USUARIOS, GRUPOS Y PERMISOS

USUARIOS Y GRUPOS

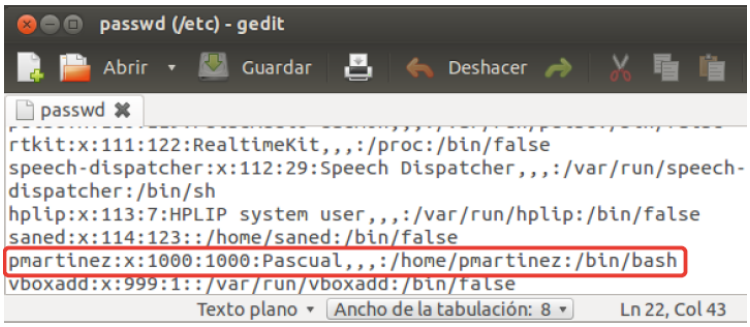
Usuario → Persona virtual, se identifica en un sistema para hacer uso de un determinado nivel de acceso. Misma persona puede identificarse con diferentes usuarios.

Grupo → Conjunto de personas virtuales que cumplen un determinado rol. Asignar directivas o permisos de forma ágil.

Usuarios en Ubuntu

Cada usuario viene identificado por → UID (User Identifier o ID usuario).

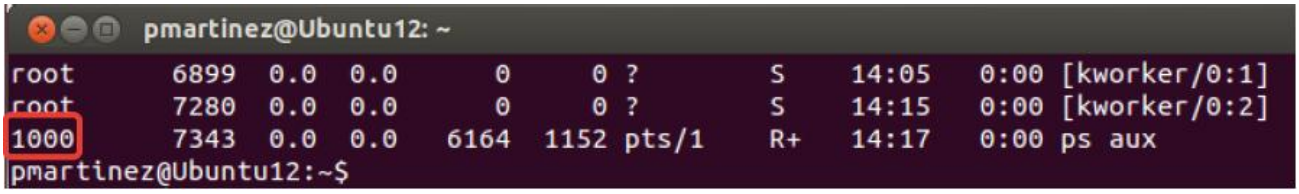
- Se genera cuando se da de alta.
- Identificador numérico.
- Información se guarda en → /etc/passwd



Primer valor → Nombre usuario.

Tercer valor → UID.

Comando "ps aux" → Muestra procesos activos. 1ª columna → UID



Root → Usuario especial que se encarga de administrar la funcionalidad del sistema.

Comandos:

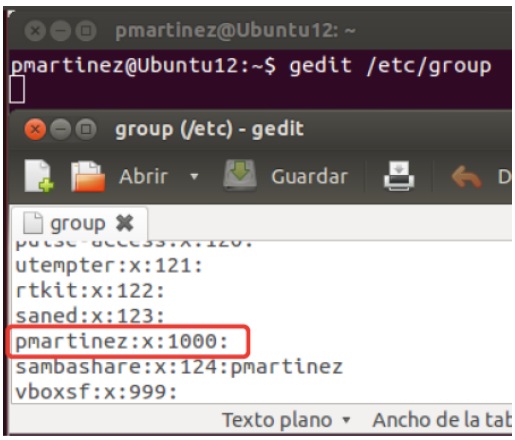
- Crear nuevo usuario → adduser
- Guardar contraseñas encriptadas → /etc/shadow
- Mostrar contraseñas encriptadas de los últimos 2 usuarios generados → /etc/shadow | tail -2
- Cambiar usuario sin cerrar la sesión → su –
- Modificar cuestiones relativas al usuario → usermod
  - Cambiar carpeta personal → sudo usermod **-d** nueva_carpeta -m pepe
  - Cambiar grupo principal → sudo usermod **-g** alumnos -m pepe
- Eliminar un usuario → userdel
  - Forzar a que borre carpeta personal → userdel **-r**

Grupos en Ubuntu

Cuando se da de alta un usuario, se genera por defecto, llamado como el usuario y conteniéndolo (grupo principal)

Identificado por → GID Group ID o ID grupo).

