

# UNIDAD 6 - INTRODUCCIÓN A LAS REDES DE ORDENADORES

1.	INTRODUCCIÓN A LAS REDES DE ORDENADORES	3
2.	CLASIFICACIÓN EN LAS REDES DE ORDENADORES	3
2.1.	SEGÚN ÁREA GEOGRÁFICA	3
2.1.1.	REDES DE ÁREA LOCAL (LAN)	4
2.1.2.	REDES DE ÁREA METROPOLITANA (MAN)	5
2.1.3.	REDES DE ÁREA EXTENSA (WAN)	5
3.	INTERNETWORKING	6
3.1.	SEGÚN TECNOLOGÍA DE TRANSMISIÓN	7
3.1.1.	REDES BROADCAST	7
3.1.2.	REDES PUNTO A PUNTO	7
4.	MEDIOS DE TRANSMISIÓN	9
4.1.	CABLES METÁLICOS	9
4.1.1.	CABLE DE PARES	10
4.1.2.	CABLE COAXIAL	11
4.2.	FIBRA ÓPTICA	12
4.3.	TRANSMISIÓN INALÁMBRICA	13
4.4.	REDES INALÁMBRICAS LAN (802.11) – WLAN o WiFi	14
5.	ARQUITECTURA DE RED	15
5.1.	TOPOLOGÍA	15
5.2.	MODELOS DE REFERENCIA	15
5.2.1.	EL MODELO DE REFERENCIA OSI	16
5.2.2.	EL MODELO DE REFERENCIA TCP/IP	20
5.2.3.	COMPARATIVA OSI-TCP/IP	21
6.	DISPOSITIVOS DE RED	22
7.	CABLES DE RED	23
8.	PROTOCOLO IP	24
8.1.	DIRECCIONAMIENTO IPv4	24
8.2.	CLASES DE REDES	24
8.2.1.	CLASE A	25
8.2.2.	CLASE B	25
8.2.3.	CLASE C	25
8.2.4.	CLASES ESPECIALES	26
8.3.	MÁSCARAS DE RED DE CLASES MÁS UTILIZADAS	26
8.4.	REDES PRIVADAS - DIRECCIONES IP PRIVADAS	26
9.	SUBNETTING, SUBREDES Y MÁSCARAS DE RED	27
9.1.	LA MÁSCARA DE SUBRED	27
9.2.	SUBNETTING	27
9.3.	SUPERNETTING	28
9.4.	EJEMPLO REAL - SUBNETTING	28
10.	FICHEROS DE CONFIGURACIÓN TCP/IP	31

11.	GESTIÓN DE PUERTOS	36
11.1.	¿TCP O UDP?	36
11.2.	PUERTOS MÁS UTILIZADOS	36
11.3.	GESTIÓN DE PUERTOS EN LINUX	37
11.4.	GESTIÓN DE PUERTOS EN WINDOWS	37

# 1. INTRODUCCIÓN A LAS REDES DE ORDENADORES

En tan solo unos años las redes de ordenadores han pasado de ser algo esotérico solo conocido y utilizado por unos pocos a ocupar un primer plano en cualquier medio informativo de carácter general.

Un **sistema informático en red** es aquel S.I. interconectado con uno o más equipos y que es capaz de prestar/ejecutar algún tipo de servicio colaborando con el resto de equipos de la red. El tipo de servicio va desde envío de datos, cálculo conjunto, o cualquier tipo de servicio colaborativo o de cliente/servidor. Estos sistemas se fundamentan en **modelos de referencia** que establecen las características y las especificaciones necesarias para poder comunicarse entre diferentes entidades con objeto de intercambiar información. Los modelos de referencia más usados son OSI y TCP/IP. Están formados por capas o niveles para definir protocolos y estándares, reducir la complejidad, controlar los flujos de comunicación y facilitar su evolución. El modelo OSI ha quedado como un modelo teórico, mientras que el TCP/IP es el estándar abierto de Internet cuyos protocolos más característicos son: IP, Ethernet, WiFi, TCP y UDP. Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un **sistema operativo de red**. Ejemplos de sistemas operativos en red o NOS (Network Operating System) son: Windows Server y Ubuntu Server que veremos en temas posteriores.

No es objetivo entrar en demasiados detalles por lo tanto tocaremos todo pero de forma general: tipos de redes, medios de transmisión, arquitectura de redes, dispositivos y protocolos.

Una vez conocidos los fundamentos teóricos estudiaremos la configuración del protocolo TCP/IP en tarjetas de red, así como los puntos de acceso WiFi. Usaremos el software *Packet Tracer* de Cisco.

# 2. CLASIFICACIÓN EN LAS REDES DE ORDENADORES

Según su escala (o área geográfica) se suelen clasificar en:

- Redes de área local (LAN, Local Area Network)
- Redes de área metropolitana (MAN, Metropolitan Area Network)
- Redes de área extensa (WAN, Wide Area Network)

De acuerdo con su tecnología de transmisión las redes se clasifican en:

- Redes broadcast (multidifusión)
- Redes punto a punto

## 2.1. SEGÚN ÁREA GEOGRÁFICA

Es bastante habitual clasificar las redes por su ámbito, es decir por el alcance máximo para el cual se han diseñado. En este sentido se suele hablar de redes locales (LAN, Local Area Networks) y redes de área extensa o WAN (Wide Area Network). En ocasiones se describe una categoría intermedia denominada MAN (Metropolitan Area Networks), aunque hay muy pocas tecnologías que incluyan en este grupo.

En realidad es inexacto realizar una división de las redes o tecnologías en base a la distancia, ya que se pueden encontrar ejemplos en los que las tecnologías tradicionalmente consideradas WAN se utilizan en distancias cortas. Análogamente las redes LAN pueden utilizarse para cubrir distancias de cientos de kilómetros (Ej: FDDI, aunque sea más caro). Es decir: **aunque esta clasificación sea por distancia a veces se hace por "servicio que presta" u objetivo de diseño.**

Por eso probablemente la mejor clasificación de redes LAN y WAN se pueda efectuar en base al objetivo de diseño; si es el transporte de datos normalmente se trata de una LAN, mientras que si es el transporte de voz generalmente se trata de una WAN (aunque finalmente también es utilizada para transmisión de datos).

Distancia entre procesadores	Procesadores ubicados en el mismo ...	Ejemplo
1 m	Sistema	Multiprocesador
10 m	Habitación	LAN
100 m	Edificio	
1 Km	Campus	
10 Km	Ciudad	MAN
100 Km	País	WAN
1.000 Km	Continente	
10.000 Km	Planeta	

### 2.1.1. REDES DE ÁREA LOCAL (LAN)

Las redes de área local tienen *generalmente* las siguientes características:

- **Tecnología broadcast:** el medio de transmisión es compartido por todos los elementos interconectados.
- **Cableado específico**, instalado normalmente a propósito (no usa infraestructura previa)
- **Velocidad de 1 a 1000 Mb/s** (De aquí en adelante todas las velocidades mostradas irán en Mb/s, es decir, Megabits/s)
- **Extensión máxima de unos 3 KM** (ojo: FDDI o Interfaz de Datos distribuido por FIBRA ÓPTICA llega a 200 Km)

Las LANs más conocidas y extendidas son la **Ethernet** a 10 Mb/s, la **IEEE 802.5** o **Token Ring** a 4 y 16 Mb/s, y la **FDDI** a 100 Mb/s. Estos tres tipos de LAN han permanecido prácticamente sin cambios desde finales de los ochenta, por lo que a menudo se les referencia en la literatura como 'LANs tradicionales' ('legacy LANs' en inglés) para distinguirlas de otras más modernas aparecidas en los 90, tales como la **Fast Ethernet** (100 Mb/s) o la **Gigabit Ethernet** (1000 Mb/s).

El alcance limitado de las LANs permite saber el tiempo máximo que un paquete tardará en llegar de un extremo a otro de la red, lo cual permite aplicar diseños que de otro modo no serían posibles, y simplifica la gestión de la red. Como consecuencia del alcance limitado y del control en su cableado, las redes locales suelen tener un retardo muy bajo en las transmisiones (decenas de microsegundos) y una tasa de errores muy baja.

La **topología** básica de las redes locales suele ser de bus (ej. Ethernet), de anillo (Token Ring o FDDI) o de estrella. Sin embargo, pueden hacerse topologías más complejas utilizando elementos adicionales, tales como repetidores, puentes, conmutadores, etc., (elementos que veremos más adelante).



Los tipos más utilizados de LAN son: Ethernet, Fast Ethernet, Gigabit Ethernet y las LAN inalámbricas 802.11 (que luego veremos). Vemos los 3 primeros:

## REDES ETHERNET (802.3)

Ethernet, también conocido como **10BASE** opera a **10Mbps**. Tiene distintas alternativas según el tipo de cableado: 10BASE-5 (coaxial grueso), 10BASE-2 (coaxial delgado), 10BASE-T (par trenzado) y 10BASE-F (fibra óptica).



## REDES FAST ETHERNET

Fast Ethernet, también conocido como **100BASE** opera a **100Mbps**. También tiene distintas alternativas según el tipo de cableado: 100BASE-T2 (2 pares de UTP), 100BASE-T4 (4 pares de UTP), 100BASE-TX (par trenzado) y 100BASE-FX (fibra óptica). Surge ante la necesidad de crear una LAN de bajo coste compatible con Ethernet y que funcione a 100 Mbps.

## REDES GIGABIT ETHERNET

Gigabit Ethernet, también conocido como **1000BASE**, transmite a velocidades en torno a los **1000Mbps (1Gbps)**. También tiene distintas alternativas según el tipo de cableado: 1000BASE-SX (fibra óptica multimodo), 1000BASE-LX (fibra óptica monomodo o multimodo), 1000BASE-CX (cable de cobre blindado especial) y 1000BASE-T (4 pares UTP categoría 5).

Estos dos últimos tipos de redes desbancaron rápidamente a FDDI.

TYPE	SPEED	CABLE	CABLE IMAGE
Fast Ethernet	10/100Mbps	Cat5	
Gigabit Ethernet	10/100/1000Mbps	Cat5e/Cat6a	

### 2.1.2. REDES DE ÁREA METROPOLITANA (MAN)

En principio se considera que una MAN abarca una distancia de unas pocas decenas de kilómetros, que es lo que normalmente se entiende como área metropolitana. Existe solamente una red característica de las MANs, la conocida como **IEEE 802.6** o **DQDB** (Distributed Queue Dual Bus), que puede funcionar a diversas velocidades entre 34 y 155 Mb/s con una distancia máxima de unos 160 Km. En realidad la distinción de MANs en base a la distancia es un tanto arbitraria, ya que FDDI puede llegar a 200 Km pero raramente se la clasifica como MAN, al no ser un servicio ofrecido por las compañías telefónicas, cosa que sí ocurre con DQDB en algunos países.

La tecnología DQDB ha tenido escasa difusión.

### 2.1.3. REDES DE ÁREA EXTENSA (WAN)

Las redes de amplio alcance se utilizan cuando no es factible tender redes locales, bien porque la distancia no lo permite por el costo de la infraestructura o simplemente porque es preciso atravesar terrenos públicos en los que no es posible tender infraestructura propia. En todos estos casos lo normal es utilizar para la transmisión de los datos los servicios de una empresa portadora (ej: Telefónica).

Las redes WAN se implementan casi siempre haciendo uso de enlaces telefónicos que han sido diseñados principalmente para transmitir la voz humana, ya que este es el principal negocio de las compañías telefónicas. Normalmente la infraestructura esta fuera del control del usuario, estando supeditado el

servicio disponible a la zona geográfica de que se trate. Conseguir capacidad en redes WAN suele ser caro, por lo que generalmente se solicita el mínimo imprescindible.

Hasta tiempos recientes las conexiones WAN se caracterizaban por su lentitud, costo y tasa de errores relativamente elevada. Con la paulatina introducción de fibras ópticas y líneas digitales en las infraestructuras de las compañías portadoras las líneas WAN han reducido apreciablemente su tasa de errores; también se han mejorado las capacidades y reducido los costos. A pesar del inconveniente que en ocasiones pueda suponer el uso de líneas telefónicas tienen la gran virtud de llegar prácticamente a todas partes, que no es poco.

Un ejemplo de redes WAN son las **redes CATV** o de televisión por cable (EEUU).

### 3. INTERNETWORKING

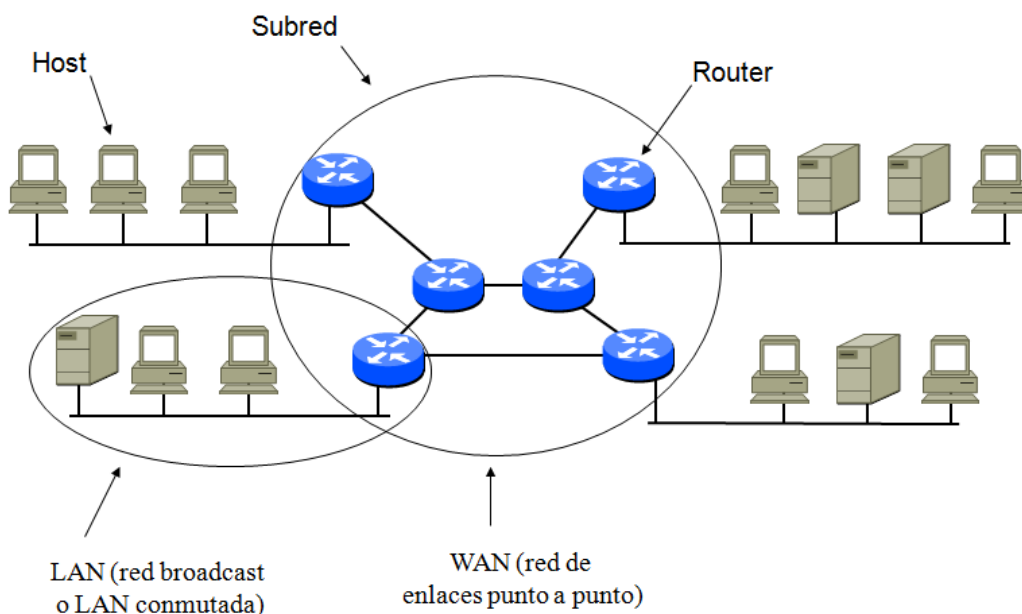
Se llama **Internetworking** a la interconexión de redes diferentes. Las redes pueden diferir en tecnología (ej: Ethernet-Token Ring) o en tipo (LAN-WAN).

