Redes de ordenadores

IES
Miguel
Hernández

1º Bachillerato

1. Introducción

Internet es una red mundial de ordenadores que permite comunicarse y compartir información con todo el mundo. Su nombre procede de las palabras INTERconnected NETworks, es decir, redes interconectadas.

Las redes de ordenadores están presentes en todos los rincones de nuestra sociedad, desde los hogares hasta las grandes empresas. Su uso mejora nuestra calidad de vida y proporciona servicios tan variados como el acceso a Internet, intercambio de datos, comercio electrónico, conexión entre dispositivos, VoIP, gestión de la domótica en el hogar, etc.

Las nuevas tecnologías aportan muchos beneficios a los usuarios, pero también implican ciertos riesgos que afectan a derechos fundamentales como la privacidad, por lo que es necesario adoptar medidas de seguridad, especialmente cuando se trabaja en la red Internet.

EJERCICIO 1

Visualiza el vídeo de Chema Alonso "¿Sabes lo que pasa cuando das a 'sí, acepto' en una app?" que puedes encontrar en el siguiente enlace VÍDEO
En la carpeta que tienes compartida con el profesor crea un documento de texto llamado **ej1redes** y haz una reflexión de entre 100 y 120 palabras sobre lo que se dice en el vídeo anterior.

2. Fundamentos de las redes

¿Qué es una red de ordenadores?

Una red de ordenadores es un conjunto de ordenadores interconectados entre sí, lo que permite compartir recursos (impresoras, discos duros, etc.) e información (programas y datos) entre ellos.

Ventajas de usar una red de ordenadores

Entre las ventajas de usar una red de ordenadores podemos destacar:

- Posibilidad de compartir periféricos, tales como impresoras, plotters, modem, etc.
- Posibilidad de compartir información a través de bases de datos, archivos, etc.
- Eliminación de datos duplicados en ordenadores.
- Posibilidad de disponer de un control de usuarios más exhaustivo.
- Posibilidad de generar copias de seguridad más rápidas y seguras.
- Posibilidad de comunicación entre los usuarios de los ordenadores de la red.

Proceso de comunicación

En cualquier red o sistema de comunicación podemos encontrar los siguientes elementos de funcionamiento:

- El emisor, que genera una señal (petición u origen de la comunicación).

- El codificador de esta señal, que prepara la comunicación para que pueda viajar por la línea.
- La línea o medio de comunicación por donde viaja la información.
- El decodificador de la señal, que recoge la señal y la vuelve a traducir para que el receptor la procese.
- El receptor o elemento destinatario de la señal.

En las redes informáticas, los ordenadores (hosts) hacen el papel de emisores y receptores al mismo tiempo. La línea o canal por donde circula la comunicación es el medio físico por el que viajan los datos, ya sean cables o medios no guiados.

Los componentes de la red deben poseer interfaces que sean capaces de conectar los distintos dispositivos y elementos de la red y que preparen la señal para que viaje por el medio establecido: por ejemplo las tarjetas de red de los ordenadores o los módems.

Para que el emisor y receptor puedan comunicarse necesitan utilizar el mismo sistema de reglas, a este sistema se le llama protocolo, siendo el más utilizado para redes informáticas el protocolo TCP/IP, que es propio de la red internet.

3. Hardware de red

Para conectar varios ordenadores en red necesitamos una serie de componentes.

Adaptador o Interfaz de red (tarjeta de red)

Su función es convertir la información que quiere enviar el ordenador en señales que se puedan transmitir por el medio.

Dirección MAC

La dirección MAC o dirección física, es un identificador único de 6 bytes en hexadecimal que asignan los fabricantes a las tarjetas y dispositivos de red. Los 3 primeros bytes hacen referencia al OUI, Identificador Único de Organización, por lo que son iguales para todos los productos de un mismo fabricante.

En la siguiente imagen vemos la dirección MAC de un equipo **60:e3:27:05:b2:c6** la cual corresponde a una tarjeta de red TP-LINK

```
administrador@administradorALDACE:~$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 60:e3:27:05:b2:c6
          Direc. inet:10.2.1.254  Difus.:10.2.1.255  Másc:255.255.255.0
          Dirección inet6: fe80::62e3:27ff:fe05:b2c6/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:3435404 errores:0 perdidos:293 overruns:0 frame:0
          Paquetes TX:3827309 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:2462537533 (2.4 GB)  TX bytes:3453075839 (3.4 GB)
```

Hub o Concentrador

Se utiliza para conectar varios ordenadores en red. El hub recibe la señal de una estación de trabajo o segmento de la red que la quiere transmitir y la emite por sus diferentes puertos. El uso del hub está en desuso, puesto que su mecanismo de transmisión de la señal se basa en difundir los paquetes de datos por todos los puertos a la vez, estén o no ocupados por un cable o por un PC encendido en ese momento. Por ejemplo, un hub de ocho puertos transmite la señal a los ocho puertos a la vez. El ordenador destinatario recibe la información y el resto la omiten

Switch o Conmutador

Un conmutador o switch hace la misma función que un hub, pero de manera más eficiente, pues es capaz de reconocer qué puertos en ese momento tienen actividad (están conectados a una estación de trabajo, una impresora, etc.) y transmitir la señal sólo a éstos, e incluso aprende a qué PC de destino va dirigida, lo que redunda en mayor rapidez. La evolución de las redes Ethernet ha hecho que los switchs se impongan definitivamente sobre los hubs.

Router

su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir interconectar dos redes. Generalmente, el router es el dispositivo que conecta una red LAN a Internet o una LAN a otras LAN.

Hoy en día es habitual que los routers incorporen tecnología Wi-Fi para conectar dispositivos portátiles. También es habitual que tengan más de un puerto de conexión (cuatro puertos RJ45), lo que los convierte también en pequeños switchs.

Repetidor

La señal de transmisión se atenúa, o incluso se pierde, cuanto mayor es la distancia a la que se desea transmitir. Un repetidor es un dispositivo hardware encargado de amplificar o regenerar la señal de transmisión.

EJERCICIO 2

Después de ver el siguiente VÍDEO crea un documento de texto llamado **ej2redes** en tu carpeta compartida y señala las ventajas y desventajas de usar un sistema Mesh en lugar de repetidores.

