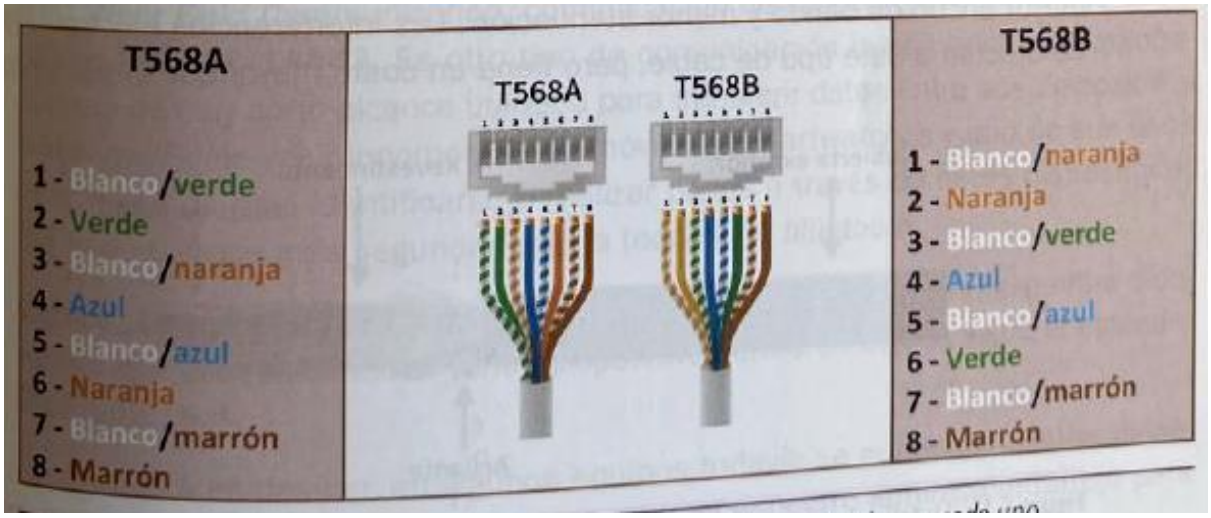
TEMA 05 – SISTEMAS INFORMÁTICOS EN RED

Redes informáticas

- Introducción
    - Conjunto de sistemas informáticos y dispositivos conectados
    - Permite que puedan comunicarse y compartir datos, recursos y servicios
    - Ventajas
        - Compartir
        - Reducción de costes
        - Mejora la comunicación
        - Gestión más eficiente
    - Desventajas
        - Menor seguridad
        - Necesidad de tenerla bien configurada y operativa
- Componentes de una red
        - Emisor, receptor/dispositivo final, dispositivo intermedios y canal/medi
    - Dispositivos finales, equipos o hosts
        - Ordenadores, impresoras con tarjetas de red y dirección IP, teléfonos IP, tablets, smartphones, smartTV…
        - Necesitan una tarjeta de red y un medio a través del cual conectarse (cable o inalámbrica)
    - Dispositivos intermedios
        - Conectan los dispositivos finales entre sí o una red con otra
        - Switch/commutador:
            - Conecta varios equipos de una red entre sí
            - Conecta varios segmentos de una red
            - Cableado RJ-45, se conecta a cada equipo a través del puerto Ethernet
            - En los puertos SFP se puede conectar un cable óptico, de cobre o RJ45 para añadir un equipo o conectarlo a otro switch o router
                - SFP: Small Form-factor Pluggable Transceiver (transceptor enchufable de factor de forma pequeño)
                - Versiones actualizadas: SFP+, SFP28, QSFP+, QSFP28
            - Anterior- también se usaban hubs o concentradores
                - Hubs envían cada mensaje a todos
                - Switches guardan interna- las direcciones MAC y la 1ª vez manda el mensaje a todos, pero luego asocia cada MAC a un puerto y solo envía el paquete a ese puerto
                - Más óptimo, rápido y fiable que los hubs
        - Puente o bridge:
            - Conecta 2º+ segmentos de una red o la divide en segmentos
            - También trabaja con direcciones MAC físicas
        - Punto de acceso:
            - Para extender el alcance de la red inalámbrica
            - Suelen ser omnidireccionales

        - Router:
            - Para conectar diferentes redes entre sí
            - Pueden ser tipo hardware o software
            - Trabajan con direcciones IP o lógicas en el lvl. 3 del modelo OSI
            - También
                - Establece la mejor ruta para la información
                - Adapta las señales de una red a otra
                - Organiza la información de las diferentes rutas
        - Módem:
            - Para la conexión a internet
            - El router se conecta al módem para que le provea de internet
                - A través de un ISP (Internet Service Provider)
                - A su vez, provee la señal de internet al resto de la red
            - En el ámbito doméstico van integrados (módem-router)
            - Si la señal llega por fibra óptica, el dispositivo que lo recie se llama ONT (Optical Node Terminal, terminal de nodo óptico)
        - Firewall:
            - Filtrar el tráfico que entra o sale de un equipo o red
            - Pueden ser hardware conectado al router o software en un equi
        - Repetidor:
            - Regenerar la señal
            - El uso principal es extender la longitud de la red
        - Transceptos (transceiver):
            - Para cambiar el tipo de medio de transmisión
            - Ejemplo: de fibra óptima a par trenzado
    - Medios de transmisión
        - Canales a través de los cuales va la info y los datos entre dispositivos
        - Por cable o guiados:
            - Par trenzado
                - Alambres de cobre trenzados en pares de hilos
                - Para evitar la interferencia electromagnética
                - Se agrupan en una cubierta de PVC
                - Se utilizan en redes locales cableadas o utilizan RJ45
                - Tipos:
                    - UTP (Unshielded Twisted Pair, par trenzado sin apantallar)
                        - Fácil, flexible y bajo coste para montar
                        - Muy sensible a interferencias electromagéticas
                    - STP (Shielded Twisted Pair)
                        - Más protección, más caro, menos flexible
                        - Cada par apantallado por malla de Al
                    - FTP (Foiled Twisted Pair, par trenzado con pantalla total)
                        - Pantalla protectora sobre todos los cable
                        - No tan protegido STP, más barato y flexibl