Los dispositivos que permiten la interconexión de redes diversas son (los estudiamos más adelante):

- Repetidores y amplificadores
- Puentes (Bridges)
- Routers y Conmutadores (Switches)
- Pasarelas de nivel de transporte o aplicación (Gateways)

Un ejemplo de una red completa podemos verlo a continuación. Se define como completa porque interconecta distintos tipos (en este caso LAN-WAN):

#### Escenario típico de una red completa (LAN-WAN)



### 3.1. SEGÚN TECNOLOGÍA DE TRANSMISIÓN

Según la tecnología de transmisión y el tipo de red por ámbito tenemos la siguiente clasificación:

	Redes LAN	Redes WAN
Redes broadcast	Ethernet, Token Ring, FDDI	Redes vía satélite, redes CATV
Redes de enlaces punto a punto	LANs conmutadas	Frame Relay, ATM

#### 3.1.1. REDES BROADCAST

En las **Redes Broadcast** el medio de transmisión es compartido por todos los ordenadores interconectados. Normalmente cada mensaje transmitido es para un único destinatario, cuya dirección aparece en el mensaje, pero para saberlo cada máquina de la red ha de recibir o 'escuchar' cada mensaje, analizar la dirección de destino y averiguar si va o no dirigido a ella; las normas de buena educación 'telemática' establecen que un ordenador debe descartar sin más análisis todo mensaje que no vaya dirigido a él; sin embargo, algunos programas llamados '*sniffers*' se dedican a 'cotillear' todo lo que pasa por el cable, independientemente de quien sea su destinatario. La única protección efectiva en las redes broadcast es el *encriptado* de la información.

A veces en una red broadcast lo que se quiere es precisamente enviar un mensaje a todas las máquinas conectadas. Esto se llama un **envío broadcast**. Asimismo es posible enviar un mensaje dirigido a un subconjunto de todas las máquinas de la red (subconjunto que ha de estar definido previamente); esto se conoce como **envío multicast** (y el subconjunto se denomina grupo multicast). En algunos contextos cuando se habla de broadcast o multicast el caso en el que el mensaje va dirigido a una máquina concreta se denomina **envío unicast**.

#### 3.1.2. REDES PUNTO A PUNTO

Las **Redes Punto a Punto** se construyen por medio de *conexiones* entre pares de ordenadores, también llamadas *líneas*, *enlaces*, *circuitos* o *canales* (en inglés los términos equivalentes son '*lines*', '*links*', '*circuits*', '*channels*' o '*trunks*'). Una vez un paquete es depositado en la línea el destino es conocido de forma unívoca y no es preciso en principio que lleve la dirección de destino parcial, solo la final.

Los enlaces que constituyen una red punto a punto pueden ser de tres tipos de acuerdo con el **sentido de la transmisión**:

- **Simplex**: la transmisión sólo puede efectuarse en un sentido
- **Semi-dúplex o 'half-duplex'**: la transmisión puede hacerse en ambos sentidos, pero no simultáneamente
- **Dúplex o 'full-duplex'**: la transmisión puede efectuarse en ambos sentidos a la vez.

Al unir múltiples máquinas con líneas punto a punto es posible llegar a formar redes de topologías complejas en las que no sea trivial averiguar cuál es la ruta óptima a seguir para ir de un punto a otro. Como contraste, en una red broadcast el camino a seguir de una máquina a otra es único, no existen ordenadores intermedios y el grado de ocupación es el mismo para todas ellas.

Cada uno de los ordenadores que participa en una red de enlaces punto a punto es un **nodo** de la red. Si el nodo tiene un único enlace se dice que es un **nodo terminal** o 'end node', de lo contrario se dice que es un **nodo intermedio** o de **encaminamiento** o 'routing node'. Cada nodo intermedio ha de tomar una serie de decisiones respecto a por donde debe dirigir los paquetes que reciba, por lo que también se les llama **odos de conmutación de paquetes, nodos de conmutación, conmutadores o encaminadores** (los términos equivalentes en inglés son respectivamente *packet switching nodes, switching nodes, switches y routers*). Dependiendo del tipo de red que se trate nosotros utilizaremos las denominaciones **router** o **conmutador (switch)**.

Cualquier ordenador puede actuar como un router en una red si dispone del programa apropiado; sin embargo, se prefiere normalmente utilizar para este fin ordenadores dedicados, con sistemas operativos en tiempo real y software específico, dejando los ordenadores de propósito general para las aplicaciones del usuario; esto da normalmente mayor rendimiento y fiabilidad. Tradicionalmente al ordenador de propósito general que se conecta a la red como nodo terminal mediante un router se le denomina **host**. El conjunto de líneas de comunicación y routers que interconectan a los hosts forman lo que se conoce como la **subred de comunicaciones**, o simplemente **subred**.

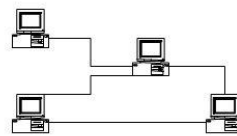
Para llegar de un nodo a otro en una red se ha de atravesar uno o varios enlaces; el número de enlaces se denomina en inglés '**hops**', que significa saltos, y depende de la trayectoria seguida y de la topología de la red. Cuando dos nodos no vecinos (es decir a más de un 'hop' de distancia) desean intercambiar información lo han de hacer a través de uno o varios nodos intermedios. Cuando un paquete se envía de un nodo al siguiente normalmente el paquete es transmitido en su totalidad y almacenado; solo entonces el nodo receptor intenta enviar el paquete al siguiente nodo de la red. Esto es lo que se conoce como una **red de almacenamiento - reenvío** ('store-and-forward') o **red de conmutación de paquetes** ('packet-switched'), también como 'store-and-forward packet switching'. Esta forma de proceder permite una elevada fiabilidad incluso en entornos hostiles donde el número de errores puede ser elevado.



## Types of Networks

### ■ Point-to-point network

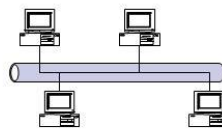
- ☐ Two end hosts connected by a link
- ☐ Usually for long distance connections
- ☐ Examples: dialup, SONET/SDH



Point-to-Point Network

### ■ Broadcast network

- ☐ A number of stations share a common transmission medium
- ☐ Local networks
- ☐ Examples: Ethernet, wireless local area networks



Broadcast Network



## 4. MEDIOS DE TRANSMISIÓN

El medio de transmisión es probablemente la parte más perdurable del diseño de una red. Esto unido a la existencia de múltiples opciones hace especialmente importante la acertada elección del medio de transmisión en el diseño de una red. Afortunadamente existen estándares de cableado que reducen a un pequeño número las posibilidades que merece la pena considerar.

### 4.1. CABLES METÁLICOS

El cable metálico es el medio de transmisión más utilizado cuando se trata de cubrir distancias no muy grandes y/o se necesitan capacidades no demasiado elevadas. La información se transmite a través del cable en forma de ondas electromagnéticas, o sea corrientes eléctricas alternas de alta frecuencia. A los efectos que ahora nos ocupan la situación es prácticamente la misma tanto si los bits se transmiten de forma digital o analógica (es decir modulados en una señal portadora). El metal utilizado casi siempre es el cobre ya que combina una buena conductividad con un coste razonable.

#### PROBLEMAS DE LOS CABLES METÁLICOS

Cuando se quiere transmitir un caudal elevado de información es necesario en general utilizar un gran ancho de banda, lo cual conlleva el uso de frecuencias elevadas. Los principales problemas que se presentan al transmitir señales de elevada frecuencia en un cable de cobre son la atenuación, el desfase y la interferencia electromagnética.

##### 1) Atenuación

Cualquier señal al propagarse por un medio de transmisión pierde potencia, es decir se atenúa con la distancia. En el caso del cable de cobre dicha atenuación se debe fundamentalmente a dos factores:

- **Resistencia del cable:** esto provoca la pérdida en forma de calor de parte de la energía de la señal original. Dado que la resistencia disminuye con el aumento de sección del cable la atenuación debida a esta causa es menor cuanto mayor es el grosor de éste.
- **Emisión electromagnética al ambiente:** el cable por el que se propaga la onda electromagnética actúa como una antena emisora, por lo que parte de la energía se pierde en forma de emisión electromagnética al ambiente.

##### 2) Desfase

Cuando se propaga la onda electromagnética a través del medio la velocidad de propagación no es exactamente la misma a todas las frecuencias. El desfase es proporcional a la distancia recorrida; por otro lado el receptor será tanto más sensible al desfase cuanto mayor sea la velocidad con que se transmite la información. Por tanto el problema del desfase es mayor cuando se utiliza un canal con un gran ancho de banda para transmitir información a una gran velocidad y distancia. En muchos casos es posible transmitir a mayor distancia si se está dispuesto a reducir velocidad, e inversamente transmitir a mayor velocidad si se utiliza una distancia menor.

##### 3) Interferencia Electromagnética

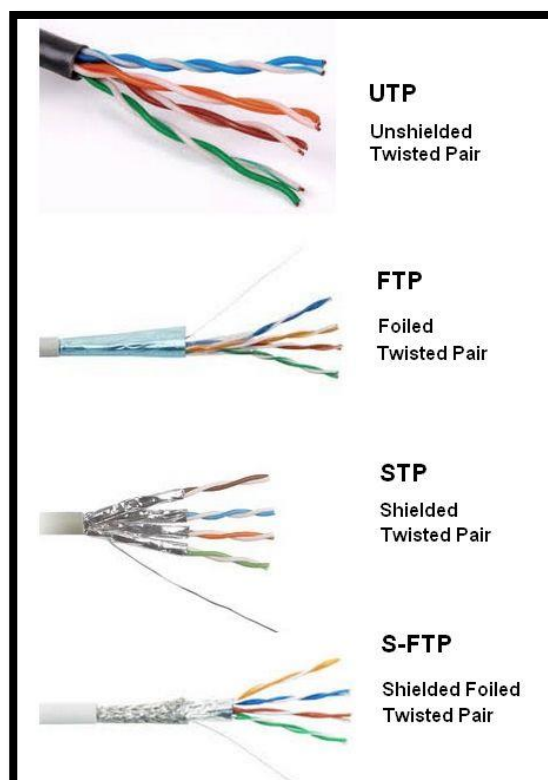
El cable de cobre es también susceptible de recibir interferencias electromagnéticas del ambiente. Esto puede alterar la señal correspondiente a los datos transmitidos hasta ser irreconocible. Este problema es menos grave en el caso del cable apantallado y raramente ocurre cuando se trata de cable coaxial.

Un tipo de interferencia electromagnética más difícil de evitar es el denominado crosstalk (diafonía), que es la interferencia se produce entre señales que discurren simultáneamente por cables paralelos. El crosstalk es el fenómeno conocido como 'cruce de líneas' que a veces se da en la red telefónica, produciendo que oigamos una segunda conversación a lo lejos mientras mantenemos una comunicación telefónica.

### 4.1.1. CABLE DE PARES

Este es el tipo de cable utilizado en la mayoría de las redes locales actuales y en el sistema telefónico. Consiste en un par de hilos de cobre aislados de alrededor de medio milímetro de diámetro. En las redes locales se utiliza casi siempre cable de cuatro pares. Los pares están trenzados entre sí formando una doble hélice, como una molécula de ADN, por lo que se le suele denominar cable de **pares trenzados o TP (Twisted Pair)**. De esta forma se reduce la interferencia eléctrica que reciben de fuentes próximas (por ejemplo de los pares vecinos) y la que pueden emitir al exterior.

Generalmente se utiliza el cable **UTP** (Unshielded Twisted Pair) que no está apantallado; más raramente se emplea cable apantallado, que se denomina **STP** (Shielded Twisted Pair); este cable es bastante voluminoso debido a la pantalla, lo cual encarece su precio y costo de instalación, por lo que existe una variante más barata en la que la pantalla está formada por papel de aluminio global en vez de por malla de cobre por cada par; así se consigue reducir considerablemente el precio y el diámetro del cable (parámetro que determina en buena medida el costo de instalación); a este cable se le conoce como **FTP**. El **S-FTP** es otra variante del anterior con una pantalla de malla adicional. Generalmente la atenuación disminuye (y el precio aumenta) a medida que mejora el apantallamiento del cable.



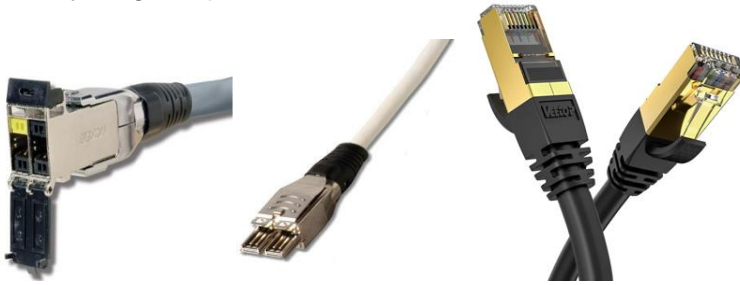
La frecuencia y el caudal máximos que se pueden transmitir por cable de pares depende de múltiples factores: el grosor del cable, la distancia, el tipo de aislamiento, la densidad de vueltas de trenzado, etc. Como ejemplos de su utilización podemos mencionar Gigabit Ethernet, que transmite 1 Gb/s por cuatro pares (250 Mb/s por cada par) a distancias de hasta 100m y ADSL que transmite 2 Mb/s por un solo par a distancias de hasta 5 Km.

En la siguiente tabla aparecen las categorías actualmente definidas o en curso de definición, y las frecuencias máximas correspondientes.

