1**. Un número binario puede ser 101110 pero no 101120 porque el dígito 2 no es admitido.
Los ordenadores sólo utilizan 0 y 1, por lo que utilizan el sistema binario.
Notación: Como el número 101110 existe tanto en binario como en decimal, se hace necesario cuando estamos utilizando distintos sistemas utilizar una notación, de forma que anotaremos con un subíndice el sistema que estamos utilizando. Para **binario** utilizamos **101110_2** y si fuera decimal 101110_{10}

Bit y byte

El bit es un número binario con una única cifra. De forma que con **un bit** solo se puede escribir **0** o **1** y **se anota por b. Hay 2^1 = 2 números distintos (del 0 al 1)**
El byte va a ser un conjunto de 8 bits. Para entender cuántos números distintos se pueden escribir con 1 byte, seguimos el siguiente razonamiento:

- Con **dos bit** se puede escribir **00**, **01**, **10**, **11. Hay 2^2 = 4 números distintos (del 0 al 3)**
- Con **tres bit** se pueden escribir **000, 001, 010, 011, 100, 101, 110, 111**. Hay **2^3 = 8 números distintos (del 0 al 7)**
- Por tanto, con cada bit se doblan los números posibles a escribir. De esta forma estamos preparados para definir que es el byte.
  El **byte es un número binario de 8 cifras y se anota por B**. Al ser 8 cifras, se pueden escribir **2^8 = 256 números distintos (del 0 al 255)**

La importancia del byte se debe a que con un byte, se pueden representar 256 caracteres alfanuméricos distintos, que son necesarios para escribir cualquier texto en nuestro lenguaje. Si escribimos en el bloc de notas la palabra hola y lo guardamos como prueba.txt y miramos a continuación en propiedades cuánto ocupa el archivo veremos que ocupa 4 bytes. Esto se debe a que para cada letra se ha utilizado un byte (código ascii extendido).
Debido a esta equivalencia, muchas veces **al byte se le identifica con carácter**. De forma que se dice que el archivo prueba.txt ocupa 4 bytes o 4 caracteres.

Una pregunta sería porque hacen falta 1 byte para una letra. ¿Por qué hacen falta 8 bits que sirven para representar 256 caracteres distintos para una letra si sólo tenemos cerca de 30 letras en el abecedario? Hay que tener en cuenta que en nuestro lenguaje utilizamos el abecedario, pero tenemos distintas representaciones para las mayúsculas y las minúsculas, además tenemos vocales acentuadas y no acentuadas, también tenemos signos de puntuación y paréntesis; e

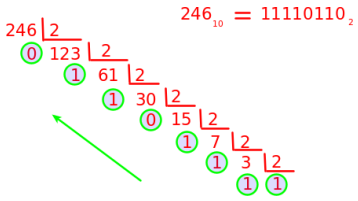
incluso escribimos dígitos numéricos en nuestros textos y caracteres invisibles, llamados de control como el tabulador e intro.

Con vistas al cálculo de direcciones IP en las redes que vemos en el siguiente libro es muy importante recordar la idea de potencia vista aquí:

- Con 1 byte u 8 bits, se pueden representar 2^8=256 números distintos, del 0 al 255 (del 00000000 al 11111111)
- Con 16 bits, se pueden representar 2^{16}=65536 números distintos, del 0 al 65535 (del 0000000000000000 al 1111111111111111)

Conversión decimal a binario

Para convertir un número decimal a binario, se realizan divisiones enteras por 2, utilizando el cociente entero para dividir de nuevo por 2, hasta que el cociente sea 0 o 1. Para obtener el número binario, coger como cifra más significativa el último cociente, y después todos los restos, empezando desde los últimos.



Miguel Ángel García Lara (CC BY-NC-SA)

Conversión binario a decimal

Cada bit se multiplica por una potencia de 2, comenzando desde el bit menos significativo (por la derecha)

Ejemplo: Convertir 11110110_2 a decimal
$11110110= 0*2^0 + 1*2^1 + 1*2^2 + 0*2^3 + 1*2^4 + 1*2^5 + 1*2^6 + 1*2^7 =$
$= 0*1 + 1*2 + 1*4 + 0*8 + 1*16 + 1*32 + 1*64 + 1*128 =$
$= 2 + 4 + 16 + 32 + 64 + 128 = 246$

Se obtiene $11110110_2 = 246_{10}$

El anterior proceso, se podría resumir en sumar la potencia de 2 correspondiente cuando el bit es 1, y no sumar nada cuando el bit es 0.
Aquí se refleja una tabla con 4 ejemplos de binario a decimal, utilizando este esquema.