- Importante planificar por dónde se va a cablear para evitar las interferencias (aparte de apantalla-)
  - Evitar que vaya en paralelo con cables eléctricos
  - Evitar cercanía a cables de corriente y luces
  - Evitar fuentes de calos
- Los cables pueden ser de varias categorías
- 2 estándares (B en España):



- Cable coaxial
  - Núcleo de cobre por el que viajan las ondas electromagnéticas
  - Protegido por un aislante y una malla trenzada
  - Antes se usaba con frecuencia para redes LAN bus y tramos finales de las redes de fibra
  - Cada vez se usa menos porque se usa fibra hasta el hogar (FTTH): más velocidad, menos interferencia
- Fibra óptica
  - Núcleo de cable de plástico o vidrio por el que viajan los haces de luz
  - Cubre mayores distancias
  - Tiene mayor ancho de banda
  - Menor atenua-
  - Las interferencias electromagnéticas no le afectan
  - Coste mayor
  - Tipos: multimodo (varios) o monomodo (un haz de luz)

- Inalámbricos:
  - WiFi
    - Ondas de radio electromagnéticas
    - Estándar IEEE 802.11
    - Redes WLAN
    - Una de las tecnologías más utilizadas actual-

- WIMAX (Worldwide Interoperatibility for Microware Acces)
    - Estándar IEEE 802.16
    - Utiliza microondas para llevar internet a zonas rurales o que es imposible llevar el cable
- Bluetooth
    - Estándar IEEE 802.15 (IEEE 802.15.1)
    - Enlace punto a punto de radiofrecuencia
    - Distancias cortas (10-15m) tipo PAN o WPAN
    - Versión 5 ha mejorado la velocidad y el alcance
    - Alternativa: Wi-Fi Direct (forma fácil y directa de usar tecnología wifi para transmitir archivos de forma rápida)
- NFC (Near Field Communication)
    - Estándar ISO/IEC 14443
    - Comunicación inalámbrica por radiofrecuencia de muy corto alcance
    - Transferir datos entre dos dispositivos cercanos
    - Más seguridad que la tecnología bluetooth
- Zigbee, Z-Wave o Thread
    - Zigbee: estándar IEEE 802.15.4
    - Para internet de las cosas

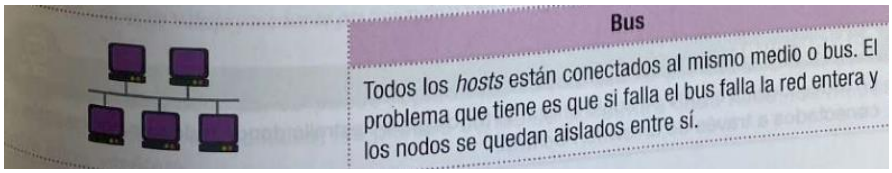
▪ En desuso: IrDA (infrarrojos)