Categoría	Frecuencia máxima (MHz)	Vueltas/metro	Tipo cable	Tipo conector	Uso Ethernet (Mb/s)
1	No se especifica	0	UTP	RJ45	No se utiliza
2	1	0	UTP	RJ45	1
3	16	10-16	UTP	RJ45	10-100
4	20	16-26	UTP	RJ45	10-100
5/5e	100	26-33	UTP	RJ45	100-1000
6	250	?	UTP	RJ45	4000
7	600	?	SFTP	Nuevo	10000
7a	1000	?	SFTP	Nuevo	10000-40000
8	2000	?	SFTP	Nuevo	40000-

*Tabla 1 - Categorías de los cables de pares trenzados*

Base y latiguillo para los recientes cables categoría 7/7a (más gruesos que los RJ45), y latiguillo para cat8.



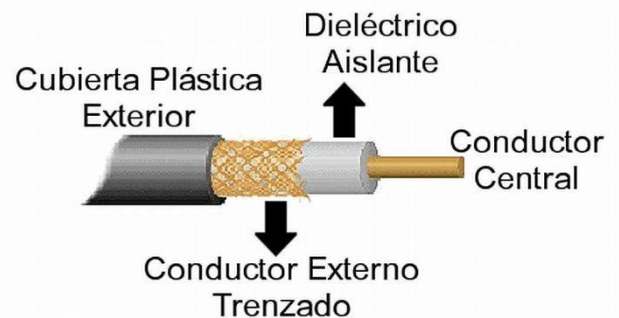
Las categorías 1 y 2 no forman parte de las normativas de cableado estructurado (composición de cables a partir de otros) y no se utilizan (de hecho no son UTP en sentido estricto, ya que carecen de trenzado). Para cableado estructurado actualmente están definidas las categorías 3, 4 y 5. El cable más utilizado hoy en día es el de categoría 5, ya que su costo es solo un poco superior al de las categorías 3 y 4 y tiene unas prestaciones muy superiores.

Actualmente están en desarrollo las normas 9 y 10 que alcanzarían 25 y 75GHz respectivamente.

#### 4.1.2. CABLE COAXIAL

El **cable coaxial** es otro medio de transmisión común. Su mejor apantallamiento le da una menor atenuación e inmunidad electromagnética, por lo que es más adecuado para grandes distancias y/o capacidades.

El cable coaxial está formado por un *núcleo de cobre* rodeado de un material aislante; el aislante está cubierto por una pantalla de material conductor, que según el tipo de cable y su calidad puede estar formada por una o dos mallas de cobre, un papel de aluminio, o ambos. Este material de pantalla está recubierto a su vez por otra capa de material aislante. El cable coaxial debe manipularse con cuidado ya que por ejemplo un golpe o doblez excesivo pueden producir una deformación en la malla que reduzca el alcance del cable.

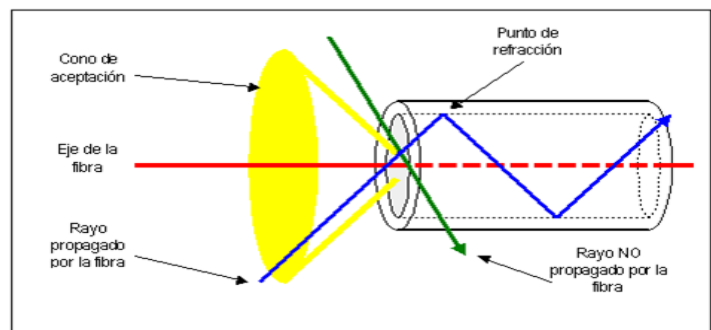
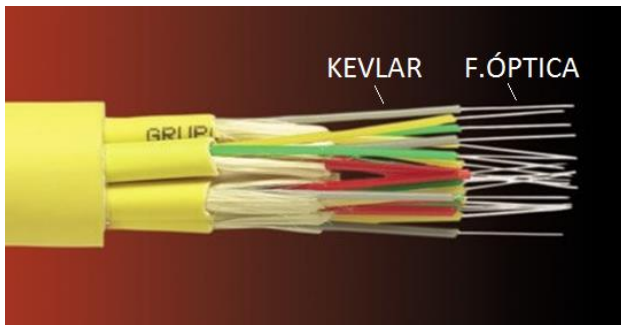


El cable coaxial más utilizado en la actualidad es el de **75  $\Omega$**  (Ohmios) de impedancia también llamado **cable coaxial de banda ancha**, que no es ni más ni menos que el cable coaxial de antena de televisión. Se emplea en comunicaciones telefónicas como nivel intermedio entre el cable de pares y la fibra óptica. También es la base de las redes de televisión por cable. En redes locales se utiliza en algunos casos cuando se quiere tener gran capacidad sin recurrir al uso de fibra óptica.



Por su construcción el cable coaxial tiene una alta inmunidad frente al ruido, y puede llegar a tener unos anchos de banda considerables. En distancias de hasta 1 Km es factible llegar a anchos de banda de 1 GHz y capacidades de hasta 5 Gb/s.

## 4.2. FIBRA ÓPTICA



El cable de fibra óptica está apantallado y reforzado por Kevlar (especie de nylon muy resistente) y otra serie de capas protectoras (al agua, al ruido eléctrico y al calor). Un mismo cable puede llevar hasta 200 fibras. No vamos a entrar en detalles técnicos de la composición y funcionamiento de la fibra óptica pero diremos que basa su funcionamiento en el fenómeno de la **reflexión total**: para conseguir que la luz que sale del emisor sea 'capturada' por la fibra hasta su destino y no se pierda por difusión hacia el exterior se aprovecha una propiedad de las ondas conocida como **reflexión**, consistente en que cuando una onda pasa de un medio con un índice de refracción a otro con índice menor, la onda es parcialmente reflejada hacia el primero, como si la superficie que separa ambos medios actuara como un espejo y quedando atrapada la onda en dicho medio.

Existen básicamente dos sistemas de transmisión de datos por fibras ópticas: los que utilizan **LEDs** (Light-Emitting Diode) y los que utilizan **diodos láser**:

- En los sistemas que utilizan **LEDs** la transmisión del pulso de luz (equivalente a un bit) genera múltiples rayos de luz al viajar por la fibra, pues se trata de luz normal no coherente; se dice que cada uno de estos rayos tiene un *modo* y la fibra que se utiliza para transmitir luz de emisores LED (luz no coherente) se denomina **fibra multimodo**.
- Por el contrario los **diodos láser** emiten luz coherente, generan un único rayo de luz y la fibra se comporta como un guía-ondas; la luz se propaga a través de la fibra en un solo modo, sin dispersión; por este motivo la fibra utilizada para luz láser se llama **fibra monomodo**. Las fibras monomodo se utilizan para transmitir a grandes velocidades y/o a grandes distancias.

Podemos comprender la diferencia en la propagación de la luz normal y la luz láser comparando el haz de luz generado por una linterna y el generado por un puntero láser; en la linterna el haz se abre en un cono más o menos ancho, mientras que en el puntero láser la apertura es prácticamente nula, es decir el haz mantiene la misma anchura independientemente de la distancia a la que se proyecte la luz.

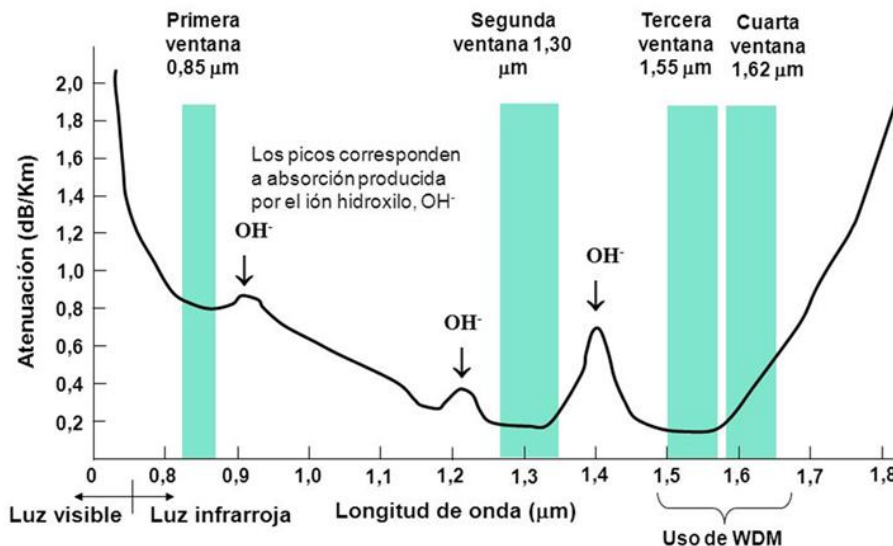
**Normalmente en redes locales (LAN)**, con distancias no superiores a 2 Km, se utilizan fibras multimodo con emisores LED. Estos equipos son más baratos que los láser, tienen una vida más larga, son menos sensibles a los cambios de temperatura y más seguros. A muy altas velocidades (por encima de 400-600 Mb/s) es necesario utilizar emisores láser, ya que los emisores de luz normal no pueden reaccionar con la rapidez suficiente. Por eso en algunas redes locales como Gigabit Ethernet se utilizan emisores láser cuando se quiere gran velocidad pero no se requiere gran alcance. Dado que los cableados de red local no disponen normalmente de fibra monomodo se ha extendido en los últimos años el uso de emisores láser en fibra multimodo.

**En redes de área extensa (WAN)** siempre se utiliza fibra monomodo y emisores láser. El mayor costo de los emisores se ve en este caso sobradamente compensado por la reducción en equipos intermedios (amplificadores y regeneradores de la señal).

Las tecnologías de red local (LAN) llegan a velocidades de transferencia de hasta 1 Gb/s sobre fibra óptica (Gigabit Ethernet por ejemplo). En redes de área extensa el mayor costo de la fibra estimula su mejor aprovechamiento, por lo que se llega actualmente a velocidades de 2,5 y 10 Gb/s.

La fibra monomodo es mucho más cara que la multimodo, esto es así porque a pesar de enviar un único rayo, su velocidad es ilimitada. La fibra multimodo es más utilizada porque es más barata y aunque puede enviar más “rayos” a la vez, el grosor del cable y la complejidad que implica tener más de gestionar más de un rayo simultáneamente limita su velocidad.

## Atenuación en fibra óptica según la longitud de onda



### 4.3. TRANSMISIÓN INALÁMBRICA

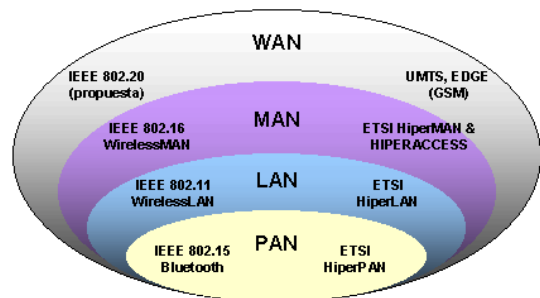
Hasta aquí hemos visto como las ondas eléctricas transmitidas por hilos de cobre, o las ondas luminosas transmitidas por fibras ópticas, nos permitían transportar bits. En realidad las ondas eléctricas y luminosas son dos tipos de ondas electromagnéticas. En las transmisiones inalámbricas se utiliza **el aire** para transmitir bits.

La agencia ETSI (European Telecommunications Standards Institute) definió **LAN/MAN/WAN** como el standard básico para redes inalámbricas.

Existen muchos tipos de transmisión inalámbrica: Infrarrojos, Radio, Microondas Terrestres, Microondas por Satélite... Los más comunes hoy en día son las redes:

- **WPAN** - Wireless Personal Area Network (802.15) ej: Bluetooth o RFID.
- **WLAN** (802.11) Wireless Local Area Network también conocido como Wi-Fi.
- **WMAN** (802.16) Wireless Metropolitan Area Network ej: Wi-Max (parecido a Wi-Fi pero de mayor cobertura)
- **WWAN** (802.20) Wireless Wide Area Network, ej: todas las tecnologías de telefonía móvil: GPRS, EDGE, HSPA, 3G, 4G, etc...