Binario	2^7 = 128	2^6 = 64	2^5 = 32	2^4 = 16	2^3 = 8	2^2 = 4	2^1 = 2	2^0 = 1	Suma	Decimal
00000000	0	0	0	0	0	0	0	0	0+0+0+0+0+0+0+0=0	0
10101100	1	0	1	0	1	1	0	0	128+32+8+4	172
00111110	0	0	1	1	1	1	1	0	32+16+8+4+2	62

11111111	1	1	1	1	1	1	1	1	128+64+32+16+8+4+2+1	255

Múltiplos del byte

Normalmente cuando se habla de que un archivo ocupa 5 megas, esa información es incompleta, pues ocupará 5 megabytes o 5 megabits. (Mega solo significa un millón, 1.000.000). Los sistemas operativos nos dan la información de los archivos en bytes, sin embargo en otros ámbitos la información suele ser en bits.

Los operadores telefónicos al contratar ADSL o **fibra**, nos ofrecen una **velocidad de 100 megas /seg**, pero eso sigue siendo **incorrecto**, y lo que ofrecen **realmente es 100 Megabits / seg** (que es 8 veces inferior a la velocidad de 100 Megabytes / seg). Todas las velocidades vistas en esta unidad de trabajo 8, son en bi

En este módulo se ha seguido siempre el convenio de que **cuando se habla de bits se anota por b** y **cuando se habla de bytes se anota por B**.

Se incluye la tabla de múltiplos KB, MB, GB, TB

Nombre	Notación	Equivalencia
Bit	**b**	
Byte	**B**	8 b
Kilobyte	**KB**	1000 B = 10^3 B
Megabyte	**MB**	1000 KB = 10^3 KB = 10^6 B
Gigabyte	**GB**	1000 MB = 10^3MB = 10^9 B
Terabyte	**TB**	1000 GB = 10^3 GB = 10^{12} B
Petabyte	**PB**	1000 TB = 10^3 TB = 10^{15} B
Exabyte	**EB**	1000 PB = 10^3 PB = 10^{18} B

Diferencia entre Kilobyte y Kibibyte

Desde que comenzó la informática se consideró 1 Kilobyte = 1024 bytes = 2^{10} B

Sin embargo, kilo significa 1000 y nunca debe ser 1024. Esto ha generado que se hayan normalizado 2 notaciones con nombres distintos (estándar IEC 80000-13 del año 2008)

- Utilizando múltiplos de 1000, se habla de Kilobyte (KB), Megabyte (MB), Gigabyte (GB), Terabyte (TB).
- Utilizando múltiplos de 1024, se habla de Kibibyte (KiB), Mebibyte (MiB), Gibibyte (GiB), Tebibyte (TiB); donde **Kibibyte** es la contracción de **Kilobyte binario.**

Este tema genera mucha controversia en la informática, pues son más de 50 años donde 1 KB = 1024 B.
Incluso, Ubuntu y Windows utilizan distintas notaciones.
Cuando se instaló Windows y Linux en máquinas virtuales con un disco duro de 1 TB, ambos sistemas operativos reconocen discos de distintos tamaños. Ubuntu reconoce un disco duro de 1000 GB (utilizando múltiplos de 1000), mientras que Windows reconoce un disco duro de 939 GB (utilizando múltiplos de 1024).

7.- Direccionamiento lógico. Clases de redes y división en subredes.

Direcciones IP Versión 4. IPv4.

En anteriores libros se ha estudiado el direccionamiento físico con las direcciones MAC. En este libro se va a estudiar el direccionamiento lógico, o lo que es lo mismo las direcciones IP de las redes.
Todos los equipos que estén en la misma red, tienen una dirección IP única pero con la misma dirección de red.

El direccionamiento IP es la parte encargada de asignar de forma correcta a cada equipo una dirección IP, de forma que los equipos puedan comunicarse correctamente entre sí.
El estudio se va a concretar en la versión IPv4.
Una dirección IP tiene 32 bits, como cada 8 bits forman 1 byte, una dirección IP tiene 4 bytes.
Como sería muy incómodo dar una dirección IP con sus 32 bits (32 cifras binarias) se sustituye cada 8 bits por su valor decimal, separándose con puntos.