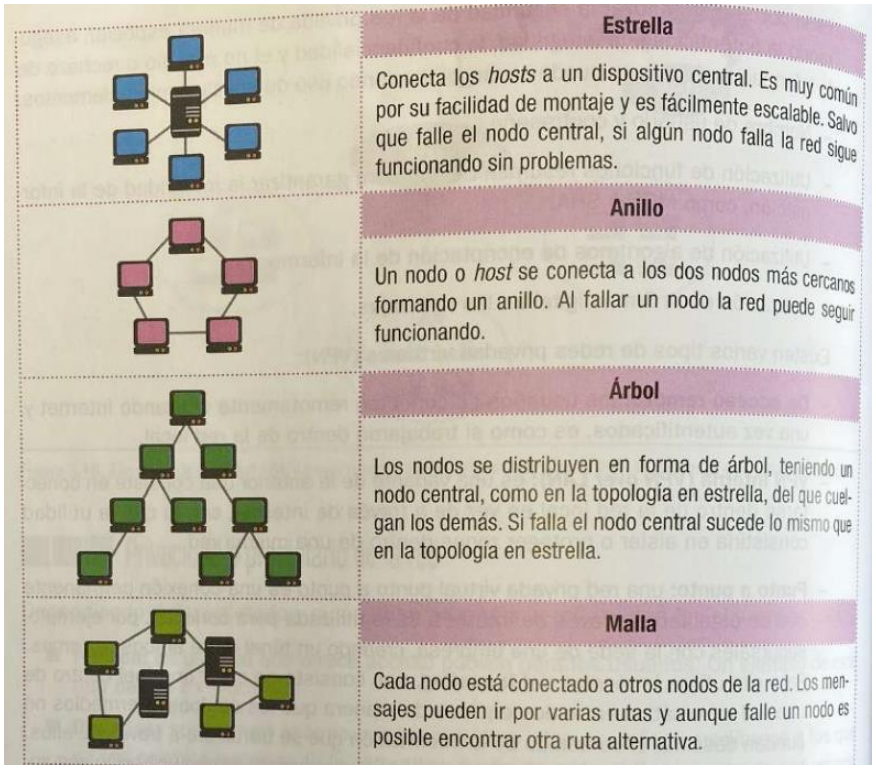
o Ancho de banda, velocidad y latencia
  ▪ Ancho de banda: capacidad del medio a la hora de transmitir esa info
    - Cantidad de datos que se pueden transmitir a la vez
    - Banda ancha: ancho suficiente- grande y la conexión a alta vel
  ▪ Throughput (rendi- del canal): vl a la que se transcriben esos datos
    - En bits por segundo (bps, kbps, Mbps, Gps…)
  ▪ Latencia: T que tarda la info en ir de un punto a otro
  ▪ Otros factores: calidad y fiabilidad de esa colección (QoS, quality of service)
o Control de acceso al medio
  ▪ Se encarga de controlar cómo se va a utilizar el medio físico por el que viajará la info
  ▪ Están los que utilizan un tipo de acceso controlado
    - CSMA: Carrier Sense Multiple Access (acceso múltiple con detección de portadora)
    - CSMA/CD: with Collision Detection
    - CSMA/CA: with Collision Avoidance
o Protocolos y estándares
  ▪ Protocolo: conjunto de reglas que describen cómo se rigen las comunicaciones
  ▪ Estándar: formalización de un protocolo
  ▪ Instituciones que publican normas para establecer estándares:
    - IEEE: Institute of Electrical and Electronics Engineers
    - ISO: International Organization of Standardization
    - EIA: Electronic Industries Alliance
  ▪ Normas más extendidas en relación con redes informáticas:

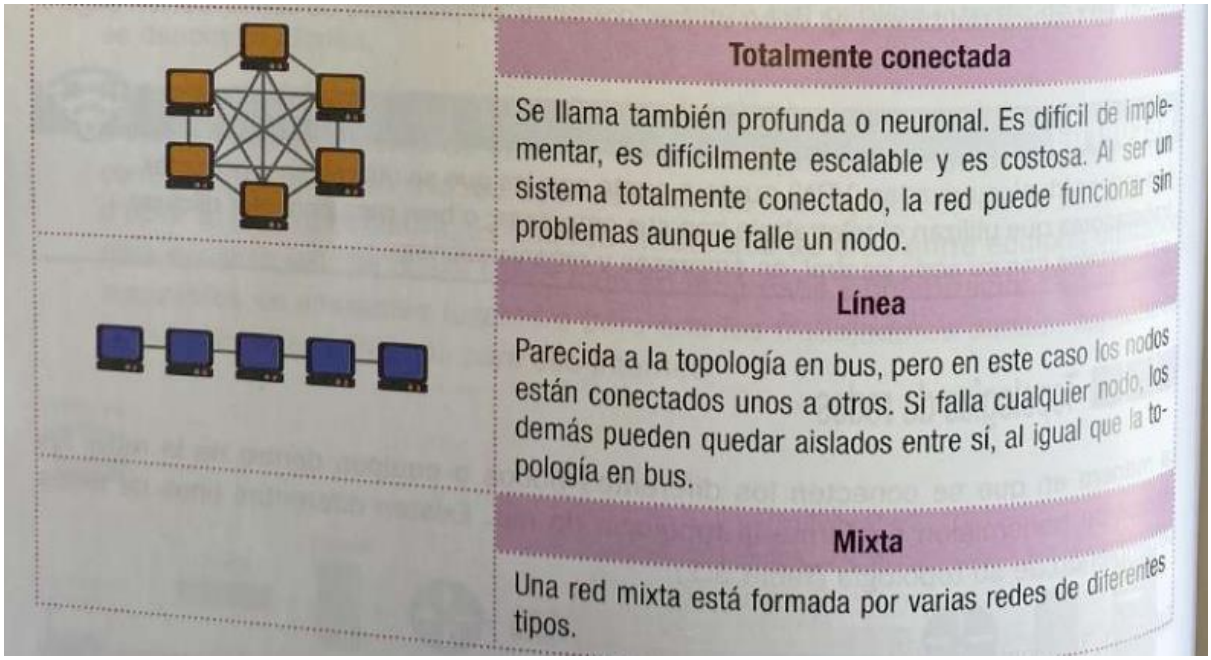
                - IEEE 802.3: estándar de las redes tipo Ethernet
                - IEEE 802.11: estándar para las redes inalámbricas
                - IEEE 802.15: estándar para redes inalámbricas de tipo personal o WPAN (.1: bluetooth, .4: ZigBee)
                - EIA/TIA T568A y T568B: normas para los cables de redes LAN
- Tipos de redes
    - Dirección de los datos
        - Símplex o unidireccional: los datos van en solo una dirección
        - Half-duplex o semidúplex: los datos pueden ir en ambas direcciones, pero no simultánea-
        - Full-dúplex o dúplex: pueden ir en las dos direcciones simultánea-
    - Destinatarios
        - Unidifusión o unicast: los datos van de un usuario a otro
        - Multidifusión o multicast: los datos van de un usuario a varios
        - Difusión o broadcast: los datos van de un usuario a todos
    - Medio físico
        - Cableadas
        - Inalámbricas
        - Híbridas
    - Relación de los equipos de la red
        - Entre iguales o peer 2 peer (p2p): todos los nodos son iguales
        - Cliente-servidor
    - Dimensión y alcance
        - PAN (WPAN): Personal Area Network
            - Muy corto alcance (10m aprox)
            - Estándar 802.15
        - LAN (WLAN, HAN, VLAN): Local Area Network
            - Áreas pequeñas (cientos de metros)
            - Estándares 802-3 para cable y 802.11 para inalámbricas
            - Inaámbrica: WLAN
        - MAN: Metropolitan Area Network
            - Una o varias ciudades cercanas (varios km)
        - WAN: Wide Area Network
            - Redes de mayor alcance y dimensión
            - Desde distintas ciudades, países o continentes
    - Privacidad o propietario de la red
        - Pública
        - Privada (si utiliza parte pública y parte privada, híbrida)
        - Red privada virtual o VPN
            - Crea una red virtual entre 2o+ equipos a través de internet
            - Cada equipo ve a los demás como si estuviesen en una red local
            - Sobre todo en empresas y organizaciones que tengan sucursales en diferentes lugares o para teletrabajar

