Unidad 4: Sistemas Informáticos en red.

Un sistema informático en red es un conjunto de dispositivos interconectados que comparten recursos y se comunican entre sí a través de una red. Estos sistemas permiten a los usuarios compartir archivos y recursos, así como acceder a servicios y aplicaciones de forma remota.

Algunos ejemplos de sistemas informáticos en red incluyen servidores, estaciones de trabajo, dispositivos de almacenamiento en red (NAS), routers, switches, firewalls y otros dispositivos de red.

La configuración de un sistema informático en red puede variar dependiendo de la necesidad de cada organización o empresa. Algunas redes pueden ser locales (LAN) y limitadas a un área geográfica determinada, mientras que otras pueden ser redes de área extensa (WAN) que conectan diferentes sucursales o ubicaciones remotas.

La implementación de sistemas informáticos en red requiere considerar aspectos como la seguridad de la red, la gestión de usuarios y permisos de acceso, la administración de la red, la asignación de direcciones IP y la configuración de protocolos de comunicación, entre otros aspectos.

En resumen, los sistemas informáticos en red son fundamentales para la interconexión y comunicación de dispositivos en una organización, facilitando el acceso a información y recursos de forma eficiente y segura.

Componentes de una red.

El **emisor** que envía el **mensaje** hacia el **receptor** a través del **canal** o **medio.**

La **tarjeta de red** es un componente hardware necesario para la conexión de red. También es necesario el **software** que se utiliza para poder conectar el equipo a la red.

Los **dispositivos finales, equipos o hosts**, son los dispositivos conectados a una red pueden ser ordenadores, impresoras con tarjetas de red y dirección IP, smartphones, tables, smartTV.

Los **dispositivos intermedios** en una red son aquellos que se encargan de facilitar la comunicación entre los dispositivos finales, como computadoras, tablets, smartphones, entre otros. Algunos ejemplos de dispositivos intermedios en una red son:

1. Switches: Son dispositivos que se encargan de enviar datos de un dispositivo a otro en una red local (LAN). Ayudan a distribuir la información de forma eficiente y a segmentar la red en distintas subredes.

2. Puente o Bridge: conecta dos o más segmentos de una red, o divide una red en varios segmentos.

3. Routers: Son dispositivos que se encargan de dirigir el tráfico de datos entre diferentes redes, como una red local y la red de internet. Permiten establecer la conexión entre las distintas subredes y garantizar que los datos lleguen a su destino de forma segura y eficiente.

4. Puntos de acceso inalámbrico (Access Points): Son dispositivos que permiten la conexión inalámbrica de dispositivos a una red. Permiten la conexión de dispositivos como smartphones, tablets, laptops, entre otros, a la red de forma inalámbrica.

5. Firewalls: Son dispositivos que se encargan de proteger la red contra amenazas externas, como virus, malware, ataques cibernéticos, entre otros. Permiten controlar el tráfico de datos y filtrar el acceso a la red para proteger la información sensible.
¿Qué es la DMZ?

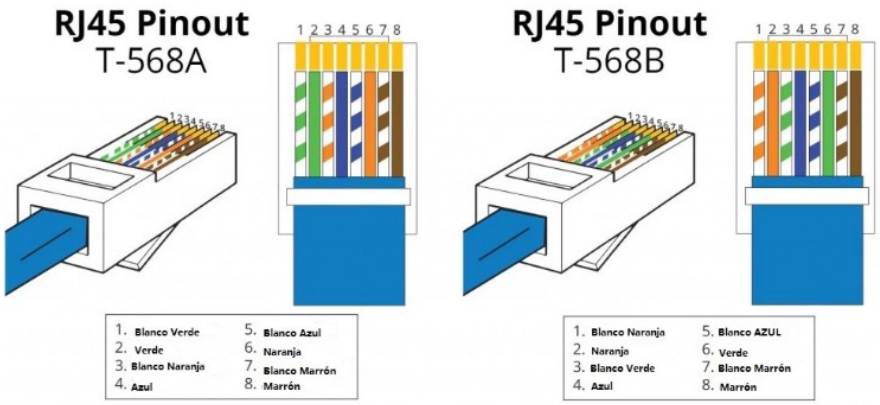
6. Repetidores: Equipos que se utilizan para regenerar la señal. Recibe la señal atenuada y la amplifica. La atenuación es la pérdida de señal a medida que viaja por el medio.

Estos son solo algunos ejemplos de dispositivos intermedios en una red, existen muchos otros dispositivos que cumplen funciones específicas para garantizar el funcionamiento eficiente y seguro de una red de comunicación.

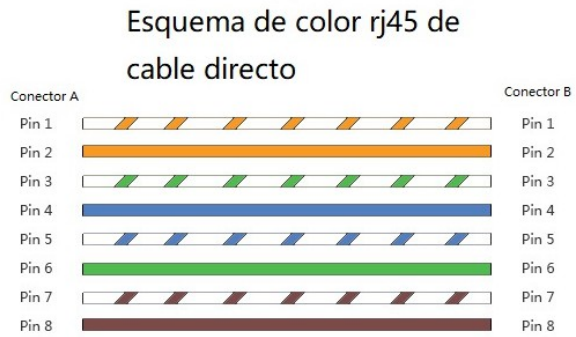
Los **medios de transmisión** son:
Los medios de transmisión en una red se refieren a los diferentes tipos de cables o tecnologías utilizadas para enviar datos entre dispositivos conectados. Pueden ser guiados o por cable, o no guiados o inalámbricos.

