EXAMEN PRÁCTICO REDES Y SERVICIOS EN RED

José María Fernández Saavedra 1 DAW

EJERCICIO 1: Direcciones IP  
  
A:

Dada la dirección 10.23.11.107   
Clase: A  
Tipo: Privada  
Máscara: 255.0.0.0  
Dirección IP de red: 10.0.0.0  
Dirección IP de Broadcast: 10.255.255.255  
Dirección IP del primer host:10.0.0.1  
Dirección IP del último host: 10.255.255.254  
  
B:

Dada la dirección 192.168.20.154/20  
Bits de red: 16  
Bits de subred: 4 (por el prefijo 20)  
Bits de Host: 12   
Número de subredes: 16  
Número de hosts direccionables por subred: 4096 (4094 si quitamos el broadcast y la propia subred)  
Máscara de subred: 255.255.240.0  
Dirección IP de la subred: 192.168.16.0  
Dirección IP del primer host de la subred:192.168.16.1  
Dirección IP del último host de la subred: 192.168.31.254  
Dirección IP de broadcast de la subred: 192.168.31.254  
  
C:

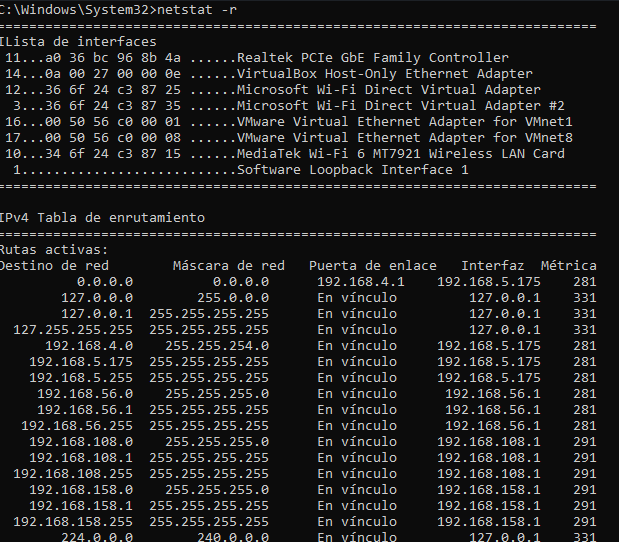
¿Qué clase de red es la más óptima para configurar una red de 10000 hosts?:

Para una red de 10000 hosts la mejor clase sería la B, permite hasta 16384 redes, dando opción hasta a 65534 equipos por red.

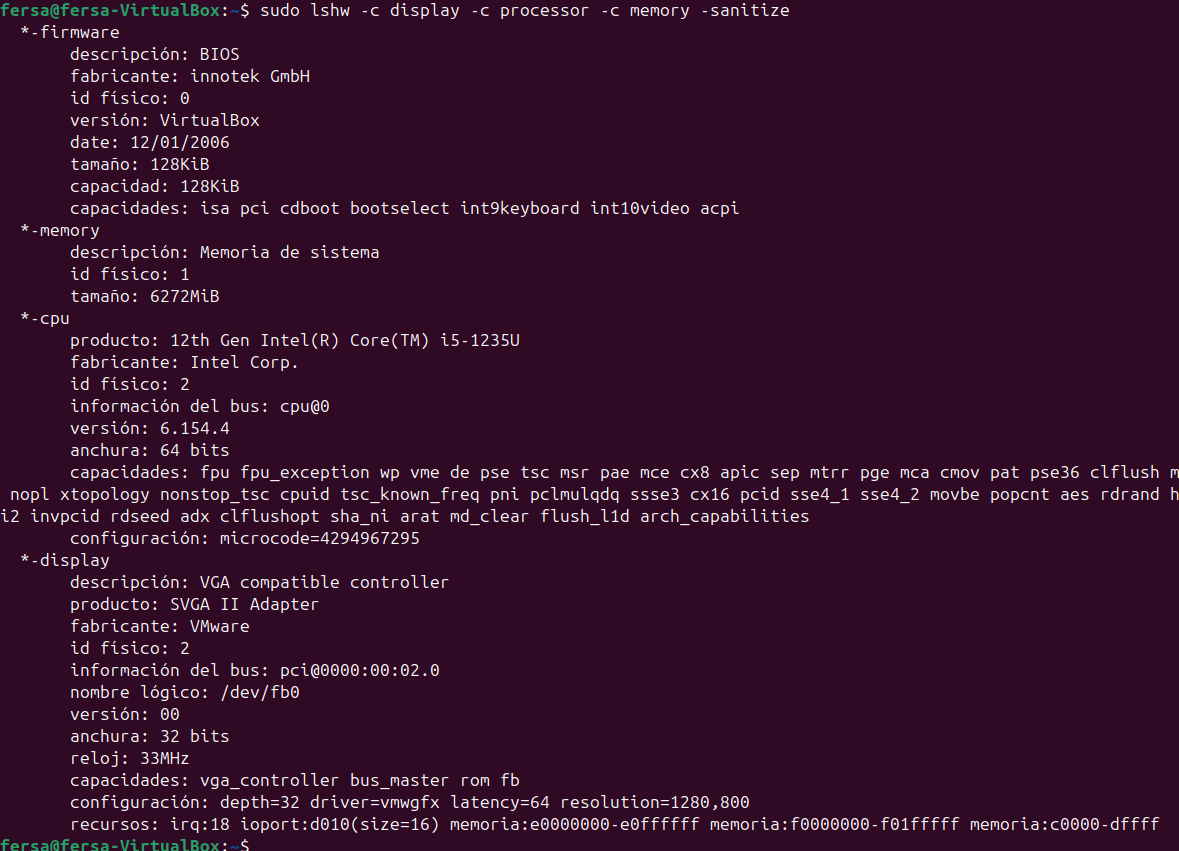
2:

He usado el comando ifconfig | grep ether para obtener la MAC adress de mi máquina virtual, con ella he ido a la página [MAC address 08:00:27 | MAC Address Lookup](https://maclookup.app/search/result?mac=08:00:27:f2:5d:e8)  
Con la MAC:

08:00:27:f2:5d:e8   
He sacado los datos:  
El prefijo 08:00:27 está registrado a PCS Systemtechnik GmbH  
Empresa localizada en 600 Suffold StLowell MA 0185US.  
Está clasificada como MA-L (Mac Address Block large) conteniendo 16 millones de direccones MAC.  
Fue registrada inicialmente el 9 de Noviembre del 2000.  
  
  
3:   
Con netstat -r he visto la tabla de entrutamiento tanto del protocolo IPv4 como del IPv6

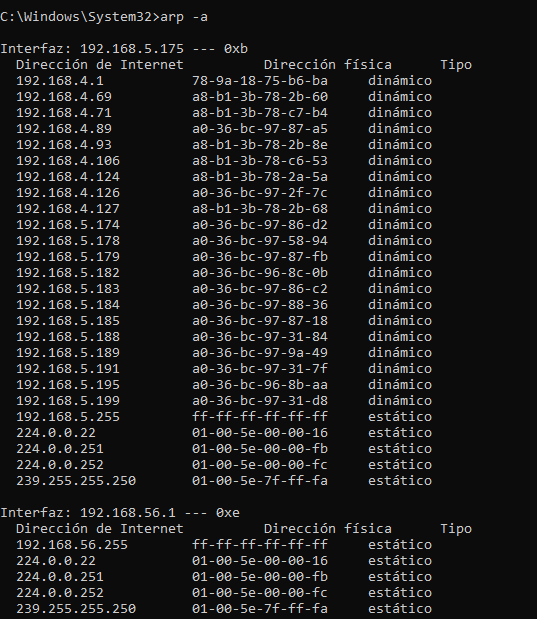
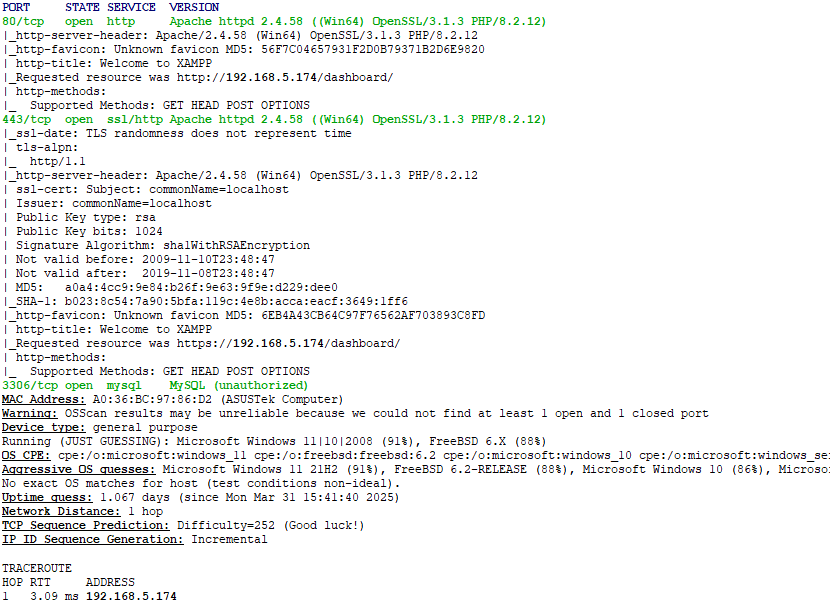


De la tabla de enrutamiento he sacado todos los destinos de red a los que está conectado este dispositivo junto con uss máscaras de red, su puerta y la interfaz. Además la lista de interfaces contiene las MAC de cada uno y el nombre de cada una.