EJERCICIO 3

Después de leer el artículo del siguiente enlace crea un documento de texto llamado **ej3redes** en tu carpeta compartida y señala las diferencias entre un router y un punto de acceso
ARTÍCULO

4. Medios de comunicación

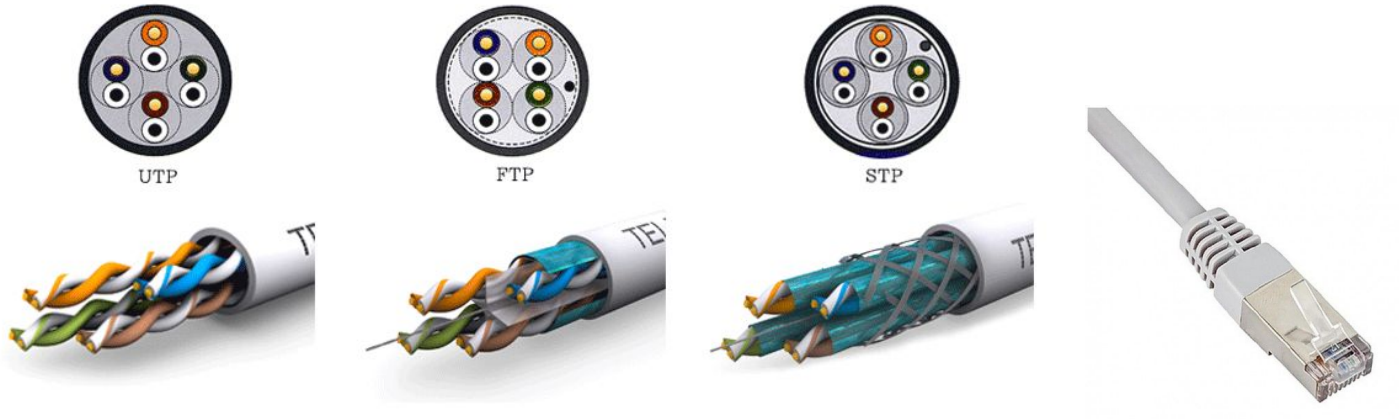
Son el cableado y los conectores que enlazan los componentes de la red. Existen diferentes tipos de medios de comunicación, agrupados en dos grandes categorías: **medios cableados y medios inalámbricos.**

Medios cableados

La conexión entre los ordenadores y dispositivos de red (routers, switchs, etc..) se realiza mediante cables. Existen varios estándares para redes cableadas, aunque los más utilizados son el Ethernet y la fibra óptica.

Ethernet

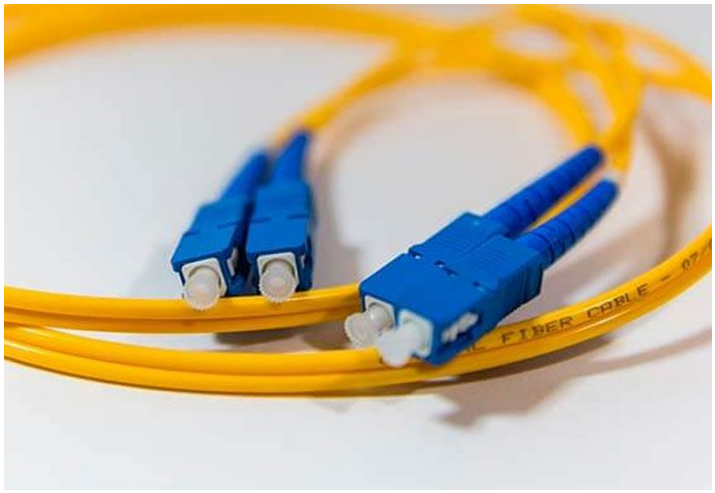
El cableado empleado en estas redes es el par trenzado (UTP, FTP o STP), según vaya sin apantallar, apantallado globalmente o apantallado en el que cada par va apantallado.

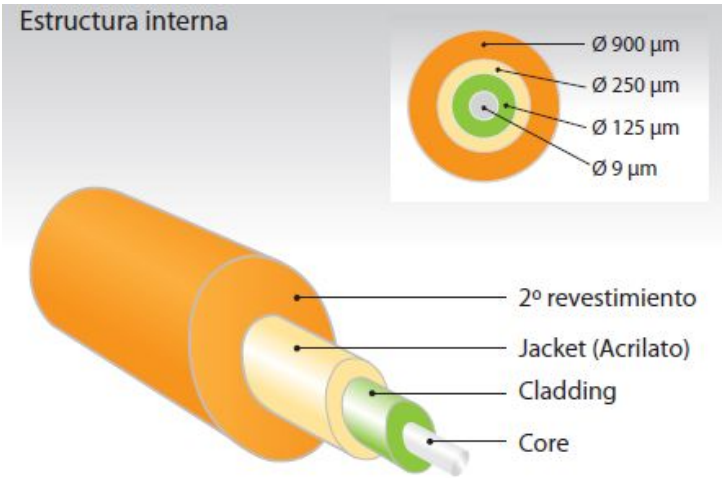


Este tipo de cableado es el más utilizado para redes LAN.

Fibra óptica

La fibra óptica es un medio de transmisión cada vez más empleado en las redes de datos y telecomunicaciones. Un cable de fibra óptica está compuesto por un grupo de fibras ópticas, cada una de las cuales es un hilo muy fino de material transparente (vidrio o material plástico) por el que se envían pulsos de luz que representan los datos a transmitir. La fuente de luz puede ser láser o un LED.





Redes inalámbricas

Las redes de área local inalámbrica o WLAN proporcionan un sistema de comunicación muy flexible al eliminar por completo la utilización de cables. Esto ha hecho que en los últimos años hayan tenido una gran aceptación. Aun así, las WLAN no intentan sustituir por completo a las LAN que utilizan cable, sino que sirven como complemento de éstas, debido principalmente a que su velocidad de transmisión es menor que el de las que utilizan cable.

Bluetooth

Es un protocolo de comunicaciones entre dispositivos para la transmisión de voz y datos. Permite realizar conexiones de corto alcance. Se utiliza en teclados, ordenadores, impresoras, cámaras digitales, manos libres, smartphones, etc.

