

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

Configuración de la red en sistemas operativos	2
Configuración de las máquinas virtuales	2
Configuración del adaptador de red	2
Configuración de la red en Windows	3
Configuración de la red en Ubuntu.	4
Ubuntu Desktop Edition controla, de forma predeterminada, la configuración automática de la red a través de Network Manager, mientras que la versión Server favorece una configuración manual. Anteriormente se utilizaba el archivo /etc/network/interfaces.	4
NetworkManager	4
Netplan	6
Configuración de la red del equipo anfitrión	6
Configuración del nombre del PC	6
Configuración de un AP inalámbrico	8
Compartición de archivos y carpetas	10
Compartir archivos y directorios en Windows	10
Compartir archivos y directorios en Ubuntu	14
Permisos y carpetas compartidas	21
Configuración de la seguridad de recursos compartidos en Windows (ESTO YA LO VIMOS)	21
Configuración de la seguridad de recursos compartidos en Ubuntu	22
Comandos de red	23
ping	23
ipconfig e ifconfig	23
netstat	25
arp	25
tracert y traceroute	26
route	27
netsh	27
iwconfig	28
Herramientas gráficas de red Windows	28

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

1. Configuración de la red en sistemas operativos

1.1. Configuración de las máquinas virtuales

Partimos de que tenemos instaladas 2 máquinas virtuales, una de Windows y otra de Ubuntu. Vamos a comunicar estas máquinas para que puedan comunicarse entre sí y con el PC anfitrión asegurando una red virtual en la que vamos a compartir recursos como haríamos con PCs independientes.

Vamos a usar:

- Dirección de red privada de clase C
 - Dirección de puerta de enlace
 - Máscara de entrada
 - Dirección del equipo anfitrión
 - Dirección IP de la máquina Windows
 - Dirección IP de la máquina Ubuntu
 - DNS
1. Seleccionamos la máquina virtual Windows
 2. Accedemos a la configuración de la misma y hacemos clic en Red.
 3. Por defecto aparecerá activo el primer adaptador (Adaptador 1) y en la lista **conectado a** veremos **NAT**. Vamos a cambiar esta opción para poder configurar una red virtual entre todas las máquinas, escogeremos **Adaptador puente**. Vemos nuevas opciones de configuración que dejaremos con las opciones por defecto.

NOTA: Si el adaptador de red de la MV está configurado como NAT, estamos indicando que usamos la IP del host anfitrión como "IP pública" y que esta será traducida por cualquier otra en el sistema operativo. De esta forma, no podemos controlar el direccionamiento IP de cada MV, cada una adopta una dirección IP perteneciente a redes distintas.

4. Volvemos a realizar los pasos del 1 al 3 seleccionando la MV Ubuntu.

NOTA: Cuando configuramos la red con Adaptador puente, podemos escoger entre usar nuestro propio adaptador de red o cualquier otro adaptador virtualizado. Si usamos PC portátiles utilizar adaptadores virtuales puede dar problemas, se aconseja usar el adaptador de red del ordenador.

1.1. Configuración del adaptador de red

Si la red es cableada y la instalación y configuración del hardware se ha llevado a cabo correctamente procederemos a la configuración del mismo siguiendo los Apartados 1.3 y 1.4. En el caso

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

de redes inalámbricas debemos además conectar a la red que nos proporciona el punto de acceso o router inalámbrico.

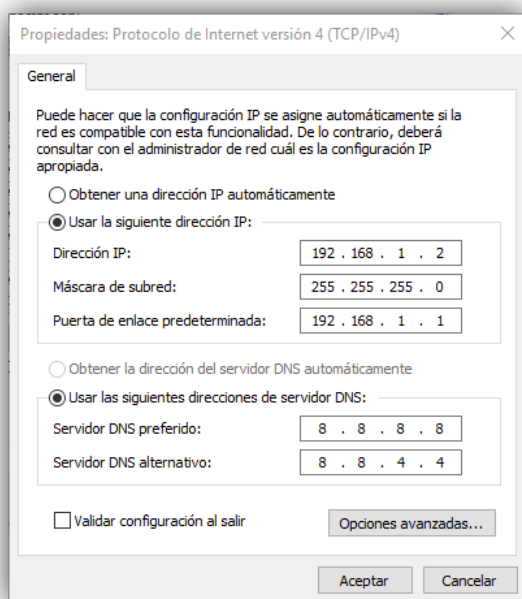
En el caso de Windows, en la barra de tareas al hacer clic sobre el icono de red, aparecerán todos los nombres SSID de las redes inalámbricas que están a nuestro alcance. Los datos relativos al tipo de seguridad, canal, modo, etc., son transferidos desde el dispositivo central inalámbrico y configurados de forma automática. Aún así, podemos observar esta información a través de **Inicio -> Configuración -> Red e Internet -> Wifi -> Configuración de red avanzada -> Cambiar las opciones del adaptador -> Doble clic sobre el adaptador -> clic en **Propiedades inalámbricas**.**

Para el caso de Ubuntu, accedemos al icono de red en la barra de menú, junto a las opciones de apagado o configuración del sistema. Al hacer clic sobre el icono vemos las opciones de configuración de red y una lista de nombres de redes que están a nuestro alcance. Después de seleccionarla, se solicitará el password de acceso. Tras escribirlo correctamente pasaremos a la configuración del direccionamiento ip del adaptador.

1.2. Configuración de la red en Windows

Accedemos con un usuario administrador al sistema y seguimos los siguientes pasos.

1. Accedemos a **Inicio -> Configuración -> Red e Internet -> Ethernet -> Cambiar opciones del adaptador**. Veremos la interfaz (tarjeta de red) o interfaces que tengamos instaladas. Clic con el botón derecho sobre ella y **Propiedades**.



2. Vamos a configurar el protocolo de internet versión 4 (TCP/IPv4), para lo que haremos doble clic en la lista sobre el elemento. Veremos la ventana de propiedades del protocolo.

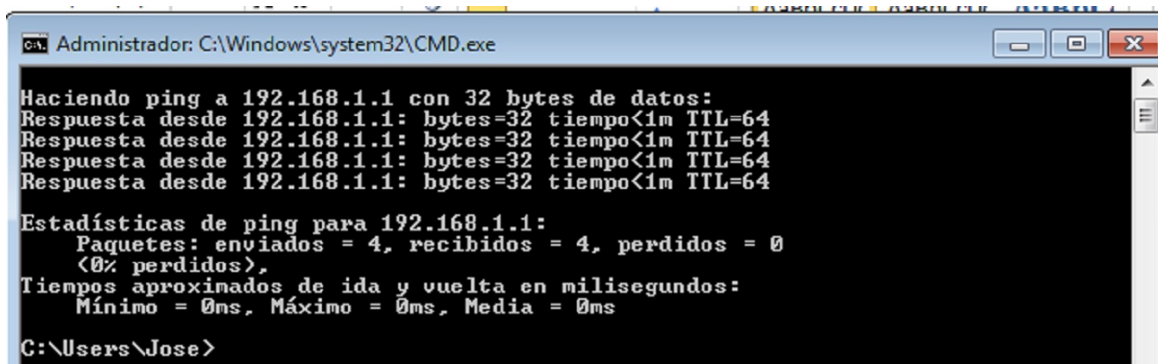
3. Activaremos Usar la siguiente dirección IP rellenando los cuadros: Dirección IP, Máscara de subred, Puerta de enlace predeterminada y servidor DNS preferido. El cuadro de diálogo debe ser similar al que se observa en la figura siguiente.

4. Vamos a asegurarnos de que la configuración es correcta usando el comando PING con la puerta de enlace. En el cuadro de texto Escribe para buscar escribimos **cmd** para acceder al intérprete de comandos de Windows. Escribimos **ping** a la dirección de la puerta de enlace (En la imagen 192.168.1.1, en nuestro caso, la que corresponda con la dirección de puerta de enlace de

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

nuestra red) y pulsamos ENTER, nuestra pantalla debe ser similar a la de la figura siguiente.



```
Administrador: C:\Windows\system32\CMD.exe

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Jose>
```

- Si no existe respuesta y vemos el texto Host de destino inalcanzable o Tiempo de espera agotado debemos revisar la configuración del adaptador. (En el aula 203, de hecho la configuración de la red es 10.0.204.0/24 siendo la puerta de enlace 10.0.204.1)
- Al poner la IP manualmente, debemos tener en cuenta que no puede repetirse dentro de la misma red.

1.3. Configuración de la red en Ubuntu.

Ubuntu Desktop Edition controla, de forma predeterminada, la configuración automática de la red a través de **Network Manager**, mientras que la versión Server favorece una configuración manual. Anteriormente se utilizaba el archivo `/etc/network/interfaces`.