#### Posicionamiento de Estándares Wireless

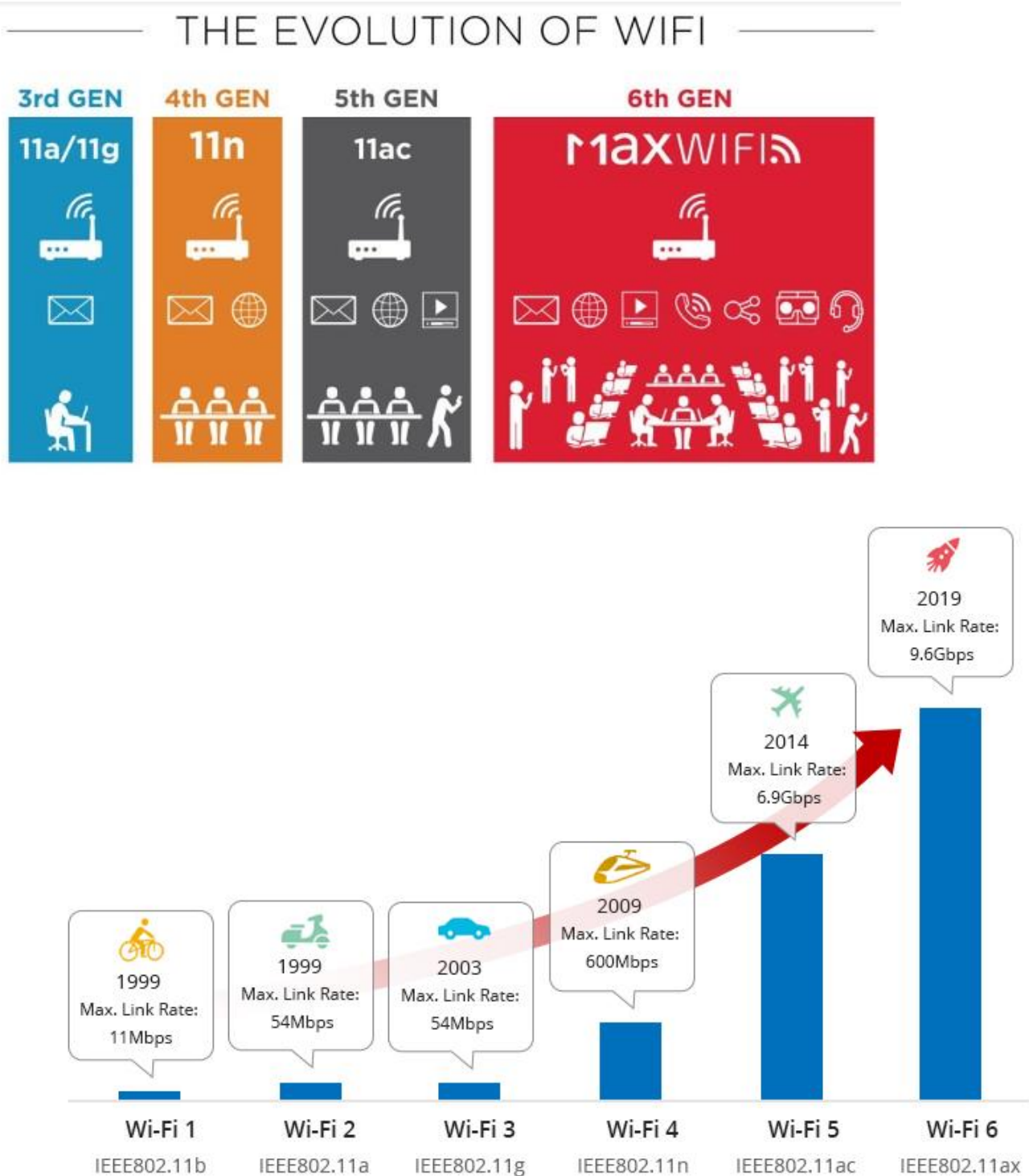




#### 4.4. REDES INALÁMBRICAS LAN (802.11) – WLAN O WIFI

El estándar básico es **802.11**, trabajando en una banda de frecuencia de 2.4GHz, tiene un ancho de banda de 20MHz y alcanza los 2Mb/s.

El resto de especificaciones vinieron después.



## 5. ARQUITECTURA DE RED

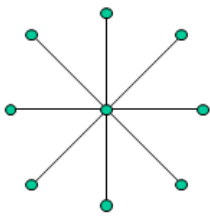
Hasta ahora hemos visto todos los elementos y tecnologías que conforman una red, pero todo esto ha de materializarse en "algo" que permita que todo funcione en conjunto de forma eficiente, ese algo es **una arquitectura de red**. A la arquitectura se le suele llamar también **modelo de referencia**.

Otro término asociado con la arquitectura de una red es la estructura, dicha estructura se refiere a la **topología** de la red.

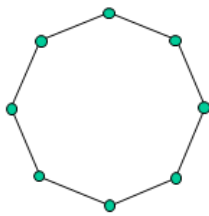
### 5.1. TOPOLOGÍA

La **topología** es la forma que tienen los distintos elementos interconectados de la red. Algunas formas más comunes:

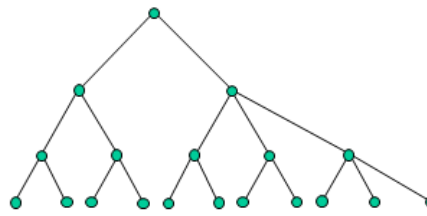
Algunas topologías típicas de redes punto a punto



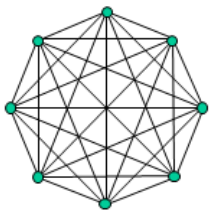
Estrella



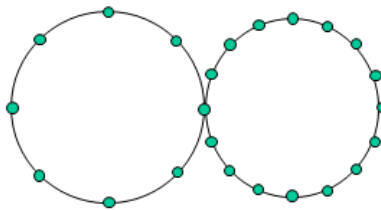
Anillo



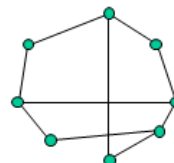
Estrella distribuida, árbol sin bucles o 'spanning tree'



Malla completa



Anillos interconectados



Topología irregular  
(malla parcial)

### 5.2. MODELOS DE REFERENCIA

Las dos arquitecturas de redes más importantes en la actualidad, corresponden a los protocolos **OSI** (Open Systems Interconnection, la cual es importante a nivel didáctico pero NO SE UTILIZA) y **TCP/IP** (Transmission Control Protocol/Internet Protocol).

Conviene destacar que la arquitectura es una entidad abstracta, más general que los protocolos o las implementaciones concretas en que luego se materializan éstos. Típicamente para cada capa de una arquitectura existirán uno o varios protocolos, y para cada protocolo habrá múltiples implementaciones. Las implementaciones cambian continuamente; los protocolos ocasionalmente se modifican o aparecen otros nuevos que coexisten con los anteriores o los dejan anticuados; sin embargo una vez definida una arquitectura ésta permanece esencialmente intacta y muy raramente se modifica.

### 5.2.1. EL MODELO DE REFERENCIA OSI

En los primeros días de las redes no existía una forma "estándar" de interconexión, ni en cuanto a nivel físico ni en cuanto a lógica interna de la red.

En 1977 la ISO (International Organization for Standardization) consideró que esta situación no era la más conveniente, por lo que entre 1977 y 1983 definió la arquitectura de redes OSI con el fin de promover la creación de una serie de estándares que especificaran un conjunto de protocolos independientes de cualquier fabricante.

El éxito de los protocolos OSI en la práctica ha sido mucho menor de lo inicialmente previsto (**sirvió como base a TCP/IP**, y en su momento los fabricantes se decidieron por la mayor simplicidad y eficiencia de éste último. Por otra parte los protocolos OSI tienen fallos que TCP/IP no tiene). Por tanto, **la importancia de OSI es para entender una arquitectura de RED dividida en niveles**.

El modelo OSI define siete capas:

- Física
- Enlace
- Red
- Transporte
- Sesión
- Presentación
- Aplicación

La ISO ha especificado protocolos para todas las capas, aunque algunos son poco utilizados. En función del tipo de necesidades del usuario no siempre se utilizan todas ellas. Algunos de los protocolos:

#### LA PILA OSI

**Nivel de Aplicación**  
Servicios de red a aplicaciones

**Nivel de Presentación**  
Representación de los datos

**Nivel de Sesión**  
Comunicación entre dispositivos de la red

**Nivel de Transporte**  
Conexión extremo-a-extremo y fiabilidad de los datos

**Nivel de Red**  
Determinación de ruta e IP (Direccionamiento lógico)

**Nivel de Enlace de Datos**  
Direccionamiento físico (MAC y LLC)

**Nivel Físico**  
Señal y transmisión binaria

Tecnologías y protocolos de red (modelo OSI)	
Nivel de aplicación	DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, Telnet, SIP
Nivel de presentación	ASN.1, MIME, SSL/TLS, XML
Nivel de sesión	NetBIOS, Session Description Protocol
Nivel de transporte	SCTP, SPX, TCP, UDP
Nivel de red	AppleTalk, IP, IPX, NetBEUI, X.25
Nivel de enlace	ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi, STP
Nivel físico	Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232



## LA CAPA FÍSICA

---

Esta capa transmite los **bits** entre dos entidades (nodos) directamente conectadas. Puede tratarse de un enlace punto a punto o de una conexión multipunto (una red broadcast, por ejemplo Ethernet). La comunicación puede ser dúplex, semi-dúplex o simplex. Si la información se transmite por señales eléctricas se especifican los voltajes permitidos y su significado (1 o 0) y análogamente para el caso de fibra óptica. Se especifican las características mecánicas del conector, la señalización básica, etc.

## LA CAPA DE ENLACE (DATA LINK)

---

La principal función de la capa de enlace es ofrecer un servicio de comunicación fiable a partir de los servicios que recibe de la capa física, también entre dos entidades contiguas de la red. Esto supone que se realice detección y posiblemente corrección de errores. A diferencia de la capa física, que transmitía los bits de manera continua, la capa de enlace transmite los bits en grupos denominados **tramas** (frames en inglés) cuyo tamaño es típicamente de unos pocos cientos a unos pocos miles de bytes. En caso de que una trama no haya sido transmitida correctamente se deberá enviar de nuevo; también debe haber mecanismos para reconocer cuando una trama se recibe duplicada. Generalmente se utiliza algún mecanismo de control de flujo, para evitar que un transmisor rápido pueda 'abrumar' a un receptor lento.

Las redes broadcast utilizan funciones especiales de la capa de enlace para controlar el acceso al medio de transmisión, ya que éste es compartido por todos los nodos de la red. Esto añade una complejidad a la capa de enlace que no está presente en las redes basadas en líneas punto a punto, razón por la cual en las redes broadcast la capa de enlace se subdivide en dos subcapas: la inferior, denominada subcapa MAC (Media Access Control) se ocupa de resolver el problema de acceso al medio, y la superior, subcapa LLC (Logical Link Control) cumple una función equivalente a la capa de enlace en las líneas punto a punto.

Como **ejemplos de protocolos** de la subcapa MAC podemos citar los **IEEE 802.3** (Ethernet), **IEEE 802.5** (Token Ring), el ISO 9314 (**FDDI**) o el 802.11 (**Wi-Fi**). El protocolo de subcapa LLC de todas las redes locales broadcast es el IEEE 802.2.

## LA CAPA DE RED

---

La capa de red se ocupa del control de la subred. Esta es la capa que tiene 'consciencia' (sabe que existe) de la topología de la red, y **se ocupa de decidir por qué ruta va a ser enviada la información**; la decisión de la ruta a seguir puede hacerse de forma estática, o de forma dinámica en base a información obtenida de otros nodos sobre el estado de la red.

De forma análoga a la capa de enlace la capa de red maneja los bits en grupos discretos que aquí reciben el nombre de **paquetes**; motivo por el cual a veces se la llama la capa de paquete. Los paquetes tienen tamaños variables, pudiendo llegar a ser muy elevados, sobre todo en protocolos recientes, para poder aprovechar eficientemente la elevada velocidad de los nuevos medios de transmisión (fibra óptica, etc.). Por ejemplo en TCP/IP el tamaño máximo de paquete es de 64 KBytes, pero en el nuevo estándar, llamado IPv6, el tamaño máximo puede llegar a ser de 4 GBytes (4.294.967.296 Bytes).

Entre las funciones de la capa de red cabe destacar, aparte de la ya mencionada de elegir la ruta a seguir, el **control del tráfico** para evitar situaciones de congestión o 'atascos'.

Algunos **ejemplos de protocolos** utilizados en la capa de red son los protocolos **X.25**, el **IP** (Internet Protocol) o el **AppleTalk** (protocolo de red para redes Macintosh)

En las redes de tipo broadcast el nivel de red es casi inexistente, ya que desde un punto de vista topológico podemos considerar que en una red broadcast los nodos están interconectados todos con todos, por lo que no se toman decisiones de encaminamiento. Sin embargo veremos que la unión de redes

broadcast mediante puentes suscita en algunos casos la necesidad de efectuar tareas propias del nivel de red en el nivel de enlace.

## LA CAPA DE TRANSPORTE

---

La capa de transporte es **la primera que se ocupa de comunicar directamente nodos terminales**, utilizando la subred como un medio de transporte transparente gracias a los servicios obtenidos de la capa de red. Por esta razón se la ha llamado históricamente la capa host-host.

La principal función de la capa de transporte es fragmentar de forma adecuada los datos recibidos de la capa superior (sesión) para transferirlos a la capa de red, y asegurar que los fragmentos llegan y son recompuestos correctamente en su destino.

El control de flujo, que ha aparecido en capas anteriores, es necesario también en la capa de transporte para asegurar que un host rápido no satura a uno lento. La capa de transporte realiza también su propio control de errores, que resulta ahora esencial pues algunos protocolos modernos han reducido o suprimido totalmente el control de errores de las capas inferiores, ya que con las mejoras en la tecnología de transmisión de datos éstos son menos frecuentes y se considera más adecuado realizar esta tarea en el nivel de transporte.

Salvo el caso de transmisiones multicast o broadcast el nivel de transporte se ocupa siempre de una comunicación entre dos entidades, lo cual le asemeja en cierto sentido al nivel de enlace. Por esto existen grandes similitudes entre ambas capas en cuestiones tales como el control de errores o control de flujo.

En Internet existen dos **protocolos de transporte**: TCP y UDP. Los veremos más adelante.

## LA CAPA DE SESIÓN

---

Esta capa **gestiona, establece o finaliza las conexiones entre usuarios finales**. Así pues, ha de asegurar que una vez establecida la sesión se ejecute el servicio para el que se estableció dicha sesión, reanudándola en caso de error. Mantiene el "enlace" entre las dos máquinas. Por ejemplo, mediante los servicios de la capa de sesión un usuario podría establecer una conexión como terminal remoto de otro ordenador.

Ej de protocolo: NetBIOS

## LA CAPA DE PRESENTACIÓN

---

Hasta aquí nos hemos preocupado únicamente de intercambiar bits (o Bytes) entre dos usuarios ubicados en dos ordenadores diferentes. Lo hemos hecho de manera fiable y entregando los datos a la sesión, es decir al usuario, pero sin tomar en cuenta el significado de los bits transportados.

La capa de presentación se ocupa de **realizar las conversiones necesarias para asegurar que dichos bits se presentan al usuario de la forma esperada**. Por ejemplo, si se envía información alfanumérica de un ordenador ASCII a uno EBCDIC será preciso efectuar una conversión, o de lo contrario los datos no serán interpretados correctamente. Lo mismo podríamos decir de la transferencia de datos enteros, flotantes, etc. cuando la representación de los datos difiere en los ordenadores utilizados.