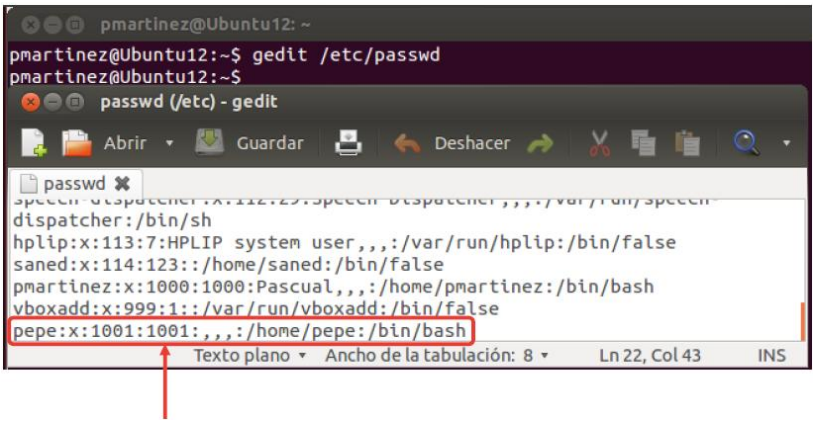
- Se genera cuando se da de alta.
- Identificador numérico.
- Información se guarda en → /etc/group



Primer valor → Nombre grupo.

Tercer valor → GID.

Si revisamos el fichero /etc/paswwd → El cuarto valor es el GID del grupo principal del usuario.



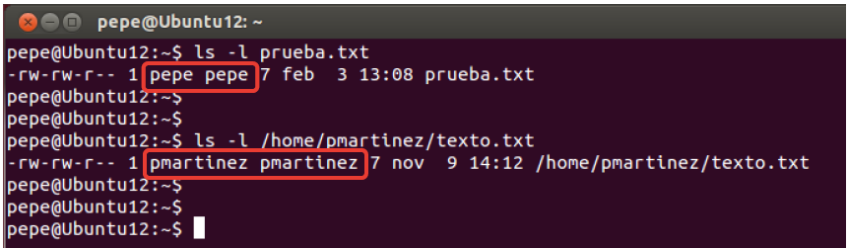
Comandos:

- ✓ Crear nuevo grupo → addgroup
- ✓ Establecer un grupo principal distinto al valor por defecto → --ingroup
  - Crear usuario y asignar "directores" como grupo principal → sudo adduser –ingroup directores pepe
- ✓ Quitar un usuario de un grupo → deluser usuario grupo
- ✓ Añadir usuario al grupo "alumnos", como grupo secundario → sudo adduser pmartinez alumnos
- ✓ Modificar cuestiones relativas al grupo → groupmod
  - Cambiar nombre → sudo groupmod **-n** nueva_nombre pepe
  - Cambiar GID → sudo groupmod **-g** nuevo_GID grupo
- ✓ Eliminar un grupo → groupdel

PERMISOS UBUNTU

Definen el nivel de acceso de un usuario.

Por defecto el usuario propietario será el usuario que ha creado el fichero o carpeta, y el grupo propietario será el grupo principal del usuario propietario.