Ejemplo
La dirección IP: 11010001 11011000 00110111 00000011 se escribe 209.216.55.3
Todos los equipos que están en la misma red, tienen la misma dirección de red, llamado identificador de red (netid). Después cada equipo, tiene un número que le identifica de forma única dentro de la red, llamado identificador de equipo o host (hostid).

La dirección IP de un equipo tiene ambas partes, por ejemplo en la IP anterior:
11010001 11011000 00110111 00000011
Netid - identifidor red Hostid - identificador equipo (host)

Todos los equipos de esta red comienzan por 209.216.55.X donde X va de 0 a 255, aunque no son válidos ni el 0 ni el 255 como vamos a ver ahora mismo.

Esta IP al ser de clase C (se entenderá por qué en siguientes apartados) tiene 24 bits para la dirección de red y 8 bits para dirección de equipo; pero no es así siempre. Depende de las clases de redes se utilizan más o menos bits para la dirección de red.

Direcciones específicas. Reglas y convenios.

Existen unas reglas y convenios en cuanto a determinadas direcciones IP qué hay que conocer:

- La dirección 0.0.0.0 identifica al host actual, por lo que no se puede utilizar para ninguna red.
- La dirección con **el campo identificador de equipo todo a ceros se utiliza para indicar la dirección de red, y por tanto no se puede utilizar para ningún equipo.**
- Se conoce por broadcast o multidifusión o multicast a la posibilidad de enviar un mensaje a todos los equipos de la misma red. Para este objetivo se reservan algunas direcciones, de forma que ningún equipo puede tener esa red.
  La dirección 255.255.255.255 es el broadcast de todas las redes, de forma que si se envía algo a esa dirección, se envía ese datagrama a todos los equipos de la red.
  La dirección con **el campo identificador de equipo todo a unos se utiliza como la dirección broadcast de la red indicada, y por tanto no se puede utilizar para ningún equipo.**

- Todas las redes tienen una **máscara de red,** para calcular la máscara se ponen **todos los bits de la dirección de red a 1, y todos los bits del host a 0**. El objetivo de la máscara es

marcar los límites de la red, de forma que todos los equipos de la misma red tienen la misma máscara.

- La dirección 127.0.0.1 se utiliza para loopback. Cuando se envía un mensaje a esta IP, se devuelven a la dirección de origen todos los mensajes sin intentar enviarlos a ninguna parte. Se trata de probar la conectividad local.

Como consecuencia de las reglas 2 y 3 **siempre hay dos direcciones que no se pueden asignar a ningún equipo, que son el primero (por ser la dirección de red) y el último (por ser el broadcast de la red)**

Puerta de enlace

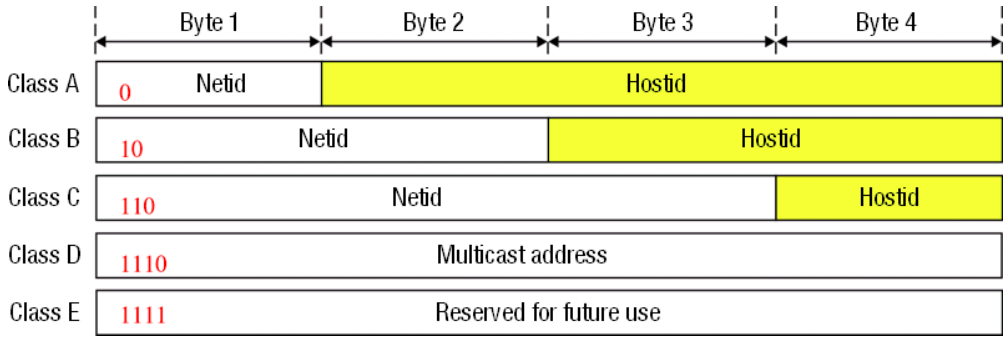
Cuando configuremos las IP en los ordenadores, habrá que configurar cual es la puerta de enlace. La puerta de enlace es una IP de nuestra red, y es el equipo por el que salimos al exterior (con el que nos comunicamos con otras redes). Habitualmente es la dirección IP del router con el que nos conectamos a Internet.