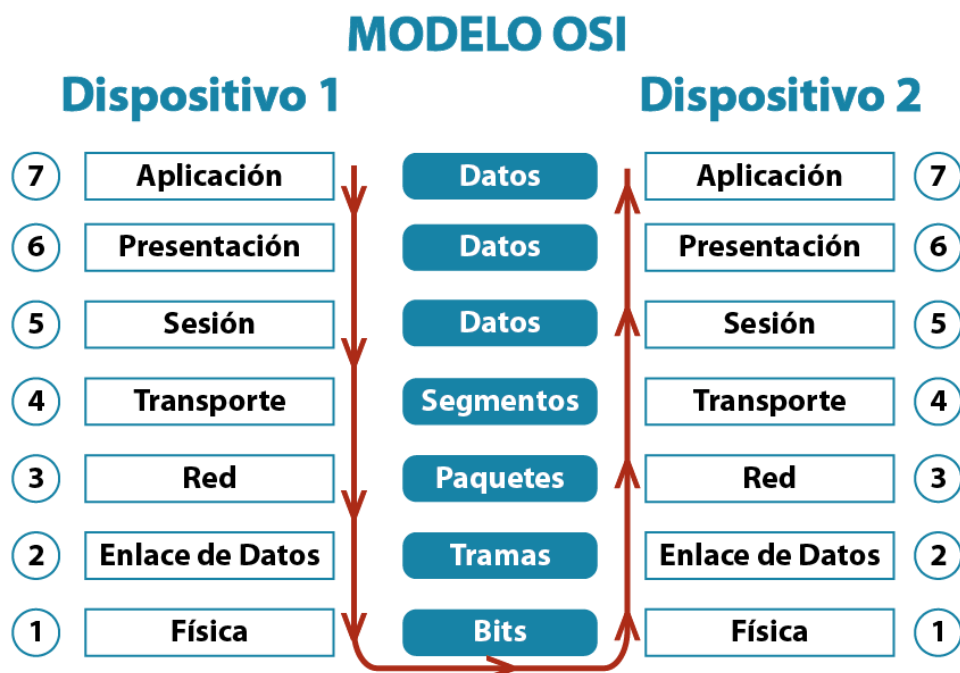
Ej de protocolo: MIME o XML

## LA CAPA DE APLICACIÓN

La capa de aplicación comprende los servicios que el usuario final está acostumbrado a utilizar en una red telemática, por lo que a menudo los protocolos de la capa de aplicación se denominan **servicios**. Dado que se crean continuamente nuevos servicios, existen muchos protocolos para la capa de aplicación, uno o más por cada tipo de servicio.

**Ejemplos de protocolos** estándar de la capa de aplicación: **SMTP**, **FTP** y **HTTP** de Internet, etc.

## TRANSMISIÓN DE DATOS EN EL MODELO OSI (RESUMEN)



### 5.2.2. EL MODELO DE REFERENCIA TCP/IP

La familia de protocolos de Internet (TCP/IP) es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre ordenadores .

- La capa host-red o de acceso a red
- La capa internet
- La capa de transporte
- La capa de aplicación



### LA CAPA HOST-RED

Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP no dice gran cosa respecto a ella, salvo que debe ser capaz de conectar el host a la red por medio de algún protocolo que permita enviar paquetes IP. Podríamos decir que para el modelo TCP/IP esta capa se comporta como una 'caja negra'. Cuando surge una nueva tecnología de red una de las primeras cosas que aparece es un estándar que especifica de qué forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa internet ya puede utilizar esa tecnología de manera transparente.

### LA CAPA INTERNET

Esta capa es el 'corazón' de la red. Su papel equivale al desempeñado por la capa de red en el modelo OSI, es decir, se ocupa de **encaminar los paquetes de la forma más conveniente** para que lleguen a su destino, y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa internet da únicamente un servicio de conmutación de paquetes no orientado a conexión. Los paquetes pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados al usuario de forma adecuada.

A diferencia de lo que ocurre en el modelo OSI, donde los protocolos para nada intervienen en la descripción del modelo, la capa internet define aquí un formato de paquete y un **protocolo, llamado IP (Internet Protocol)**, que se considera el protocolo 'oficial' de la arquitectura.

## LA CAPA DE TRANSPORTE

Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (host a host) en la red. Aquí se definen dos **protocolos**:

1. El **TCP** ('*Transmission Control Protocol*') ofrece un servicio **CONS** (fiable), con lo que los paquetes (aquí llamados **segmentos**) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar que por ejemplo un host rápido sature a un receptor más lento. Ejemplos de **protocolos de aplicación** que utilizan TCP (no quiere decir que sean protocolos de transporte) son el **SMTP** (Simple Mail Transfer Program, correo electrónico) y el **FTP** (File Transfer Protocol).
2. El **UDP** ('*User Datagram Protocol*') que da un servicio **CLNS** (no fiable). UDP no realiza control de errores ni de flujo. Una aplicación típica donde se utiliza UDP es la transmisión de voz y vídeo en tiempo real; aquí el retardo que introduciría el control de errores produciría más daño que beneficio: es preferible perder algún paquete que retransmitirlo fuera de tiempo. Otro ejemplo de **protocolo de aplicación** que utiliza UDP (no quiere decir que sean protocolos de transporte) es el **NFS** (Network File System); aquí el control de errores y de flujo se realiza en la capa de aplicación.

## LA CAPA DE APLICACIÓN

Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La experiencia ha demostrado que las capas de sesión y presentación son de poca utilidad, debido a su escaso contenido, por lo que la aproximación adoptada por el modelo TCP/IP parece más acertada.

La capa de aplicación contiene todos los **protocolos de alto nivel** que se utilizan para ofrecer servicios a los usuarios. Entre estos podemos mencionar tanto los 'tradicionales', que existen desde que se creó el TCP/IP: terminal virtual (**TelNet**), transferencia de ficheros (**FTP**), correo electrónico (**SMTP**) y servidor de nombres (**DNS**), como los más recientes, como el servicio de news (**NNTP**), el Web (**HTTP**), el Gopher, etc.

Para entender todo esto mejor vamos a ver un video sobre el modelo.

### 5.2.3. COMPARATIVA OSI-TCP/IP

- En OSI primero fue el modelo, después los protocolos; en TCP/IP primero fueron los protocolos, luego el modelo
- En OSI el modelo es bueno, los protocolos malos (muchos errores); en TCP/IP ocurre al revés
- En OSI los productos llegaban tarde, eran caros y tenían muchos fallos.
- En TCP/IP los productos aparecían rápido, estaban muy probados (pues los usaba mucha gente), y a menudo eran gratis. Esto es debido a la política que se siguió, con OSI había intereses políticos, con TCP/IP se seguía una filosofía de desarrollo LIBRE.
- Las redes broadcast no se tuvieron en cuenta inicialmente para OSI, hubo que incluir una capa MAC que dificultaba el diseño.

#### Recurso

Vídeo de Moodle: Modelo TCP-IP (6 minutos)



## 6. DISPOSITIVOS DE RED

De forma normal los dispositivos de red que podemos encontrarnos son los siguientes:

### REPETIDOR

Debido a los problemas de atenuación de ciertos medios de transmisión, se necesita algo que repita la señal. Trabaja en el **nivel 1 o físico**.



### HUB

Permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Ya no se usan, debido al gran nivel de colisiones y tráfico de red que propician. Son concentradores "tontos" (reenvía a todos). Trabaja en el **nivel físico**.



### SWITCH

Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (**nivel de enlace**) del modelo OSI. Funciona como un "HUB inteligente", no hay tantas colisiones porque se envían los datos a un destinatario determinado.

Un conmutador interconecta dos o más segmentos de red (**IGUALES**, es decir, **misma TOPOLOGÍA**) fusionándola en una sola, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs.



### PUENTE

Los puentes realizan la interconexión de redes LAN a nivel de la capa 2 (**nivel de enlace**). La diferencia con los switches es que interconectan redes del mismo o de distinto tipo (distinta topología). Por ejemplo, podríamos fusionar una Token Ring con una Token Bus.



### ROUTER

En español, enrutador o encaminador. Es un dispositivo de hardware para interconexión de redes de ordenadores que opera en la capa 3 (**nivel de red**). Es como un "switch inteligente" porque además de hacer todo lo que puede hacer un switch tiene capacidad de enrutar. Se usa para redes que son iguales en las capas superiores pero no tiene por qué ser igual en las inferiores. Por ejemplo, con un router nos conectamos a internet, nosotros podemos tener una Ethernet y nos estamos conectando a una red punto a punto donde las capas inferiores seguramente son distintas, no así las superiores.



### GATEWAY

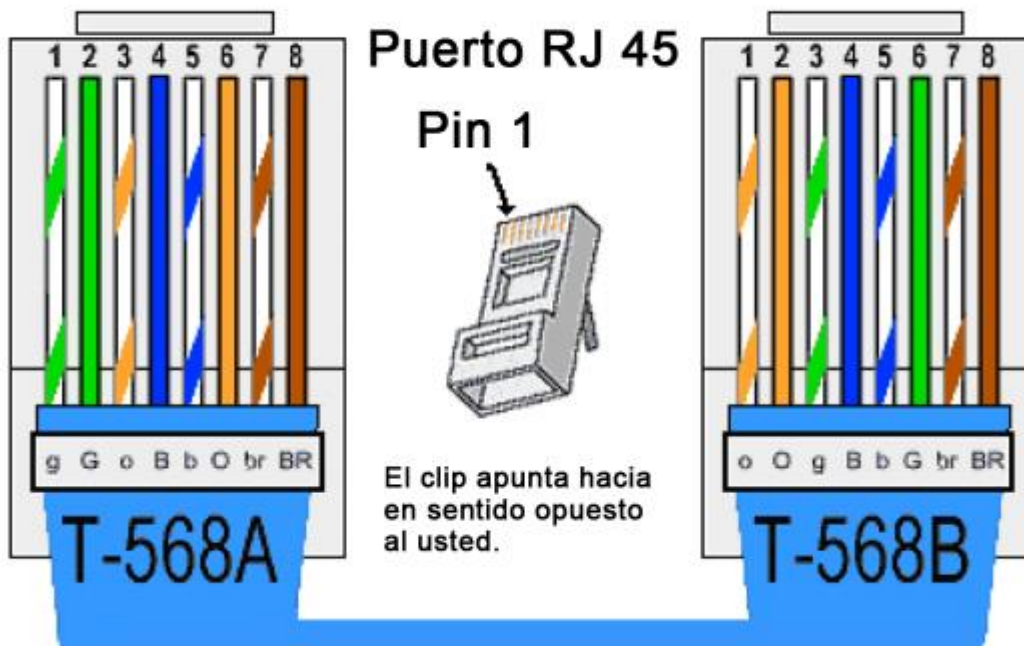
Un **gateway** (puerta de enlace) es una especie de "router", es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.



## 7. CABLES DE RED

Hay dos tipos principales de cables de red, los **directos** y los **cruzados**. Los primeros son los que conectan el PC con el dispositivo de red (hub, router, etc). Los cruzados se utilizan para conectar dos PCs de forma directa. Para hacerlos se utiliza una crimpadora.

### Cable de conexión cruzada Ethernet RJ 45



#### TAREA

Curso Packet Tracer Skills For All. Partes 1, 2 y 3

## 8. PROTOCOLO IP

**IP (Internet Protocol) es el protocolo de TCP/IP que trabaja a nivel de red.** Es un protocolo sin conexión, por tanto, carece de seguridad en la entrega de paquetes. Cuando la transmisión necesita seguridad ésta debe ser proporcionada por un protocolo de un nivel superior en nuestro caso TCP.

IP es el protocolo base para las transferencias de datos en Internet, y por extensión en la mayoría de las redes actuales. Existen dos versiones: IPv4 y IPv6 (No vamos a entrar a verlos en detalle, simplemente decir que IPv4 usa direcciones de 32bits y es el que se utiliza en la actualidad, IPv6 utiliza direcciones de 64bits. Los paquetes IP contienen muchos datos, además del origen y destino)

### 8.1. DIRECCIONAMIENTO IPV4

- Los campos dirección origen y dirección destino en la cabecera IP contienen, cada uno, una dirección de 32 bits agrupados en grupos de 8 bits (de ahí que se expresen con 4 números decimales separados por puntos X.X.X.X).
- Ej: 11000000.11100100.00010001.00111001 se escribe como 192.228.17.57.

138.

4

. 54

. 3

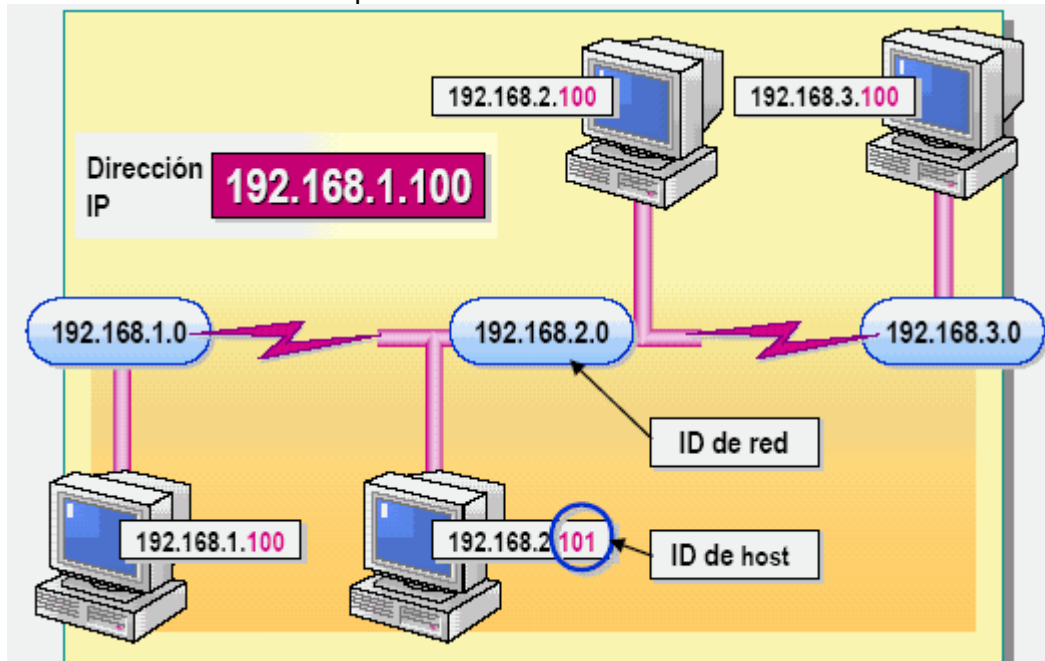
10001010

00000100

00110110

00000011

- Cada uno de estos números varía entre 0 y 255 ( $2^8-1$ ), aunque hay algunas restricciones. (Existen direcciones reservadas Ej: 0.0.0.0 de multidifusión)
- La dirección IP de un host permite identificarlo de forma unívoca dentro de la red.