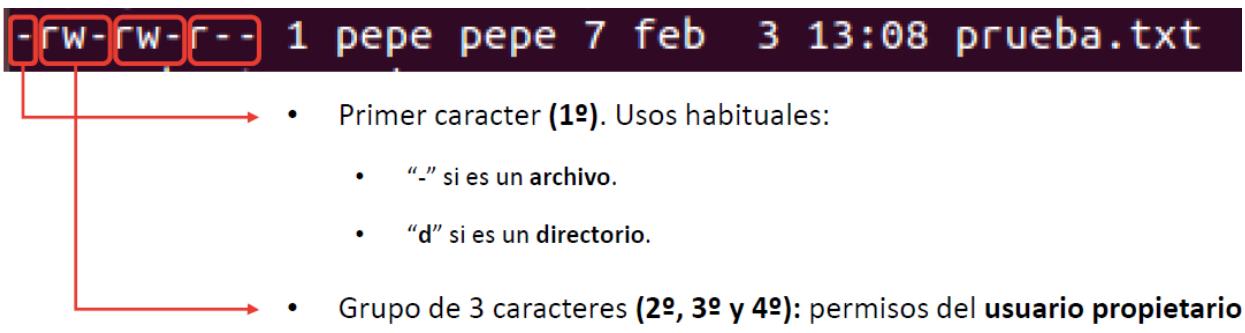


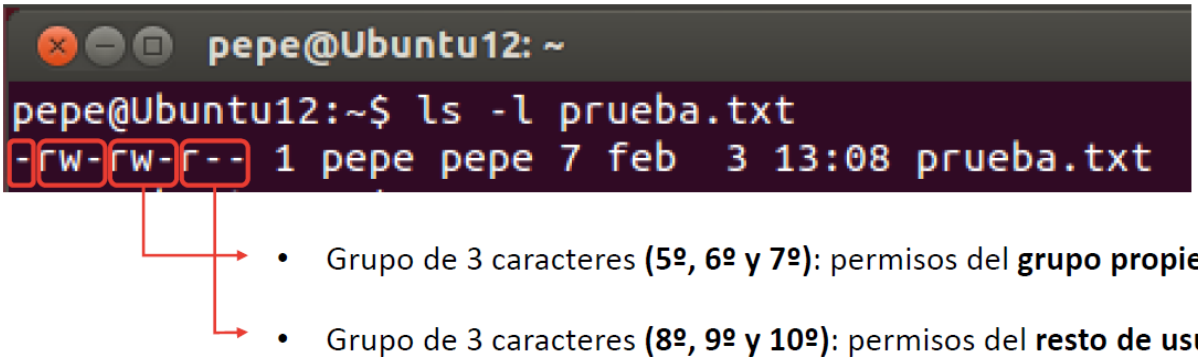
Niveles de acceso

Permisos de lectura → r

Permisos de escritura → w

Permisos de ejecución → x





Estructura:

Posición 1 → Lectura.

Posición 2 → Escritura.

Posicion3 → Ejecución.

Símbolo '**–**' en cualquier posición → No tiene el permiso.

Asignación de permisos

chmod → $ chmod opciones permiso ruta

Opciones:

- -r → Incluya subdirectorios.
- -c → Muestre fichero/directorios que modifican.

Permisos:

¿A quién va asociado el permiso? → u: Usuario; g: Grupo; o: Resto; a: Todos.

¿Añadimos o quitamos permiso? → +: Otorgar; –: Restringir.

¿Qué tipo de permiso? → r: Lectura; w: Escritura; x: Ejecución.

Al grupo propietario le añadimos el permiso de escritura → chmod g+w archivo.txt

Al usuario y grupo propietario le añadimos el permiso de ejecución sobre el fichero y al resto le quitamos el permiso de lectura → chmod ug+x, o-r archivo.txt

Código octal → Permisos se agrupan en 3 grupos de 3 posiciones o bits.

Existen 8 posibilidades de permisos.

NUMERO	BINARIO	LECTURA (r)	ESCRITURA (w)	EJECUCION (x)
0	000	✘	✘	✘
1	001	✘	✘	✓
2	010	✘	✓	✘
3	011	✘	✓	✓
4	100	✓	✘	✘
5	101	✓	✘	✓
6	110	✓	✓	✘
7	111	✓	✓	✓

REDES

Direccionamiento IP

Red → Conjunto de dispositivos que interactúan entre si y puede intercambiar información.

Clasificación, según su dimensión:

- **LAN** → Redes de área local. Salas, edificio o conjunto de edificios. Hasta pocos km. No implique cruzar una vía pública.
- **MAN** → Redes de área metropolitana. Grupo instalaciones cercanas o ciudad. Transmitir voz, datos o señales TV.
- **WAN** → Redes de área amplia. Área geografía extensa. País o continente.