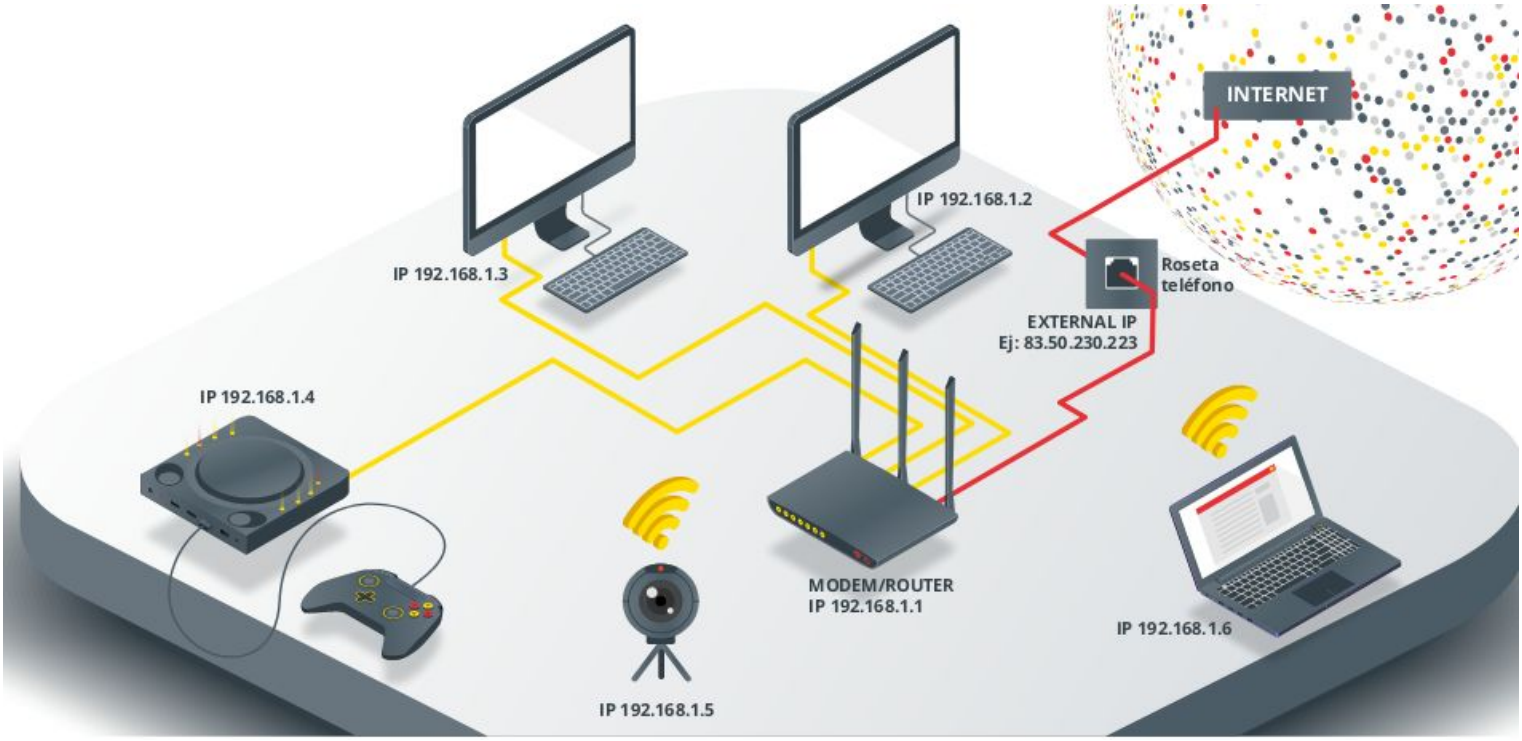
Wi-Fi

Es una tecnología inalámbrica que realiza la conexión mediante ondas electromagnéticas a una distancia aproximada de 100 metros como máximo. Las características de estas redes están recogidas en la norma 802.11 que incluye varios estándares.

- 802.11 b : Fue el primer estándar desarrollado en 1999 y ofrecía una velocidad de 11 Mbps.
- 802.11 g : Surge en 2003 y amplía la velocidad hasta los 54 Mbps. Además de aumentar la velocidad, consiguió que los aparatos compatibles con él fuesen más baratos de producir debido a su sencillez.
- 802.11 n : En 2009 llega uno de los estándares más extendidos en la actualidad. Su principal característica es el aumento de la velocidad hasta los 600 Mbps y el uso de hasta 4 antenas.
- 802.11. ac : En 2013 nace este estándar que es el que la mayoría de dispositivos utiliza actualmente. Permite velocidades de hasta 3,46 Gbps.
- 802.11 ax : En 2018 se desarrolla el estándar ax que eleva la velocidad hasta los 10,53 Gbps. Todavía no está tan extendido como el estándar ac

Componentes de una red WiFi

- **Dispositivo cliente**: son los que solicitan la conexión a la red inalámbrica como los ordenadores portátiles, tablets, smartphones, etc.
- **Punto de acceso** (en inglés Access Point): elemento tecnológico que conecta los dispositivos clientes entre sí o con el resto de la infraestructura cableada de la organización. También sirven como puertas de enlace a otras redes, como Internet. Comúnmente se le conoce como router, aunque este dispositivo también es capaz de realizar otras tareas



Wimax

Es una tecnología similar al WiFi pero que utiliza microondas. Aunque su alcance es mucho mayor, puede llegar hasta los 70 km, su velocidad es inferior, hasta 1 Gbps.

EJERCICIO 4

Un amigo quiere montar una cafetería en la que los clientes puedan ir con sus portátiles, tablets o usar los 3 ordenadores que pondrá a su disposición para que puedan trabajar o utilizar los equipos mientras se toman un café o desayunan.

Te pide que le ayudes a montar la red de la cafetería. Te dice que necesita 3 ordenadores con conexión a Internet. Una impresora en la que puedan imprimir los 3 ordenadores. Además quiere que los clientes que lleven sus portátiles y tablets puedan conectarse a Internet e imprimir en la impresora.

Crea un documento de texto llamado **ej4redes** en tu carpeta compartida y haz un listado con los elementos de red (cables, dispositivos, etc..) que necesitará montar la red de su negocio

5. Seguridad en redes inalámbricas

Nos hallamos inmersos en una era inalámbrica en la que dispositivos como ordenadores personales, smartphones o tablets y elementos IoT[1] pueden llegar a estar interconectados entre sí sin necesidad de hacer uso del cable.

No obstante, si la red inalámbrica no es segura, existen riesgos muy importantes. Por ejemplo, un delincuente podría:

- **Robo de información confidencial**. Cuando un intruso se conecta a nuestra red privada podría llegar a acceder a nuestra información (documentos, fotos, vídeos) y si cuenta con los suficientes conocimientos podría acceder a nuestros dispositivos, así como a los datos que estamos enviando y recibiendo de Internet.