### 8.2. CLASES DE REDES

- Cada dirección IP codifica una red y un host dentro de esa red.



- ◆ El número de bits de la dirección que se destinan a la identificación de la red y a la identificación del host dentro de dicha red puede variar de unos casos a otros (depende de la clase de red).
- ◆ En general, observando los primeros bits (empezando por la izquierda) de cada dirección, se averigua el tipo de red de que se trata (en cuánto al nº Máximo de hosts que puede albergar) y su dirección concreta.
- ◆ Los bits restantes codifican el host de que se trata dentro de esa red.
- ◆ Fundamentalmente hay tres tipos de redes: clase A, clase B y clase C.

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
<b>A</b>	<b>0.0.0.0</b>	<b>127.255.255.255</b>	<b>128*</b>	<b>16.777.214</b>	<b>Redes grandes</b>
<b>B</b>	<b>128.0.0.0</b>	<b>191.255.255.255</b>	<b>16.384</b>	<b>65.534</b>	<b>Redes medianas</b>
<b>C</b>	<b>192.0.0.0</b>	<b>223.255.255.255</b>	<b>2.097.152</b>	<b>254</b>	<b>Redes pequeñas</b>
<b>D</b>	<b>224.0.0.0</b>	<b>239.255.255.255</b>	<b>no aplica</b>	<b>no aplica</b>	<b>Multicast</b>
<b>E</b>	<b>240.0.0.0</b>	<b>255.255.255.255</b>	<b>no aplica</b>	<b>no aplica</b>	<b>Investigación</b>

\* El intervalo **127.0.0.0** a **127.255.255.255** está reservado como dirección loopback y no se utiliza.

### 8.2.1. CLASE A

- Pocas redes, cada una con muchos hosts.
- El primero de los 32 bits que tiene cada dirección es un 0 (el que está más a la izquierda).
- Los siete bits siguientes codifican la red y los 24 restantes la identificación del host dentro de esa red.
- Los valores posibles para la red varían entre 1 (el valor de los 8 primeros bits sería 00000001) y 126 (el valor de los 8 primeros bits sería 01111110).
- Hay  **$(2^7-2)= 126$  redes** posibles de tipo A (no se usan ni la 0.0.0.0 ni la 127.0.0.0) . Cada una de ellas puede contener  **$(2^{24}-2)= 16.777.214$  hosts** distintos.
- Este sistema de direccionamiento se utiliza, por tanto, para redes de grandes dimensiones.

### 8.2.2. CLASE B

- Un número medio de redes, cada una con un número medio de computadores.
- Los dos primeros bits de la dirección son 10.
- Los 14 bits siguientes codifican la red, los 16 restantes los hosts.
- Los valores para el primer byte de la dirección van desde 128 (el valor para los 8 primeros bits sería 10000000) a 191 (el valor para los 8 primeros bits sería 10111111).
- Teniendo en cuenta lo de antes, son posibles  **$2^{14}-2=16.384$  redes** de tipo B (desde la de dirección 128.0.0.0 a la de dirección 191.255.0.0)
- Cada una de estas redes puede contener  **$2^{16}-2 =65.534$  hosts** distintos, los codificados por los 16 bits restantes del campo de dirección.

### 8.2.3. CLASE C

- Muchas redes, cada una con pocos computadores.
- Los tres primeros bits tienen el valor 110.
- Los 21 bits siguientes codifican la red y los 8 restantes el host dentro de la red.
- El primer byte tiene un valor comprendido entre 192 (el valor para los 8 primeros bits sería 11000000) y 223 (el valor para los 8 primeros bits sería 11011111) .
- Es posible codificar  **$(2^{21}-2)= 2.097.152$  redes** distintas de  **$(2^8-2)= 254$  hosts** diferentes cada una.

### 8.2.4. CLASES ESPECIALES

- Clase D: Empieza con 1110, se entiende que los 28 bits restantes codifican una dirección de multidifusión, es decir, una dirección especial en donde no hay un único destinatario (sino varios que pueden pertenecer incluso a redes distintas).
- Clase E: Empieza con 11110, se reserva para protocolos especiales y futuras implementaciones.

### 8.3. MÁSCARAS DE RED DE CLASES MÁS UTILIZADAS

N indica los bits para la red (N=Net), H los bits para equipos (Host=Equipo):

**Clase A :** N.H.H.H

11111111.00000000.00000000.00000000

Máscara de subred por default para clase A es 255.0.0.0

**Clase B :** N.N.H.H

11111111.11111111.00000000.00000000

Máscara de subred por default para clase B es 255.255.0.0

**Clase C :** N.N.N.H

11111111.11111111.11111111.00000000

Máscara de subred por default para clase C es 255.255.255.0

Cualquier máscara que no sea una de estas 3 me está diciendo que se está usando subnetting o supernetting.

### 8.4. REDES PRIVADAS - DIRECCIONES IP PRIVADAS

Tenemos que distinguir entre las **direcciones IP Públicas** (las vistas más arriba) y las **direcciones IP Privadas**, estas últimas se utilizan para comunicaciones dentro de una intranet. Existen rangos de direcciones que NO se pueden utilizar para IP Públicas, se usan solamente para asignar direcciones dentro de redes locales:

Rangos Redes Locales	
Desde	Hasta
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

La **máscaras de red en una subred privada se pueden restringir para usar menos direcciones de las que nos permite dicha red**. Por ejemplo, si cogemos una clase de Tipo B y no queremos manejar 65.535 direcciones, pongamos que solamente 200 para host podemos hacer lo siguiente: en vez de usar la máscara original 255.255.0.0, la restringimos a 255.255.255.0, con lo que estamos "desaprovechando" Ips, pero es que tampoco nos hacen falta más. De esta forma tendremos 254 hosts en una Intranet privada pero usando una clase tipo B. El rango es más limitado y controlable. Un ejemplo de esto que se comenta se daría en la subred de profesores:

Red	Desde	Hasta	Máscara de subred
Administrativa	10.0.0.0	10.0.0.255	255.255.255.0
Profesores	172.16.0.0	172.16.0.255	255.255.255.0
Alumnos	192.168.0.0	192.168.0.255	255.255.255.0

## 9. SUBNETTING, SUBREDES Y MÁSCARAS DE RED

### 9.1. La Máscara De Subred

Puesto que, por definición, a cada clase le corresponde una máscara, siempre que configuramos nuestro ordenador con la IP, éste es capaz de mostrar la máscara automáticamente, con lo que es bastante normal que no nos preguntemos para qué sirve esta máscara.

En un entorno doméstico en el que apenas hay unos pocos hosts (ordenador, portátil, teléfonos móviles), no parece importante ir más allá con las subredes, con lo que nos bastará con una máscara estándar de red de clase C 255.255.255.0 que es la habitual. De este modo, en casa podremos tener un máximo de 254 equipos en una misma red.

```

      255      255      255      0
Clase C 11111111.11111111.11111111.00000000
      [          red          ].[ hosts]
      255      255      255      192
      11111111.11111111.11111111.11000000
      [          red          ] sr[hosts]

```

### 9.2. Subnetting

Dividir una dirección en varias subredes es lo que se conoce como **SUBNETTING**. ¿Para qué sirve? Pues para de forma manual o automática (mediante servidores DHCP) asignar direcciones dentro de un rango para dividir una LAN en distintas SUB-LANs.

En caso de que lo que queramos sea por ejemplo administrar una oficina que esté dividida en varios departamentos y que formen redes independientes, necesitaremos utilizar la máscara de subred o diferentes enrutadores para separar las redes.

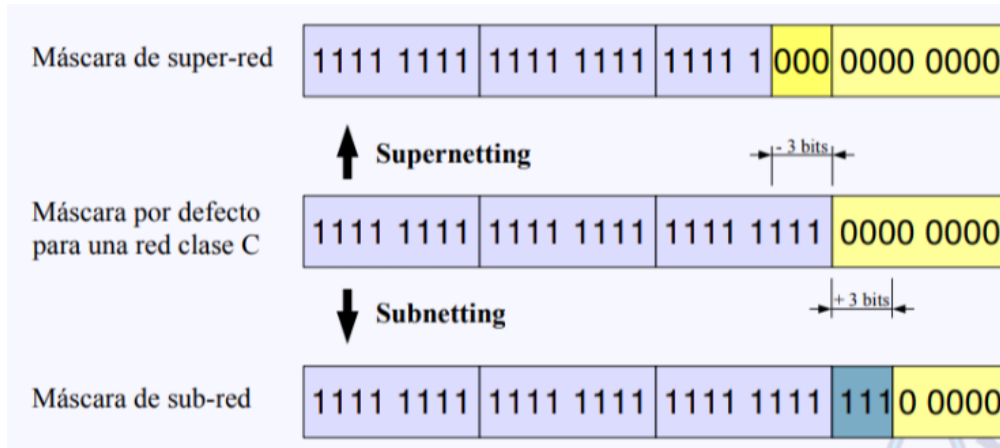
Una subred dentro de una red se configura "tomando" bits de la parte de los hosts. Por ejemplo:



En este caso hemos tomado "prestados" dos bits de la zona hosts, de tal modo que podemos crear  $2^2 = 4$  subredes, permitiendo la existencia de, por ejemplo, 4 departamentos separados cuyos ordenadores no podrían verse entre sí. El número de IPs disponibles para hosts quedaría en  $2^6 - 2 = 62$ . Restamos 2 porque la primera dirección corresponde con la dirección de red y la última es la dirección de multidifusión.

### 9.3. Supernetting

De la misma forma que existe el subnetting, está el supernetting que consiste en coger bits de la parte de la red para tener más hosts disponibles. De esta forma podemos encontrarnos una dirección de clase C (ej: 192.168.7.29) con lo que parece que es una máscara de clase B (255.255.248.0), pero en realidad se está utilizando una super-red (tomando 3 bits extra). En este caso podríamos tener  $(2^{8+3}-2)= 2046$  hosts:



### 9.4. Ejemplo Real - Subnetting

Vamos a crear una red local con 3 departamentos separados entre sí. Diseñaremos una tabla con todas las direcciones:

En primer lugar, elegimos la clase de la red que vamos a preparar. Para este caso y sabiendo que se trata de una red local pequeña, elegimos una **clase C**, por ejemplo 192.168.1.0 (**Podríamos haber elegido cualquier red PRIVADA entre 192.168.1.0 y 192.168.255.0. El último número (0) NO se puede usar dado que son los 8 bits de clase C que NO podemos “tocar”. También se suele denotar con una X aquellos bits que NO podemos tocar: 192.168.1.X y 192.168.255.X. Lo que es importante es entender que en una red de clase C no se podrán tener más de 256 direcciones ( y 254 HOST).**

192.168.1.0 al ser de clase C obligatoriamente tiene la máscara → 255.255.255.0

Para montar 3 subredes se requieren 2 bits =  $2^2 = 4$  totales, de las que usaremos 3.

Pasamos la máscara a binario:

255.255.255.0 = 11111111.11111111.11111111.00000000

Tomamos dos bits de la parte hosts:

11111111.11111111.11111111.11000000 = 255.255.255.192

En esta ocasión no necesitamos saber a qué subred pertenece la dirección IP 192.168.1.0, pero si fuera necesario porque no lo hemos ubicado, **haríamos una multiplicación (AND)** de la dirección por la máscara de subred:

```
11000000.10101000.00000001.00000000 -> 192.168.1.0
11111111.11111111.11111111.11000000 -> 255.255.255.192
-----
11000000.10101000.00000001.00000000 -> 192.168.1.0
```

Ejemplo, ¿A qué subred pertenecería el Host 192.168.1.8?

11000000.10101000.00000001.00001000 -> 192.168.1.8  
 11111111.11111111.11111111.11000000 -> 255.255.255.192

-----  
 11000000.10101000.00000001.00000000 -> 192.168.1.0 , es decir, también pertenece a la primera subred.