Guiados o por cable:

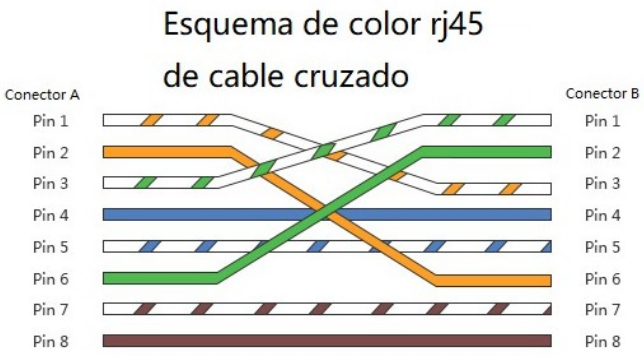
1. Cable de par trenzado: es el medio de transmisión más utilizado en redes de área local (LAN). Consiste en alambres de cobre entrelazados en pares de hilos, para evitar o reducir la interferencia electromagnética.
En los cables de par trenzado hay se han definido dos estándares para redes locales o LAN, T568A y T568B, los cuales proporcionan esquemas de cableado para la terminación de los cables con conectores RJ45.
Construiremos en clase un cable de red.



Un **cable de red directo** (los dos extremos con el mismo estándar, se suele usar el tipo B) es un tipo de cable de par trenzado que se usa en las redes de área local para conectar dos dispositivos diferentes (como un ordenador a un switch, un ordenador a un router…).



Un **cable de red cruzado** (un extremo de cada estándar) para conectar dos dispositivos del mismo tipo (como dos ordenadores, dos switch,…)



2. Fibra óptica: es un medio de transmisión que utiliza pulsos de luz para enviar datos a través de filamentos de vidrio u otros materiales transparentes. Ofrece una alta velocidad de transmisión y mayor capacidad de ancho de banda que otros medios de transmisión. Es actualmente la más utilizada.

3. Cable coaxial: es un tipo de cable compuesto por un conductor central rodeado por una capa aislante y una malla metálica. Se utiliza en redes de televisión por cable y en algunos sistemas de red de área local (LAN).

4. Transmisión inalámbrica: este tipo de medio de transmisión utiliza ondas de radio o microondas para enviar datos entre dispositivos sin la necesidad de cables físicos. Ejemplos incluyen Wi-Fi, Bluetooth y redes celulares.

Estos son solo algunos ejemplos de medios de transmisión en una red, y la elección del medio dependerá de factores como la distancia de transmisión, la velocidad de transmisión, la seguridad y la confiabilidad requerida en la red.

Tipos de redes.

- Atendiendo al método de transmisión de los datos en la red:

Simplex o unidireccional: los datos van sólo en una dirección.
Half-duplex o semidúplex: los datos pueden ir en ambas direcciones pero no simultáneamente.
Full-duplex o dúplex: los datos pueden ir en las dos direcciones de manera simultánea.

- Atendiendo al método de transmisión de la red:

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.

- Atendiendo al medio físico:

Cableadas: utilizan como medio físico o de transmisión medios guiados o cables.

Inalámbricas: utilizan como medio físico o de transmisión medios no guiados como radiofrecuencias, infrarojos o microondas.
Híbridas: utilizan en la misma red los dos tipos de medios anteriores.

- Atendiendo a la función que realizan los nodos:

Entre iguales o Peer to peer(p2p): todos los nodos son iguales entre sí, no hay ninguno haciendo la función de servidor.
Cliente-servidor: uno o varios nodos hacen la función de servidores y sirven peticiones a los demás equipos o nodos que hacen las veces de cliente, que lanzan las peticiones al servidor.

- Atendiendo a su tamaño:

PAN: Red de área personal. Corto alcance, 10 m. Se suele formar conectando los dispositivos mediante bluetooth (smartphone, tablets…)
LAN: Red de área local. Siguen siendo pequeñas pero mayores que la anterior. Cientos de metros como mucho. Oficinas, una empresa, un centro educativo. Si es inalámbrica se puede denominar **WLAN.** Se conectan por cable de par trenzado o wifi.
MAN: red de área metropolitana. Mayor que la LAN. Puede abarcar una o varias ciudades cercanas. Varios km.
WAN: Red de área extensa. Son las redes de mayor alcance y dimensión. Distintas ciudades, países o continentes. Pueden conectar diferentes equipos, redes LAN o redes MAN.

- Atendiendo al propietario y quién tiene acceso:

Pública: Red de acceso público a los usuarios. Internet.
Privada: Red a la que sólo tienen acceso sus propietarios y los usuarios acreditados.
Red privada virtual o VPN: Red virtual entre dos o varios equipos a través de internet, de manera que cada equipo ve a los demás como si estuviesen en una red de área local. Se crea los que se llama un túnel VPN. Empresas y organizaciones que tengan sucursales en diferentes lugares.

Topologías de redes

La manera en que se conectan los diferentes equipos dentro de una red.

- **Topología en bus**: todos los nodos están conectados a un mismo cable de red central.
- **Topología en estrella**: todos los nodos están conectados a un dispositivo central, como un concentrador o switch.
- **Topología en anillo**: los nodos están conectados en un circuito cerrado, donde la información circula en una sola dirección.
- **Topología en malla**: cada nodo está conectado directamente a todos los demás nodos de la red.
- **Topología en árbol**: los nodos están organizados en forma jerárquica, con un nodo raíz que conecta a varios nodos secundarios.
- **Topología mixta**: combina diferentes tipos de topologías en una misma red, adaptándose a las necesidades específicas de cada área.

En redes locales o LAN se suele utilizar la topología en estrella donde todos los nodos están conectados a través de un switch central.

Modelo OSI

El modelo OSI (Open Systems Interconnection) es un marco de referencia para entender cómo funciona la comunicación entre diferentes dispositivos de red. Fue desarrollado por la Organización Internacional de Normalización (ISO) en la década de 1980 y consta de siete capas que representan distintas funciones en el proceso de comunicación de red. Estas capas son:

1. **Capa física**: La capa más baja del modelo OSI, se encarga de la transmisión de datos a través del medio físico, como cables o ondas de radio.

2. **Capa de enlace de datos**: Se encarga de la comunicación entre dispositivos directamente conectados y de detectar y corregir errores en la transmisión de datos.

3. **Capa de red**: Se encarga de enrutar los datos a través de la red y de determinar la mejor ruta para su entrega.

4. **Capa de transporte**: Se encarga de segmentar, enviar y reensamblar los datos transmitidos de extremo a extremo.

5. **Capa de sesión**: Se encarga de establecer, mantener y finalizar sesiones de comunicación entre dispositivos.