- Asegurar privacidad de la red privada
    - Usuario y contraseña
    - Hash
    - Algoritmos de encriptación de la info
    - Utilización de la firma digital en los mensajes
    - Tipos VPN:
        - De acceso remoto
        - VPN interna (VPN over LAN)
            - Variante de la anterior
            - Conectarse dentro de red local en vez de internet
            - Utilidad: aislar o proteger zonas dentro de una misma red
        - Punto a punto
            - Conexión permanente que se establece a través de internet
            - Uso: sucursales con la sede
            - Utiliza la técnica del tunneling: túnel dentro de una red informática entre 2 equipos de manera que los equipos intermedios no puedan descifrar el contenido de la info que se transfiere a través de ellos

- Topologías de redes







Totalmente conectada

Se llama también profunda o neuronal. Es difícil de implementar, es difícilmente escalable y es costosa. Al ser un sistema totalmente conectado, la red puede funcionar sin problemas aunque falle un nodo.

Línea

Parecida a la topología en bus, pero en este caso los nodos están conectados unos a otros. Si falla cualquier nodo, los demás pueden quedar aislados entre sí, al igual que la topología en bus.

Mixta

Una red mixta está formada por varias redes de diferentes tipos.

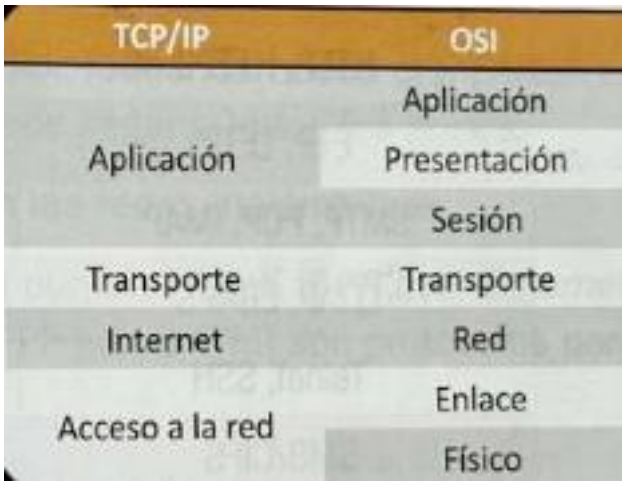
- Mapas físicos y lógicos de una red
    - Para diseñar o estudiar una red, es necesario realizar un mapa físico y lógico
    - Pueden solucionar problemas de diseño o de seguridad
    - Útiles para documentar la red una vez creada
    - Mapa lógico
        - Gráfico esquemático que permite ver los elementos de una red
        - Mediante programas simuladores de red (Packet Tracer)
    - Mapa físico: también se puede representar la red dentro del espacio real
        - Mediante software de diseño

Modelos de referencia

- Modelo OSI
  - OSI: Open Systems Interconnection
  - Modelo teórico de referencia
  - Utilizado para interconexión de diferentes tipos de sistemas
  - 7 niveles: cada uno tiene una función bien definida
  - Cada nivel se comunica con los adyacentes añadiendo una serie de cabeceras o información a los paquetes que se trasladen vertical-

Capa o nivel	**Función**
Aplicación	Permite a las aplicaciones acceder a las demás capas.
Presentación	Cifra y comprime los datos.
Sesión	Permite a los usuarios establecer más de una sesión.
Transporte	Se asegura y confirma que los datos han llegado a su destino.
Red	Encamina de la manera más adecuada (óptima) los datos por la red.
Enlace	Agrupa los datos y se encarga de que no haya errores en la transmisión.
Física	Se encarga de todo lo relativo a la parte física de la transmisión.