1.3.1. NetworkManager

NetworkManager incluye un **servicio** que administra las conexiones y los cambios en la red y una **aplicación gráfica** y otra para la **Interfaz de Línea de Comandos (CLI)** que permiten al usuario administrar las conexiones de red (Este servicio se instala por defecto con Ubuntu Desktop, en el caso de Ubuntu Server el servicio iniciado será **Networkd**).

NetworkManager anulará la configuración de **DHCP** sobrescribiendo el archivo `/etc/resolv.conf`, e incluso si se ha configurado **DNS** en `/etc/dhcp/dhclient.conf`.

NetworkManager por defecto solo manejará interfaces no declaradas en el archivo `/etc/network/interfaces`. Si queremos que gestione todas las interfaces de red independientemente del fichero anterior, deberemos modificar la configuración de **NetworkManager** editando el archivo `/etc/NetworkManager/NetworkManager.conf`

- Si `managed=true`, **NetworkManager** gestionará todas las interfaces de red.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

- Si `managed=false`, **NetworkManager** manejará solo las interfaces de red que no estén declaradas en el archivo `/etc/network/interfaces`.

NetworkManager almacena en archivos individuales la información de las conexiones de red conocidas. A estos archivos se les conoce como **perfiles**. Los **perfiles** se almacenan en el directorio `/etc/NetworkManager/system-connections/`.

```
ubuntu@ubuntu-VB: /etc/NetworkManager/system-connections$ ls
'Conexión cableada 1.nmconnection'  netplan-enp0s3.nmconnection
ubuntu@ubuntu-VB: /etc/NetworkManager/system-connections$ sudo cat netplan-enp0s3.nmconnection
[connection]
id=netplan-enp0s3
uuid=1eef7e45-3b9d-3043-bee3-fc5925c90273
type=ethernet
interface-name=enp0s3
permissions=
timestamp=1651822103

[ethernet]
mac-address-blacklist=
wake-on-lan=0

[ipv4]
address1=192.168.0.11/24,192.168.0.1
dns-search=
method=manual
```

De forma gráfica (Iniciamos sesión con un usuario administrador)

- En la barra superior localizamos el icono de **red** y hacemos clic sobre él. Veremos un listado de interfaces de red. Debemos seleccionar **Configuración de red Cableada** y activamos la pestaña **Ajustes de IPV4**.
- Configuramos la ventana de forma que **Método** sea **Manual**. Clic sobre **Añadir** para incluir la dirección IP al sistema. La ventana de configuración debe quedar como se muestra en la Figura 1.3. Clic en **Aplicar**.
- Para probar la conectividad con la puerta de enlace usaremos el comando PING en el terminal, Clic sobre Inicio y a continuación escribimos Terminal. Escribimos ping a la puerta de enlace (En la imagen sería 192.168.1.1; en el aula 203, la puerta de enlace es 10.0.204.1)



The screenshot shows the 'Cableada' (Wired) network configuration window. The 'IPV4' tab is selected. Under 'Método IPV4', the 'Manual' option is chosen. The 'Direcciones' (Addresses) section contains one entry: IP 192.168.1.130, mask 255.255.255.0, and gateway 192.168.1.1. The 'DNS' field is set to 8.8.8.8. The 'Automático' toggle for DNS is turned off.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

NOTA: En las máquinas Windows, al ejecutar el comando PING, solo se emiten 4 respuestas del equipo con el que comunicamos. En Linux, el comando no solo da más de 4 respuestas, sino que seguirá comprobando la comunicación hasta que pulsemos la combinación de teclas CTRL+C o CTRL+Z.

1.3.2. Netplan

Netplan es un software de gestión de red que aparece en Ubuntu 17.10 como reemplazo de **NetworkManager**. Se utiliza tanto en Ubuntu server como Desktop.

/etc/netplan

<https://www.ochobitshacenunbyte.com/2021/04/26/netplan-configurar-la-red-en-ubuntu-20-04/>

1.4. Configuración de la red del equipo anfitrión

La configuración de red del equipo anfitrión se llevará a cabo de igual modo que en los Apartados 1.2 o 1.3, en función de si el sistema operativo instalado es Windows o Linux. Sólo debemos seguir los pasos del apartado que corresponda y comprobar la configuración con el comando **ping**.

Una vez que las MV y el equipo anfitrión estén configurados en red es aconsejable comprobar todas las posibles conexiones, ejecutando el comando **ping** con cada uno de los componentes de red.

1.5. Configuración del nombre del PC

Cuando trabajamos con equipos en red, deben tener una dirección IP asignada válida dentro del rango de direcciones de nuestra red. Además, damos nombres a nuestros equipos, y si no tenemos un servidor todos los PCs pertenecerán al mismo **grupo de trabajo**.

Los grupos de trabajo son un concepto propio de Windows. Un grupo de trabajo permite agrupar equipos. Cada uno de estos PCs tiene usuarios creados localmente. Todos estos usuarios pueden acceder a los recursos compartidos del grupo.

Configuración del nombre y grupo de trabajo en Windows 10

Existen varias formas de modificar estos elementos. Para usar la funcionalidad del sistema operativo que estamos estudiando, cambiaremos el nombre del PC usando las nuevas ventanas de configuración de Windows 10.

1. Clic con el botón derecho del ratón sobre **Inicio -> Sistema**. Localizar el botón Cambiar el **nombre de este equipo** y hacer clic sobre él.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

2. A continuación, aparece un nuevo cuadro de diálogo, donde se muestra el nombre actual del equipo y un cuadro de texto en blanco, es aquí donde debemos especificar el nuevo nombre. Escribimos **PC120**. Clic en **Siguiente**.
3. La acción que estamos realizando necesita del reinicio del sistema. Clic sobre **Reiniciar ahora**.

La secuencia de pasos anteriores modifica el nombre del equipo, pasemos ahora a cambiar el grupo de trabajo.

1. En el cuadro de texto de **Cortana** escribimos **Panel de control**. Clic sobre la aplicación que aparece entre los resultados.
2. Clic en **Sistema** y clic sobre **Cambiar el nombre de este equipo (avanzado)**.
3. En el cuadro de diálogo veremos los datos de nombre y grupo actuales. Clic sobre **Cambiar**.
4. Desde la nueva pantalla podremos modificar el nombre del equipo y en la zona inferior especificar si pertenecemos a un **Dominio Windows** o bien a un **Grupo de Trabajo**. En **Grupo de trabajo** escribimos **CLASE**. Clic en **Aceptar**.
5. El asistente solicita que se realice el reinicio del sistema para que los cambios surtan efecto. Realizar la acción y habrá finalizado el proceso.

Configuración del nombre del equipo en Ubuntu

Para cambiar el nombre del equipo en Ubuntu:

- Clic sobre el botón de **Configuración del sistema** en la barra lateral. En la zona de **Sistema** clic sobre **Detalles**. Cambiamos el valor del cuadro **Nombre del dispositivo** por el nuevo nombre, en nuestro caso **PC130**.
- Modificaremos el fichero **/etc/hostname**. Con esta acción conseguiremos que el cambio sea permanente.
- Ejecutaremos la orden **sudo hostname nuevo_nombre**, en cuyo caso el nuevo_nombre solo tendrá efecto el tiempo que mantengamos iniciada sesión en el equipo.

Para la modificación del fichero hostname podemos usar el editor vi: **sudo vi /etc/hostname** o bien desde el entorno gráfico ejecutar **gksudo** sobre una aplicación: **gksudo gedit /etc/hostname**. Llamaremos al PC Ubuntu con el nombre **PC130**.

NOTA: En Linux podemos configurar grupos de trabajo con SAMBA (servicio que permite la compartición de ficheros con Windows)

En Ubuntu, el archivo **/etc/hosts** asigna el nombre de host a la dirección IP de forma local. Por ejemplo, si añadimos al fichero hosts la línea **192.168.72.10 fileserv**, permitirá acceder a esa máquina con el nombre **fileserv** en lugar de la IP.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

1.6. Configuración de un AP inalámbrico

A la hora de configurar un punto de acceso o router inalámbrico existen una serie de parámetros básicos que deben ser establecidos.

- **Características del dispositivo.** Entre las características del dispositivo de red encontramos la dirección IP que adoptará y por la que los demás equipos lo identificarán en la red y los datos de usuario y password para el acceso al mismo.
- **Nombre SSID.** Nombre de la red inalámbrica.
- **Modo de red.** El modo de red establece el tipo de dispositivos que pueden conectarse a la red inalámbrica. Podemos optar por escoger entre **modo mixto** para que puedan conectar dispositivos G y N, **modo N** para que la red solo esté formada por dispositivos de tipo N, etc.
- **Broadcast SSID.** Esta opción hace visible o no la red. A veces, para asegurar la infraestructura y evitar accesos de intrusos, se oculta la red y se hacen más difíciles los ataques de estos.
- **Canal.** Cada banda de frecuencia que se use utilizará una serie de canales para transmitir información. De todos ellos, debemos escoger el canal que queremos usar. Si disponemos de dos puntos de acceso cercanos, debemos usar canales diferentes de transmisión para que no se produzcan interferencias en la transmisión.
- **Seguridad WEP, WAP o WAP2.** Uso de contraseña de acceso a la red. WEP es un modo de encriptación más débil que WAP o WAP2, siendo este último el más usado hoy día.
- **Configuración del servidor DHCP.** En caso de que dispongamos de un router inalámbrico probablemente este de soporte DHCP, de forma que asignará direcciones IP de forma dinámica a todos los equipos de la red. Podemos establecer el rango de direcciones IP que vamos a usar, qué direcciones no pueden usarse, etc. Tendremos igualmente opción a deshabilitar el servidor y realizar la configuración de direccionamiento de direccionamiento ip de forma manual.