7.1- División de redes en clases.

Hay 5 clases principales de redes: A, B, C, D, E:

- Las clases normales son A, B, C.
- D son redes multicast (redes multidifusión)
- E son direcciones reservadas

La distinción de las clases va a venir dadas por cuántos bits se utilizan para el número de red y los valores de los primeros bits. En la siguiente imagen se muestra esa información para cada clase.



Fijarse en la figura, que en la clase A, se utilizan 8 bits (1 byte) para dirección de red y 24 bits (3 bytes) para identificador de equipo.
En clase B, se utilizan 16 bits (2 bytes) para dirección de red, y 16 bits (2 bytes) para dirección de host o equipo.
En clase C, se utilizar 24 bits (3 bytes) para dirección de red, y 8 bits (1 byte) para dirección de host o equipo.
El objetivo es poder tener redes más grandes y redes más pequeñas, a más bits para equipo, se puede tener una red más grande.

Clase A

Dirección de red:
Se utilizan 8 bits de red, con el primer bit a 0.
Si nos fijamos en el primer byte, este puede ir de 00000000 a 01111111 que **en decimal va de 0 a 127**. Se puede ver de otra forma, y de los 8 bits, el primero siempre es 0, por lo que las posibles redes vienen dadas por 7 bits: $2^7 = 128$

Pero las redes 0 y 127 no se pueden utilizar, pues la red 0 representa a todas las redes, recordar que el propio equipo se reconoce por la dirección 0. Y la red 127 representa el loopback.
Por tanto **solo hay 126 redes posibles de clase A**.

Dirección de equipo o host:
La dirección de **equipo** la forman 24 bits**, 2^{24}** por tanto la red puede tener aproximadamente 16 millones de equipos.

Observación: **Solo hay 126 posibles redes de clase A, pero con muchísimos equipos.**

Ejemplo de clase A	
Dirección de red	126.0.0.0
Primer equipo	126.0.0.1
Último equipo	126.255.255.254
Broadcast red	126.25.255.255
Máscara de red	255.0.0.0

Clase B

Dirección de red

Se utilizan **16 bits de red, con los 2 primeros bit a 10**.
Si nos fijamos solo en primer byte, este puede ir desde 10000000 a 10111111 que **en decimal va de 128 a 191**. Aquí hay que tener en cuenta, que estamos hablando solo del primer byte. Pero que el segundo byte, también es dirección de red.
¿Cuántas redes puede haber? De las 16 cifras para la red, las 2 primeras son obligatorias (10), por tanto **2^{14}=16384 redes**

Dirección de equipo o host

La dirección de **equipo** la forman 16 bits, **2^{16} = 65536,** pero en toda red, no se puede utilizar la primera ni la última. La primera, porque representa la dirección de red, y la última porque es el broadcast de la red. De ahí, que las redes de clase B **pueden tener 65534 equipos o hosts**.

Ejemplo de clase B	
Dirección de red	150.85.0.0
Primer equipo	150.85.0.1
Último equipo	150.85.255.254
Broadcast red	150.85.255.255
Máscara de red	255.255.0.0

Clase C

Dirección de red

Se utilizan **24 bits de red con los 3 primeros bit a 110**.
Si nos fijamos solo en primer byte, este puede ir desde 11000000 a 11011111 que **en decimal va de 192 a 223**. Pero la red 192 está reservada para redes privadas.
¿Cuántas redes puede haber? De las 24 cifras para la red, las 3 primeras son obligatorias (110), por tanto, 2^{21}, aproximadamente 2 millones de redes.

Dirección de equipo o host

La dirección de **equipo la forman 8 bits, $2^8 = 256$,** por tanto la red puede tener 256 equipos, pero como no se pueden utilizar ni la primera ni la última, las redes de clase C **pueden tener 254hosts.**

Ejemplo de clase C	
Dirección de red	196.220.53.0
Primer equipo	196.220.53.1
Último equipo	196.220.53.254
Broadcast red	196.220.53.255
Máscara de red	255.255.255.0

Clases D y E.

No se utilizan para la configuración general de las redes
Clase D son las redes que **comienzan por 1110** por lo que van **desde la 224 a 239** y que se utilizan para **multidifusión**.