Protocolo Ethernet → Protocolo de comunicación que describe, tanto las características física de los elementos de conectividad, como los formatos de las tramas o paquetes que se transmiten.

Para llevar a cabo la distribución de la información a través de una red, Ethernet utiliza → Direcciones **MAC** (Media Access Control adress) para identificar cada dispositivo individualmente.

- Únicas a nivel global para cada interfaz de red.
- Se asocian al hardware durante su fabricación.
- Llamadas direcciones físicas.
- Compuestas por 48 bits en formato hexadecimal.

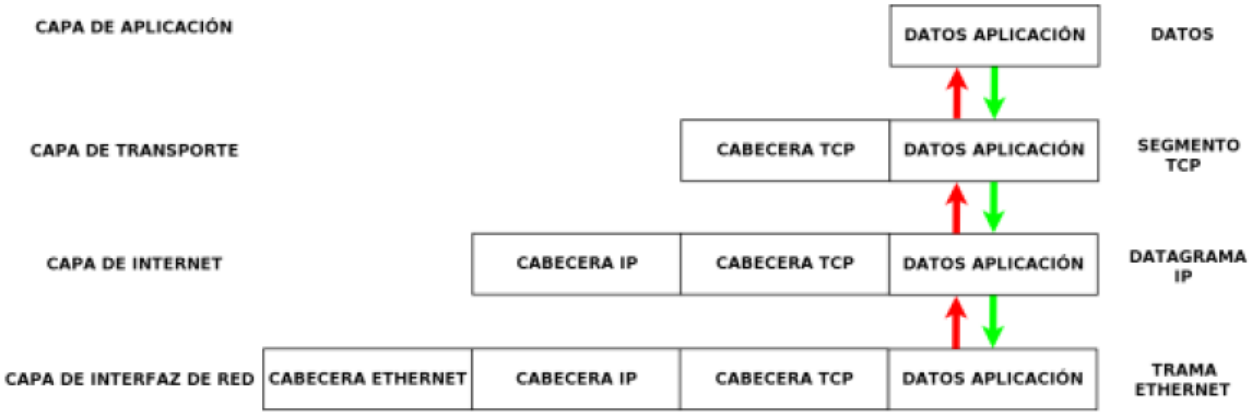
Modelo TCP/IP

Serie de protocolos de red que permiten la identificación e intercambio de información entre dispositivos de una red.

- **TCP** (Protocolo de Control de Transmisión) → Proporciona mecanismos de control de flujo y errores, entre extremos de la comunicación.
- **IP** (Dirección del Protocolo de Internet) → Proporciona mecanismos de interconexión entre redes. Proporciona información sobre donde se tienen que enviar los paquetes de datos.

Se estructura en **4 capas**:

1. **Aplicación** → Protocolos utilizados por las aplicaciones para proporcionar servicios de usuario o intercambiar datos. HTTP, FTP, PHP3, SSH, DNS…
2. **Transporte** → Se encarga de que la información se transmita sin errores y con calidad de servicio. TCP, UDP.
3. **Internet** → Se encarga de que pueda enviarse paquetes desde cualquier punto. IP.
4. **Enlace o interfaz de red** → Definir el método que utilizan los dispositivos para acceder al medio de comunicación. Ethernet.



Cuando enviar datos de aplicación → Los datos descienden por la pila de protocolos en el host emisor y la escalan en el host receptor.

En cada capa se va añadiendo cierta información de control para que el envío sea correcto → **Cabecera o encabezado.**

Proceso de ir añadiendo información en cada capa → **Encapsulación.**

Direccionamiento IP

Direcciones lógicas → Identifican individualmente a cada interfaz de red de cada dispositivo dentro de una red en un momento dado → Direcciones IP.