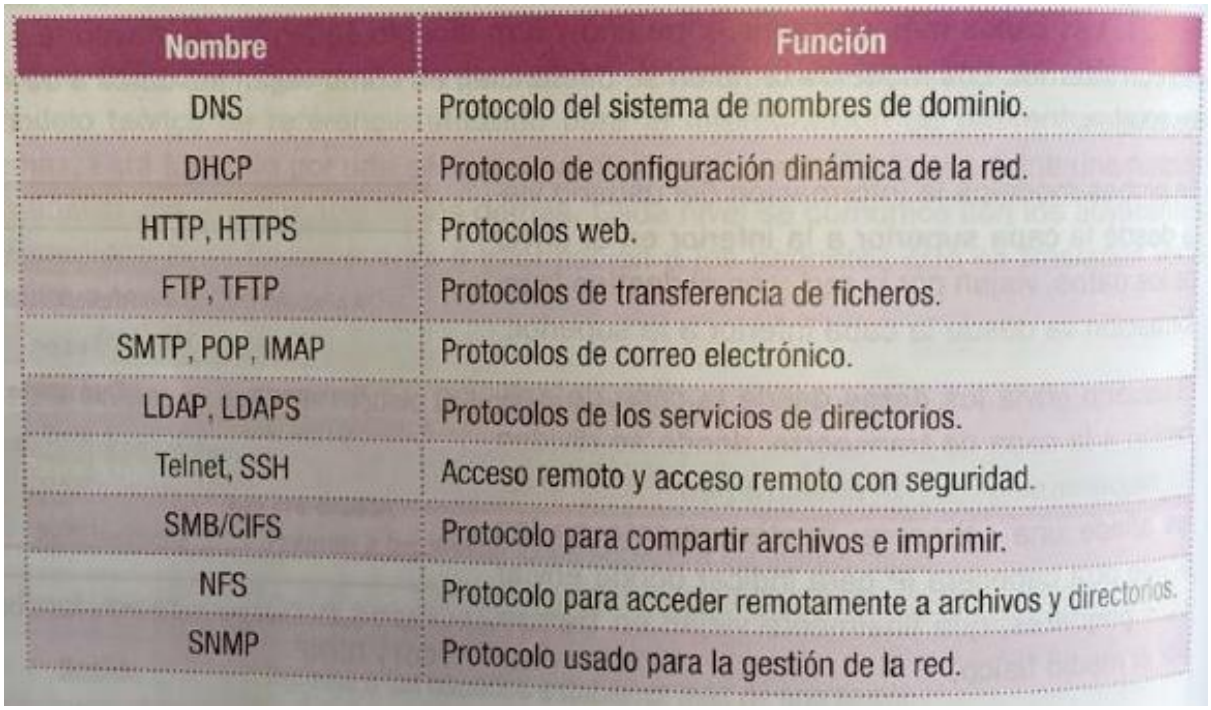
- TCP/IP (Transmission Control Protocol, Internet Protocol)
  - 4 capas o niveles que realizan una función similar a las del OSI
  - Cada capa realiza una función para preparar el envío y la recepción de los datos a través de una red
  - Es el utilizado en las redes LAN
- Comparación entre los modelos OSI y TCP/IP



  - Las capas más similares son las de transporte y la de red con internet
  - Los modelos también se diferencian en cómo viajan los datos a través de los niveles
- Protocolos utilizados en las redes
  - Protocolos del modelo TCP/IP en relación con la capa donde trabaja

TCP/IP	Protocolos
Aplicación	DNS, DHCP, HTTP, FTP, TFTP, SMTP, POP, IMAP, LDAP, Telnet, SSH, SMB, NFS, SNMP
	TLS/SSL
Transporte	
	TCP, UDP, SCTP
Internet	IP, ARP, RARP, ICMP, IGMP, IPSEC
Acceso a la red	Ethernet, Wi-Fi, PPP

- Se denomina pila de protocolos
  - Aplicación



Nombre	Función
DNS	Protocolo del sistema de nombres de dominio.
DHCP	Protocolo de configuración dinámica de la red.
HTTP, HTTPS	Protocolos web.
FTP, TFTP	Protocolos de transferencia de ficheros.
SMTP, POP, IMAP	Protocolos de correo electrónico.
LDAP, LDAPS	Protocolos de los servicios de directorios.
Telnet, SSH	Acceso remoto y acceso remoto con seguridad.
SMB/CIFS	Protocolo para compartir archivos e imprimir.
NFS	Protocolo para acceder remotamente a archivos y directorios.
SNMP	Protocolo usado para la gestión de la red.

  - Transporte
    - TCP (Transmission Control Protocol): crear conexiones y garantizar la entrega de los datos
    - UDP (User Datagram Protocol): no requiere conexión y envía la info a través de mensajes o datagramas
    - SCTP (Stream Control Transmission Protocol): reúne las características de los dos anteriores y está orientado a la conexión y la transferencia la realiza transmitiendo mensajes
    - TLS (Transport Layer Security): para la transferencia de la info entre sitios web de forma segura y cifrada
  - Internet
    - IPv6 y IPv4: protocolos encargados de encaminar los datos a través de su dirección IP, no están orientados a la conexión y trabajan con datagramas