Clase E comienzan por 1111 por lo que van **desde la 240 a la 254 y que están reservadas** para uso futuro (la 255 no se puede utilizar por ser el broadcast general de todas las redes)

Redes privadas

Algunos direcciones IP se reservan para redes privadas, lo que significa que esas IP no se pueden asignar a ningún ordenador en Internet.

Tabla de direcciones privadas

Clase	Rango	Número de redes
A	10.x.x.x	1
B	172.16.x.x a 172.31.x.x	16
C	De 192.168.x.x a 192.168.255.x	256

Las redes privadas se utilizan para la intranet. Para entenderlo, como mejor se explica es con la estructura de los domicilios particulares. En ellos, se tiene el router facilitado por el operador telefónico, ese router une 2 redes:

- La dirección IP pública o externa, es la que está conectada a Internet, y es única en Internet.
- La IP privada o interna, es la que está en la red del domicilio, con el resto de aparatos (móviles, ordenadores, impresora, Smart-tv), la IP de cada aparato es distinta. Es esta IP privada, donde se utilizan esta redes privadas.
  De hecho, la privada de muchos routers, es la misma (muy habitual la 192.168.0.1), eso no crea ningún problema, pues no están en la misma red. Cada domicilio se ve desde fuera con su IP externa, que esas si son únicas en Internet.

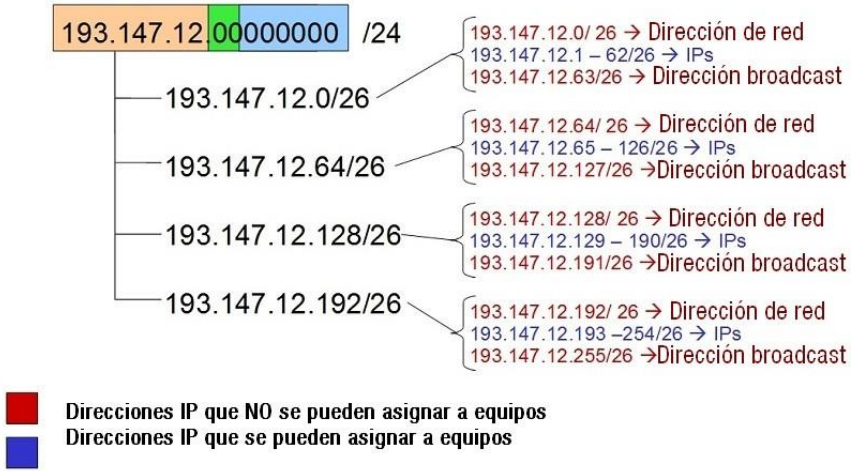
Para averiguar nuestra IP pública o externa del router, abrir en el navegador web la dirección http://cualesmiip.es/

7.2.- División de redes en subredes.

A la hora de diseñar la red de una empresa uno de los aspectos que hay que tener en cuenta es optimizar el uso de las redes.
En principio si todos los equipos están en la misma red, tendrán visibilidad entre ellos. Si no queremos que tengan visibilidad las distintas aulas, necesitaremos que estén en subredes distintas.

El direccionamiento IP nos da la posibilidad de crear subredes, donde cada una de ellas tendrá su dirección de subred, su broadcast de subred y un rango de IP permitidas.

En la siguiente imagen se muestra una red de clase C, (por empezar por 193), donde se ha subdividido en 4 subredes. Como una red de clase C, tiene 256 posibles equipos (realmente 254), al dividirla en 4 subredes, se tienen 4 subredes de 64 equipos (realmente 62, al no poder utilizar la dirección de subred y la dirección de broadcast).



En el ejemplo de la figura, al haber 4 subredes, 2 bits de identificador de equipo de la clase C pasan a ser dirección de subred, de forma que el identificador de subred son 26 bits y el identificador de equipo son 6 bits.

Al dividir la red en subredes, se calcula la máscara, dirección de subred y broadcast de la subred con las mismas normas que en las redes.

Para aclarar todos estos términos, se incluye a continuación dos ejercicios de división en subredes.

8.- Configuración de routers.