IPv4	IPv6
Dirección IP de 32 bits 4.300 millones de direcciones Direcciones reutilizan y enmascaran Notación numérica con punto decimal 192. 168.5.18 Configuración DHCP o manual	Dirección IP de 128 bits 7,9 x 10^{28} direcciones Dispositivos pueden tener una dirección exclusiva Notación hexadecimal alfanumérica 2001:0db8:85a3:08d3:1319:8a2e:0370:7332 Configuración automática

Se asignan a cada dispositivo, cuando se conecta a una red. No puede haber dentro de la misma red, 2 interfaces conectadas con la misma dirección IP.

Clases de direcciones IP

Cada dirección IP identifica:

- ✓ Dispositivos conectados a una red.
- ✓ La propia red a la que esta conectado.

Una parte de la dirección se utiliza para identificar la red y la otra para identificar el dispositivo.

Clases	Red / Dispositivo	Características	Rango direcciones	Rango direcciones privadas
A	**1er byte: Red** Resto: Dispositivos	Muchos dispositivos conectados. Pocas redes.	**0**.0.0.0 - **127**.255.255.255	10.0.0.0 - 10.255.255.255
B	**2os byte: Red** Resto: Dispositivos	Menos dispositivos. Más redes.	**128**.0.0.0 - **191**.255.255.255	172.16.0.0 - 172.31.255.255
C	**3os byte: Red** Ultimo: Dispositivos	Muchas redes con menos dispositivos.	**192**.0.0.0 - **223**.255.255.255	192.168.0.0 - 192.168.255.255
D	Ningún byte red ni dispositivos	Envió información a múltiples destinos simultáneamente.	**224**.0.0.0 - **239**.255.255.255	
E		Usos futuros	**240**.0.0.0 - **247**.255.255.255	

Mascara de subred

Cada interfaz TCP/IP tiene asociada una máscara de subred

Numero de **4 bytes**, se combina con la dirección IP, mediante operación lógica AND, para determinar cual es la red a la que pertenece dicha dirección.

Indica que parte de la dirección IP identifica la red y que parte identifica el host.

- **Bits que estén a 1 en la máscara** → Referencia a dirección que corresponde a la red.

Clases	Comienzo de clase	Final de clase	Mascara de red	Bits de red reservados (R)	Cantidad de redes 2^{n-R}	Cantidad host 2^{m-2}
A	0.0.0.0	127.255.255.255	255.0.0.0.0	1	128	16.777.214
B	128.0.0.0	191.255.255.255	255.255.0.0	2	16.384	65.534
C	192.0.0.0	223.255.255.255	255.255.255.0	3	2.097.152	254
D	224.0.0.0	239.255.255.255	No se aplican			
E	240.0.0.0	255.255.255.255				

Notación CIDR

CIDR (Classles Inter-Domain Routing) → Permite simplificar la forma de interpretar las direcciones IP.

CIDR para IPv4 → Representa mediante un separador "/" y un numero "N" (entre 0 y 32), añadidos a la IP.

192.168.0.0/24 → Indica que las mascara de red tiene 24 bits. Primeros 24 bits de la máscara son 1 y el resto 0.

Direcciones IP reservadas

Direcciones que ser reservan para usos especiales y que no se pueden asignar a un dispositivo.

- **Todos los bits a 0 en la parte correspondiente al dispositivo** → Dirección de la red.
- **Todos los bits a 1 en la parte correspondiente al dispositivo** → Dirección de broadcast.
- **Todos los bits a 0**, 0.0.0.0 → Dirección comodín. Cuando un dispositivo no esté conectado a una red (podría tener esta dirección).
- 127.0.0.0/8 → Direcciones para realizar **loopback** (paquetes de información no salen a la red, sino que retornan internamente a la misma máquina que realiza el envío).

Direcciones IP privadas y publicas

Dirección IP privadas → Dirección que solo tiene utilidad dentro de una red local, una organización privada y cerrada, sin necesidad de estar conectada a internet.