Bien, ahora, tomando 2 bits para la subred tenemos que las direcciones de las posibles subredes son:

11000000.10101000.00000001.00000000 -> **192.168.1.0/26**  
 11000000.10101000.00000001.01000000 -> **192.168.1.64/26**  
 11000000.10101000.00000001.10000000 -> **192.168.1.128/26**  
 11000000.10101000.00000001.11000000 -> **192.168.1.192/26**

(Vemos que su dirección se obtiene poniendo a cero todos los bits correspondientes a host. Nomenclatura en **formato CIDR: X.X.X.X/bits de mascara**)

Para obtener el **primer host de cada subred**, ponemos todos los bits de la parte de host a 0 excepto el último:

11000000.10101000.00000001.00000001 -> 192.168.1.1  
 11000000.10101000.00000001.01000001 -> 192.168.1.65  
 11000000.10101000.00000001.10000001 -> 192.168.1.129  
 11000000.10101000.00000001.11000001 -> 192.168.1.193

Para obtener la dirección del **último host**, ponemos todos los bits de la parte host a 1, excepto el último, que será 0:

11000000.10101000.00000001.00111110 -> 192.168.1.62  
 11000000.10101000.00000001.01111110 -> 192.168.1.126  
 11000000.10101000.00000001.10111110 -> 192.168.1.190  
 11000000.10101000.00000001.11111110 -> 192.168.1.254

Para obtener la dirección de **multidifusión o broadcast**, ponemos a 1 todos los bits de host:

11000000.10101000.00000001.00111111 -> 192.168.1.63  
 11000000.10101000.00000001.01111111 -> 192.168.1.127  
 11000000.10101000.00000001.10111111 -> 192.168.1.191  
 11000000.10101000.00000001.11111111 -> 192.168.1.255

Y para poder entender “de modo humano” todos estos bits, los pasamos a decimal y obtenemos la tabla de subredes (el **/n** índice el número de bits utilizados para equipos):

Dpto.	Subred	Hosts	Broadcast	Máscara
1o	192.168.1.0/26	192.168.1.1 a 192.168.1.62	192.168.1.63	255.255.255.192
2o	192.168.1.64/26	192.168.1.65 a 192.168.1.126	192.168.1.127	255.255.255.192
3o	192.168.1.128/26	192.168.1.129 a 192.168.1.190	192.168.1.191	255.255.255.192
4o	192.168.1.192/26	192.168.1.193 a 192.168.1.254	192.168.1.255	255.255.255.192

Usando esta tabla podremos ubicar cualquier host en cualquiera de las subredes sin necesidad de hacer nuevos cálculos. Se trataría, pues, de un mapa ideal de nuestra red local.

Por ejemplo, para instalar un ordenador nuevo en el tercer departamento, podríamos elegir cualquier dirección IP entre la 192.168.1.129 y la 192.168.1.190 que esté disponible. Este ordenador sólo podría ver ordenadores de su subred correspondiente, de tal modo que cada departamento comparte recursos sólo con ordenadores que forman parte de esa subred.

Así, mediante el uso de máscaras de red, podremos diseñar cualquier tipo de red en nuestra casa u oficina. Por supuesto, esta tarea sencilla se puede convertir en un auténtico quebradero de cabeza cuando se trata de grandes empresas con cientos de hosts divididos en muchos departamentos, pero los cálculos que se realizan son los mismos. Si planteamos correctamente la red desde el principio, después será mucho más fácil ubicar equipos en los departamentos o redes que nos interesen.

### Ejercicios para practicar:

- A partir de la dirección de clase C 192.168.1.X/24, montar 2 subredes, indicando direcciones de subred, hosts, broadcast y máscara.
- A partir de la dirección de clase C 192.168.5.X/24 montar 6 subredes, indicando direcciones de subred, hosts, broadcast y máscara.
- A partir de la dirección de clase B 172.20.100.X/24 montar 3 subredes, indicando direcciones de subred, hosts, broadcast y máscara (restringimos la máscara a 24 bits para usar 256 direcc).

Hay que tener en cuenta que se podría haber hecho el ejercicio con una dirección de clase A o B, pero por simplificar se ha tomado una de clase C.

Para los ejercicios rellenar la siguiente tabla:

Dpto.	Subred (IP/bits)	Hosts (1 a N)	Broadcast	Máscara
1º				
2º				
...				
...				

Nota: Existen calculadores de subnetting/supernetting en internet: <http://jodies.de/ipcalc>

## 10. CONFIGURACIÓN TCP/IP

### 10.1. FICHEROS DE CONFIGURACIÓN

Desde Ubuntu 17.10 se emplea la herramienta *NetPlan* para gestionar y administrar la configuración de red con la intención de sustituir la configuración clásica (mediate el archivo */etc/network/interfaces*).

Antes de realizar la configuración de la red, podemos conocer las interfaces de red identificadas por el sistema para su posterior configuración mediante los comandos:

```
ip a (o ip addr)
```

```
sudo lshw -class network
```

El directorio */etc/netplan* alberga a los archivos de configuración de *Netplan*. Para las distribuciones Ubuntu Desktop encontramos en dicho directorio los archivos:

- *01-network-manager-all.yaml* → que establece la primera configuración
- *02-network-manager-all.yaml* → para la segunda si se dispone, etc

de tal manera que se aplican estas configuraciones en el mismo orden numérico del comienzo de su nombre. La configuración de estos archivos ha de realizarse con privilegios de administrador y debemos seguir la siguiente sintaxis respetando los caracteres espacio:

```
network:
  version: 2
  renderer: NetworkManager/networkd
  ethernets:
    Nombre_dispositivo:
      dhcp: yes o no
      addresses: [DIRECCIÓN IP/MÁSCARA DE RED]
      gateway4: GATEWAY
      nameservers:
        addresses: [IP1 o NOMBRE1, IP2 o NOMBRE_2]
```

Donde:

- ♦ *Renderer*: nombre del gestor de red punto Network;anager es usado en sistemas de escritorio y networkd en servidores.
- ♦ *Nombre\_dispositivo*: se sustituye por el nombre de la interfaz para configurar.
- ♦ *dhcp4*: se indican los valores yes o no, si se configura por DHCP o con direccionamiento estático respectivamente.
- ♦ *Addresses*: se indica la dirección IP con notación prefijo o CIDR
- ♦ *Gateway4*: señala la puerta de enlace.
- ♦ *Nameservers*: indica las direcciones IP de los servidores DNS o sus nombres siguiendo el formato indicado.

#### Ejemplos:

1. Configuración dinámica de interfaz ethernet:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enps03:
      dhcp4: yes
```



## 2. Configuración estática de interfaz ethernet:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enps03:
      dhcp4: no
      addresses: [192.168.1.50/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.8.4]
```

## 3. Ejemplo con dos interfaces de red una dinámica y otra estática:

```
vespin@clienteUbuntu:~$ cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses: [192.168.2.14/24]
```

Para aplicar la configuración netplan guardada usamos el comando:

```
vespin@clienteUbuntu:~$ sudo netplan apply
```

Con el siguiente comando vemos el resultado de su aplicación:

```
vespin@clienteUbuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ff:21:b9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 85313sec preferred_lft 85313sec
    inet6 fe80::a00:27ff:feff:21b9/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:70:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.14/24 brd 192.168.2.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb1:70b4/64 scope link
        valid_lft forever preferred_lft forever
```



Si queremos mostrar solo una de las interfaces de red:

```
vespin@clienteUbuntu:~$ ip a show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:70:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.14/24 brd 192.168.2.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb1:70b4/64 scope link
        valid_lft forever preferred_lft forever
```

La configuración hardware de nuestros dispositivos de red:

```
vespin@clienteUbuntu:~$ sudo lshw -class network
*-network:0
    descripción: Ethernet interface
    producto: 82540EM Gigabit Ethernet Controller
    fabricante: Intel Corporation
    id físico: 3
    información del bus: pci@0000:00:03.0
    nombre lógico: enp0s3
    versión: 02
    serie: 08:00:27:ff:21:b9
    tamaño: 1Gbit/s
    capacidad: 1Gbit/s
    anchura: 32 bits
    reloj: 66MHz
    capacidades: pm pcix bus_master cap_list ethernet physical tp 10bt 10bt
d 100bt 100bt-fd 1000bt-fd autonegotiation
    configuración: autonegotiation=on broadcast=yes driver=e1000 driververs
n=5.13.0-40-generic duplex=full ip=10.0.2.15 latency=64 link=yes mingnt=255 mu
lcast=yes port=twisted pair speed=1Gbit/s
    recursos: irq:19 memoria:f0200000-f021ffff ioport:d020(size=8)
*-network:1
    descripción: Ethernet interface
    producto: 82540EM Gigabit Ethernet Controller
    fabricante: Intel Corporation
    id físico: 8
    información del bus: pci@0000:00:08.0
    nombre lógico: enp0s8
    versión: 02
    serie: 08:00:27:b1:70:b4
    tamaño: 1Gbit/s
    capacidad: 1Gbit/s
    anchura: 32 bits
    reloj: 66MHz
    capacidades: pm pcix bus_master cap_list ethernet physical tp 10bt 10bt
```

Para llevar a cabo una configuración de los servidores DNS de manera temporal podemos modificar el archivo `/etc/resolv.conf` directamente. Pero esta acción no es recomendable ya que NetPlan lo configura y actualiza dinámicamente a través de `systemd-resolve`.

El orden de los mecanismos de resolución de nombres en los sistemas Linux viene establecido en el fichero `/etc/nsswitch.conf`. Este archivo es editable por el administrador. La siguiente línea del fichero establece la resolución de nombres, donde, de izquierda a derecha se, indica el orden de resolución:

```
hosts:          files mdns4_minimal [NOTFOUND=return] dns
```

Donde:

- ♦ *files*: fichero `/etc/hosts`
- ♦ *mdns4\_minimal [NOT\_FOUND=return]*: utilizar el protocolo *mDNS* (para los nombres acabados en `.local`).
- ♦ *dns*: fichero `/etc/resolv.conf`

El archivo `/etc/hosts` contiene entradas con asignaciones entre direcciones IP y nombres de host. Por defecto, y según la definición del fichero `/etc/nsswitch.conf` el archivo `/etc/hosts` tiene prioridad sobre la configuración DNS del equipo por lo que se intenta resolver una dirección IP de un host coincidente con una entrada del archivo `/etc/hosts` no se resolverá a través de DNS.

Ejemplo del archivo `/etc/hosts`:

```
vespin@clienteUbuntu:~$ cat /etc/hosts
127.0.0.1        localhost
127.0.1.1        clienteUbuntu
#192.168.2.10     clienteUbuntu     clienteUbuntu.vanesa.local
192.168.2.10     clienteUbuntu     clienteUbuntu.vanesa.local
```

## 10.2. Comandos Para Verificación Y Monitorización De Red

Ya hemos visto cómo podemos establecer la configuración de los adaptadores de red de manera permanente. no obstante se pueden realizar modificaciones de las interfaces temporalmente empleando otros comandos. Existen multitud de comandos que ayudan a monitorizar y verificar el correcto uso de la red la principal son *ip* y *ss*. Estos dos comandos han sustituido al tradicional *ifconfig*, aunque sigue funcionando en las nuevas versiones de Ubuntu. En Windows usamos el comando *ipconfig*.

El comando *ip* es muy potente, algunas de las acciones de configuración son:

- ♦ listar las interfaces activas e inactivas: *ip a*
- ♦ deshabilitar una interfaz: *ip link set <interfaz> down*
- ♦ habilitar una interfaz: *ip link set <interfaz> up*
- ♦ configurar una interfaz: *ip addr add <IP/mascara> dev <interfaz>*
- ♦ eliminar una dirección IP: *ip addr del <IP/mascara> dev <interfaz>*
- ♦ mostrar la tabla de enrutamiento: *ip route show*
- ♦ añadir una puerta de enlace predeterminada: *ip route add 0.0.0.0/0 via IP dev <interfaz>*
- ♦ mostrar la tabla ARP (*Address Resolution Protocol*): *ip neighbour show*. Abreviatura: *ip n show*

Ejemplo:

```
vespin@clienteUbuntu:~$ ip neighbour show
192.168.2.11 dev enp0s8 FAILED
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 STALE
192.168.2.10 dev enp0s8 FAILED
```

Con este comando mostramos las asociaciones entre las direcciones físicas MAC y direcciones IP del segmento de red local en un equipo. Estas asociaciones se almacenan en una tabla ARP también llamada caché ARP y son necesarias para incluir las direcciones en las tramas de la capa de enlace. Además permite conocer a qué equipos de la red se ha conectado un host.

En la última columna nos indica el estado de la máquina (del «vecino») cuando se ha detectado algún problema de conexión:

- REACHABLE: la entrada ARP es válida y hay conectividad.
- STALE: la entrada ARP es válida pero no hay conectividad.
- FAILED: no hay conectividad y la MAC no ha sido detectada.
- DELAY: a la espera de confirmación tras el envío de un paquete.