                - IPSec: incorpora la seguridad a los protocolos IP
                - ARP (Addredd Resolution Protocol) y RARP (Reverse): se utilizan para conocer la IP de un host a través de la MAC o al revés
                - ICMP (Internet Control Message Protocol): para enviar mensajes de control entre redes (para ver si hay conexión y comprueba la latencia)
                - IGMP (Internet Group Management Protocol): gestionar la multidifusión en las redes
            - Acceso a la red
                - Ethernet: protocolo para acceder al medio
                - Wifi: para acceder al medio en las redes inalámbricas
                - PPP (Point to Point Protocol): para las conexiones punto a punto
    - Número de puerto
        - Cada protocolo suele trabajar en un número de puerto por defecto
        - El puerto de origen se asigna de forma dinámica para que pueda haber más de una comunicación a la misma aplicación
        - El puerto de destino suele ser un puerto predeterminado (configurable)
        - En general, no puede haber 2 apps escuchando un mismo puerto
        - Número de 16 bits (0 a 65535)
        - Los 1024 primeros se les conoce como puertos bien conocidos
            - Reservados para apps y servicios más utilizados
    - Protocolo de transferencia de hipertexto (transferencia de info)
        - HTTP (Hypertext Transfer Protocol) o HTTPS (Secure, sobre SSL/TLS)
        - Permiten la transferencia desde un servidor con archivos de tipo HTML
        - Cliente usa un navegador web
        - HTTP: puerto 80 por defecto
        - HTTPS: puerto 443 por defecto
            - Solamente navegador y servidor web pueden descifrar el certificado SSL
    - Transferencia de ficheros
        - FTP (File Transfer Protocol)
        - Sobre TCP
        - Puerto 21 por defecto
        - TFPT (Trivial): bajo protocolo UDP, más simple y rápido, menos seguro
            - Para archivos pequeños cuando no se requiere mucha segurida
            - Puerto 69
        - FTPS (Secure File Transfer Protocol): FTP sobre SSL
        - SFTP (Secure): FTP sobre SSH
            - Hay que autenticarse y se cifra la info
            - Puerto 22
    - Conexión remota (acceso a equipos remotos)
        - El equipo debe tener un servidor y el desde el que se accede un cliente o un programa como Putty
        - Telnet: no seguro
            - Puerto 23
            - Casi no se usa actual-

        - SSH
            - Puerto 22
            - Mediante intérprete de órdenes o comandos
            - Genera una clave pública y otra privada
            - La pública se envía al destino y se asocia a la cuenta de origen
    - Protocolos de escritorio remoto
        - Igual que el anterior, pero usando el entorno gráfico
        - VNC (Virtual Network Computing)
            - Software libre
            - Puerto 5900
        - RDP (Remote Desktop Protocol)
            - Por Microsoft
            - Puerto 3389
            - Se puede usar en Linux con XRDP (implementación de software libre de este protocolo)
    - Protocolos de correo electrónico
        - SMTP y SMTP seguro (SMTP sobre TLS/SSL)
            - Enviar correos desde una app cliente de correo
            - Puerto 464 y 587 en su forma segura
        - POP3 y POP3 seguro (POP3 sobre TLS/SSL)
            - Para recibir correos desde una app cliente de correo
            - Puerto 110 y 995 en su forma segura
        - IMAP o IMAP seguro (IMAP sobre TLS/SSL)
            - En lugar de POP3 para no descargar los correos desde el servidor en el equipo propio, sino trabajando con ellos en el servidor
            - Puerto 143 y 993 en su forma segura
    - Protocolo para compartir recursos
        - SMB
        - Puerto 445
    - Protocolos para copias remotas
        - RCP (Remeto Copy): en Linux, no seguro
        - SCP (Secure Copy Protocol): versión segura del anterior, RCP sobre SSH
        - RSYNC: permite copiar y sincronizar carpetas remotas
    - Protocolos de directorio activo
        - Para iniciar sesión en los ordenadores a través de internet
        - Para controlar quién se puede conectar y quién tiene acceso a determinados recursos
        - LDAP (Lightweight Directory Acces Protocol) y LDAPS
        - Windows: lo usa Active Directory
        - Linux: a través de OpenLDAP
        - Puerto 289 y 636 para la versión segura

Direccionamiento

- Direcciones IP
    - Una parte identifica la red y otra a cada equipo o host dentro de la red
    - IPv4

        - 32 bits (cada uno 8 bits)
        - De 0 a 255 cada uno separado por un punto (notación decimal con puntos o punteado)
    - IPv6
        - Surgieron cuando las IPv4 no eran suficientes ante el gran creci-
        - 128 bits
        - 8 grupos de 16 bits (hexadecimales) separados por ":"
        - Cada grupo de 4 bits se representa con un dígito hexadecimal
        - Mayor seguridad (IPSec)
        - No es necesario representar todos los 0 (0000:0000 -> 0:0) o ::
    - Dirección de loopback o de bucle local
        - Para hacer referencia a la interfaz de la red propia
        - Sirve para conectarse al equipo propio a través de apps y servicios que utilizan TCP/IP
        - En IPv4 se suele utilizar 127:0.0.1 y para IPv6 ::1
        - Para referirse por el nombre: localhost
    - Dirección de broadcast o de difusión
        - Para mandar un mensaje al resto de los equipos en una red IPv4
        - Se obtiene poniendo 1 a todos los bits de la dirección de red destinados a los hosts
        - IPv6 no tienen broadcast, se usan unicast y para varios nodos multicast
    - Direcciones IP públicas y privadas
        - Públicas: visibles desde Internet
        - Privadas: dentro de la LAN
- Máscara de subred
    - Para diferenciar entre la parte de la dirección que identifica a la red y la parte que identifica a cada host de la red
    - Para dividir una red en subredes
    - En IPv4 la máscara de subred tiene 32 bits, al igual que las direcciones IPv4
    - Se puede expresar como IPv4 o como CIDR (Classless Inter-Domain Routing)

Máscara de subred	CIDR	Bits de red	Bits de *hosts*
255.255.255.0	/24	24	8
255.255.0.0	/16	16	16
255.0.0.0	/8	8	24