Para comenzar la configuración

1. En el manual del fabricante del punto de acceso o router inalámbrico buscamos la dirección IP que tiene asignada el componente por defecto.
2. Conectamos nuestro PC al dispositivo vía cable.
3. Abrimos el navegador y escribimos en la barra de dirección <http://ip>.
4. Accedemos a la web de configuración del punto de acceso o router. El acceso se hace a través del usuario y password que están establecidos por defecto y que veremos en el manual del fabricante.
5. En la web de configuración modificamos la información básica de acceso, es decir usuario y contraseña de acceso a la Web de configuración.
6. Modificamos la dirección de red, sustituyéndola por una red privada de clase A, B o C en función de nuestras necesidades (este paso es opcional)
7. Introducimos el nombre de la red.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

8. Modificamos el modo que vamos a utilizar en función de los tipos de dispositivos que vamos a usar o permitir que se conecten a la red.
9. Activamos la seguridad de la red. Se aconseja usar WAP2 y crear contraseñas que estén compuestas como mínimo por 8 caracteres entre los que incluyamos letras, números y símbolos especiales.
10. La ocultación de la red, desactivación del DHCP y el canal son opcionales.
11. Guardamos la nueva configuración. Desconectamos el cable de red y probamos el acceso a la red a través de cualquier PC con acceso inalámbrico.

Wireless-B Broadband Router

Setup | **Wireless** | **Security** | **Applications & Gaming** | **Administration** | **Status**

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Basic Setup

Obtain an IP automatically ▾

Host Name:

Domain Name:

MTU: ☐ Enable ☒ Disable Size:

Speed & Duplex: ▾

Local IP Address: . . .

Subnet Mask: ▾

Local DHCP Server: ☒ Enable ☐ Disable

Start IP Address:

Number of Address:

DHCP Address Range:

Client Lease Time: minutes (0 means two day)

Static DNS 1: . . .

Static DNS 2: . . .

Static DNS 3: . . .

WINS: . . .

Basic Setup

The Basic Setup section is the basic configuration for the router. Some ISPs (Internet Service Providers) will require you to enter the DHCP settings. These settings are obtained from your ISP. If you are not configured to obtain an IP address from the DHCP server, you should set a static IP address from the Advanced Setup > Management section.

Completing this section is all that is required to get the router set up for your network. Please look at the Internet connection section to configure the Internet connection.

[More...](#)

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

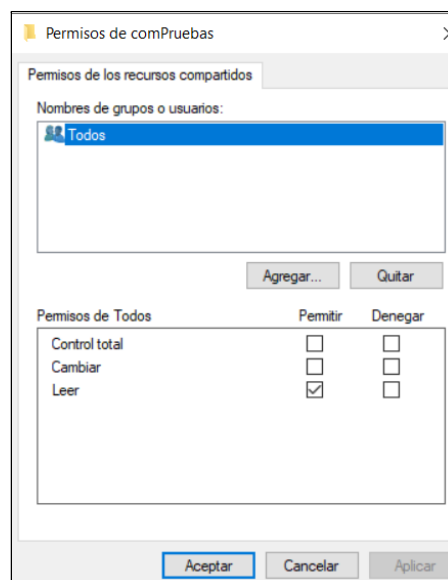
2. Compartición de archivos y carpetas

2.1. Compartir archivos y directorios en Windows

La compartición de carpetas en equipos Windows es sencilla. Vamos a compartir una carpeta que hemos creado previamente en el escritorio, esta se denomina **CompWindows**.

Compartir el directorio CompWindows

1. Clic con el botón derecho del ratón sobre **CompWindows** y **Propiedades**.
2. En el cuadro de diálogo que aparece haremos clic en la pestaña **Compartir**.
3. Centramos nuestra atención en la zona **Uso compartido avanzado** y haremos clic en el botón **Uso compartido avanzado**.
4. Clic sobre **Compartir esta carpeta**. Veremos el nombre del recurso compartido. El nombre de red del recurso no tiene por qué ser igual al nombre real de la carpeta. Este nombre será el que los usuarios vean cuando accedan a las carpetas compartidas del PC.
5. Clic en Permisos. Entre los usuarios y grupos a los que se comparte el recurso debe aparecer **Todos** y en la parte inferior sólo la casilla de verificación **Leer** estará activa.



6. Aceptamos todas las ventanas abiertas. El recurso ya está disponible.

Acceder al directorio CompWindows desde otra máquina windows

Podemos acceder a la carpeta compartida desde otro equipo Windows usando la notación **\\pc_servidor** o accediendo a **Red** en el explorador de archivos.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

OPCION 1

1. Clic en Inicio -> Explorador de archivos
2. En la barra de dirección escribimos la IP de nuestra máquina virtual Windows(Ej: \\192.168.1.120) o el Nombre del equipo Windows (Ej: \\PC120) y pulsamos ENTER.

OPCION 2

1. Clic en **Inicio -> Explorador de archivos.**
2. En el panel lateral clic en **Red.**
3. Veremos una lista con todos los equipos que estén en red. Doble clic sobre **PC120.**

Tanto en opción 1 como en opción 2, al finalizar los pasos indicados debemos especificar un usuario válido para el acceso al recurso. Este usuario debe ser uno de los creados en PC120. Así, escribimos el usuario y contraseña con el que iniciamos sesión en nuestra MV Windows 10 y veremos los directorios compartidos, accediendo a los mismos con los permisos que se establecieron. El acceso a **CompWindows** es de solo lectura.

NOTA: Tras acceder a la carpeta realizaremos alguna modificación sobre ella, como crear un subdirectorio. Observaremos que se nos alerta de que no tenemos permisos suficientes para realizar la operación (recordamos que el acceso es de lectura)

Acceder al directorio CompWindows desde la MV Ubuntu

1. Clic sobre **Carpeta personal** del panel lateral de Ubuntu
2. Clic en **Otras ubicaciones.** En la parte central observaremos todos los equipos que están en la red además de la carpeta **Red de Windows.**

Si hacemos doble clic sobre **Red de Windows** observaremos los grupos de trabajo de los PC con sistema operativo Windows (dentro de una misma red podemos configurar grupos de equipos con grupos de trabajo diferentes, aunque todos los equipos tengan el mismo direccionamiento IP). Al seleccionar un **grupo de trabajo** veremos todos los equipos que forman parte del mismo y acceder al PC con el recurso compartido.

Si hacemos doble clic sobre el PC con el recurso compartido, el recurso será alcanzado más rápidamente.

3. Doble clic sobre **PC120.** Ubuntu nos pedirá un usuario y contraseña válidos para el acceso. Al igual que en el apartado anterior, escribiremos el nombre de usuario y contraseña que usamos para iniciar sesión en Windows.
4. Igualmente, si procedemos a modificar el contenido de **CompWindows** veremos un mensaje de alerta con el texto **Permiso denegado.**

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

SMB (Server Message Block)

SMB es el protocolo usado por Windows para la compartición de directorios e impresoras. Actualmente se le conoce con el nombre CIFS (Common Internet File System). SMB fue creado por IBM, quien lo fue modificando posteriormente con ayuda de Microsoft. Es un protocolo que trabaja a nivel de aplicación y contempla dos niveles de seguridad:

- **Seguridad orientada a recursos.** Cada recurso compartido tiene una contraseña de acceso de forma que el usuario solo debe conocer esta.
- **Seguridad orientada a los usuarios.** Cada recurso compartido será accesible en función de los privilegios del usuario que quiera acceder.

Acceso a recursos compartidos windows desde Ubuntu con el intérprete de comandos

Anteriormente accedíamos a la carpeta compartida de Windows a través del entorno gráfico de Ubuntu de forma sencilla y rápida. Hemos estudiado que los sistemas operativos de Microsoft utilizan el protocolo SMB para la compartición de recursos y para el acceso a los mismos, de forma que para poder acceder desde un equipo Linux a un recurso compartido windows será necesario usar este protocolo.