6. **Capa de presentación**: Se encarga de la representación de datos para su intercambio entre sistemas heterogéneos.

7. **Capa de aplicación**: La capa más alta del modelo, se encarga de proporcionar servicios de red a las aplicaciones de usuario, como el correo electrónico o la navegación web.

El modelo OSI facilita la comprensión y el diseño de redes de comunicación al dividir el proceso en capas que se ocupan de funciones específicas, permitiendo la interoperabilidad entre diferentes tipos de dispositivos y tecnologías de red.

Modelo TCP/IP

El modelo TCP/IP es un modelo de red que se utiliza para la comunicación en Internet y en muchas redes locales. Se compone de cuatro capas diferentes: la capa de aplicación, la capa de transporte, la capa de red y la capa de enlace de datos. Cada capa se encarga de diferentes funciones para asegurar una comunicación efectiva entre dispositivos en una red. El modelo TCP/IP es ampliamente utilizado en todo el mundo y es la base de la comunicación en Internet. Usa los protocolos TCP (protocolo de control de transmisión) e IP (protocolo de internet).

Tanto en el modelo OSI como en el modelo TCP/IP, la información del usuario viaja desde la capa superior a la inferior en el envío de los datos, viajan por la red, y en el destino la información va desde la capa inferior a la superior.

En el modelo TCP/IP el usuario envía los datos desde la capa de aplicación a la capa de transporte, donde se dividen en segmentos (TCP) o datagramas (UDP) y se les añade una cabecera;

posteriormente se les añade otra cabecera IP para indicar dónde enviar esos paquetes, que finalmente viajan en tramas por el medio físico.

UDP (Protocolo de Datagramas de Usuario) y **TCP** (Protocolo de Control de Transmisión) son dos protocolos de comunicación diferentes que se utilizan para enviar información en Internet.

Principales diferencias entre UDP y TCP

- •TCP tiene que establecer una conexión entre el emisor y el receptor para transmitir datos, mientras que UDP transmite paquetes a otro dispositivo sin tener que establecer un canal ni preguntar si el receptor está listo.
- •UDP es más rápido que TCP porque no ordena ni comprueba los errores de los paquetes de datos.
- •TCP es más fiable que UDP. Comprueba que no haya errores y garantiza que los paquetes de datos se entregan a la aplicación que se comunica en el orden correcto.
- •TCP es ligeramente más seguro que UDP y es más difícil insertar datos maliciosos porque rastrea todos los paquetes de datos.

Resumen: la principal diferencia entre TCP y UDP es el método en que establecen la conexión, que a su vez afecta a la velocidad y seguridad de cada protocolo.

Protocolos del modelo TCP/IP

Habíamos dicho que el modelo TCP/IP está compuesto por cuatro capas: la capa de aplicación, la capa de transporte, la capa de red y la capa de enlace de datos.

- Capa de aplicación: en esta capa se encuentran los protocolos que permiten la comunicación entre aplicaciones.
HTTP (Hypertext Transfer Protocol): Protocolo utilizado para la transferencia de información en la World Wide Web.
HTTPS (Hypertext Transfer Protocol Secure): Versión segura de HTTP que utiliza encriptación para proteger la información transmitida.
FTP (File Transfer Protocol): Protocolo utilizado para la transferencia de archivos entre dispositivos en una red.
SMTP (Simple Mail Transfer Protocol): Protocolo utilizado para la transmisión de correos electrónicos.
POP3 (Post Office Protocol version 3): Protocolo utilizado para la recepción de correos electrónicos en un servidor de correo.
IMAP (Internet Message Access Protocol): Protocolo utilizado para acceder y gestionar correos electrónicos almacenados en un servidor remoto.
DNS (Domain Name System): Protocolo utilizado para convertir nombres de dominio en direcciones IP, permitiendo la identificación de los recursos de la red.
DHCP (Protocolo de Configuración Dinámica de Hosts, es un protocolo que asigna direcciones IP de forma automática a los dispositivos conectados a una red. Permite la gestión centralizada de direcciones IP y otros parámetros de configuración de red, como la puerta de enlace y los servidores DNS. DHCP simplifica la administración de redes al eliminar la necesidad de asignar manualmente direcciones IP a cada dispositivo.

Telnet es un protocolo que permite la comunicación entre dispositivos a través de una red TCP/IP. Permite a un usuario conectarse de forma remota a un servidor o dispositivo para acceder a una interfaz de línea de comandos y ejecutar comandos como si estuviera físicamente presente en el dispositivo.
SSH (Secure Shell) es un protocolo que permite a los usuarios acceder de forma segura a un servidor remoto. Utiliza encriptación para proteger la comunicación entre el cliente y el servidor, evitando que los datos sensibles puedan ser interceptados por terceros.
NFS (Network File System) es un protocolo que permite a los sistemas informáticos compartir archivos y directorios a través de una red. Fue desarrollado por Sun Microsystems en la década de 1980 y se ha convertido en uno de los protocolos más utilizados para compartir archivos en entornos de red de área local (LAN) o de área amplia (WAN).
El protocolo NFS permite a los usuarios acceder a archivos remotos como si estuvieran almacenados en su propio sistema local, lo que facilita la colaboración y el intercambio de archivos entre dispositivos conectados a la red. Es una herramienta fundamental para facilitar el intercambio de archivos y la colaboración en entornos de red, permitiendo a los usuarios acceder y compartir archivos de forma remota de manera eficiente y segura.

- Capa de transporte: en esta capa se encuentran los protocolos de transporte, como **TCP** (Protocolo de Control de Transmisión) y **UDP** (Protocolo de Datagrama de Usuario), que se encargan de manejar la conexión y el envío de datos entre dos dispositivos.

- Capa de red: en esta capa se encuentra el protocolo **IP** (Protocolo de Internet), que se encarga de enrutar los paquetes de datos entre nodos de una red.

- Capa de enlace de datos: en esta capa se encuentran los protocolos que se encargan de la transmisión de datos a través de un medio físico, como **Ethernet** y **Wi-Fi**.