Dirección IPv4 de la red: 192.168.0.0
Máscara de subred: 255.255.255.0

También se puede expresar de la siguiente forma, donde una barra y un número indican el número de bits que se van a dedicar a la red (notación CIDR):

192.168.0.0/24

...AND entre la dirección

- Clases de redes IPv4

Clase	Intervalo	Bits de red	Bits de *hosts*	Máscara de subred	Dirección de *broadcast*
A	0.0.0.0 127.255.255.255	8	24	255.0.0.0 /8	x.255.255.255
B	128.0.0.0 191.255.255.255	16	16	255.255.0.0 /16	x.x.255.255
C	192.0.0.0 223.255.255.255	24	8	255.255.255.0 /24	x.x.x.255
D	224.0.0.0 239.255.255.255	Utilizada para multicast			
E	240.0.0.0 255.255.255.255	Redes experimentales y para investigación			

  - 10.X.X.X, 172.16.X.X, 192.168.X.X: redes privadas
- Puerta de enlace
  - Dirección IP del dispositivo que permite conectar dispositivos con protocolos diferentes
  - Por defecto: 192.168.0.1 o 192.168.1.1
  - Se necesita además un nombre de usuario y una contraseña
- Subnetting
  - Con máscara 255.255.255.0 se reservan 254 equipos o hosts
  - Dividir una red en varias subredes
  - Necesario para reducir el número de equipos, mejorar seguridad y controlar mejor el tráfico en esa red
  - Para dividir la red en dos, hay que aumentar en 1 bit más la máscara de subred

Red1: 192.168. 0. 0 — 11000000.10101000.0000000.00000000
255.255.255.128 — 11111111.11111111.1111111.10000000
Red2: 192.168. 0.128 — 11000000.10101000.0000000.10000000
255.255.255.128 — 11111111.11111111.1111111.10000000

La red queda divida en las dos siguientes subredes que podrían direccionar cada una 2^7-2 *hosts* = 126 *hosts*.

Red1: 192.168.0.0/25
Direcciones válidas: 192.168.0.1 a 192.168.0.126
Dirección de *broadcast:* 192.168.0.127

Red2: 192.168.0.128/25
Direcciones válidas: 192.168.0.129 a 192.168.0.254
Dirección de broadcast: 192.168.0.255

- Servidores DHCP y DNS
  - La configuración estática: asignar manualmente
  - Configuración dinámica (DHCP): evita que 2 equipos tengan = IP
  - Los nombres de los equipos se pueden asignar también mediante un servidor DNS dentro de una red local

Conexión

- Redes cableadas

Tabla 5.8. Diferentes tipos de cables de red

Nombre	Tipo de cable	Distancia máxima del segmento	Velocidad máxima
100Base-T	Par trenzado	100 m	100 Mbps
100Base-FX	Fibra óptica	2 km	100 Mbps
1000Base-T	Par trenzado	100 m	1 Gbps
1000Base-LX	Fibra óptica	5 km	1 Gbps
10GBase-T	Par trenzado	100 m	10 Gps
10GBase-LX	Fibra óptica	10 km	10 Gps

- Redes inalámbricas

Estándar	**Banda**	**Velocidad máxima**
IEEE 802.11a	5 GHz	54 Mbps
IEEE 802.11b	2.4 GHz	11 Mbps
IEEE 802.11g	2.4 GHz	54 Mbps
Wifi 4 (IEEE 802.11n)	2,4 GHz y 5 GHz	450 Mbps
Wifi 5 (IEEE 802.11ac)	5 GHz	3,5 Gbps
Wifi 6 (IEEE 802.11ax)	2,4 GHz y 5 GHz	9,6 Gbps
Wifi 6E (IEEE 802.11ax)	2,4 GHz, 5 GHz y 6 GHz	9,6 Gbps

    - Seguridad en las redes inalámbricas
        - Redes abiertas
        - Redes con seguridad
            - WEP (Wired Equivalent Privacy)
                - Cifrado simple (clave estática de 68 o 128bits)
            - WPA (Wifi Protected Access)
                - Clave de 256 que cambia dinámica- en cada paquete
                - También incluye comprobación de la integridad de la inf
            - WAP2
                - Versión mejorada del anterior
                - Utiliza un algoritmo de cifrado más avanzado (AES)
            - WPA3
                - Cifrado más robusto
                - El cifrado es individual y ofrece mayor protección
        - Medidas que puede adoptarse para aumentar la seguridad:

        - Filtrado de la MAC (Media Access Control)
            - Solo se permite el acceso a aquellos dispositivos que tengan una dirección MAC concreta que previa- se ha almacenado como autorizada
        - Desactivar la difusión del SSID (Service Set Identifier)
            - El SSID es el identificador o nombre de la wifi propia
            - Desactivando su difusión no podrá ser visto por otros
        - Cambiar el SSID y la contraseña que vengan por defecto
        - Utilizar el cifrado más robusto que sea posible
- Conexión a internet
    - ADSL (Asymmetric Digital Subscriber Line): desapareciendo por fibra y otroas
    - Fibra: más utilizada actual-
    - PoE (Power over Ethernet): energía llega o se suministra usando el mismo cable
    - WIMAX: método inalámbrico para zonas donde no llega la fibra
    - Móvil
    - Conexiones a través de proxy
        - Dispositivo que se utiliza para que otros equipos tengan acceso a internet a través de él y así mejorar la seguridad y privacidad
        - Función de intermediario o puente
        - Preserva el anonimato de la IP
        - Controla acceso, filtra contenido, actúa como caché
        - Tipos
            - Web: acceder a través de la web a otros sitios web
            - Caché
            - Inverso: mejorar seguridad en la red de destino
            - NAT: ocultas las direcciones de los usuarios
            - Transparente: simple- actúa de intermediario