- **Disminución del ancho de banda.** Las conexiones tienen una capacidad determinada, el ancho de banda, que se reparte entre los dispositivos que estén conectados, de forma que cuantos más equipos se conecten, más lento será el intercambio de información, llegando a ser imposible usar Internet: las páginas web tardan demasiado en cargar o los videos de YouTube no se visualizan con normalidad. Dependiendo del número de intrusos y del uso que hagan de nuestra red podemos llegar a perder la conexión.

[1] El Internet de las Cosas (en inglés Internet of Things, abreviado IoT), es una red de objetos cotidianos interconectados con acceso a Internet.

- **Infectar los dispositivos con malware.** Alguien que acceda a nuestra red podría instalar malware en los dispositivos conectados a la misma lo que puede repercutir gravemente a nuestra seguridad.

- **Realizar ciberdelitos en tu nombre.** Cuando contratamos una conexión a Internet, nuestro proveedor vincula la dirección IP que tengamos en ese momento con el nombre del titular, de la misma manera que un número de teléfono está asociado a su suscriptor. Cualquier acción, ilegal o no, que se lleve a cabo desde nuestra red estará asociada directamente con el titular de la línea, es decir, con nosotros, y aunque se demuestre que hubo alguna intrusión en nuestro sistema, puede generarnos algún quebradero de cabeza.

Sabiendo todo lo que un atacante puede hacer desde nuestra red es importante que la protejamos de manera correcta.

A continuación se incluyen varios pasos sencillos que puedes seguir para proteger tu red y routers inalámbricos:

Evita la utilización de la contraseña predeterminada

Es muy fácil para un hacker descubrir cuál es la contraseña predeterminada del fabricante de tu router inalámbrico y utilizarla para acceder a la red inalámbrica. Por lo tanto, es conveniente que cambies la contraseña de administrador de tu router inalámbrico. A la hora de establecer la contraseña nueva, trata de elegir una serie compleja de números y letras, e intenta evitar la utilización de una contraseña que pueda adivinarse fácilmente

No permitas que el dispositivo inalámbrico indique su presencia

Desactiva la difusión del identificador de red SSID (Service Set Identifier) para evitar que el dispositivo inalámbrico anuncie su presencia al mundo que te rodea.

Modificar el nombre de la red wifi o (SSID)

Es muy recomendable cambiar el nombre de nuestra wifi por defecto para que no incluya ningún tipo de información que pudiera ser de utilidad para un potencial atacante (nombre de la organización, proveedor de servicios contratado, modelo de router, etc.).

Configurar red wifi con cifrado WPA2 o WPA3

En las configuraciones de los routers, normalmente se ofrecían tres modalidades de cifrado: WEP, WPA y WPA2. Posteriormente, se incorporó una más robusta y la que más se recomendaba habilitar: WPA2-PSK(AES). Sin embargo, en octubre de 2017, se descubrió una vulnerabilidad denominada “ataque KRACK” que permitía a un atacante interceptar, descifrar y manipular el tráfico de una red inalámbrica con el tipo de cifrado anteriormente mencionado. Ante este problema se ha desarrollado una nueva versión del protocolo WPA llamada WPA3

Lo que no se debe tener configurado bajo ningún concepto es el cifrado WEP, ya que es muy inseguro y alguien con los conocimientos necesarios podría robar la contraseña de la red wifi en poco tiempo.

Desactivar WPS

Se trata de un mecanismo que facilita la conexión de dispositivos con nuestro router a través de un código PIN de 8 dígitos. El dispositivo que se quiere conectar a la wifi debe transmitir el código numérico al router y éste a cambio le enviará los datos para acceder a la red.

Tener activada esta opción implica una nueva forma de conexión que podría ser utilizada por un atacante para acceder a nuestra red wifi, ya que el tiempo que se necesita para averiguar un PIN de 8 dígitos es mucho menor que el que necesitaría para averiguar una contraseña WPA2-PSK(AES) configurada en la red.

Habilitar el filtrado por dirección MAC

Mediante este mecanismo se pretende que únicamente las direcciones MAC que se encuentren incluidas en el router puedan conectarse a la red.

Habrá que incluir las direcciones que entendamos como oportunas en nuestro router y para ello deberemos acceder a las opciones en el dispositivo para establecer este control de acceso. Como paso previo, hemos de conocer la dirección MAC de los diferentes dispositivos que queramos añadir, bien sean ordenadores, teléfonos móviles, tablets, etc.

Control de equipos en la red

Los router cuentan con una opción en la que muestran los dispositivos conectados a la red. Accediendo a esta sección de la página de configuración podemos conocer un listado de los dispositivos conectados en tiempo real.

EJERCICIO 5

Configura el router wifi que te proporcionará el profesor con todas las medidas vistas anteriormente para que sea lo más seguro posible.

Crea un documento de texto llamado **ej5redes** en tu carpeta compartida y explica cómo has realizado cada uno de los pasos vistos arriba.

6. Clasificación de las redes

Las redes se pueden clasificar atendiendo a diversos criterios, tales como su área de cobertura, topología, tecnología, funcionalidad, etc.

Según su área de cobertura

La clasificación más habitual suele ser la que distingue entre el tamaño o área de cobertura de la red.

De menor a mayor tamaño tenemos:

Red de área personal (PAN)

Son redes que comunican diferentes dispositivos que están en un radio de pocos metros. Suelen utilizar tecnologías de conexión inalámbricas como Bluetooth o infrarrojos.

Red de área local (LAN)

Son redes de tamaño reducido que, por lo general, no ocupan más que una oficina o quizá un edificio y son redes muy rápidas.

Redes de área metropolitana (MAN)

Abarcan desde algunos edificios hasta ciudades enteras. Su ejemplo más conocido son las redes Wimax.

Redes de área extensa (WAN)

Son redes que recorren grandes distancias hasta el punto de interconectar países y continentes. Internet es un ejemplo de red que, por su extensión, pertenece a este último tipo de redes.

EJERCICIO 6

Crea un documento de texto llamado **ej678redes** en tu carpeta compartida y realiza este ejercicio y los dos siguientes.

Indica ejemplos de los diferentes tipos de redes según su área de cobertura. Nombra las que sean próximas a tí o participes en ellas directamente.

EJERCICIO 7

¿Qué tipo de redes se utilizan al enviar un email a un amigo que tienes al lado? ¿Y si está en Suecia?