En resumen, cada una de las capas del modelo TCP/IP tiene protocolos específicos que se encargan de diferentes funciones en la comunicación de datos a través de una red.

Número de puerto

Un puerto es como una puerta virtual a través de la cual se puede establecer una comunicación entre dos dispositivos. En un sistema informático, cada aplicación que necesita comunicarse a través de la red utiliza un número de puerto único asignado por el sistema operativo. 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, pero es configurable. Por ejemplo, se puede tener un servidor web escuchando los puertos 80 y 443, dependiendo del protocolo con el que se accedan. En general, no puede haber dos aplicaciones escuchando un mismo puerto. Por ejemplo, para tener dos servidores web en funcionamiento, se puede hacer que cada uno escuche en un número de puerto diferente. Cuando se accede a este servidor se indican la dirección IP (que identifica al equipo dentro de la red) y el número de puerto (que identifica a la aplicación dentro del servidor). El conjunto de dirección IP y número de puerto se denomina **socket**.
El rango de números de puerto va desde 0 hasta 65535 (16 bits, de 0 a 2^{16} -1), y están divididos en tres grupos:

- Puertos bien conocidos (del 0 al 1023): están reservados para servicios estándar, como el puerto 80 para HTTP o el puerto 25 para SMTP.
- Puertos registrados (del 1024 al 49151): son utilizados por aplicaciones específicas.

- Puertos dinámicos o privados (del 49152 al 65535): son utilizados por aplicaciones efímeras y pueden ser asignados por el sistema operativo de forma temporal.

Por lo tanto, un sistema informático puede tener múltiples puertos abiertos o sockets configurados para manejar múltiples comunicaciones simultáneas con diferentes servicios o aplicaciones. La cantidad de puertos o sockets disponibles para su uso dependerá de la capacidad y configuración del sistema en cuestión.

Algunos números de puerto comúnmente utilizados para varios protocolos:

- HTTP: 80
- HTTPS: 443
- FTP: 21
- FTPS: 990
- SSH: 22
- Telnet: 23
- SMTP: 25
- POP3: 110
- IMAP: 143
- DNS: 53
- SNMP: 161
- LDAP: 389
- RDP: 3389

Estos son sólo algunos ejemplos y pueden variar dependiendo de la configuración del sistema o red.

Direccionamiento IP

El direccionamiento IP es un sistema de numeración utilizado para identificar de manera única a cada dispositivo en una red de comunicaciones. Las direcciones IP están formadas por una serie de números que se dividen en cuatro bloques separados por puntos, por ejemplo: 192.168.1.1. Estas direcciones se utilizan para enviar y recibir información entre los dispositivos conectados a una red, permitiendo que los datos sean entregados de forma correcta a su destino. Existen dos tipos de direcciones IP: las direcciones **IPv4**, que son las más comunes y constan de 32 bits (4 grupos de 8 bits, es decir, 4 bytes) que se representan con 4 números decimales, y las direcciones **IPv6**, más recientes, que consisten de 128 bits (8 grupos de 16bits) que se representan con números hexadecimales y permiten una mayor cantidad de direcciones disponibles. Por ejemplo: 15ba:0000:0000:0000:0000:20ef:2020:2200. Se puede representar también como 15ba:0:0:0:0:20ef:2020:2200, o como 15ba::20ef:2020:2200

La **dirección de loopback** es una dirección especial que se utiliza para establecer una comunicación interna en un dispositivo, sin necesidad de que la información salga o entre en la red física. En IPv4, la dirección de loopback es 127.0.0.1, mientras que en IPv6 es ::1. Esta dirección se utiliza principalmente para realizar pruebas de red y diagnósticos en el propio dispositivo.
Para referirse a la dirección de loopback por el nombre se usa la palabra **localhost**. Se utiliza mucho para desarrollar y probar el software.

La **dirección de broadcast**, también conocida como dirección de difusión, es una dirección especial utilizada en redes para enviar un mensaje a todos los dispositivos de la red. En una red de área local (LAN), la dirección de broadcast es una dirección IP especial que termina en 255 en la

parte del host, lo que indica que el mensaje debe ser transmitido a todos los dispositivos en la red. Por ejemplo, si la dirección IP de un dispositivo en una red es 192.168.1.5, la dirección de broadcast para esa red sería 192.168.1.255.

Máscara de subred

Una mascara de subred es una serie de números binarios o decimales que se utilizan para dividir una red en subredes más pequeñas. La mascara de subred determina qué parte de una dirección IP pertenece a la red y qué parte pertenece a los dispositivos individuales en esa red. Se utiliza en la configuración de redes informáticas para organizar y administrar eficientemente las direcciones IP y mejorar la seguridad y el rendimiento de la red.

Se puede expresar en forma de dirección IPv4 (decimal con puntos) o bien con la notación CIDR (Classless Inter-Domain Routing, enrutamiento entre dominios sin clases)

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

Ejemplo:

Dirección IPv4 de la red 192.168.16.0
Dirección de máscara de subred 255.255.255.0 ó /24
24 bits destinados a la red y 8 bits

Clases de redes IPv4

Según el rango de direcciones IP tenemos la siguiente clasificación:

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			

En las redes de clase A el rango de direcciones 127.0.0.0 a 127.255.255.255 no se utiliza porque se reserva como dirección de loopback.
La dirección de red 0.0.0.0 se reserva para indicar cualquier valor posible en algunos casos, y en otros para indicar que no se ha asignado una dirección IP.
Los rangos de direcciones 10.0.0.0 a 10.255.255.255, 172.16.0.0 a 172.31.255.255 y 192.168.0.0 a 192.168.255.255 se reservan para ser utilizadas en redes privadas.

Puerta de enlace

La **puerta de enlace**, también conocida como **gateway**, es un dispositivo que actúa como intermediario entre diferentes redes informáticas para facilitar la comunicación entre ellas. Se encarga de enrutar el tráfico de datos entre redes, traducir protocolos de comunicación y gestionar la seguridad de la conexión. La puerta de enlace puede ser un hardware específico o un software configurado en un equipo de red. Es fundamental para la interconexión de redes y el acceso a internet.
En una red local, indicará la dirección del dispositivo que proporciona salida a internet. Para acceder al router hay que conocer su dirección IP que, por defecto, suele ser 192.168.0.1 ó 192.168.1.1. Se necesitará además un nombre de usuario y contraseña.