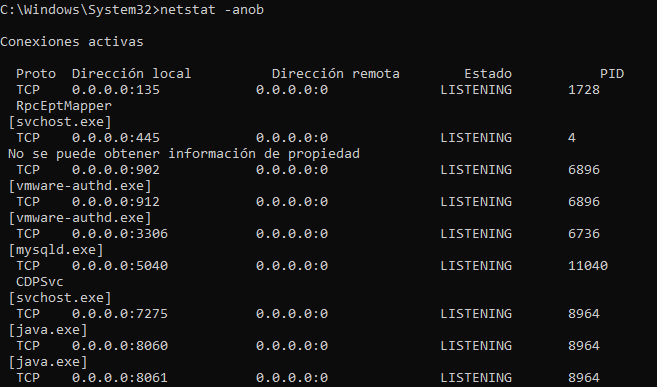
4:  
Usando lshw -sanitize sacamos la información del sistema eliminando la información potencialmente confidencial como las direcciones IP, números de serie y etc.  
Podemos filtrar la información por clases de dispositivos, por ejemplo, con el procesador, la memoría y el display usando -c class:  
  


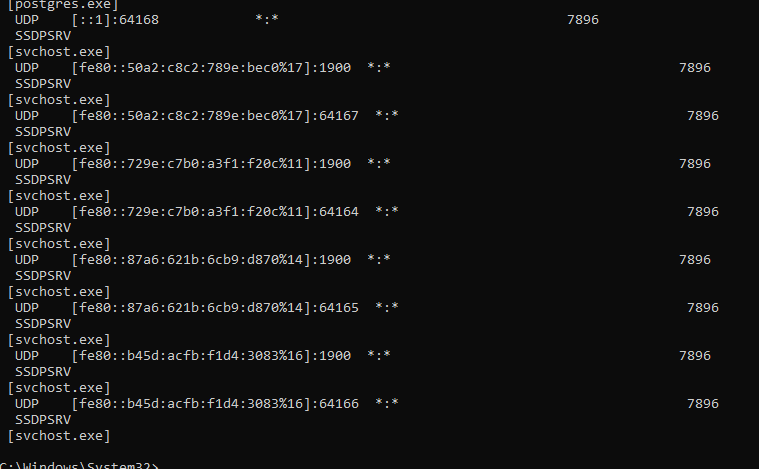
En este caso el comando ha sido lshw -c display -c processor -c memory -sanitize, lo ejecuto en modo superusuario para no dejarme nada fuera.

En esa información podemos sacar toda la información de los dispositivos de las clases que hemos elegido, como la memoria con su capacidad, los datos de la cpu desde su nombre hasta su anchura y todos los datos del display.

5:  
Usando el comando arp -a en el cmd de Windows he sacado la tabla ARP del host:  
  
  
De aquí podemos ver todas las direcciones IP y sus correspondientes direcciones MAC que están conectadas a este dispositivo.  
  
  
  
  
  
  
  
  
6: NMAP  
He hecho un escaneo intenso a la IP 192.168.5.174 con NMAP y ha el resultado ha sido:  


De aquí podemos interpretar varias cosas.  
La MAC address: A0:36:BC:97:86:D2 que corresponde a un ordenador de ASUSTek  
NMAP ha supuesto que el dispositivo está usando Windows 11.  
Después en un intento más agresivo ha llegado a detectar que el dispositivo tiene Microsoft Windows 11 21H2.  
Ha adivinado que lleva 1067 días activo desde ( Mon Mar 31 15:41:40 2025)  
Que está a un salto de red de distancia.  
Que la predicción de la secuencia del TCP es de dificultad 252   
La secuencia de generación de la IP ID es incremental.  
  
Lo más destacable es que hemos conseguido acceso a los puertos:  
80/tcp: Corresponde a un servicio http de Apache.   
443/tcp: Corresponde a un servicio ssl/http de Apache.  
Estos dos puertos corresponden a XAMPP  
el último puerto. 3306/tcp, aunque está abierto, está desautorizado, pero podemos saber que resulta ser MySQL.

7:  
Usando el comando en el cmd de Windows:  
netstat -nabo  
  




Vemos todos los procesos que tienen sockets TCP y UDP establecidos junto con las IPS, los puertos y el PID de cada proceso.