En Windows (también en Linux pero menos que el anterior) se usa el comando **arp** para conocer, incluso modificar, las entradas de la tabla de encaminamiento.

```
C:\Users\Vanesa>arp -a

Interfaz: 192.168.1.18 --- 0x6
Dirección de Internet      Dirección física      Tipo
192.168.1.1                f0-81-75-b8-15-a0    dinámico
192.168.1.13               f4-f5-d8-8c-e7-74    dinámico
192.168.1.15               02-31-92-0c-9f-24    dinámico
192.168.1.16               d8-d4-3c-fd-f8-9f    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 169.254.198.151 --- 0xf
Dirección de Internet      Dirección física      Tipo
169.254.255.255            ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

Otro comando muy utilizado y que también nos puede ayudar a identificar y mostrar multitud de detalles de las interfaces de red es **lshw** (list hardware), como vimos anteriormente.

Otro de los comandos más empleados para comprobar una conexión de red es mediante el comando **ping** usado tanto en Windows como en Linux este comando envía paquetes de prueba a un destino especificado y nos informa del tiempo de respuesta en caso de existir conexión su sintaxis es la siguiente:

***ping [opciones] destino***

donde *destino* es un nombre de dominio o la dirección IP para detener la salida por pantalla de los tiempos de respuesta. Se puede usar la combinación de teclas CTRL+C para detenerlo. Gracias a él podemos comprobar si un adaptador de red funciona correctamente o si se tiene acceso a otros equipos dentro de la red local o fuera de ella (como en Internet).

### 10.3. Gestión De Puertos

Todos los sistemas operativos tienen la capacidad de gestionar los puertos de entrada/salida para aceptar o rechazar la escucha de determinadas aplicaciones. No confundir este tipo de puertos (lógicos) con los puertos de conexión de periféricos (físicos).

- Puerto de origen: número que identifica la aplicación que origina la comunicación en el host.
- puerto de destino: número asociado a la aplicación de destino en el host remoto.

por tanto en las comunicaciones TCP y udp los juegos han dedicado en el encabezado de cada segmento de la capa de transporte el número de puerto de origen y el número de puerto de destino.

Pero, ¿cuál es la diferencia entre abrir un tipo de puerto u otro?

#### 10.3.1. ¿TCP o UDP?

**UDP** es un protocolo no orientado a conexión. Es decir cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional. La transferencia de datos es realizada sin haber realizado previamente una conexión con la máquina de destino (maquina B), y el destinatario recibirá los datos sin enviar una confirmación al emisor (la maquina A). Esto es debido a que la encapsulación de datos enviada por el protocolo UDP no permite transmitir la información relacionada al emisor. Por ello el destinatario no conocerá al emisor de los datos excepto su IP.

Contrariamente a UDP, el protocolo **TCP** está orientado a conexión. Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena recepción. Aquí interviene el control CRC de datos que se basa en una ecuación matemática que permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar los datos corruptos.

En resumen, **TCP** es para conexiones seguras y es más lento, pero confiable, el **UDP** no es seguro ni confiable, pero es más rápido, y los 2 se complementan depende para lo que use. Por lo general los juegos o las transmisiones en vivo como una videollamada usan **UDP**, porque la conexión debe de ser lo más rápido posible sin interrupciones, pero esto implica posibles "saltos" (tanto en juegos como en videollamadas por ejemplo, esto es porque se pierde parte de la información pero la información es constante y no se atrasa. Cuando se abre una página web se usa **TCP** porque la información es segura aunque tarde mas, o cuando se ve un video por youtube, se puede ver que dura más cargando pero cuando carga todo el video se ve bien y no tiene errores.

#### 10.3.2. Puertos Más Utilizados

Existen 3 tipos de puertos lógicos asociados a su número:

1. **puertos bien conocidos:** números desde 0 al 1023. Reservados para aplicaciones y servicios como HTTP, FTP o HTTPS
2. **puertos registrados:** números del 1024 al 49151. son puertos empleados por las aplicaciones de usuario cuando conectan con servidores.
3. **puertos dinámicos, privados o efímeros:** del 49152 al 65535. usados principalmente por aplicación de intercambio de archivos punto a punto.

Puertos bien conocidos de TCP/UDP

Puerto preasignado	Protocolo	Aplicación
80	TCP	HTTP
21	TCP/UDP	FTP
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
110	TCP/UDP	POP3
119	TCP/UDP	NNTP
137	TCP/UDP	serv. de nombres NetBIOS
161	TCP/UDP	SNMP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare sobre IP
458	TCP/UDP	Apple QuickTime
500	TCP/UDP	ISAKMP

Tomando como ejemplo el puerto 80 de la aplicación HTTP: si un usuario desea acceder a una página web el proceso sería el siguiente:

El host cliente indica el encabezado del segmento de la capa de transporte el puerto de destino bien conocido (el 80 ya que es un servicio HTTP) y como puerto de origen un número aleatorio a partir del 1024. De esta manera se pueden establecer simultáneamente multitud de comunicaciones sobre un mismo servidor HTTP. Cuando el servidor se comunica con el correspondiente cliente éste indica en el encabezado del segmento su puerto de origen 80 y puerto destino el de la aplicación y comunicación concreta del host cliente.

Como ya sabemos los segmentos se encapsulan dentro de paquetes de la capa de red y el encabezado de los paquetes de la capa de red indica las direcciones IP de origen y destino. A la combinación de una dirección IP y un puerto se le denomina **socket** por tanto una comunicación entre 2 hosts bien establecida por una pareja de **socket**.

Un ejemplo de socket es 192.168.1.55: 80 formado por la dirección IP y el puerto 80. Este socket indica que pertenece a un servidor HTTP al ser un puerto bien conocido como es el 80.

### 10.3.3. Gestión De Puertos En Linux

En sistemas Linux el comando **ss** viene a sustituir a *netstat*. Son muchas las utilidades de este comando y presenta la siguientes sintaxis:

**ss [opciones] [filtro]**

Algunas de las acciones más habituales realizar con **ss**:

- ◆ mostrar información sobre las conexiones asociadas a los sockets: **ss -a**
- ◆ listar los sockets en escucha de nuestro host: **ss -l**
- ◆ información de sockets TCP: **ss -t**
- ◆ recoger estadísticas: **ss -s**

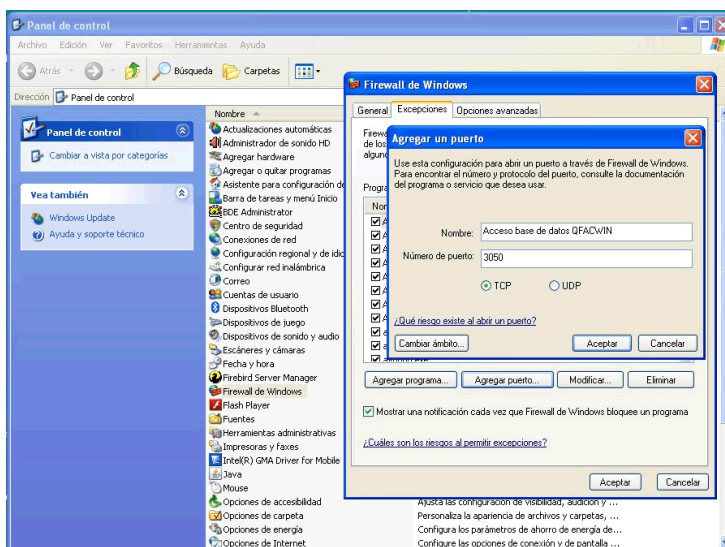
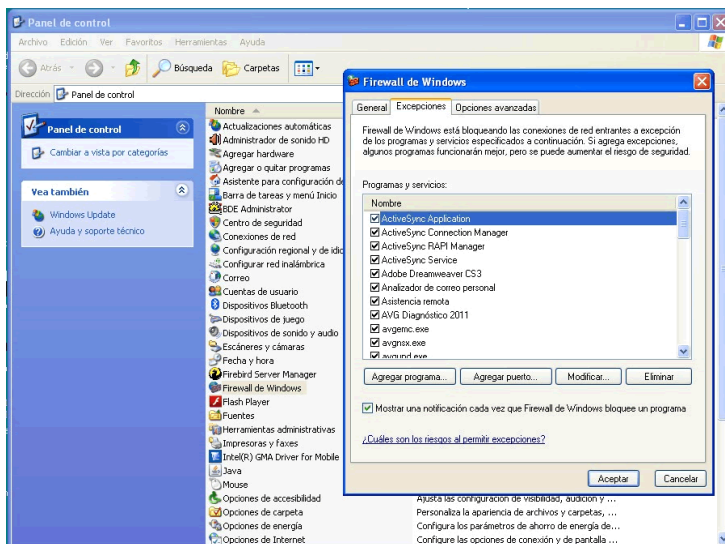
```
vespin@clienteUbuntu:~$ ss -s
Total: 870
TCP: 13 (estab 0, closed 0, orphaned 0, timewait 0)

Transport Total      IP      IPv6
RAW         0         0         0
UDP         7         5         2
TCP        13         7         6
INET        20        12         8
FRAG         0         0         0
```

### 10.3.4. Gestión De Puertos En Windows

**Familia NTLDR:** Abrimos el cortafuegos. Desde la pestaña "Excepciones" pinchamos en "Agregar puerto". Se le asigna un nombre, se indica tipo de puerto (TCP/UDP) y finalmente se le pone un nombre.

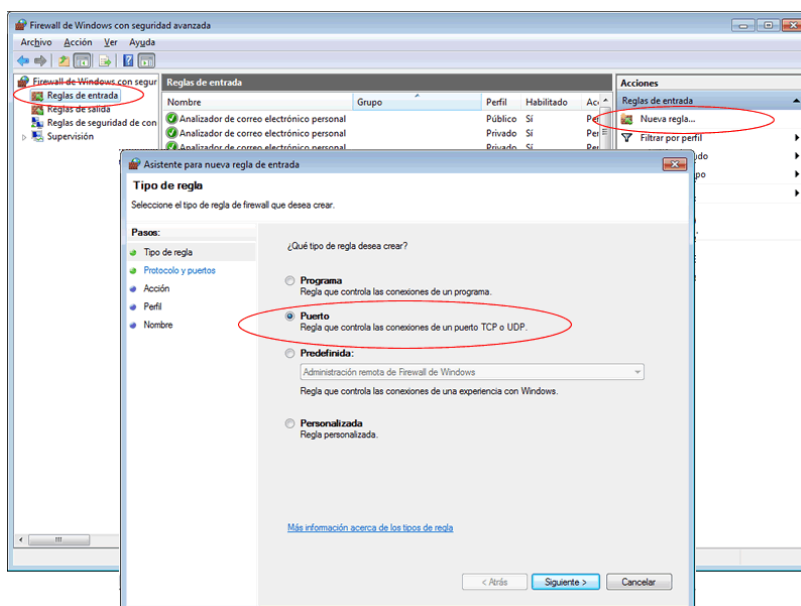
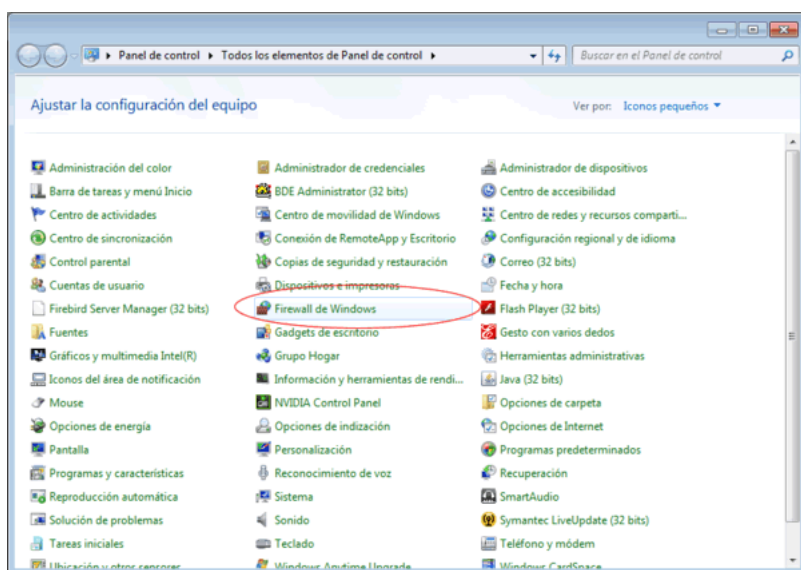
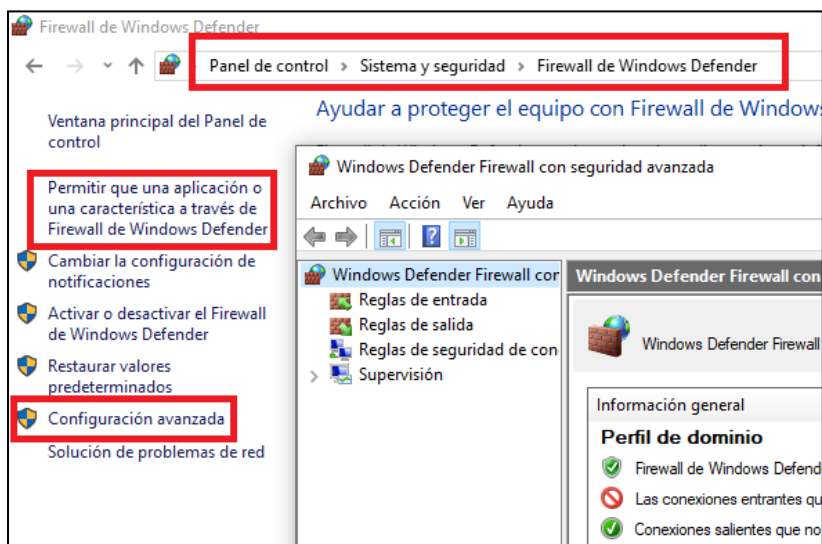




Desde BOOTMGR:

Podemos abrir el cortafuegos y permitir que una aplicación permita todas sus conexiones (Permitir que una aplicación o característica a través de Firewall....”, pero esto no sería adecuado en el caso de querer controlar en detalle un puerto.

Abrimos el Cortafuegos, luego en configuración avanzada. En las reglas de entrada/salida añado una nueva regla y en tipo de regla le digo que es una regla tipo PUERTO. Escojo si es TCP o UDP y luego el número de puerto. Posteriormente se indica si quiero permitir/denegar la conexión. Finalmente se le dice sobre que dominio se aplica y se le pone un nombre.



Asistente para nueva regla de entrada

**Protocolo y puertos**

Especifique los puertos y protocolos a los que se aplica esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

☒ TCP

☐ UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

☐ Todos los puertos locales

☒ Puertos locales específicos:

Ejemplo: 80, 443, 5000-5010

**Indique el puerto 3050**

[Más información acerca de protocolos y puertos](#)

< Atrás    Siguiente >    Cancelar

Asistente para nueva regla de entrada

**Acción**

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☒ Permitir la conexión

Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ Permitir la conexión si es segura

Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☐ Bloquear la conexión

[Más información acerca de las acciones](#)

< Atrás    Siguiente >    Cancelar



Asistente para nueva regla de entrada

**Perfil**

Especifique los perfiles en los que se va a aplicar esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Cuándo se aplica esta regla?

☒ **Dominio**  
Se aplica cuando un equipo está conectado a su dominio corporativo.

☒ **Privado**  
Se aplica cuando un equipo está conectado a una ubicación de redes privadas.

☒ **Público**  
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

[Más información acerca de los perfiles](#)

< Atrás    **Siguiente >**    Cancelar

Asistente para nueva regla de entrada

**Nombre**

Especifique el nombre y la descripción de esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

**Ponga un nombre y una descripción que le sirvan para reconocer esta nueva regla de entrada:**

Nombre:  
Base de datos QFACWIN

Descripción (opcional):  
Puerto para conectar con la base de datos de QFACWIN

< Atrás    **Finalizar**    Cancelar