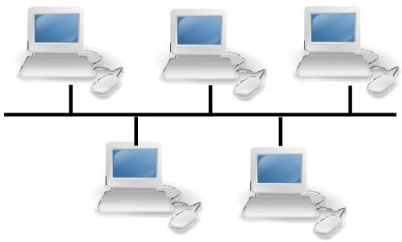
EJERCICIO 8

Explica la diferencia entre dos términos que normalmente se utilizan para lo mismo. Internet y WiFi

Según su topología

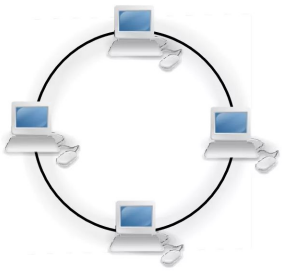
La topología de una red hace referencia a la distribución física del cableado para la interconexión de los equipos. Las principales topologías son:

Bus



Esta red, ya en desuso, se caracteriza por tener un único canal de comunicación al cual se conectan los distintos dispositivos. La circulación de toda la información por un único canal la convierte en una red lenta, además en caso de rotura del cable principal, toda la red deja de funcionar.

Anillo

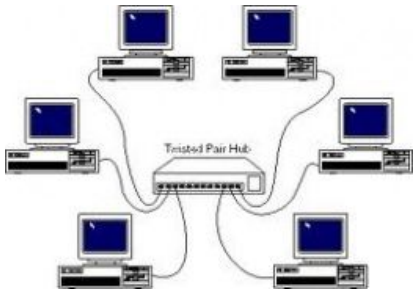


Es una red cerrada en la que los equipos se sitúan de una forma similar a la del bus, pero en este caso formando un anillo completamente cerrado. La información circula en un sentido y cada ordenador analiza si es el destinatario de la información. Tiene los mismos inconvenientes que el bus.

Estrella

En este tipo de redes todos los ordenadores están conectados a un dispositivo específico que se encarga de transmitir la información. Este dispositivo suele ser un hub o más frecuentemente, un switch. La rotura

de uno de sus enlaces no influye en el funcionamiento del resto. Esta es la topología habitual de las redes de área local.



Según su privacidad

Red pública

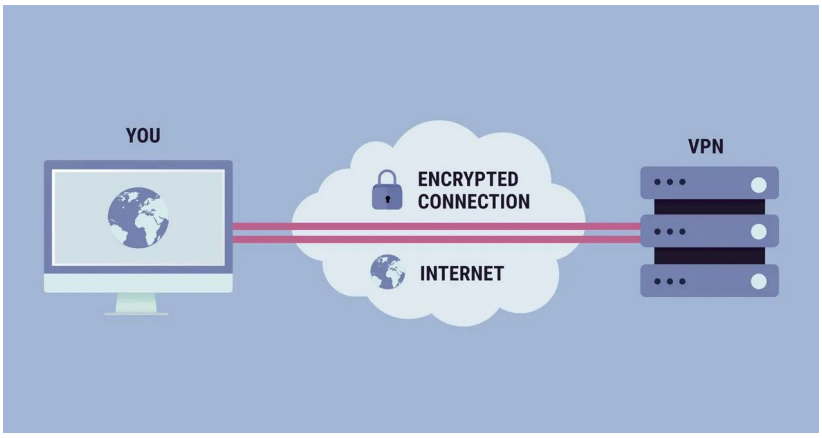
Se caracteriza por ser una red que puede utilizar cualquier persona. Internet es una red pública que conecta redes de todo el planeta.

Red privada

Es una red con acceso exclusivo para los usuarios y equipos que la forman, por ejemplo, la red del instituto.

VPN (Red Privada Virtual)

Una VPN es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían.



Con una VPN habilitada, todos los datos que envías y recibes viajan a través de un túnel cifrado para que nadie pueda acceder a tu información privada. Eso significa que, incluso si un ciberdelincuente consiguiese interceptar tus datos, no podría descifrarlos.

EJERCICIO 9

Crea un documento de texto llamado **ej9redes** en tu carpeta compartida y explica 2 usos que puedas darle a una VPN en tu casa.

Según su relación funcional

Atendiendo a la relación que se establece entre los diferentes equipos de una red, se distinguen dos arquitecturas básicas:

Cliente - Servidor

Son redes que se basan en la distribución de tareas, distinguiendo dos tipos de equipos en la red:

- **Servidor:** Es un equipo de la red que provee servicios al resto de equipos, denominados clientes. Algunos de estos servicios son:
  - Gestión de usuarios.
  - Almacenamiento
  - Conexión a Internet
  - Acceso a bases de datos.
  - Correo electrónico
  - Impresoras

- **Cliente:** Son ordenadores que dependen, total o parcialmente, de los recursos de un equipo servidor, a los que acceden a través de la red

Redes entre iguales (P2P, Peer to Peer)

Son redes que no diferencian entre clientes ni servidores, ya que todos los nodos se comportan como iguales entre sí. Los equipos actúan simultaneamente como clientes y servidores respecto a los demás nodos de la red, permitiendo el intercambio directo de información en cualquier formato entre los ordenadores interconectados. Algunos de los servicios más populares de este tipo de redes son:

- **Intercambio de archivos**: Consiste en el envío y recepción de documentos, de forma directa, entre los ordenadores de varios usuarios conectados a Internet. Este intercambio se basa en la idea de que los usuarios deben compartir para poder descargar usando aplicaciones como **BitTorrent, eMule,** etc.
- **VoIP**: Es el servicio de telefonía IP utilizado para enviar voz digitalmente a través de Internet.

EJERCICIO 10

Crea un documento de texto llamado **ej10redes** en tu carpeta compartida y contesta a las siguientes preguntas.
Según las clasificaciones de redes vistas anteriormente. ¿Cómo clasificarías la red del aula de Informática? ¿Qué servicios no puedes utilizar si el ordenador del profesor está apagado? ¿Qué tipo de ordenador sería éste?

7. Origen de las redes y modelos de referencia

A principios de 1980, las empresas descubren las ventajas de conectar los ordenadores entre sí, por lo que se produce un enorme crecimiento en la cantidad y tamaño de las redes de ordenadores. Cada fabricante utilizaba su propia tecnología, incompatible con la de otros fabricantes, por lo que cada vez resultaba más difícil conectar redes que usaran tecnologías de distintos fabricantes.

Para solucionar esta incompatibilidad, la Organización Internacional para la Estandarización (ISO) desarrolló el modelo de referencia OSI en 1984, con el objeto de estandarizar el diseño de las redes para que pudieran conectarse entre sí.

El modelo OSI es teórico, por lo que no está pensado para hardware o protocolos especificos. A nivel práctico, uno de los más difundidos es el modelo TCP/IP, que es la familia de protocolos utilizados en Internet.