En Linux **SAMBA** es la implementación libre del protocolo SMB, permitiendo la compartición de recursos entre sistemas operativos Windows y Linux. Para poder acceder a un recurso Windows debemos ser clientes samba y tener al menos el paquete **smbclient** instalado en el sistema.

Para poder visualizar los recursos compartidos de Windows desde el intérprete de comandos:

1. Abrimos el **terminal** de Ubuntu, escribimos: **sudo apt-get update** para actualizar los repositorios de software
2. Escribimos **sudo apt-get install smbclient** para descargar e instalar el cliente SMB
3. Ya podemos hacer uso del comando **smbclient** para acceder a los recursos de la máquina Windows 10. En primer lugar, debemos listar los recursos compartidos de Windows. Ejecutamos la orden **sudo smbclient -L IP -U usuario**, sustituyendo **IP** por la dirección ip de la máquina Windows, que en nuestro caso es 192.168.1.120 y **usuario** por el usuario con el que iniciamos sesión.
4. Pulsamos ENTER e introducimos la contraseña del usuario. Tras la autenticación veremos una lista (**opción -L**) con el total de recursos compartidos del sistema como se muestra a continuación:

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

```
12.8.
usuario@PC130:~$ sudo smbclient -L 192.168.1.120 -U isabel
sudo: unable to resolve host PC130
Enter isabel's password:
Domain=[PC120] OS=[Windows 7 Ultimate 7600] Server=[Windows 7 Ultimate 6.1]

Sharename      Type      Comment
-----
ADMIN$         Disk      Admin remota
C$             Disk      Recurso predeterminado
CompPruebas    Disk
CompWindows    Disk
IPC$           IPC       IPC remota
Users          Disk
```

Para poder copiar o modificar la carpeta compartida según los privilegio dados:

1. Tras ejecutar **smbclient -L** conocemos los nombres de las carpetas compartidas. Para acceder a cada una de ellas usaremos nuevamente **smbclient** del siguiente modo: **sudo smbclient //IP/directorio -U usuario**, siendo **IP** la dirección ip de la máquina que tiene el recurso compartido y **directorio** el nombre de la carpeta compartida, más bien el nombre de la carpeta en la red.

Ejemplo: **sudo smbclient //192.168.1.120/CompWindows -U Isabel**

2. De igual modo que al listar los recursos compartidos, se nos pedirán credenciales de acceso. Escribiremos el password del usuario y accederemos a un entorno similar al que encontramos cuando accedemos a un servidor ftp. El prompt cambia a **smb:\>**.

```
smb: \> help
?
cancel      allinfo      altname      archive      blocksize
close       case_sensitive cd            chmod        chown
exit        del          dir          du           echo
history     get          getfacl      hardlink     help
lowercase  iosize      lcd          link         lock
mget        ls          l            mask         md
open        mkdir       more         mput         newer
posix       mkdir       posix_encrypt posix_open   posix_mkdir
posix_rmdir posix_unlink print         prompt       put
pwd         q           queue        quit         readlink
rd          recurse    reget        rename       reput
rm          rmdir      showacl     setmode      stat
symlink     tar        tarnode     translate    unlock
volume     vuid       wdel        logon        listconnect
showconnect ..          !

smb: \>
```

3. En esta interfaz usaremos:
 - a. **get**. Para copiar un elemento del recurso compartido al directorio desde el que hemos iniciado sesión en smb.
 - b. **put**. Para modificar o copiar un elemento en el recurso compartido. Ya que la carpeta es de solo lectura a la hora de usar esta orden nos aparecerá un mensaje de alerta con el texto **NT_STATUS_ACCESS_DENIED**.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

4. Para finalizar la sesión usaremos el comando **quit** o **exit**.

Además del uso de **smbclient** existe otra forma de acceder al contenido de un recurso compartido y es mediante el comando **smbmount**. Al igual que montamos unidades de disco o CD podemos montar carpetas compartidas, de forma que podamos acceder a ellas como si accediéramos a cualquiera de nuestros directorios.

1. **smbmount** es una herramienta que se incluye en el paquete **smbfs** con que antes de poder usarla debemos tener esta paquete instalado en el sistema: **sudo apt-get install smbfs**
2. Tras ejecutar **smbclient -L** conocemos todos los recursos compartidos. Supongamos que observamos un directorio compartido llamado **pruebas** y la máquina es **192.168.1.120**. Accedemos como usuario **Isabel**.
3. Debemos tener preparado un directorio vacío que será el lugar donde podremos observar los elementos del recurso compartido. En **/media** crearemos una carpeta llamada **pruebas**.
4. Escribimos la orden **sudo smbmount //192.168.1.120/pruebas /media/pruebas -o user=isabel** y pulsamos ENTER. Al acceder al directorio **/media/pruebas** visualizaremos el contenido de la carpeta compartida pruebas. La sintaxis smbmount es: **smbmount //equipo/recurso directorio_de_montaje**.

El proceso de liberación o desmontaje del recursos es similar al montaje sustituyendo **smbmount** por **smbumount**.

2.2. Compartir archivos y directorios en Ubuntu

Vamos a crear una carpeta en el escritorio con el nombre **CompLinux**.

Compartir el directorio **CompLinux**

1. Clic con el botón derecho del ratón sobre la carpeta y en el menú contextual seleccionamos **Propiedades**.
2. Clic sobre la pestaña **Recurso compartido de red local**.
3. Activamos la casilla compartir esta carpeta. Puede que cuando utilicemos esa acción se muestre una ventana de alerta con el texto **El servicio de compartición no está instalado**, haremos clic en **Instalar el servicio**.
4. Daremos acceso de escritura y modificación a los usuarios que accedan a nuestra carpeta, así activaremos **Permitir a otras personas crear y eliminar archivos en esta carpeta**.
5. Clic en **Crear compartición**.
6. Como vamos a permitir acceso de escritura Ubuntu nos advertirá de la realización de modificaciones en los permisos del directorio, permitimos que realice estas modificaciones haciendo clic en **Añadir los permisos automáticamente**.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

NFS (Network File System)

NFS es un **sistema de archivos de red** o **sistema de archivos distribuido** por el que podemos acceder a recursos compartidos remotos de forma transparente. Al igual que montamos unidades o particiones dentro de nuestro disco duro usando un sistema de archivos **Ext4** podemos montar unidades de disco remotas con **NFS**, de forma que el usuario verá una unidad **NFS** como una de sus unidades locales.

NFS es la forma que usa Linux para compartir archivos y directorios con otros sistemas operativos Linux.

ACCESO A RECURSOS COMPARTIDOS LINUX

Todo equipo Linux está configurado para ser cliente **NFS**, de forma que todos podrán acceder a las carpetas compartidas de otros hosts (siempre que estos den permiso para ello). Al ser **NFS** un sistema de archivos, el acceso a una carpeta compartida Linux se realiza mediante el montaje de la unidad remota en uno de los directorios de nuestro sistema de ficheros. El comando a ejecutar será: **sudo mount -t nfs IP:recurso directorio_de_montaje**.

Por ejemplo, si tenemos una máquina con IP 192.168.1.110 en la que hemos instalado Ubuntu y tiene una carpeta compartida llamada /home/juan/ComPC110 podemos acceder a ella escribiendo: **sudo mount -t nfs 192.168.1.110:/home/juan/CompPC110 /media/PC110** siendo /media/PC110 el directorio vacío donde visualizaremos el contenido del recurso compartido.

NOTA: Normalmente, cuando se configuran unidades de red en servidores, se configura en las máquinas Linux clientes el fichero **/etc/fstab** de forma que las unidades de red sean montadas automáticamente al iniciar sesión. El administrador creará una carpeta en un lugar accesible por el usuario en la que montará el sistema de archivos **NFS**. El proceso es automático, inapreciable y transparente para este.

CONFIGURAR EL SISTEMA PARA SER SERVIDOR NFS

Configurar un sistema para que sea servidor NFS significa permitir que comparta archivos y directorios con otros sistemas Linux. Convertiremos a un equipo Ubuntu en servidor NFS instalando el paquete **nfs-kernel-server** y modificando el fichero **/etc/exports**.

Las líneas de **/etc/exports** deben ser del tipo:

carpeta_compartida host o red (opciones de compartición)

Por ejemplo, podemos encontrar una línea del tipo:

/home/juan/compLinux 192.168.1.110 (rw)

Indicamos que tenemos una carpeta compartida (/home/juan/comLinux), permitimos que el pc con ip 192.168.1.110 pueda acceder a ella y pueda leer y escribir su contenido (rw).

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

Cada vez que modifiquemos este fichero debemos reiniciar el servidor nfs ya que este no tiene registradas las últimas modificaciones. Ejecutamos **sudo /etc/init.d/nfs-kernel-server restart**.

NOTA: Podemos configurar los ficheros /etc/host.allow y /etc/host.deny para permitir o denegar el acceso de los equipos a los recursos compartidos.

