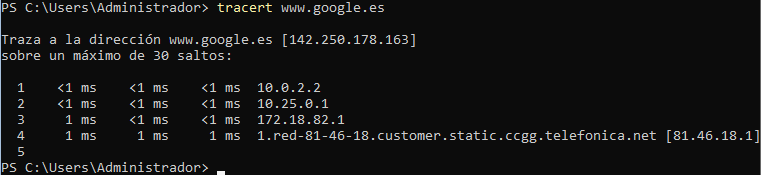
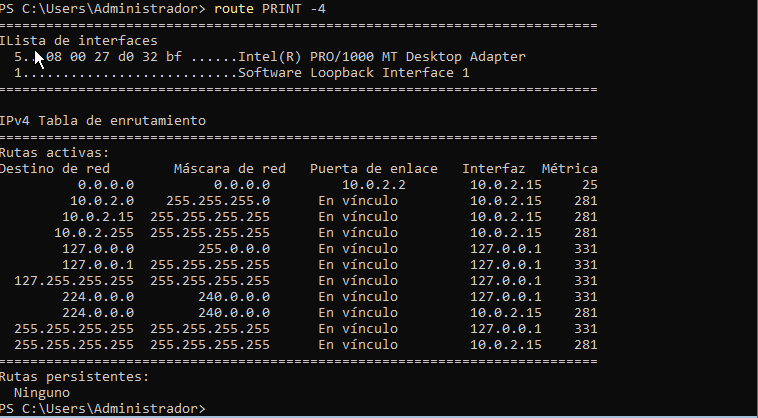
**OPERACIONES BÁSICAS SOBRE WINDOWS SERVER**

Prueba y comenta los siguientes comandos básicos sobre una máquina de Windows Server que puede ser lanzada en Amazon EC2, Azure o en una máquina virtual (puedes descargarte la ISO de windows server desde al área de usuarios):

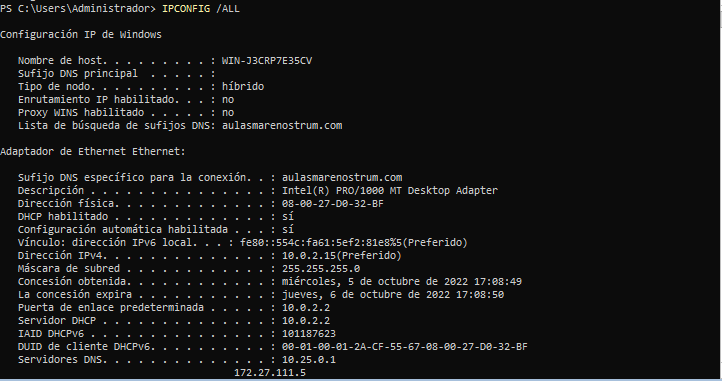
Probar el comando tracert y analizar la información.



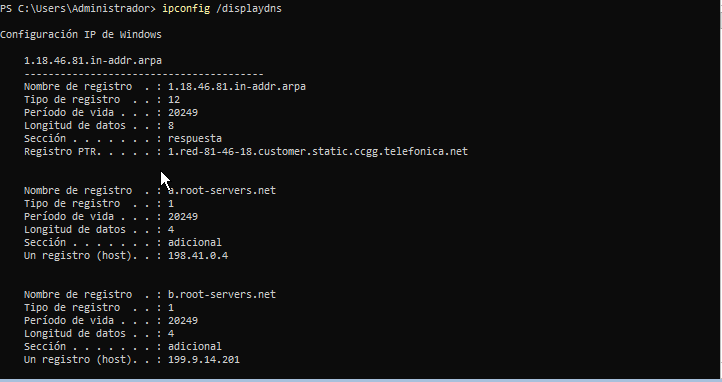
Probar el comando route y analizar la información.



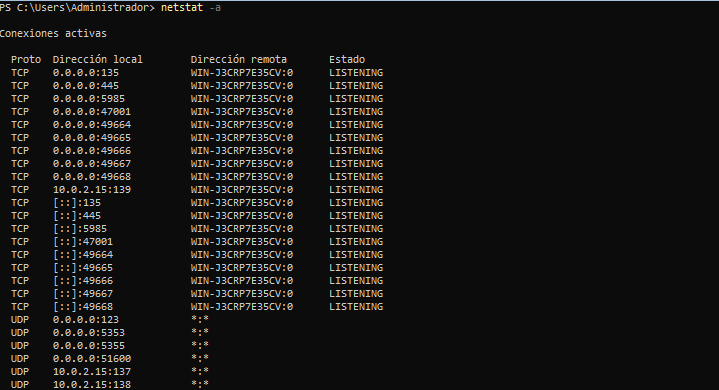
Probar el comando ipconfig /all y analizar la información.