Modelo de referencia OSI

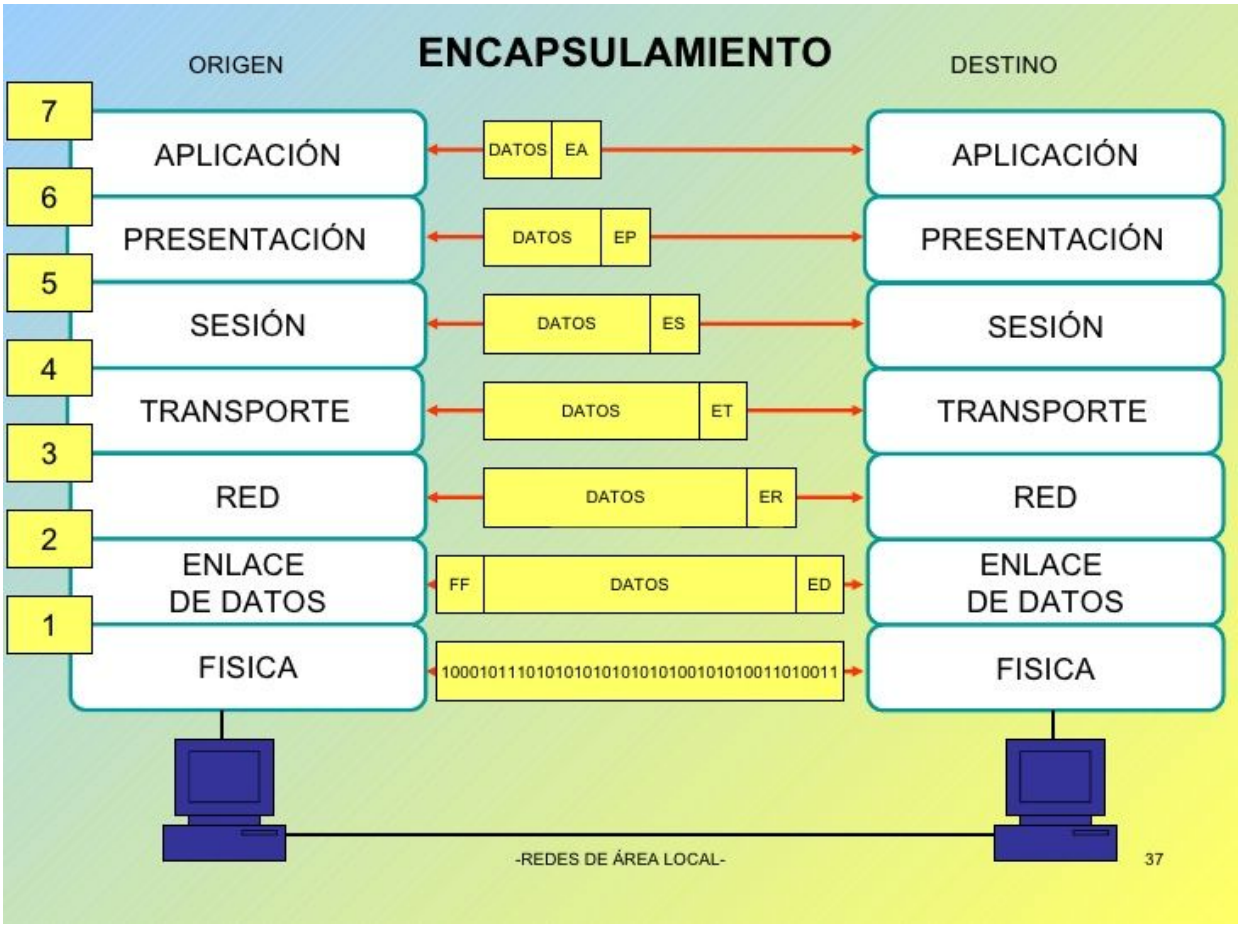
OSI, Open System Interconnection, es un modelo que ayuda a fabricantes y empresas a crear redes compatibles, independientemente de la tecnología utilizada.

OSI divide la comunicación entre dos equipos en 7 niveles, a través de los que se envían los datos entre emisor y receptor. Cada capa trabaja de forma independiente a las demás, sin saber qué hace la capa inferior o la superior. Lo único que sabe una capa es que tiene que ofrecer unos servicios a la capa inferior y que debe solicitar unos servicios a la capa superior.

MODELO OSI		
Capa	Nivel	Función
7	Aplicación	Suministra servicios de red a las aplicaciones de usuario. Por ejemplo navegadores, correo electrónico, aplicaciones VoIP, etc.
6	Presentación	Es responsable que la información se pueda enviar de manera que el receptor la pueda entender. Por ejemplo, la conversión para que

		protocolos como el tcp/ip puedan hablar con el ipx/spx. Esta capa también permite cifrar los datos y comprimirlos.
5	Sesión	Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole.
4	Transporte	La capa de transporte garantiza que los mensajes lleguen a su destinatario sin errores, en la secuencia correcta y sin pérdidas de datos. Además fragmenta los datos que recibe de la capa de sesión y los pasa a la capa de red.
3	Red	Selecciona la ruta por la que se enviarán los datos por la red.
2	Enlace	Se encarga de temas como la topología de la red, detección de errores y del acceso a la red.
1	Capa Física	Se encarga de las especificaciones físicas y funcionales para realizar la conexión. ¿Qué voltaje utilizar para enviar un 1 o 0? ¿Cuántos microsegundos dura cada dígito? ...

A medida que los datos pasan de una capa a otra inferior, se encapsulan y se les añade información adicional.



EJERCICIO 11

Crea un documento de texto llamado **ej11redes** en tu carpeta compartida y contesta a las siguientes preguntas.