Acceso al recurso compartido **CompLinux** desde un equipo Windows

1. Antes de acceder desde Windows a la carpeta compartida **CompLinux** vamos a preparar un usuario en Ubuntu para que pueda ser usado por Windows en el acceso.
 - En la MV de Ubuntu accedemos al **terminal** y ejecutaremos el comando **sudo smbpasswd -a Usuario** (siendo usuario alguno de los usuarios que tengamos creados en el sistema e inicien sesión en él)
 - Escribimos el password para sudo y a continuación creamos una contraseña SMB para el usuario.

NOTA: **smbpasswd** permite configurar las contraseñas de los usuarios SAMBA. Los usuarios samba se usarán a la hora de acceder a recursos compartidos de Windows. Los usuarios samba existen previamente en el sistema operativo Linux. La opción **-a** añade un usuario Linux al fichero **smbpasswd**.

2. Clic en **Inicio -> Equipo**. Centramos nuestra atención en el panel izquierdo y hacemos clic en **Red**.
3. En la parte central aparecerán los equipos que están en red con Windows, entre ellos nuestro **PC130** correspondiente a la MV Ubuntu. En caso de que la red tarde en actualizarse y no se visualice el equipo Linux teclearemos en la barra de dirección **\\192.168.1.130** y pulsaremos ENTER.
4. Doble clic sobre la carpeta **CompLinux**. Pedirá credenciales de acceso. Escribimos el nombre del usuario y contraseña que agregamos a la base de datos de usuarios de samba en el punto 2 y veremos el contenido del directorio.

Configuración de SAMBA

Podemos convertir a Linux en un servidor de recursos de Windows con SAMBA, ya hemos visto cómo de forma automática, al compartir una carpeta en el entorno gráfico se instala el paquete y Windows puede acceder al directorio.

Sin embargo, podemos afinar aún más la compartición configurando el servidor y haciendo que Ubuntu pertenezca al grupo de trabajo de Windows, modificando los ficheros de configuración del paquete.

El fichero de configuración de samba es **/etc/samba/smb.conf**.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

CONFIGURACIÓN DE ASPECTOS GLOBALES

1. **gksudo gedit /etc/samba/smb.conf**. Abrimos el fichero /etc/samba/smb.conf con el editor de texto en entorno gráfico **gedit** y permisos de administrador.
2. El fichero está compuesto por multitud de líneas, algunas de ellas son comentarios (empiezan con el símbolo #), es decir, líneas que no serán tenidas en cuenta. Encontramos varias zonas, las zonas se diferencian porque empiezan con **[palabra]**, por ejemplo **[dirUsu]** indica que donde se encuentre comienza la zona que se llama **dirUsu**. Vamos a buscar la zona **[global]**.
3. En **[global]** localizamos la línea **workgroup=...** En esta línea indicamos el grupo de trabajo al que pertenece la máquina. En windows llamábamos al grupo de trabajo CLASE, modificamos la línea para que se muestre: **workgroup=CLASE**
4. Buscaremos la línea security y la modificaremos de forma que: **security = user**, para que los recursos sean accesibles en función de los privilegios de cada usuario. Puede que la línea esté tal y como queremos y lo único que debamos hacer es eliminar el comentario de la misma.
5. Para que los cambios surtan efecto debemos reiniciar los servicios de SAMBA: **smbd** y **nmbd**. Ejecutamos: **/etc/init.d/smbd restart** y a continuación **/etc/init.d/nmbd restart**.
6. Aún no hemos realizado ninguna compartición, solo hemos modificado datos comunes que permiten configurar aspectos generales del servidor. Desde este momento y si no se han producido errores en el proceso veremos como Linux también pertenece al grupo de trabajo **CLASE**.

CONFIGURACIÓN DE LA CARPETA COMPARTIDA

Vamos a compartir un nuevo directorio llamado **CompSAMBA**, previamente debemos crear este en el escritorio como hicimos con CompLinux.

1. Accedemos a **/etc/samba/smb.conf** mediante **gksudo gedit /etc/samba/smb.conf**
2. Nos desplazamos al final del documento y comenzamos una nueva zona (recurso compartido). Escribimos **[CompSAMBA]**
3. Bajo esta zona tendremos que indicar dónde está ubicada la carpeta real que queremos compartir. Escribiremos: **path = /home/usuario/Escritorio/CompSAMBA**.
4. Además, aunque no es obligatorio, podemos escribir una breve descripción del contenido de la carpeta: **comment = Carpeta de pruebas para SAMBA**.
5. Para que pueda ser vista desde la ventana del explorador de Windows 10 escribiremos: **browsable = yes**.
6. Para permitir el acceso de invitado sin necesidad de indicar contraseñas configuraremos la propiedad guest ok: **guest ok = yes**
7. Para conseguir que solo se pueda leer su contenido escribiremos: **read only = yes**.
8. Finalmente, el fichero debe quedar como se muestra a continuación.

```
[CompSAMBA]
path = /home/usuario/Escritorio/CompSAMBA
comment = Carpeta de pruebas para SAMBA
```

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

browsable = yes

guest ok = yes

read only = yes

9. Para finalizar, como el fichero de configuración de samba se ha cambiado, el servicio debe reiniciarse para que este sea leído y pueda usarse la carpeta compartida **CompSAMBA**. Escribiremos las siguientes líneas:

- **sudo restart smbd o /etc/init.d/smbd restart**
- **sudo restart nmbd o /etc/init.d/nmbd restart**

NOTA: Existen multitud de propiedades que podemos agregar ya no solo a nuestros recursos compartidos, sino al resto de secciones. Si el alumno lo desea puede ver información relacionada con el tema en el siguiente enlace <https://samba.org/samba/docs/man/Samba-HOWTO-Collection/> (colección HOWTOs de samba)

USUARIO Y GRUPOS DE LA COMPARTICIÓN

Con el uso de la propiedad **guest ok = yes** en el fichero de configuración de samba smb.conf permitimos que cualquier usuario pueda acceder al recurso, ya que lo hace como invitado, pero, ¿qué ocurre si quiero controlar quién accede al recurso compartido y qué permisos tiene? Para hacer esto debo seguir los pasos siguientes:

1. Accedemos a **smb.conf** y cambiamos el valor de la propiedad **guest ok = no**.
 2. Reiniciar los servicios **smbd** y **nmbd**. A partir de ahora el acceso desde Windows no es posible ya que el recurso no tiene acceso de invitado
 3. Agregamos aquellos usuarios que puedan acceder a la carpeta usando **smbpasswd** y escribimos **smb.conf** los parámetros **valid users**, **read list**, **write list** o **admin users** para cada recurso compartido.
- **valid users = @grupo1, @grupo2, ... @grupoN**. Usuarios que tienen acceso al recurso compartido.
 - **read list = @grupo1, @grupo2, ... @grupoN**. Indicamos aquellos grupos que van a tener acceso al recurso compartido como solo lectura.
 - **write list = @grupo1, @grupo2, ... @grupoN**. Indicamos aquellos grupos que van a tener acceso al recurso compartido como escritura.
 - **admin users = usuario**. Usuarios individuales que administran el recurso.

[CompSAMBA]

path = /home/usuario/Escritorio/CompSAMBA

comment = Carpeta de pruebas para SAMBA

browsable = yes

guest ok = no

read only = yes

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

valid users = @¹usu12, usu3

write list = usu3

SWAT

Swat es una herramienta que se usa para la configuración del fichero `/etc/samba/smb.conf` de forma gráfica y sencilla. Podemos instalar el paquete con la siguiente orden en modo texto: **sudo apt-get install swat**, o bien hacer uso del **Centro de Software de Ubuntu**.

Una vez la hayamos instalado accederemos a ella a través del navegador escribiendo en la barra de direcciones: **http://localhost:901²**.

NOTA: Para acceder a SWAT debemos usar el usuario root. Es necesario que de antemano hayamos configurado una contraseña para root mediante el comando **sudo passwd root**.



La barra de herramientas SWAT nos permite:

- Visualizar documentación relacionada con SAMBA mediante el botón **HOME**.
- Acceder y modificar la zona de parámetros globales ([global]) a través del botón **GLOBALS**.
- Crear nuevos recursos compartidos a través de **SHARES**.
- Compartir impresoras a través de **PRINTERS**.
- Utilizar el asistente (**WIZARD**) que nos ayude en la configuración de SAMBA y a través del que podamos configurar controladores de dominio de forma rápida y fácil.
- Observar el estado del servidor SAMBA. Al hacer clic en **STATUS** veremos si **smbd** y **nmbd** se están ejecutando correctamente y podemos reiniciar estos servicios en caso de realizar modificaciones en `smb.conf`.
- Visualizar el fichero `/etc/smb.conf` al hacer clic en **VIEW**.
- Agregar a usuarios Linux a `smbpasswd` para que puedan acceder a las carpetas compartidas en Windows a través de **PASSWORD**.