Ejemplo de subnetting

Para definir una red se puede hacer con dos notaciones:

- **dirección_ip/n** (dirección IP y n.º de bits que pertenecen a los hosts)
  Por ejemplo: 192.168.0.0 /24

- **dirección ip y máscara_subred**
  Por ejemplo: Direción IP 192.168.0.0 y máscara 255.255.255.0

Con la máscara 255.255.255.0, el número de bits que se reservan para los equipos son:
2^8-2=256-2=254 equipos.
Se quitan dos, una para la dirección de red que tendrá todos los bits reservados para hosts a 0, y la otra para la dirección de broadcast dentro de la red, que tendrá a 1 todos los bits reservados para hosts.
Las direcciones IP que se pueden asignar a los equipos en esa red serían desde el 192.168.0.1 al 192.168.0.254.

El subnetting es el proceso de dividir una red IP en subredes más pequeñas, o subredes, para una mejor gestión de la red y asignación de direcciones IP más efectiva.

Por ejemplo:

Red1:	192.168.0.0	11000000.10101000.00000000.00000000
	255.255.255.128	11111111.11111111.11111111.10000000
Red2:	192.168.0.128	11000000.10101000.00000000.10000000
	255.255.255.128	11111111.11111111.11111111.10000000

Cada red podría direccionar 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

En Red1 el primer bit de host está a 0 y en Red2 el primer bit de host está a 1. Ya estos bits no se destinan a los hosts sino a la red, se denominan **bits prestados**.

Para ampliar el número de bits destinados a hosts porque se necesiten más equipos en una red local, se utilizaría la técnica de **supernetting** que consiste en quitar uno o varios bits de los destinados a la red y añadirlos a los bits destinados a los equipos.

Pasos para comprobar la dirección IP de un equipo.

Comprueba la dirección IP de un equipo con el **SO Windows**. Pasos:

1. Abre el menú Inicio y escribe "cmd" en la barra de búsqueda. Presiona Enter para abrir la ventana de símbolo del sistema.

2. En la ventana de símbolo del sistema, escribe el comando "ipconfig" y presiona Enter.

3. Busca la sección que se llama "Adaptador de Ethernet" (si estás conectado por cable) o "Adaptador de red inalámbrica" (si estás conectado por Wi-Fi).

4. En la sección correspondiente, busca la línea que dice "Dirección IPv4" o "IPv4 Address". La dirección que aparece al lado de esta línea es la dirección IP de tu equipo.

Alternativamente, también puedes obtener la dirección IP de tu equipo siguiendo estos pasos:

1. Haz clic en el icono de red en la barra de tareas (por ejemplo, en la esquina inferior derecha de la pantalla) para abrir el Centro de redes y recursos compartidos.

2. Haz clic en tu conexión actual (por ejemplo, "Conexión de red inalámbrica" o "Conexión de red Ethernet").

3. En la ventana que se abre, haz clic en "Detalles".

4. En la ventana que se abre, busca la línea que dice "Dirección IPv4" o "IPv4 Address". La dirección que aparece al lado de esta línea es la dirección IP de tu equipo.

Comprueba la dirección IP de un equipo con el **SO Linux**. Pasos:

En modo comando se comprueba con el comando **ifconfig** y el comando **ip address show**
En modo gráfico pon tú los pasos.

Comprobar la dirección IP pública de un equipo.

Existen muchas herramientas web para comprobar nuestra dirección IP pública.

Cuál es mi IP | Cómo saber mi IP pública (cual-es-mi-ip.net)

Actividades de IP

- **Actividad 1:** Si tienes la dirección IP 192.168.56.1 y la máscara de subred 255.255.255.0 calcula cuál será la dirección de red.

```
        192.168. 56.1          11000000.10101000.00111000.00000001
AND   255.255.255.0            11111111. 11111111. 11111111. 00000000
--------------------------     ----------------------------------------------
        192.168. 56.0          11000000.10101000.00111000.00000000
```

- **Actividad 2:** Dada la red 172.16.0.0/16 , indica cuál sería el rango válido de direcciones IP y la dirección de broadcast.

  Si pasas a binario la dirección de red y la máscara de subred, obtienes lo siguiente:
  10101100.00010000.00000000.00000000
  11111111. 11111111. 00000000.00000000

  El rango de direcciones válidas sería desde:
  10101100.00010000.00000000.00000001 = 192.16.0.1
  a
  10101100.00010000.11111111.11111110 = 172.16.255.254

  La dirección de broadcast la obtienes de poner a 1 todos los dígitos destinados a los hosts.
  10101100.00010000.11111111.11111111 = 172.16.255.255

- **Actividad 3:** De las siguientes direcciones IP indica cuáles sí y cuáles no pertenecerían a la red 192.168.20.0/22
  a) 192.160.20.5
  b) 192.168.22.5
  c) 192.168.24.5

  Si pasas a binario la dirección de red y la máscara de subred, obtienes lo siguiente.
  11000000.10101000.00010100.00000000
  11111111. 11111111. 11111100. 00000000

  El rango de direcciones válidas sería desde:
  11000000.10101000.00010100.00000001 = 192.168.20.1
  a
  11000000.10101000.00010111.11111110 = 192.168.23.254

  Con lo que se ve que la a) y la b) sí pertenecerían a esa red, y la última dirección, la c) no pertenecería.