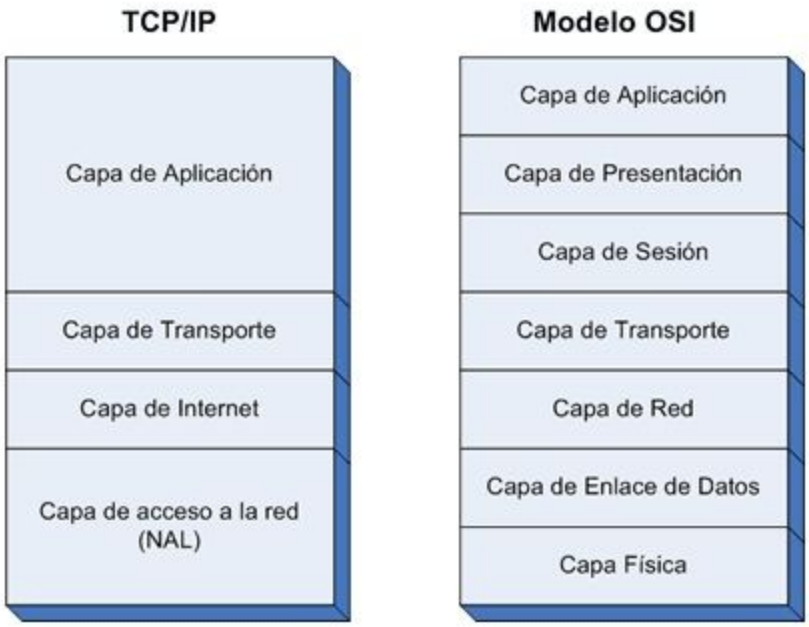
- ¿Con qué objetivo se desarrolló el modelo OSI?¿Quién lo promulgó?¿Cuándo?
- Resume los principios básicos en los que se basa el modelo OSI?
- ¿Por qué no se usa OSI en la actualidad?¿Cuándo dejó de usarse?
- ¿Es lo mismo un protocolo que un servicio?
- ¿En qué consiste la técnica “Divide y vencerás? Aparte de en informática ¿En qué otros campos se usa?
- ¿Qué es la encapsulación de datos? ¿Por qué es necesaria?
- ¿Cuándo apareció TCP/IP? ¿Se basa en el modelo OSI?

Arquitectura de protocolos TCP/IP

Un protocolo es un conjunto de reglas que utilizan todos los dispositivos para ser capaces de comunicarse entre sí.

TCP/IP es la familia de protocolos en los que se basa la red Internet. Gracias a esto se ha convertido en el estándar en el ámbito de las redes. Gracias al TPC/IP, redes heterogéneas y con distintos sistemas operativos pueden comunicarse. Asimismo, muchos componentes de hardware, como impresoras, routers, etc., incorporan en su firmware este protocolo para poder ser configurados dentro de la red.

Recibe este nombre en referencia a los dos protocolos más importantes que la componen: **Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP)**. Otros protocolos de esta familia son HTTP para acceder a páginas web, FTP para la transferencia de ficheros y SMTP y POP para correo electrónico.



En el siguiente vídeo podrás ver un símil de cómo trabaja la arquitectura TCP/IP

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

EJERCICIO 12

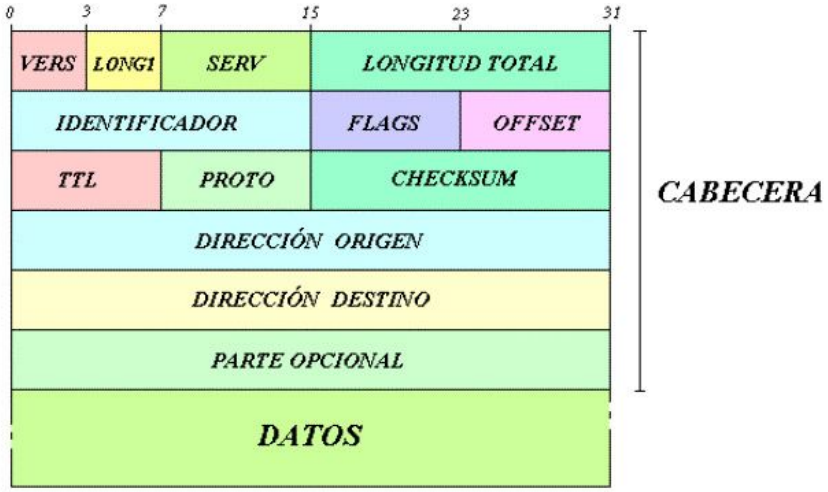
Crea un documento de texto llamado **ej12redes** en tu carpeta compartida y crea una tabla en la que relaciones cada una de las capas de la arquitectura TCP/IP con sus protocolos.

Protocolo TCP

Este protocolo se encarga principalmente de dividir la información a enviar en paquetes y asegurarse de que estos lleguen al destinatario sin errores y ordenados. Ya que cada uno de estos paquetes viaja por la red de forma independiente, incluso por caminos diferentes.

Protocolo IP

Es un protocolo de la capa de Internet de TCP/IP. Este protocolo coge cada uno de los paquetes que le pasa y le añade la dirección de destino, la dirección de origen además de otra información relativa a los datos.



Direcciones IP

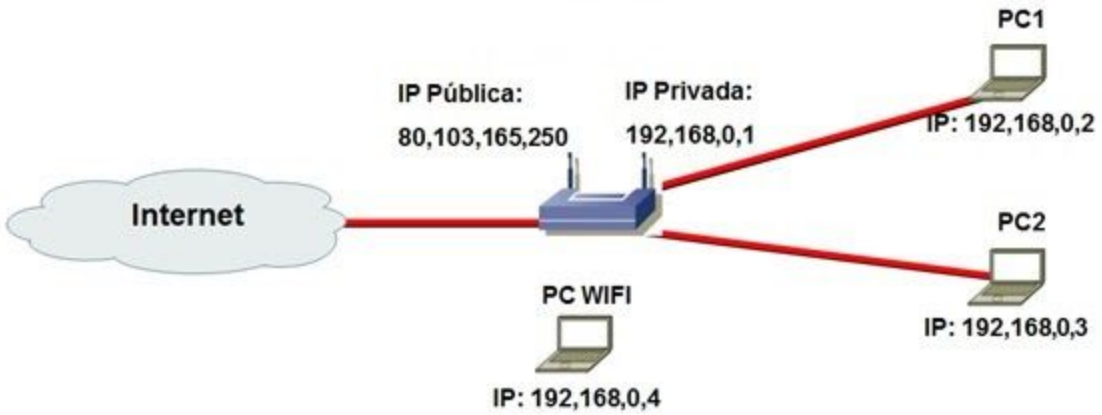
La dirección IP es un código numérico que identifica de manera unívoca a un equipo dentro de una red. Existen dos versiones de IP que se diferencian en el número de bits que la forman y por tanto del número de dispositivos a los que se pueden asignar en la red.

- **IPv4:** Están formadas por 4 bytes (32 bits). Para facilitar su representación suelen escribirse con 4 números decimales comprendidos entre el 0 y el 255, separados por puntos. Los ordenadores pueden tener cualquier dirección IP, excepto las acabadas en 0 que están reservadas para direcciones de red y las acabadas en 255 que están reservadas para broadcast. Un ejemplo de dirección IP válida para un equipo es 128.10.205.23
- **IPv6:** Están formadas por 16 bytes (128 bits. Esta versión surge para reemplazar a IPv4, que ya no dispone de direcciones suficientes para asignar a la gran cantidad de dispositivos que se han ido sumando a Internet en los últimos años. Estas direcciones se escriben como 8 grupos de cuatro dígitos hexadecimales separados por dos puntos.