CREAR RECURSOS COMPARTIDOS CON SWAT

Antes de ver cómo crear recursos compartidos con SWAT vamos a preparar el sistema:

¹ El símbolo @ se usa cuando queremos referirnos a un grupo. Para usuarios individuales escribimos directamente parámetro = usuario.

² Notación URL en la que indicamos el PC y puerto. Normalmente cuando accedemos a una dirección Web solo escribimos la dirección del servidor. Esto se permite porque http siempre usa el puerto de comunicación 80. Si éste cambiara deberíamos usar `http://dirección:puerto`.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

- Creamos una carpeta en el escritorio llamada **CompSWAT**
- Creamos tres usuarios llamados usu1, usu2 y usu3
- Creamos un grupo llamado usu12 que es un grupo secundario de los usuarios usu1 y usu2.
- Asigna contraseñas mediante smbpasswd a cada uno de los usuarios para que puedan acceder al directorio compartido.

Una vez realizadas las operaciones anteriores:

1. Accedemos a SWAT escribiendo en la barra de dirección del navegador <http://localhost:901>.
2. Escribimos **root** en **user name** y en **password** tecleamos la contraseña del superusuario.
3. Clic en **SHARES**.
4. Escribimos en el cuadro **Create Share** el nombre del recurso compartido y clic en el botón **Create Share**. Vamos a llamar al nuevo recurso **CompSWAT**.
5. Aparecen nuevas opciones de configuración del recurso que acabamos de crear. En el cuadro **comment** escribimos una breve descripción del recurso, "*Carpeta compartida para SWAT*".
6. En el cuadro **path** escribimos la ruta real del recurso compartido:
/home/usuario/Escritorio/CompSWAT.
7. En la zona de seguridad de usuario modificamos las siguientes características:
 - Seleccionamos **NO** en la lista **read only** permitiendo la escritura en el recurso
 - Seleccionamos **NO** en la lista **guest ok** para que solo puedan acceder a la carpeta usuarios con credenciales.
 - En el cuadro **valid user** escribimos **@usu12, usu3**. Permitiendo solo el acceso a los usuarios del grupo **usu12** y al usuario **usu3**.
 - En el cuadro **admin users** escribimos **usu3** de forma que lo estamos convirtiendo en administrador del recurso.
 - En el cuadro **read list** escribimos **@usu12, usu1 y usu2** tendrán acceso al recurso de solo lectura.
 - En el cuadro **write list** escribimos **usu3**. El administrador **usu3** sí podrá crear elementos y modificar el recurso.
8. La opción de navegación debe estar activa para que el recurso se visualice en el explorador de Windows, las listas **browseable** y **available** deben estar configuradas a **YES**.
9. Clic en **commit change** para confirmar las modificaciones y escribir en el fichero /etc/smb.conf
10. Por último, debemos reiniciar el servicio. Clic en el botón **STATUS** y a continuación en **restart All**.

Para comprobar las modificaciones realizadas:

1. Accedemos a la MV Windows y en ella **Inicio -> Equipo -> Red**.
2. Doble clic en **PC130**, nombre de nuestra MV Ubuntu.
3. Veremos el recurso **CompSWAT**, doble clic sobre él para acceder a su contenido. Windows nos pedirá credenciales.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

- Utilizar cada uno de los usuarios creados teniendo en cuenta que solo usu3 puede modificar el contenido del recurso compartido.

NOTA: Podemos modificar un recurso compartido desde **SHARES**, seleccionando en la lista el recurso y a continuación haciendo clic en **Choose Share**.

3. Permisos y carpetas compartidas

Hemos estudiado en el apartado anterior cómo podemos configurar un recurso compartido para que sea accesible por algunos usuarios a través de SAMBA, sin embargo, el uso habitual de control de acceso se lleva a cabo mediante la aplicación de permisos al directorio o recurso que se quiere compartir.

Ya sea en sistemas Windows o Linux, el recurso compartido se crea con acceso total para todos los usuarios y es en la configuración de permisos donde se deniegan o restringen los accesos al mismo.

3.1. Configuración de la seguridad de recursos compartidos en Windows (ESTO YA LO VIMOS)

Supongamos un sistema Windows con tres usuarios: Alberto, Juan y Maria. Tenemos una carpeta en C llamada COMP, y dentro de ella cuatro subcarpetas: JUAN, ALBERTO, MARIA y TODOS. A las carpetas JUAN, ALBERTO Y MARIA solo podrán acceder los usuarios cuyos nombres coincidan con ellas mientras que a la carpeta TODOS podrán acceder todos los usuarios, pero solo para leer su contenido.

CONFIGURACIÓN DE LOS PERMISOS

- Modificamos los permisos de COMP de forma que solo los usuarios administradores y Juan, Maria y Alberto puedan acceder a ella. El acceso será de solo lectura.
- Modificamos los permisos de los directorio JUAN, ALBERTO y MARIA de forma que a la carpeta MARIA solo pueda acceder Maria, a la carpeta JUAN solo pueda acceder Juan y a ALBERTO solo pueda acceder Alberto. Los usuarios pueden leer, escribir y modificar los contenidos de estas carpetas, pero no pueden eliminarlas, es decir aplicaremos todos los permisos a excepción del permiso control total.
- Finalmente, configuraremos la seguridad de la carpeta TODOS de forma que se agreguen los usuarios Juan, Maria y Alberto como usuarios que pueden acceder, pero solo con permisos de lectura y entrada al mismo.

CONFIGURACIÓN DE LA COMPARTICIÓN

Compartimos la carpeta con nombre de recurso COMP, modificando los permisos de compartición de forma que todos los usuarios tengan control total sobre el recurso.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

ACCESOS DESDE OTRAS MÁQUINAS VIRTUALES

Una vez realizados los pasos anteriores solo queda llevar a cabo las pruebas pertinentes y comprobar si todos los permisos se han asignado correctamente. Para ello, vamos a usar el equipo anfitrión y la máquina virtual Ubuntu para acceder a la carpeta compartida. Iremos usando los diferentes usuarios creados.

Por ejemplo, vamos a acceder desde Ubuntu a la carpeta compartida usando el usuario Maria

1. En el panel lateral clic sobre la Carpeta personal
2. Clic en Otras ubicaciones -> zona Redes, veremos la máquina Windows (PC120)
3. Doble clic sobre PC120. Antes de visualizar los recursos compartidos solicita usuario y contraseña, escribiremos maria y el password que le hayamos asignado.
4. Doble clic en COMP. Vamos a intentar crear un subdirectorio, para lo que hacemos clic en el botón derecho del ratón y crear una carpeta, veremos que la operación no es posible gracias al mensaje de alerta Error al crear la carpeta ,permiso denegado. Correcto, la carpeta COMP permite solo acceso de lectura a pesar de que el recurso se comparte con control total.
5. Intentamos acceder a la carpeta JUAN o ALBERTO. Mensaje de alerta: El contenido de la carpeta no se pudo mostrar, no tiene los permisos suficientes para ver el contenido de "JUAN". Correcto, configuramos el directorio JUAN para que solo este usuario pudiera acceder a él. Al realizar la misma operación sobre la carpeta ALBERTO observaremos el mismo resultado.
6. Doble clic sobre MARIA. Se permite el acceso y podemos modificar el contenido creando un nuevo directorio.
7. Doble clic sobre TODOS. Podemos visualizar el contenido pero no modificar este ya que al crear una carpeta me muestra el mismo mensaje de alerta que en el punto 4.

Todos los permisos funcionan correctamente y nuestro recurso compartido posee el nivel de seguridad deseado.

3.2. Configuración de la seguridad de recursos compartidos en Ubuntu

La configuración de seguridad en sistemas operativos Linux es similar a la que hemos visto en el apartado anterior para Windows. Encontraremos diferencias en los pasos a seguir a la hora de compartir un directorio y dar permisos de seguridad al mismo.

Al igual que en Windows:

- Crearemos un directorio con los subdirectorios que necesitemos
- Compartimos el recurso con acceso de escritura tanto para máquinas Linux como Windows usando SAMBA

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

- Configuraremos las opciones de seguridad (permisos) para cada carpeta incluida en él.
- Asignaremos contraseñas smb a los usuarios Linux para que puedan acceder al recurso desde máquinas Windows.
- Confirmaremos el buen funcionamiento haciendo uso de él a través de la red.

4. Comandos de red

4.1. ping

El comando ping (Packet Internet Groper) se usa para comprobar la conectividad del host local con otros equipos de una red TCP/IP mediante el envío de paquetes ICMP de solicitud y respuesta.

La sintaxis de este comando tanto para Windows como para Linux es: **ping IP**

4.2. ipconfig e ifconfig

Ambos comandos permiten visualizar las interfaces de red instaladas en el sistema y modificar estas.