Tablas de enrutamiento

Los routers son los encargados de comunicar varias redes y además, permiten asegurar la red de la empresa. Para configurar un router debemos crear lo que se denomina “tabla de enrutamiento” o “directivas de firewall”.
A la hora de escribir la tabla de enrutamiento, se utilizan los siguientes elementos:

- Interfaz: interfaz de red por donde se recibe la información.
- Origen / Destino: origen y destino del mensaje. Normalmente el origen y el destino de un mensaje es una dirección IP o conjunto de direcciones IP.
- Puerto: permitir o denegar el acceso a los puertos permite el tráfico de un servicio o lo deniega. Por ejemplo si tenemos un servidor web de nuestra empresas, tendremos que permitir el tráfico de entrada al puerto 80.
- Acción: especifica la acción que debe realizar el router. Un router puede realizar las siguientes acciones:
- Aceptar: dejar pasar la información.
- Denegar: no deja pasar la información.
- Reenviar: envía el paquete a una determinada dirección IP.

A la hora de indicar la dirección de origen o la dirección de destino es importante utilizar la máscara de red para indicar un mayor o menor número de ordenadores. En la tabla siguiente, semuestran ejemplos.

Ejemplo	Comentario
192.165.2.23/32	Representa a un único ordenador
192.165.2.0./24	Representa a todas las direcciones IP del tipo 192.165.2.X
192.165.0.0/16	Representa a todas las direcciones IP del tipo 192.165.X.X
192.0.0.0/8	Representa a todas las direcciones IP del tipo 192.X.X.X
0.0.0.0/0	Representa a todas las direcciones IP del tipo X.X.X.X

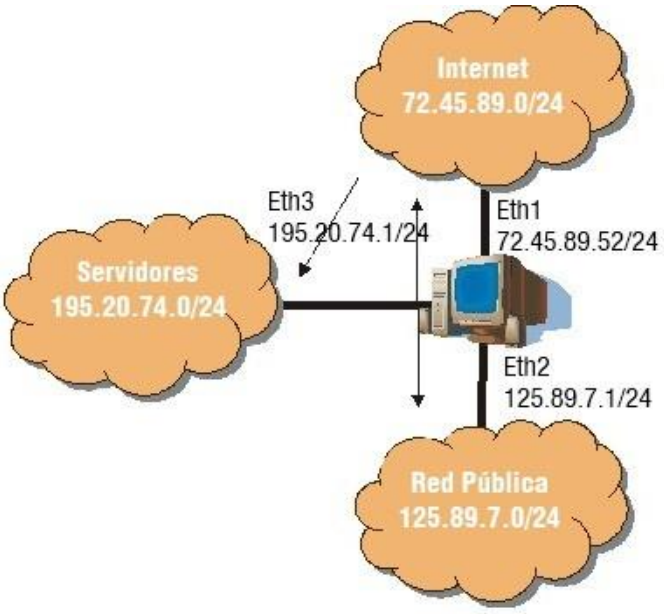
La tabla de enrutamiento representa el conjunto de reglas que actúan como medida de seguridad para determinar si se permite que un paquete pase o no.
A la hora de construir la tabla de enrutamiento se debe tener en cuenta:

- Las reglas se aplican en orden secuencial, de arriba hacia abajo. En el momento que se cumpla una, ya yo se leen el resto.
- Construir reglas desde la más específica a la más general. Esto se hace así para que una regla general no "omita" a otra más específica, pero que entra dentro del ámbito de la regla general.

Ejemplo de creación de una tabla de enrutado.

La mejor forma de explicar este apartado es con un ejemplo concreto. Se va a configurar un router con tres redes diferentes, tal como muestra la figura.
En la figura hay un ordenador con 3 interfaces o tarjetas de red (eth1, eth2 y eth3), realizando

labores de router. También están reflejadas las 3 direcciones IP de las tarjetas, que conectan a las 3 redes: Internet, Red pública y servidores.



Se deben crear el conjunto de reglas para permitir que la red pública se conecte a Internet y que los servidores sean accesibles desde Internet; el servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.
El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes.
Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.

Reglas	Interfaz	Origen	Destino	Puerto	Acción
1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.5/32	25,110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

- Regla 1. Esta regla permite el acceso entrante en el puerto 80, que es el servicio web. El host 195.20.74.5 es el servidor web. La organización no puede predecir quién quiere acceder a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.
- Regla 2. Esta regla permite el acceso entrante a los puertos 25 y 110, que son los del correo electrónico. El servidor de correo está en la dirección 195.20.74.7. Al igual que en laregla anterior, no se restringen las direcciones IP de origen.
- Regla 3. Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como la regla 1 y 2, se ejecutan antes, sí se permite el tráfico que va dirigido a los servidores web y correo electrónico. Si se pone esta regla al principio de la tabla de enrutamiento, no se podrá acceder a ningún servidor.
- Reglas 4 y 5. La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y

la quinta regla deja pasar el tráfico que va desde la red pública a la red de Internet.