  También puedes realizar la operación AND entre las direcciones IP y la máscara de subred y así obtendrías la red a la que pertenece cada una. Por ejemplo, en el caso de la a):

```
        192.160.20.5                11000000.10101000.00010100.00000101
AND   255.255.252.0         AND    11111111 . 11111111.11111100.00000000
-------------------------   ------------------------------------------------------
        192.168. 20.0               11000000.10101000.00010100.00000000
```

Lo que indica que la dirección 192.168.20.5 con la máscara de subred /22 sí pertenecería a la red 192.168.20.0/22

- **Actividad 4:** Divide la siguiente red en cuatro subredes: 192.168.10.0/24

Tomo dos bits prestados para poder dividir la red en cuatro. La máscara de subred quedaría como 255.255.255.192 /26

Red1:	192.168. 10. 0	11000000.10101000.00001010.00000000
	255.255.255.192	11111111 . 11111111.11111111.11000000
Red2:	192.168. 10. 64	11000000.10101000.00001010.01000000
	255.255.255.192	11111111 . 11111111.11111111.11000000
Red3:	192.168. 10. 128	11000000.10101000.00001010.10000000
	255.255.255.192	11111111 . 11111111.11111111.11000000
Red4:	192.168. 10. 192	11000000.10101000.00001010.11000000
	255.255.255.192	11111111 . 11111111.11111111.11000000

Red1: 192.168. 10. 0/26	Rango IP 192.168.10.1 - 192.168. 10. 62 Dirección de broadcast: 192.168. 10. 63
Red2: 192.168. 10. 64/26	Rango IP 192.168.10.65 - 192.168. 10. 126 Dirección de broadcast: 192.168. 10.127
Red3: 192.168. 10. 128/26	Rango IP 192.168.10.129 - 192.168. 10. 190 Dirección de broadcast: 192.168. 10. 191
Red4: 192.168. 10. 192/26	Rango IP 192.168.10.193 - 192.168. 10. 254 Dirección de broadcast: 192.168. 10. 255

Actividades de construcción de cables de red

Necesitas cable, conectores RJ45, crimpadora o grimpadora y un utensilio para cortar cables (cúter o tijera).

Seguridad en las redes inalámbricas.

Las redes inalámbricas son cada vez más vulnerables a ataques debido a su naturaleza de transmisión de datos a través de ondas de radio. Por lo tanto, es importante tomar medidas de seguridad para proteger la información (integridad) y la privacidad de los usuarios.
Las redes abiertas son las redes sin protección, por lo que cualquier usuario que tenga acceso a la red se puede conectar a ella sin necesidad de autentificación.

Algunas recomendaciones para mejorar la seguridad en las redes inalámbricas incluyen:

1. Encriptar la comunicación:

La encriptación **WEP** (Wired Equivalent Privacy) y **WPA** (Wi-Fi Protected Access) son dos tecnologías de seguridad utilizadas en las redes inalámbricas para proteger la privacidad de la información transmitida a través de ellas.

WEP fue uno de los primeros protocolos de encriptación utilizados en redes Wi-Fi, pero ha demostrado ser vulnerable a diversos ataques y no se considera seguro en la actualidad.

Utiliza una clave estática de 68 o 128 bits que se configura en el router inalámbrico y en todos los dispositivos que se conectan a la red. Esta clave estática se utiliza para encriptar y desencriptar los datos que se envían a través de la red, evitando que personas no autorizadas puedan acceder a la información.

Sin embargo, la tecnología WEP con clave estática se considera obsoleta y vulnerable a ataques de hackers, ya que la clave estática puede ser fácilmente interceptada y descifrada. Se recomienda utilizar protocolos de seguridad más avanzados, como WPA o WPA2, que ofrecen una mayor protección y seguridad para las redes inalámbricas.
Por otro lado, WPA es una mejora de WEP que ofrece una mayor seguridad a través de técnicas de encriptación más avanzadas. Utiliza una clave de 256 bits que cambia dinámicamente en cada paquete que se transmita. También incluye la comprobación de la integridad de la información, para comprobar que llegue correctamente y no haya sido manipulada. Utiliza el algoritmo de cifrado TKIP.

En la actualidad, se recomienda utilizar **WPA2** o **WPA3** en lugar de WEP o WPA para garantizar la seguridad de las redes inalámbricas. Estos protocolos ofrecen una mayor protección contra ataques cibernéticos y son más difíciles de vulnerar.

WPA2 utiliza un algoritmo de cifrado más avanzado, AES.
WPA3 utiliza un algoritmo de cifrado más avanzado, ya que el cifrado de datos es individual.

2. Cambiar las contraseñas por defecto: Cambiar las contraseñas predeterminadas de los routers y dispositivos conectados a la red para evitar accesos no autorizados.

3. Configurar un firewall: Utilizar un firewall para filtrar el tráfico de la red y evitar posibles ataques.

4. Ocultar el SSID (Identificador del servicio): Deshabilitar la difusión del nombre de la red (SSID) para dificultar que los hackers encuentren la red.

5. Controlar el acceso a la red: Utilizar técnicas como filtrado de direcciones MAC para controlar quién puede acceder a la red.

6. Actualizar el firmware del router: Mantener actualizado el firmware del router y de los dispositivos conectados para corregir posibles vulnerabilidades de seguridad.

7. Utilizar una red virtual privada (VPN): Utilizar una VPN para cifrar la comunicación y proteger la privacidad de los usuarios.

8. Configurar la red de invitados: Crear una red de invitados separada para los dispositivos de visitantes y restringir su acceso a la red principal.

En muchos routers domésticos existe una función llamada **WPS** (Wifi Protected Setup), que se utiliza para conectarse la router de forma fácil y rápida, normalmente a través de un PIN. Puede activarse accediendo a la configuración del router o mediante un botón.
Se utiliza cada vez menos porque aumenta la inseguridad del router, pero es una forma cómoda y rápida de entrar. Se está sustituyendo por otro método, **WiFi Easy Connect** que surgió junto con el protocolo **WPA3**.

Al seguir estas recomendaciones y estar atento a posibles vulnerabilidades, se puede mejorar la seguridad en las redes inalámbricas y proteger la información de los usuarios.

Actividad 5. Si tienes un router wifi, entra en su configuración y comprueba cómo cambiar su SSID.