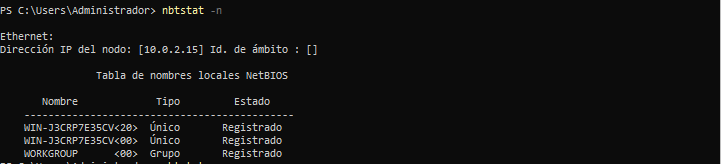
Probar el comando ipconfig /displaydns y analizar la información.



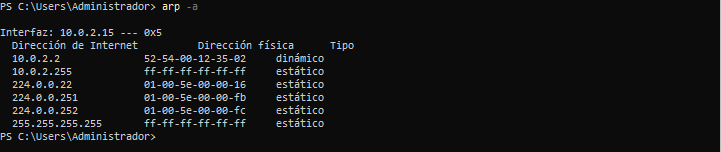
Probar el comando netstat con sus diferentes opciones y analizar la información.



Probar el comando nbtstat con sus diferentes opciones y analizar la información.



Probar el comando arp con sus diferentes opciones y analizar la información.



Probar el comando tasklist con sus diferentes opciones y analizar la información. Prueba a matar algún proceso no esencial con taskkill

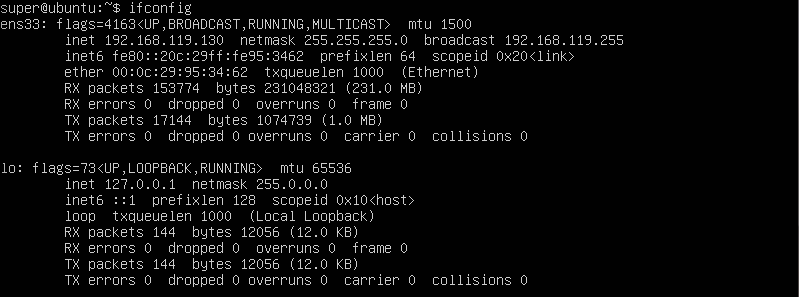


Probar el comando nslookup con sus diferentes opciones y analizar la información.

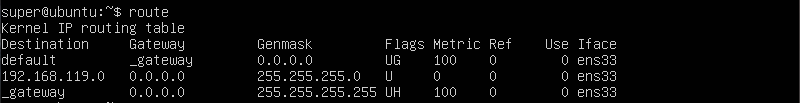


**OPERACIONES BÁSICAS SOBRE LINUX UBUNTU**

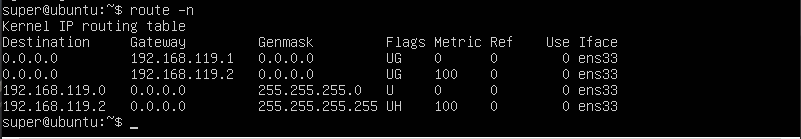
Realiza las operaciones siguientes en un Linux Ubuntu en máquina virtual, arrancado con dirección IP automática en el modo de red que prefieras (recomendado bridged o NAT para tener internet):

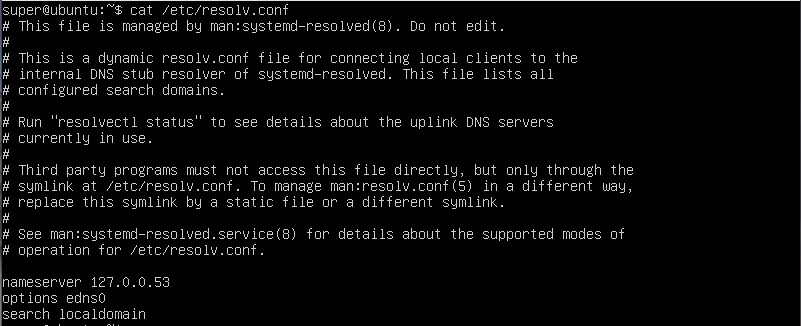
* Haz un ***ifconfig*** (sin parámetros) para ver la configuración de red. Haz una captura resaltando qué IP te ha dado el servidor DCHP en la red interna y externa.

* Mediante **route** (sin parámetros), obtén un listado de la tabla de encaminamiento. La línea que comienza por **default** es la puerta de enlace. Haz una captura de pantalla donde quede resaltado. Con la opción -n puedes ver la IP



* Mediante **route**, añade una IP cualquiera inventada de tu rango de red como segunda puerta de enlace. Haz otro **route** (sin parámetros) para comprobar que se ha añadido y captura la pantalla resaltándolo.