Según IANA (Internet Assigned Numbers Authority):

- **Clase A** → 10.X.X.X
- **Clase B** → 172.16.0.0 – 172.32.25.255
- **Clase C** → 192.168.X.X

En una misma red local las direcciones privadas serán únicas. No podemos tener 2 dispositivos/interfaces de red con la misma IP privada conectado en una misma red local. Si se tratase de redes locales distintas, si podremos tener 2 dispositivos con la misma dirección IP privada.

Dirección publica → Dirección accesible desde cualquier parte del mundo a través de internet.

Únicas a nivel global.

Las gestionan proveedores de servicios de internet (ISP).

Puerta de enlace (Gateway)

Función que realiza un dispositivo permitiendo la comunicación entre 2 o más redes diferentes.

Cuando se quiere establecer comunicación con una dirección destino que no se encuentra en la misma LAN que la dirección origen.

Permite la comunicación entre varias LAN.

Las funciones las pueden desempeñar diferentes dispositivos (servidor proxy, firewall, switch administrable…) lo mas habitual es que lo asuma un router o enrutador.

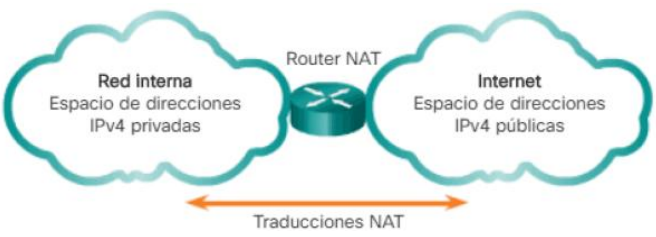
Cada router tiene una IP privada que lo identifica dentro de la LAN y una IP publica que lo identifica en la interconexión con el resto de las redes mundiales (internet).

NAT (Network Address Translation)

Los dispositivos se comunican con la puerta de enlace por IP privadas.

Cuando host quiere conectarse a internet, la puerta de enlace actúa como "representante" compartiendo la misma IP publica, se enmascaran las direcciones privadas de la red.

Enmascaramiento proporciona mayor nivel de seguridad a la red privada.



Permite que el acceso a internet de los múltiples hosts de la red local se haga con una única IP pública.

Asignación de direcciones IP

Cuando se contrata una conexión a internet, se contrata también la asignación de una IP publica, por defecto, una IP publica dinámica.

Si necesitas disponer de una IP publica estática/fija → Contratarla de forma específica a través del ISP.

¿Cómo se asignan las direcciones privadas a los host en una LAN?

Asignación dinámica → Cuando dispositivo arranca y se conecta a una LAN, asigna una IP privada que no este en uso (asignación automática DHCP). Puede ser diferente cada vez.

Asignación estática → Cuando dispositivo tiene un IP privada permanente. Cuando tenemos dispositivos que utilizamos como recursos compartidos en la red. Un servidor, disco compartido de un ordenador, impresora… Asignación manual o automática (DHCP).

Servicio DHCP (Dynamic Host Configuration Protocol)

Protocolo de la capa de aplicación.

Cuando un host se conecta a una red, envía un paquete tipo broadcast.

El servidor DHCP contesta al host mandándole una IP.

Servidor DNS

Se establece un sistema de nombres para todos los nodos conectados a internet.

Asi cualquier host público, puede ser fácilmente asociado e identificado con un nombre.

DNS (Domain Name System) se encarga de asociar/traducir nombre en direcciones IP.

- Proporcionado por servidores públicos o ISP.
- No esta centralizado en un fichero ni servidor concreto, sino servidores con estructura jerárquica.

Dominio → Permite estructurar los nombres de hosts de la misma organización o clasificación, para que sea posible identificarlos o memorizarlos con mayor facilidad.

Identificar cada host, se utiliza el nombre del host y el del dominio público.

Se represente mediante una etiqueta texto separada por puntos.

Cada etiqueta se asocia a un nivel distinto en la jerarquía de nombre de dominio.

Se pueden especificar manual o automáticamente (DHCP).