- Regla 6. Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos realizan este paso de forma predeterminada, pero es útil incluirla.

Para terminar, se muestra un ejemplo de configuración de un router con iptables, donde iptables es el servicio de enrutamiento en un servidor Linux.

```
[root@redhatserver root]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.0.0.0/24          anywhere           tcp dpt:http
ACCEPT     udp  --  10.0.0.0/24          anywhere           udp dpt:domain
ACCEPT     all  --  anywhere             anywhere           state ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
[root@redhatserver root]#
```

8.1.- Seguridad en la arquitectura de red.

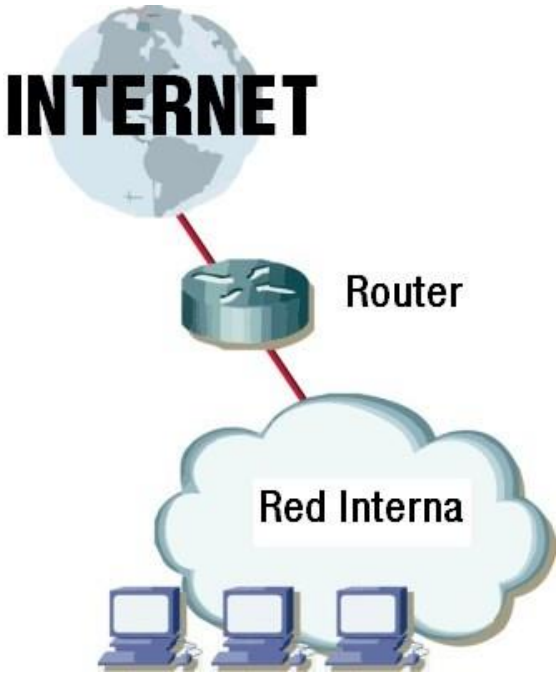
Si ponemos todos los equipos en la misma red y se produce un ataque de seguridad entonces toda la red se verá comprometida. Las arquitecturas de seguridad se utilizan para que en caso de que haya una intrusión, se pueda limitar el acceso del intruso. Existen varias arquitecturas dered, desde la más sencilla, que utiliza simplemente un router, hasta otras más complejas, basadas en varios routers, proxys y redes perimetrales (o zonas neutras).
Antes de entrar en detalle con las arquitecturas de cortafuegos, se van a describir tres elementos básicos que intervienen en ella:

- Router. Equipo que permite o deniega las comunicaciones entre dos o más redes. Al ser el intermediario entre varias redes debe estar especialmente protegido, con el enrutamiento, ya que puede ser objeto de un ataque.
- Red interna. Es la red interna de la empresa y, por lo tanto, es donde se encuentran los equipos y servidores internos. Dependiendo del nivel de seguridad que necesite la red interna se puede dividir en varias redes para permitir o denegar el tráfico de una red a otra.
- Zona neutra (o red perimetral). Red añadida entre dos redes para proporcionar mayor protección a una de ellas. En esta red suelen estar ubicados los servidores de la empresa. Su principal objetivo es que ante una posible intrusión en unos de los servidores, se aísle la intrusión y no se permita el acceso a la red interna de la empresa.

A continuación se muestran varios esquemas, comenzando por los más simples.

Esquema de red básico.

Es la configuración más simple y consiste en el empleo de un router para comunicar la red interna de la empresa con Internet. Como el router es el encargado de comunicar ambas redes es ideal para permitir o denegar el tráfico.