IPCONFIG - COMANDO PARA SISTEMAS WINDOWS

El uso del comando ipconfig sin parámetros permitirá visualizar las interfaces de red instaladas en el sistema. Muestra información de cada interfaz referida a:

- Dirección IP
- Máscara de subred
- Puerta de enlace predeterminada

Si ejecutamos **ipconfig /all** la información que muestra se amplía visualizando entre otras cosas DNS y MAC de la interfaz.

```
Selecció C:\Windows\system32\cmd.exe

Suíjo DNS específico para la conexió. . :
Vínculo: direcció IPv6 local. . . : fe80::8c16:9277:bdfd:d031%10
Direcció IPv4. . . . . : 192.168.46.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Wi-Fi:

Suíjo DNS específico para la conexió. . : cpb.tdp.com
Vínculo: direcció IPv6 local. . . : fe80::6d01:900b:5c50:b308%9
Direcció IPv4. . . . . : 192.168.1.3
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de túnel Local Area Connection* 11:

Estado de los medios. . . . . : medios desconectados
Suíjo DNS específico para la conexió. . :
```

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

Opciones destacadas:

- **/release**. Libera la dirección IP del adaptador de red. Cuando nuestro equipo es cliente DHCP, este comando nos desvincula de la última IP asignada.
- **/renew**. Renueva la dirección IP. Se usa normalmente en adaptadores clientes DHCP.

IFCONFIG - COMANDO PARA SISTEMAS LINUX

Al igual que ipconfig el comando ifconfig permite visualizar dirección ip, máscara de red, etc..., aunque el formato de visualización es diferente.

Nota: El comando ip es el futuro de los comandos de configuración de red. **ifconfig** ha quedado oficialmente en desuso para la suite **ip**.

```
ubuntu@ubuntu-VB:/etc/NetworkManager/system-connections$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel sta
qlen 1000
    link/ether 08:00:27:bd:d1:9c brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.104/24 brd 192.168.0.255 scope global dynamic noprefi
        valid_lft 7191sec preferred_lft 7191sec
    inet6 fe80::a00:27ff:febd:d19c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ubuntu@ubuntu-VB:/etc/NetworkManager/system-connections$
```

Con la instrucción **ip addr show** se mostrará ambas direcciones: IPv4 e IPv6. (**ip a** devolverá el mismo resultado)

En este caso el adaptador es “enp0s3”. La dirección ip aparece tras el nombre **inet** “192.168.0.104” y se muestran por defecto los valores de la dirección broadcast.

Opciones destacadas:

- **link**: nos sirve para configurar las interfaces de red físicas o lógicas, por ejemplo, para ver el estado de todas las interfaces de red.
 - **ip link set enp0s3 up** para activar una interfaz de red
 - **ip addr add 192.168.1.1/24 dev enp0s3** para configurar una dirección IP en una interfaz
 - **ip addr del 192.168.1.1 dev enp0s3** para eliminar una dirección IP de una interfaz

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

- **address:** permite ver y configurar las direcciones IPv4 y IPv6 asociadas a las diferentes interfaces de red. Cada interfaz debe tener al menos, una dirección IP configurada.
 - **ip link set enp0s3 down** para desactivar una interfaz de red

4.3. netstat

Sin parámetros muestra las conexiones activas. Se visualizan protocolos de comunicación, direcciones ip locales y remotas junto a números de puertos. Linux mostrará mayor información indicando procesos. Si no se reconoce por defecto en nuestro sistema Ubuntu, lo instalaremos ejecutando: **sudo apt install net-tools**.

Se puede usar como visor de red para observar la actividad de la red.

Entre las opciones que podemos usar encontramos:

- **-r.** Muestra la tabla de enrutamiento
- **-i (Linux)/ -e (Windows).** Muestra una estadística de la interfaz, de forma que veremos paquetes enviados, paquetes broadcast, errores, etc...
- **-a.** Muestra los puertos activos y pasivos, y que están esperando una conexión.
- **-l.** Muestra únicamente los puertos que están escuchando.

4.4. arp

Muestra la tabla de enrutamiento de cada host. Cada host posee una tabla de enrutamiento mediante la que se asocian direcciones MAC con direcciones IP. En Windows arp se usa con la opción -a: **arp -a**.

El comando arp se puede usar para modificar cada par ip-MAC o agregar entradas a la tabla. Recordamos que gracias a la tabla arp conocemos qué dirección MAC o dirección de red física corresponde a cada dirección ip, de forma que entre sus entradas encontramos el par **ip_router-MACrouter**, si alguien accede a nuestro ordenador puede modificar la tabla arp de forma que cambie este par por **ip_router-MACotroPC**, consiguiendo que todo el tráfico de red de mi PC sea accesible por **otroPC**. Si **otroPC** usa un software **sniffer** estará capturando todo el tráfico de red vulnerando la seguridad del sistema. A este tipo de ataque se le denomina **MitM (Man-in-the-Middle)**

Opciones destacadas:

- **-s.** Agrega una nueva entrada a la tabla de enrutamiento, su sintaxis es: **arp -s ip MAC**, ej. **arp -s 192.168.1.110 00-aa-00-62-c6-09**
- **-d.** Elimina una fila de la tabla de enrutamiento, su sintaxis es arp -id ip, ej. **arp -d 192.168.1.110**
- **-v.** Muestra las entradas de la tabla en modo detallado.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

```

C:\Users\Administrador>arp -a -v

Interfaz: 127.0.0.1 --- 0x1
Dirección de Internet      Dirección física      Tipo
224.0.0.22                 00-00-00-00-00-00    estático
224.0.0.252                00-00-00-00-00-00    estático
239.255.255.250            00-00-00-00-00-00    estático

Interfaz: 192.168.0.10 --- 0x1c
Dirección de Internet      Dirección física      Tipo
192.168.0.1                00-22-3a-e0-75-d8    dinámico
192.168.0.11               00-0c-6e-d6-19-d4    dinámico
192.168.0.13               00-1d-e0-05-1f-d7    dinámico
192.168.0.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.252                01-00-5e-00-00-fc    estático
224.0.0.253                01-00-5e-00-00-fd    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
  
```

4.5. tracert y traceroute

Son comandos que se usan para averiguar la ruta que sigue un paquete hasta llegar a una dirección destino. Podemos usarlos en el proceso de mantenimiento para investigar posibles ataques del tipo MitM. El primero de ellos, tracert, se usa en Windows mientras que traceroute se utiliza en sistemas Linux (es posible que la herramienta no está instalada por defecto, en cuyo caso ejecutaremos: `sudo apt-get install traceroute`).

Un ejemplo de uso del comando sería: `tracert www.google.com`. El resultado de la orden se muestra a continuación, donde la primera columna muestra el número de salto. En la siguiente imagen vemos la dirección ip por la que va pasando hasta llegar al destino especificado.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\>tracert google.com

Traza a la dirección google.com [216.58.219.174]
sobre un máximo de 30 saltos:

  0  1  2  3  4  5  6  7  8  9 10
--  -  -  -  -  -  -  -  -  -  -  -
  0  2 ms  2 ms  2 ms  192.168.1.1
  1  6 ms  5 ms  5 ms  1.182.149.190.dynamic.intelnet.net.gt [190.149.182.1]
  2  6 ms  6 ms  22 ms  10.192.39.173
  3  7 ms  6 ms  6 ms  10.192.37.181
  4  12 ms 11 ms 20 ms 10.192.16.113
  5  36 ms 34 ms 34 ms ix-et-9-1-5-0.tcore2.MLN-Miami.as6453.net [66.110.72.129]
  6  59 ms 33 ms 34 ms 72.14.215.97
  7  33 ms 33 ms 33 ms 209.85.253.120
  8  54 ms 41 ms 32 ms 72.14.235.211
  9  32 ms 32 ms 33 ms mia07s27-in-f14.1e100.net [216.58.219.174]
  
```

- **-h** (en Windows) Indica el número de saltos máximo para alcanzar el destino

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

4.6. route

Muestra la tabla de enrutamiento del encaminador. Además, podemos usar el comando para modificar la tabla, introducir una nueva entrada o eliminar alguna existente. En Windows es necesario usar el comando con el parámetro print del siguiente modo: **route print**

Opciones Windows:

- **add.** Agrega una entrada a la tabla. La sintaxis es **route add ip_destino mask máscara_red ip_puerta_enlace METRIC número**
- **change.** Modifica una entrada de la tabla
- **delete.** Elimina una entrada de la tabla dada su ip

Opciones Linux

- **add.** Añade una nueva entrada a la tabla. El formato de esta opción es:
route add -net ip_red -gw ip_puerta_enlace -netmask máscara_red o
route add -host ip_host -gw ip_puerta_enlace -netmask máscara_red
- **del.** Elimina una ruta de la tabla de enrutamiento. Se usan opciones similares a add.
Ejemplo: **route del -net 192.168.4.0 netmask 255.255.255.0 gw 192.168.4.1 dev eth0**

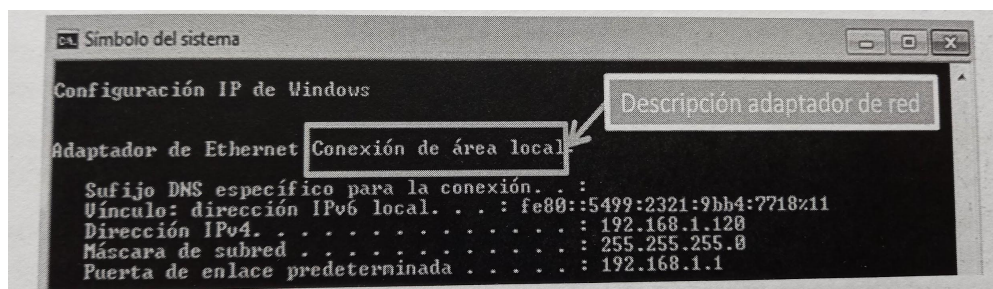
4.7. netsh

Es el comando de configuración de la red de Windows. Al teclear este y pulsar ENTER nos introducimos en su entorno de trabajo desde donde podremos usar diversidad de opciones para la configuración de red. Podemos teclear ? una vez ejecutado **netsh** para visualizar los diferentes **contextos** que podemos usar. Para modificar o visualizar información de las interfaces de red teclearemos **interface** de forma que el prompt cambiará a **netsh interface>**. En este contexto podemos usar las opciones:

- **ip show interface.** Muestra las interfaces de red conectadas al sistema
- **ip show route.** Muestra la tabla de enrutamiento
- **ip set address.** Desde este contexto de trabajo podemos añadir una nueva dirección ip a la interfaz con **ip set address “Descriptor adaptador de red” static ip máscara Gateway métrica**, ej. **ip set address “Conexión de área local” static 192.168.1.110 255.255.255.0 192.168.1.1 1**

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF



- **ip set dnsservers.** Se usa para modificar el servidor dns asociado a la interfaz. La sintaxis es `set dns "Descripción adaptador de red" static servidor_DNS [source=dhcp | primary]`. Ej. **ip set dnsservers "Conexión de área local" static 8.8.8.8 primary** o **set dnsservers "Conexión de área local" source=dhcp**.
- **ip set route.** Para modificar o introducir una ruta en la tabla de enrutamiento. La sintaxis del comando es **ip set route red/máscara "nombre_interfaz" ip_puerta_enlace**. Ej. **ip set route 172.16.0.0/16 "Internet" 172.16.0.1**.

4.8. iwconfig

Comando propio de Linux. Se utiliza para la configuración de redes inalámbricas. Entre sus opciones más comunes tenemos:

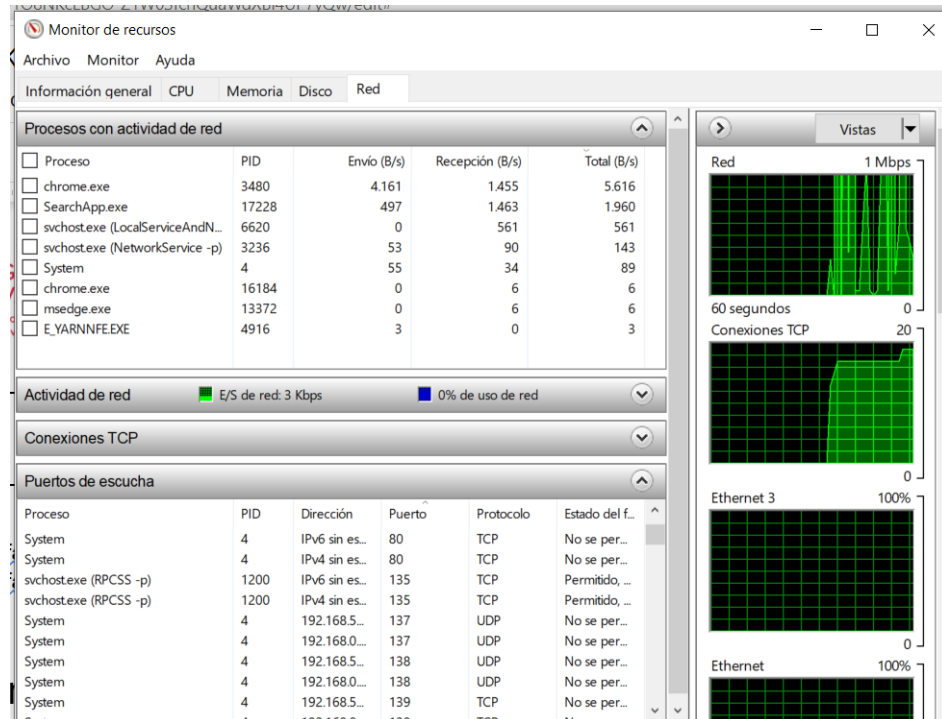
- **Interface essid.** Para modificar o agregar el SSID de la red inalámbrica
- **interface freq.** Modifica la frecuencia a la que trabajamos
- **interface key.** Para agregar o modificar la clave de red

5. Herramientas gráficas de red Windows

En Windows 10 podemos observar el tráfico de red desde el Monitor de recursos. Accedemos a él desde Inicio -> Lista de programas -> Herramientas administrativas -> Monitor de recursos.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF



Desde este entorno gráfico veremos:

- La actividad de la red en tiempo real mediante las gráficas ubicadas en la zona de la derecha
- Los puertos activos, qué procesos están haciendo uso de ellos y en qué dirección IP.
- Las conexiones TCP establecidas por cada proceso activo e involucrado en la red.

COMPUTER SYSTEMS UD7: COMPUTER NETWORKS

CFGS DAW
DPT INF

ACTIVIDADES

1. Configura la red de Windows de tu máquina Virtual (ver apartado 1.3)
2. Configura la red de Ubuntu en tu máquina Virtual (ver apartado 1.4)
3. Busca información sobre la utilidad de configuración de red NetPlan e instálala en tu MV de Ubuntu. Configura la IP estática en tu máquina virtual utilizando esta utilidad.
4. Accede a la siguiente dirección Web: <http://ui.linksys.com/> o en el cuadro de búsqueda de GOOGLE teclea “linksys simuladores”. Los simuladores van a permitir realizar configuraciones de puntos de acceso y routers sin necesidad de tener estos dispositivos físicamente. Prueba diferentes configuraciones para los routers y AP que proponen. Apunta aquellas características que no entiendas y busca en la Web su utilidad.
(Ej router wifi: <https://ui.linksys.com/BEFW11S4/v4/1.52.02/index.htm>)
5. Modifica el nivel de acceso de la carpeta **CompWindows** en la máquina virtual Windows 10 de forma que se pueda escribir en ella. Usa el comando **smbclient** para acceder. Crea un directorio llamado **pruebas**. Observa desde Windows 10 si la carpeta se ha creado con éxito. (apartado 2.1)
6. Observa los comandos que puedes usar en **smb** (usa **-help**) ¿Te son familiares? ¿Qué comando podemos usar para saber en qué directorio de nuestra máquina estamos? ¿Cómo puedo cambiar de directorio? (apartado 2.1)
7. Crea un directorio y compártelo tal como se indica en el apartado 2.2.
8. Instala el paquete **nfs-kernel-server** en tu máquina Ubuntu y comparte la carpeta creada en la actividad 7 usando el fichero **/etc/exports**. Busca información sobre las diferentes opciones que puedes utilizar en cada línea del fichero de configuración. A continuación, configura los PCs del aula de forma que tanto equipos anfitriones como MV pertenezcan a la misma red y sean accesibles desde cualquier máquina Ubuntu. Realiza pruebas, modificando ficheros **/etc/host.deny**, **/etc/host.allow** y **/etc/exports**. (ver apartado 2.2.)
9. Configura alguno de tus usuarios Ubuntu para que puedan usarse en el acceso desde Windows a la carpeta compartida de la actividad 7)
10. Modifica el recurso compartido **CompSWAT** para que sea accesible por solo algunos equipos del aula, usa los parámetros **host allow** y **host deny**. (ver apartado 2.2.)
11. Haz el ejemplo del apartado 2.3 en la MV Ubuntu
12. Desactiva la red usando **systemctl**. Vuelve a activarla modificando la dirección IP por otra de la red que no se esté usando. Observar el fichero **/etc/NetworkManager/system-connections**. (ver apartado 1.3)
13. Echa un vistazo a los comandos de **netsh**. Modifica la dirección ip de tu interfaz de red mediante **netsh**. Agrega una nueva ruta a la tabla de enrutamiento, red=191.1.1.0, máscara 255.255.255.0 y dirección de salto 192.168.1.1. (ver apartado 2.4)