Configuración de la interfaz de red

Linux

$ ifconfig

$ ip addr show

- eth0 → **interfaz de red**
- direcciónHW → **MAC**
- Direc. inet → **IPv4**
- Difus. → **IP de broadcast**
- Masc → **máscara de red**
- Direc. Inet6 → **IPv6**

Windows

```
c:\> ipconfig
```

** (posibilidad de usar la opción "/all"
para ampliar la información)

Reiniciar interfaz de red

Windows

Consulta de interfaces:

c:\> netsh interface show interface

Deshabilitar interfaz:

c:\> netsh interface set interface «Nombre de adaptador de red» admin=disable

Habilitar interfaz :

c:\> netsh interface set interface «Nombre de adaptador de red» admin=enable

Linux

Deshabilitando y volviendo a habilitar la interfaz (eth0)

$ ifdown eth0 // **$ ifup eth0**

O bien:

$ ifconfig eth0 down // **$ ifconfig eth0 up**

O bien:

$ ip link set eth0 down // **$ ip link set eth0 up**

Ping

Nos permite comprobar la conectividad entre nuestro host y el host destino (IP o nombre del host).

Si paquetes llegan al destino, responderá (hay conectividad). Si se pierden los paquetes por el camino y no hay respuesta (no conectividad).

```
ping host_destino
```

Detalle de enrutado

Podemos ver la ruta que sigue un paquete hasta llegar a su destino.

```
$ tracert host
```

REDES EN LINUX

La IP de la puerta de enlace otorga conectividad con el exterior. 192.168.0.1 (No es obligatorio, si habitual, que sea la primera IP disponible).

SERVICIO SSH

Modelo cliente-servidor

El cliente (host/dispositivo) realiza una petición y el servidor (otro host, de la LAN/internet) proporciona una respuesta.

Puerto → Cada uno de los tipos específicos de interfaces a través de las que se puede enviar y/o recibir diferentes tipos de datos.

- **Físicos**: Hardware, permite conexiones física en un dispositivo (USB, PCI, HDMI...).
- **Lógicos**: Zonas de memoria que gestiona el S.O. y se usan para el intercambio de información.

Puertos lógicos

Cada uno de los diferentes procesos, petición y respuesta, que se ejecuta en los hosts cliente y servidor, tiene asignado un numero de puerto.

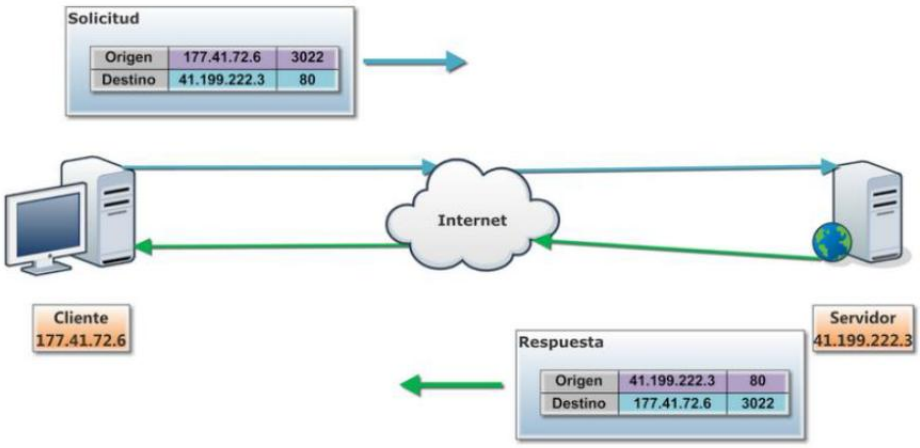
Puertos entre 0 y 1023 → Puertos conocidos. Se asignan desde el S.O.

Puertos entre 1024 y 49151 → Puertos accesibles para otros procesos y usuarios.

Socket de un proceso → Par formado por la dirección IP del host donde se ejecuta dicho proceso y el puerto del proceso.