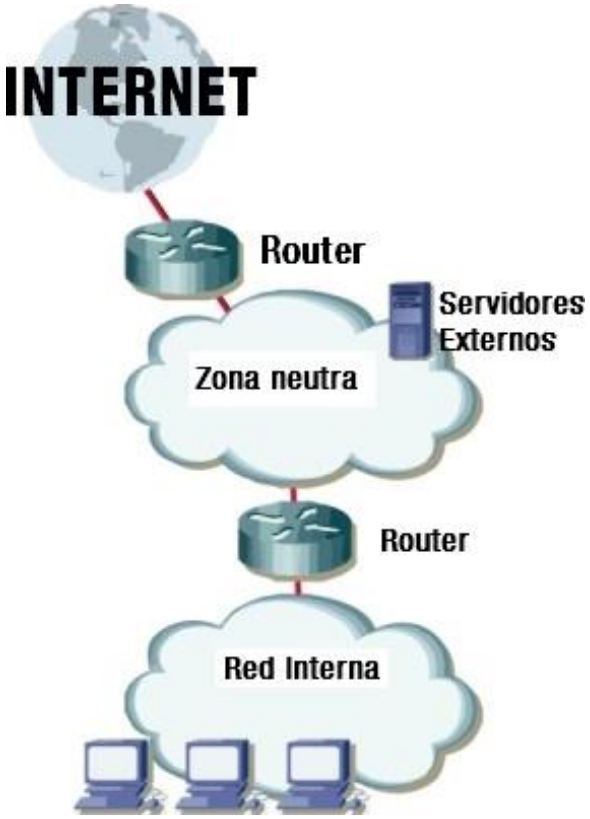
Esta arquitectura de red, aunque es la más sencilla de configurar es la más insegura de todas ya que toda la seguridad reside en un único punto: el router. En caso de que se produzca un fallo de seguridad en el router el atacante tiene acceso a toda la red interna.

Esta arquitectura es la usual en los domicilios y en pequeñas empresas.

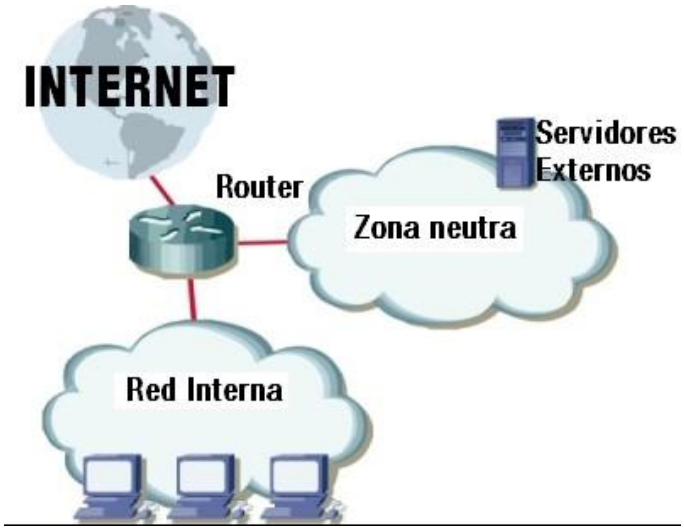
Esquema de red con una zona neutra

En el anterior esquema, si se desea tener un servidor que ofrezca servicios a Internet hay que ubicarlo en la red interna. Es peligroso poner el servidor en la red interna ya que el router permite el tráfico al servidor y, en el caso de que se produzca un fallo de seguridad el atacante tiene acceso completo a la red interna. Para solucionar este problema se añade una nueva red a la empresa que se denomina zona neutra o zona desmilitarizada.

Esta arquitectura utiliza dos routers que permiten crear un perímetro de seguridad (red perimetral o zona neutra), en la que se pueden ubicar los servidores accesibles desde el exterior, protegiendo así a la red local de los atacantes externos.
En la imagen se muestra un esquema de red con una zona neutra y una red interna utilizando dos routers.



En este esquema el router exterior está configurado para permitir el acceso desde Internet a los servidores de la zona neutra, especificando los puertos utilizados, mientras que el router interior permite únicamente el tráfico saliente de la red interna al exterior. De esta forma si se produce un fallo de seguridad y se accede a los servidores de la zona neutra, el atacante nunca podrá tener acceso a la red interna de la empresa.
Se pueden realizar otras configuraciones con zona neutra. Se puede crear una zona neutra utilizando un único router con tres interfaces (que una tres redes, tiene que ser un router profesional, no valen los routers de los operadores telefónicos que solo unen dos redes)



Aunque este esquema no es tan fiable como el anterior resulta más aconsejable que el modelo básico que no tiene ninguna zona neutra.
Estos esquemas permiten distintas modificaciones. Por ejemplo en la imagen se muestra un esquema donde hay 2 routers con zona neutra y varias redes internas. En este caso seincrementa la seguridad entre las propias redes internas de la empresa.