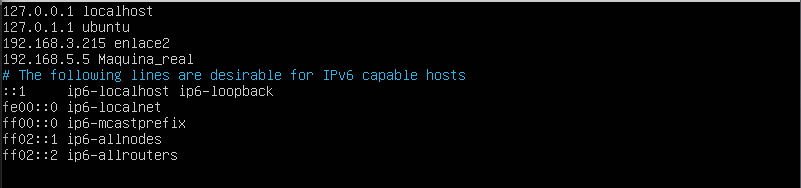


* Visualiza en pantalla el archivo **/etc/resolv.conf** que debe contener el nombre del servidor DNS que se le ha asignado automáticamente. Haz una captura de pantalla resaltándolo.

* Edita (preferentemente con el editor ‘nano’) el archivo **/etc/hosts** añadiendo dos traducciones más de direcciones IP:

*<ip inventada> enlace2*

*IPMAQREAL maquina\_real*

Haz una captura de pantalla de cómo queda el contenido de fichero una vez cambiado y guardado.

* Haz un ***ping*** a los nombres “enlace2” y “maquina\_real”. Puedes cortarlo pulsando Ctrl+C con 4 o 5 respuestas. Haz una captura de pantalla del resultado.

* Haz un **tracepath** (similar a traceroute en Ubuntu) a “enlace2” y “google.com” y haz una captura del resultado.

* Reinicia la máquina, y observa que lo asignado en los apartados anteriores se ha eliminado.

* Prueba el funcionamiento del comando ***netstat***, con sus opciones ***–i*** (estadísticas de tarjeta) ***y –ta*** (conexiones con protocolos y puertos)***.*** Haz una captura de pantalla de los resultados.

* Crea un usuario llamado prueba con una contraseña.

* Inicia otra máquina Linux (la llamaremos máquina Linux B) en el modo de red que prefieras y comprueba que tienen conectividad. Ten cuidado con las direcciones MAC de las tarjetas de las máquinas virtuales, deben ser diferentes.

* Prueba a hacer una conexión de SSH desde la máquina Linux B hacia la máquina Linux A con el usuario “prueba”, de forma exitosa. Sal de la sesión con

“exit”.

* En la máquina A, crea un archivo nuevo llamado ***/etc/hosts.deny***

(preferiblemente con el editor ‘nano’). Este archivo deniega el acceso a todos los servicios y máquinas que pongamos. Dentro del archivo introduce la siguiente línea:

***sshd:ALL EXCEPT ip\_de\_la\_máquina\_Linux\_B***

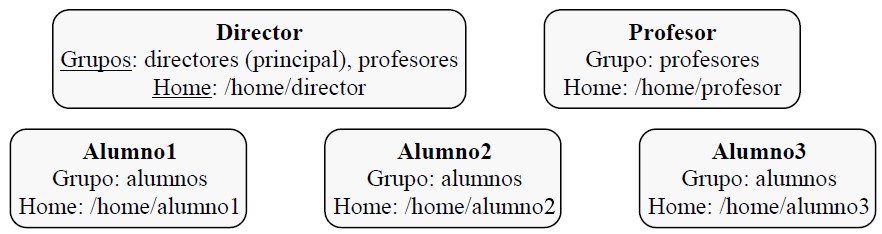
Reinicia la red en Linux y comprueba que ahora es imposible entrar la máquina virtual con **Putty** desde tu equipo. Haz capturas de pantalla de la prueba fallida.

* Entra por SSH desde la máquina B a la máquina A, ya que ahora es la única forma de acceso. Elimina el archivo ***/etc/hosts.deny*** para dejar todo como estaba y reinicia la red. Comprueba que ya puedes entrar desde tu máquina por SSH de nuevo.

* Para dar una dirección IP fija que no cambie con los reinicios: en la tarjeta de red local, pon una configuración de red correcta que tenga acceso a Internet, habría que editar el archivo **/etc/network/interfaces** o según la versión, utilizar la configuración mediante Netplan. Reinicia y comprueba que funciona.

* Crear los siguientes grupos: *directores, profesores y alumnos*.

* Crear los siguientes usuarios dentro de cada grupo y con su carpeta home:



* Crea una carpeta en raíz llamada ***/documentos*** y en dentro de ella, tres carpetas más, llamadas ***apuntes***, ***profesores***, y ***trabajos***

* Establece con **chmod** (preferiblemente en versión rápida) los siguientes permisos para cada carpeta (debes pensar también qué usuario y grupo deben ser dueño de cada carpeta con **chown y chgrp**):

−***apuntes***: Lectura/escritura para directores y profesores y lectura para el resto

−***profesores***: Los 3 permisos para directores y profesores y nada para el resto −***trabajos:*** Los 3 permisos para todo el mundo