  Por ejemplo 100e:017ab:8554:abe6:4568:ff5e:891e:abc6

Existen 2 tipos de direcciones, públicas y privadas:

- **Direcciones públicas**: Permiten que cada equipo conectado a Internet pueda ser identificado. Todo equipo conectado a Internet debe tener configurada una IP pública.
- **Direcciones privadas:** Son un conjunto de direcciones que se reservan para utilizarse en redes locales. Estas direcciones no son visibles desde Internet.



EJERCICIO 13

Crea un documento de texto llamado **ej13redes** en tu carpeta compartida en el que indiques cuáles son las direcciones IP reservadas para uso privado y en el que expliques en qué consiste NAT

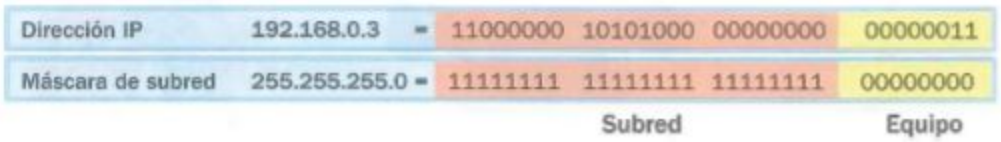
Máscara de red

En una red pueden crearse distintas subredes. Para diferenciar los equipos que pertenecen a las distintas subredes de una LAN se utilizan las máscaras de subred, que también se componen de 32 bits separados en cuatro octetos.

La dirección IP de una máquina se compone de dos partes cuya longitud puede variar: bits de red, que definen la red a la que pertenece el equipo, y bits de host, que son los que distinguen a un equipo de otro dentro de la red.

Los bits de red siempre están a la izquierda, y los de host, a la derecha. Por ejemplo; la dirección 195.10.20.4 con máscara 255.255.255.0 indica que hacemos referencia a un nodo que está en la red 195.10.20 y que es el nodo 4.

Sin embargo, la misma dirección 195.10.20.4, pero con máscara 255.255.0.0, hace referencia al nodo 4 de la subred 20, que a su vez está en la red 195.10.

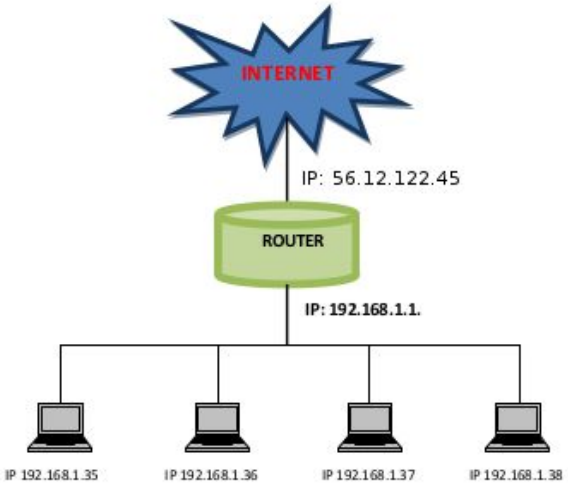


Puerta de enlace o Gateway

Para que un ordenador se pueda comunicar con otro, ambos deben pertenecer a la misma red. Cuando dos hosts no se encuentran en la misma red, se utilizan unas tablas de enrutamiento para decidir a qué

nodo se transmite la información. En este caso, el nodo al que se envía esta información actúa como pasarela (gateway) y él se encarga a su vez de transmitir esa información a la red de destino.

Un ejemplo característico es el router que tenemos en casa. Este enlaza nuestra LAN con Internet. Se caracteriza por tener una dirección IP privada (Puerta de enlace) para comunicarse con los equipos de la LAN y otra dirección IP pública suministrada por el ISP para comunicarse con Internet.

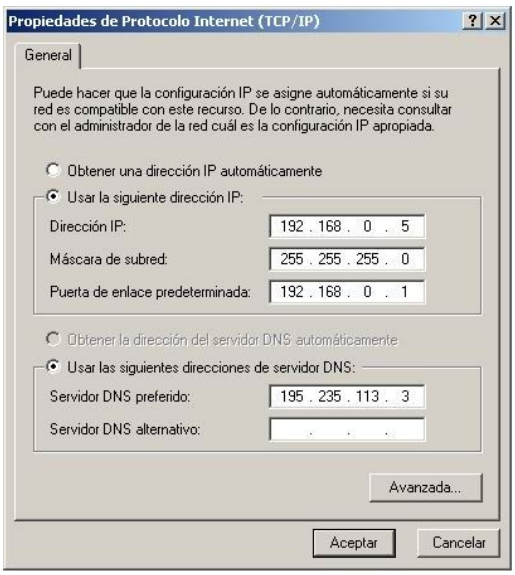


DNS

Las páginas web que podemos ver cuando estamos consultando la red de redes tienen su propia dirección IP, al igual que nuestro ordenador, nuestro router o cualquier otro dispositivo conectado a Internet. Las DNS se encargan de traducir nombres legibles para las personas - lo que es una dirección web - en identificadores binarios asociados con los equipos conectados a la red. Sin este sistema de nombres de dominio, en vez de escribir una URL tal y como la conocemos, escribiríamos una dirección IP.

Cada uno de nuestros dispositivos conectados a Internet tiene su cliente DNS. Al escribir en el navegador una dirección de Internet el cliente DNS solicita la IP a un servidor, y éste devuelve la información necesaria para que el ordenador conozca la IP del sitio. Este proceso dura milésimas de segundo.

Para que nuestro dispositivo pueda conectarse a Internet es necesario configurar todos los parámetros anteriores. Bien manualmente o de forma automática mediante DHCP. De tal forma que una posible configuración sería como la imagen siguiente.



EJERCICIO 14

- Abre una ventana de terminal con la combinación de teclas Ctrl + Alt + T
- Utiliza el comando **ifconfig** para obtener la IP, la Máscara y la MAC de tu ordenador
- Utiliza el comando **netstat -r** para obtener la IP de tu Puerta de enlace
- Utiliza el comando **arp -a | grep (IP de la puerta de enlace)** para obtener la MAC de tu Puerta de enlace.

Crea un documento de texto llamado **ej14redes** en tu carpeta compartida en el que apuntes todos los datos obtenidos anteriormente.