- Sockets permiten establecer conexiones virtuales entre procesos en ejecución.
- Favorecen el intercambio de datos de forma fiable y eficiente.

Socket = IP:puerto



Servicios de la capa de aplicacion

Servicio FTP (File Transfer Protocol) → Permite a los clientes enviar y recibir fichero de un servidor. No depende de ningún sistema operativo, permite el intercambio entre distintas plataformas.

Consta principalmente y por defecto de **2 puertos**:

- Puerto 21 → Para conectarse de forma remota a un servidor y autenticarse en él.
- Puerto 20 → Transferencias de archivos una vez autenticado.

HTTP (Hypertext Trnasfer Protocol) → Gestiona la mayor parte del trafico de internet. Cuando usuario solicita un recurso web – Solicitud se realiza mediante HTTP.

Acceder a una URL → Servicio DNS resuelve IP, envía una solicitud "get" al servidor, este devuelve un "send".

- Utiliza TCP, por defecto opera en → Puerto 80.

HTTPS (Hypertext Transfer Protocol Secure) → Para realizar transacciones de datos seguras via web. Basada en certificados digitales. Encripta todos los paquetes de datos.

- Utiliza TCP, por defecto opera en → Puerto 443.

POP3 (Post Office Protocol v3) → Servicio de **recepción de correo electrónico** que proporciona al usuario el acceso a su carpeta de mensajes entrantes. Se encarga de contar con un servidor de correo y descargar en un dispositivo local los mensajes recibidos.

- Puerto 110.

IMAP (Internet Message Acces Protocol) → Permite **acceder al servidor de correo electrónico** desde cualquier dispositivo. Mediante este protocolo los mensajes no se descargan en un dispositivo loca.

- Puerto 143.

SMTP (simple Mail Transport Protocol) → **Gestiona el envío de correo electrónico**. Los mensajes se envían desde un servidor SMTP a otro. Utiliza el servicio DNS.

- Puerto 25.

TELNET (Teletype Network) → Permite conectar un cliente con un servidor remoto. Proporciona comunicación bidireccional entre cliente y servidor. Nos permite accede o indicar sesión en otra maquina para manejarla de forma remota. La información no viaja cifrada.

- Puerto 23.

SSH (Secure Shell) → Protocolo de red para establecer comunicaciones seguras entre 2 hosts (cliente-servidor).

- Similar al TELNET, pero estableciendo conexión segura, información viaja cifrada.
  - Puerto 22.
- Ofrece confidencialidad e integridad de los datos en redes inseguras.
- Acceso remoto al Shell de sistemas Linux. Acceder a otras maquinas Linux a través de la red y trabajar con ellas como si estuviésemos en local.
- Transferencia de ficheros (SFTP).

Parte servidor

Herramienta OpenSSH.

```
# sudo apt-get install openssh-server
```

Se instala en:

```
/etc/ssh
```

Ficheros:

sshd_config: archivo de configuración del servidor SSH

ssh_config: archivo de configuración del cliente SSH

ssh_host_*_key: clave privada de la máquina (* puede ser rsa, dsa o ecdsa)

ssh_host_*_key.pub: clave pública de la máquina (idem a anterior).

Arrancarlo (si estuviera detenido):

```
# sudo service ssh start
```

Otras opciones:

 # sudo service ssh stop (para pararlo)

 # sudo service ssh status (para ver el estado)

 # sudo service ssh restart (para reiniciarlo).

Confirmar que está escuchando peticiones:

$ netstat -ltu

Es multiplataforma.

SHELL SCRIPTS

¿Qué es un Script?

Designa a un programa relativamente corto y/o sencillo. Secuencia de comandos, fichero por lotes, Shell script…

Son ejecutados instrucción a instrucción por un interprete que lee el archivo de código fuente en el momento.

Permite:

- Ejecutar comandos propios de la línea de comandos de forma integrada.
- Manipular archivos.
- Ejecución de otros scripts.