1. Investiga cómo cambiar el SSID en el manual de tu enrutador inalámbrico. Encuentra las instrucciones específicas para tu modelo de enrutador. En un lateral o en la parte de abajo verás los siguientes datos: nombre de la red wifi (SSID), clave wifi, URL para acceder al router desde tu equipo, nombre de usuario y contraseña.

2. Accede a la configuración de tu enrutador inalámbrico a través de un navegador web. Ingresa la dirección IP del enrutador en la barra de direcciones para acceder a la página de inicio de sesión.

3. Inicia sesión en la página de configuración del enrutador con el nombre de usuario y la contraseña predeterminados (que suelen ser admin/admin o admin/password). Si has cambiado la contraseña, introdúcela en su lugar.

4. Busca la sección de configuración de red inalámbrica o wireless settings en la interfaz de administración del enrutador. Allí encontrarás la opción de cambiar el SSID de la red.

5. Ingresa un nuevo nombre para tu red inalámbrica en el campo correspondiente. Puedes usar letras, números y caracteres especiales para personalizar el nuevo SSID.

6. También podrás dejar de emitir el SSID si lo tienes activo desactivando la opción **Broadcast SSID** o **Emitir SSID**.

7. Guarda los cambios y reinicia el enrutador para que la nueva configuración de red entre en vigor.

8. Conecta tus dispositivos a la red inalámbrica utilizando el nuevo SSID y contraseña si es necesario. Verifica que la conexión se haya establecido correctamente.

Recuerda que es importante elegir un SSID único y seguro para proteger tu red inalámbrica de posibles intrusiones.

Actividad 6: Comprueba la seguridad de tu wifi.

Para comprobar la seguridad de una red WiFi en Windows 11, puedes seguir estos pasos:

1. Haz clic en el ícono de red en la barra de tareas en la esquina inferior derecha de la pantalla.

2. Selecciona la red WiFi a la que estás conectado y haz clic en "Propiedades".

3. En la ventana que se abre, ve a la pestaña "Seguridad".

4. Aquí podrás ver el tipo de cifrado de la red (por ejemplo, WPA2, WPA3) y la clave de seguridad que se está utilizando.

5. También puedes verificar la seguridad de la red siguiendo estos pasos: ve a Configuración > Red e Internet > Wi-Fi y selecciona la red a la que estás conectado. Aquí podrás ver si la red es segura o no.

Si quieres asegurarte de que tu red WiFi es segura, te recomendamos utilizar un cifrado fuerte como WPA3 y cambiar regularmente la contraseña de tu red. También es importante mantener el firmware de tu router actualizado para protegerte contra posibles vulnerabilidades de seguridad.

Seguridad en las redes informáticas.

La seguridad en las redes informáticas es un aspecto fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información que se transmite a través de ellas. Algunas medidas que se pueden implementar para mejorar la seguridad en las redes informáticas son:

1. Implementar firewalls y sistemas de detección de intrusiones para proteger la red de posibles ataques externos.
2. Mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad para cerrar posibles brechas de seguridad.
3. Utilizar contraseñas fuertes y cambiarlas periódicamente para proteger las cuentas y dispositivos de accesos no autorizados.
4. Limitar los accesos a la red y a los recursos de información solo a los usuarios autorizados.
5. Utilizar cifrado para proteger la información confidencial que se transmite a través de la red.
6. Realizar copias de seguridad periódicas de la información crítica para poder recuperarla en caso de una brecha de seguridad.
7. Formar y concienciar a los usuarios sobre las buenas prácticas de seguridad informática, como no abrir correos electrónicos sospechosos o no compartir información confidencial en redes públicas.
8. Monitorizar la red en busca de posibles actividades maliciosas y responder de manera rápida y eficaz en caso de detección de una brecha de seguridad.

En resumen, la seguridad en las redes informáticas requiere una combinación de medidas técnicas, procedimentales y de concienciación para proteger de manera efectiva la información que se transmite a través de ellas.

Control de acceso

El control de acceso en seguridad informática se refiere a la práctica de limitar el acceso a sistemas, redes y datos a usuarios autorizados, con el fin de proteger la información y prevenir accesos no autorizados. Este control se puede aplicar a nivel físico, lógico y administrativo.

A nivel físico sería por ejemplo medidas de control de acceso a los edificios donde se encuentran los sistemas informáticos, como los **CPD (Centro de Proceso de Datos)**, con controles de acceso regulados por sistemas de identificación electrónica, vigilante y cámaras de seguridad…
Un CPD es un espacio físico donde se almacenan servidores, equipos de red y sistemas de almacenamiento de datos de una organización. Estos centros suelen contar con medidas de seguridad, sistemas de refrigeración y energía redundante para garantizar la disponibilidad y seguridad de los datos.

Algunas medidas de control de acceso incluyen la implementación de contraseñas fuertes, autenticación de dos factores, uso de certificados digitales, control de permisos de acceso a nivel de usuario y la implementación de políticas de seguridad que regulen el acceso a la información.

El control de acceso es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información en entornos informáticos, y es una parte esencial de cualquier estrategia de seguridad informática.

Firewall (Cortafuegos)

Un firewall es un tipo de software o hardware de seguridad que se utiliza para proteger una red informática de amenazas externas, como virus, malware, hackers y otros ataques maliciosos. El firewall monitorea y controla el tráfico de datos que entra y sale de la red, permitiendo el acceso solo a ciertos tipos de información y bloqueando el acceso a otros. Ayuda a prevenir intrusiones no autorizadas y protege la información confidencial de la red.

Un **firewall por hardware** es un dispositivo físico dedicado a proteger una red informática de amenazas externas o intrusiones. Este tipo de firewall se coloca entre la red local y la red externa (como Internet) y monitorea y controla el tráfico de datos que entra y sale de la red.

Los firewalls de hardware suelen ser más seguros que los firewalls por software, ya que funcionan de forma independiente de los sistemas operativos y aplicaciones de la red, lo que hace más difícil para los hackers a nivel de sistema eludir la seguridad del firewall. Además, los firewalls por hardware están diseñados para manejar grandes volúmenes de tráfico de datos y ofrecen un rendimiento más rápido y eficiente que los firewalls por software.