Configuración

- Configuración de la red en VirtualBox
    - Con la máquina apagada
    - Configuración -> Red -> Añadir un adaptador de red
    - Aspectos configurables:
        - Habilitar adaptador de red
        - Conectado a:
            - NAT (Network Address Translation): internet ofrecido por la máquina anfitriona, pero no puede conectarse con otras máquinas
            - Adaptador puente: la máquina virtual tiene su propia IP y puede funcionar como un nodo más de la red
            - Red interna: red entre las máquinas virtuales
            - Adaptador solo-anfitrión: red interna, pero solo entre máquina virtual y anfitrión
            - Controlador genérico: se puede añadir un controlador y añadirlo a las demás máquinas dentro de una red

        - Nombre: elegir el adaptador de red del sistema anfitrión que está conectado a la red
        - Avanzado
            - Tipo de adaptador
            - Modo promiscuo: cómo se verá el tráfico de la red, si permite todo, el de las máquinas virtuales o deniega todo
            - Para red interna solo anfitrión y puente
            - Dirección MAC: se puede cambiar la dirección MAC de la interfaz de red virtual o hacer que cambie generando una nueva aleatoria
            - Cable conectado: se puede (des)conectar el cable virtual de la red
- Configuración de la red en Linux
    - Configuración -> Red o Configuración de red cableada
    - Desde terminal
        - 'ip': muestra y modifica el enrutamiento, dispositivos de red, interfaces de red y túneles
        - 'ifconfig': muestra info y configura la interfaz de red
            - No instalado por defecto
        - 'iwconfig': muestra info y configura las interfaces de red inalámbricas
        - 'hostname': muestra o cambia el nombre de host del equipo
        - 'hostnamectl': muestra o cambia el nombre del equipo
            - Viene incorporado en 'systemd'
        - 'ping': envía petición a los hosts de la red
            - En Linux envía y recibe paquetes mientras no se corta el proceso
            - Se puede limitar con "-c"
        - 'host': utilidad para buscar DNS
        - 'nslookup': consulta los servidores de nombres de internet y resuelve las direcciones IP dado un determinado dominio
            - Se puede trabajar de modo interactivo o no interactivo
        - 'traceroute': muestra la ruta por la que van los paquetes en internet para llegar a su destino
        - 'netstat': muestra conexiones de red, tablas de enruta-, estadísticas e info sobre la interfaz de red
            - Está siendo reemplazado por 'ip' y 'ss'
        - 'ss': ver las conexiones de red del equipo propio
    - Servicios o daemonds de red
        - NetworkManager (escritorio)
            - En /etc/NetworkManager
        - 'systemd-networkd' (servidor)
            - En /etc/systemd/network
    - Netplan
        - Herramienta de administración de redes incluida en Ubuntu
        - Su configuración se encuentra en /etc/netplan
        - Trabaja con ficheros "yaml": formato para almacenar datos fácilmente legible para poder modificarlos sin problemas

- Configuración de la red Windows
    - Inicio -> Configuración -> Red e internet
    - También Panel de control -> Centro de redes y recursos compartidos
    - Se puede:
        - Ver las redes activas: tipo de acceso y conexiones de cada una
        - Cambiar configuración de uso compartido avanzado: detección de redes y uso compartido de archivos e impresoras
        - Cambiar configuración del adaptador
    - Comandos Símbolo del sistema:
        - 'getmac'
        - 'ipconfig': muestra info sobre adaptadores de red y permite su config
        - 'hostname': muestra el nombre del host o del equipo
        - 'ping': en Windows intenta el envío y recepción de 4 paquetes
        - 'tracerrt': muestra la ruta por la que van los paquetes en internet para llegar a su destino
        - 'nslookup'
        - 'netstat': muestra conexiones de red, tablas de enruta- e info sobre la interfaz de red
    - Powershell
        - 'Get-NetIPAddress': muestra la config de la dirección IP
        - 'Test-NetConnection': muestra info sobre una conexión

Monitorización y simulación de redes

- Monitorización de redes
    - Permite ver el tráfico y ver si funciona correcta-, sobrecarga, ataques o fallos
    - Herramientas:
- IPTraf
    - Linux, libre, por línea de comandos
    - Software libre
- Nmon
    - Linux, libre
    - Monitorización redes, hardware del sistema, recursos, kernel, memoria virtual, procesos…
- Wireshark: analizar tráfico de red
- Kismet: analizar redes inalámbricas
- Advanced IP Scanner
    - Ver hosts y servidores de una red LAN
    - Escanea y analiza los dispositivos de una red LAN
    - Informa de las direcciones IP y MAC, carpetas compartidas y servidores
- Nmap
    - Libre
    - Analizar redes, estado hosts, comprobar puertos abiertos, ver servidores en funciona- y SO instalados
- Simulador de redes
    - Antes de montar la red
    - Para comprobar que está correcta- diseñado y configurado
    - Cisco Packet Tracer, GNS3, Dynamips