Una de las utilidades de los cortafuegos hardware es crear las **DMZ** ("demilitarized zone") o zonas desmilitarizadas dentro de una red. Es una zona dentro de una red aislada del resto de la red.
Es una red o área de una red que se sitúa entre la red interna de una organización y la red externa (generalmente Internet). La DMZ actúa como una capa adicional de seguridad al aislar los servidores y recursos que requieren acceso desde el exterior, como servidores web o servidores de correo electrónico, de la red interna de la organización. Esto ayuda a proteger la red interna de posibles ataques externos y minimiza el riesgo de que un intruso acceda a datos sensibles o recursos críticos. La DMZ se puede conectar con el exterior, pero no con la red interna que está fuera de su zona; sin embargo, los equipos de dentro de la red sí pueden acceder a la DMZ. Por lo general, el tráfico de la red externa es el que puede tener más peligro a la red.

Un **firewall por software** es un programa informático que se instala en un dispositivo para protegerlo de amenazas en línea y de posibles ataques cibernéticos. Este tipo de firewall monitorea el tráfico de red entrante y saliente y bloquea o permite el acceso según las reglas de seguridad establecidas. Los firewalls por software son esenciales para proteger la información y la privacidad de los usuarios mientras utilizan internet. También lo puede tener integrado el sistema operativo, o el antivirus.
Ejemplos:

Windows Defender Firewall (integrado en el sistema operativo Windows)
Norton Firewall
McAfee Personal Firewall
ZoneAlarm Firewall
Comodo Firewall
...

Servidor proxy

Un servidor proxy es un dispositivo intermediario que se encarga para que otros equipos tengan acceso a internet a través de él para mejorar la velocidad de acceso a los recursos, filtrar contenido no deseado o mejorar la seguridad y privacidad al ocultar la dirección IP del usuario. Los servidores proxy pueden ser configurados en dispositivos individuales o en redes completas para manejar múltiples solicitudes de forma eficiente.

Configuración de la red en VirtualBox

La configuración de la red se puede modificar con la máquina apagada. Se puede añadir hasta 4 adaptadores de red. Configuración → Red → Adaptador.
Puedes elegir entre diferentes tipos de adaptadores de red, como NAT, Red interna, Puente (bridge) u Host-only. Cada tipo de adaptador tiene sus propias características y se utiliza para diferentes propósitos.

Si seleccionas el tipo de a**daptador Puente** (Bridge), la máquina virtual tendrá su propia dirección IP en la red del host y podrá comunicarse con otros dispositivos en la red.

Si seleccionas el tipo de **adaptador NAT** (Network Address Translation), la máquina virtual compartirá la conexión de red del host y tendrá una dirección IP privada asignada por VirtualBox. No puede conectarse con otras máquinas.

Puedes configurar la **red interna** para permitir la comunicación entre varias máquinas virtuales, pero no con el host ni con otros dispositivos en la red.

Adaptador solo-anfitrión: red interna pero sólo entre la máquina virtual y el anfitrión.

Configuración de la red en Linux

Puedes seleccionar **Configuración → Red** o directamente pulsar sobre **Cableada conectada,** y después sobre Configuración de red cableada. Se accede a una ventana con información sobre la velocidad de la conexión, la dirección IP, la dirección física o MAC, puerta de enlace predeterminada y los DNS.

Comandos:

- ip: Muestra y manipula la información de las direcciones IP y enrutamiento del sistema.
- arp -a Gestiona las tablas
- iwconfig: Muestra y configura información de las interfaces de red inalámbricas.
- hostname: Muestra el nombre del sistema.
- hostnamectl: Muestra o configura el nombre del sistema.
- ping: Prueba la conectividad de red con otro host enviando paquetes de datos.
- host: Realiza consultas de DNS para resolver nombres de host en direcciones IP y viceversa.
- nslookup: Realiza consultas de DNS para resolver nombres de host en direcciones IP y viceversa con mayor detalle que el comando 'host'.
- traceroute: Muestra la ruta que toman los paquetes de red desde tu sistema a otro host.

- netstat: Muestra estadísticas de red como conexiones activas, tablas de enrutamiento, estadísticas de interfaz, etc.
- ss: Muestra información sobre las conexiones de red del sistema, similar a 'netstat'.

Configuración de la red en Windows

Puedes seleccionar **Inicio → Configuración → Red e Internet** o **Panel de control → Centro de redes y recursos compartidos**
Aquí se ven las redes que están activas y, de cada una, su tipo de acceso y las conexiones.
Se puede establecer que la dirección IP se obtenga a través de DHCP o bien añadir una dirección IP fija.
También se puede cambiar el nombre del equipo en la red, o establecer a un dominio u otro grupo. En estos casos habrá que reiniciar el equipo para que los datos surjan efecto.

Comandos:

• getmac: muestra la dirección MAC de un equipo.
• ipconfig: muestra la configuración de red de un equipo, incluyendo la dirección IP, máscara de subred, puerta de enlace predeterminada, etc.
• hostname: muestra el nombre del equipo.
• ping: comprueba la conectividad entre dos equipos enviando paquetes de datos y recibiendo respuestas.
• tracert: muestra la ruta que sigue un paquete de datos para llegar a un destino determinado.
• nslookup: muestra la información de un servidor de nombres de dominio (DNS) o realiza la traducción de nombres de dominio a direcciones IP.
• netstat: muestra las conexiones de red activas, puertos abiertos, estadísticas de red, entre otros.

Monitorización y simulación de redes

Antes de montar una red informática, lo más adecuado es probar su funcionamiento mediante algún software de simulación de redes, lo que permitirá detectar y corregir posibles errores de diseño. Una vez montada podrás monitorizarla para detectar anomalías en su funcionamiento. Se puede ver el tráfico que circula por ella y detectar posibles ataques e intrusos dentro de la red.
El Cisco Packet Tracer es un software de simulación.

Prácticas con Packet-tracer (tecnologia-informatica.es)

Ejercicios prácticos de redes de datos con Cisco Packet Tracer by Moisés Pérez Delgado - Issuu