

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 address de mi máquina virtual, con ella he ido a la página [MAC address 08:00:27 | MAC Address Lookup](#)

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 Suffolk St Lowell MA 0185US.

Está clasificada como MA-L (Mac Address Block large) conteniendo 16 millones de direcciones MAC.

Fue registrada inicialmente el 9 de Noviembre del 2000.

3:

Con `netstat -r` he visto la tabla de enrutamiento tanto del protocolo IPv4 como del IPv6

```
C:\Windows\System32>netstat -r

=====
Lista de interfaces
11...a0 36 bc 96 8b 4a .....Realtek PCIe GbE Family Controller
14...0a 00 27 00 00 0e .....VirtualBox Host-Only Ethernet Adapter
12...36 6f 24 c3 87 25 .....Microsoft Wi-Fi Direct Virtual Adapter
3...36 6f 24 c3 87 35 .....Microsoft Wi-Fi Direct Virtual Adapter #2
16...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
10...34 6f 24 c3 87 15 .....MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.4.1           192.168.5.175 281
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
192.168.4.0         255.255.254.0       En vínculo            192.168.5.175 281
192.168.5.175       255.255.255.255     En vínculo            192.168.5.175 281
192.168.5.255       255.255.255.255     En vínculo            192.168.5.175 281
192.168.56.0        255.255.255.0       En vínculo            192.168.56.1  281
192.168.56.1        255.255.255.255     En vínculo            192.168.56.1  281
192.168.56.255      255.255.255.255     En vínculo            192.168.56.1  281
192.168.108.0       255.255.255.0       En vínculo            192.168.108.1 291
192.168.108.1       255.255.255.255     En vínculo            192.168.108.1 291
192.168.108.255     255.255.255.255     En vínculo            192.168.108.1 291
192.168.158.0       255.255.255.0       En vínculo            192.168.158.1 291
192.168.158.1       255.255.255.255     En vínculo            192.168.158.1 291
192.168.158.255     255.255.255.255     En vínculo            192.168.158.1 291
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1     331
```

De la tabla de enrutamiento he sacado todos los destinos de red a los que está conectado este dispositivo junto con sus 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 memoria y el display usando `-c class`:

```
fersa@fersa-VirtualBox:~$ sudo lshw -c display -c processor -c memory -sanitize
*-firmware
  descripción: BIOS
  fabricante: innotek GmbH
  id físico: 0
  versión: VirtualBox
  date: 12/01/2006
  tamaño: 128KiB
  capacidad: 128KiB
  capacidades: isa pci cdboot bootselect int9keyboard int10video acpi
*-memory
  descripción: Memoria de sistema
  id físico: 1
  tamaño: 6272MiB
*-cpu
  producto: 12th Gen Intel(R) Core(TM) i5-1235U
  fabricante: Intel Corp.
  id físico: 2
  información del bus: cpu@0
  versión: 6.154.4
  anchura: 64 bits
  capacidades: fpu fpu_exception wp vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush m
nopl xtopology nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 cx16 pcid sse4_1 sse4_2 movbe popcnt aes rdrand h
i2 invpcid rdseed adx clflushopt sha_ni arat md_clear flush_lid arch_capabilities
  configuración: microcode=4294967295
*-display
  descripción: VGA compatible controller
  producto: SVGA II Adapter
  fabricante: VMware
  id físico: 2
  información del bus: pci@0000:00:02.0
  nombre lógico: /dev/fb0
  versión: 00
  anchura: 32 bits
  reloj: 33MHz
  capacidades: vga_controller bus_master rom fb
  configuración: depth=32 driver=vmwgfx latency=64 resolution=1280,800
  recursos: irq:18 ioport:d010(size=16) memoria:e0000000-e0ffffff memoria:f0000000-f01fffff memoria:c0000-dffff
fersa@fersa-VirtualBox:~$
```

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:

```
C:\Windows\System32>arp -a

Interfaz: 192.168.5.175 --- 0xb
Dirección de Internet      Dirección física      Tipo
192.168.4.1                78-9a-18-75-b6-ba    dinámico
192.168.4.69               a8-b1-3b-78-2b-60    dinámico
192.168.4.71               a8-b1-3b-78-c7-b4    dinámico
192.168.4.89               a0-36-bc-97-87-a5    dinámico
192.168.4.93               a8-b1-3b-78-2b-8e    dinámico
192.168.4.106              a8-b1-3b-78-c6-53    dinámico
192.168.4.124              a8-b1-3b-78-2a-5a    dinámico
192.168.4.126              a0-36-bc-97-2f-7c    dinámico
192.168.4.127              a8-b1-3b-78-2b-68    dinámico
192.168.5.174              a0-36-bc-97-86-d2    dinámico
192.168.5.178              a0-36-bc-97-58-94    dinámico
192.168.5.179              a0-36-bc-97-87-fb    dinámico
192.168.5.182              a0-36-bc-96-8c-0b    dinámico
192.168.5.183              a0-36-bc-97-86-c2    dinámico
192.168.5.184              a0-36-bc-97-88-36    dinámico
192.168.5.185              a0-36-bc-97-87-18    dinámico
192.168.5.188              a0-36-bc-97-31-84    dinámico
192.168.5.189              a0-36-bc-97-9a-49    dinámico
192.168.5.191              a0-36-bc-97-31-7f    dinámico
192.168.5.195              a0-36-bc-96-8b-aa    dinámico
192.168.5.199              a0-36-bc-97-31-d8    dinámico
192.168.5.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

Interfaz: 192.168.56.1 --- 0xe
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
```

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:

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
|_ http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
|_ http-favicon: Unknown favicon MD5: 56F7C04657931F2D0B79371B2D6E9820
|_ http-title: Welcome to XAMPP
|_ Requested resource was http://192.168.5.174/dashboard/
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
443/tcp   open  ssl/http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_   http/1.1
|_ http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
|_ ssl-cert: Subject: commonName=localhost
|_ Issuer: commonName=localhost
|_ Public Key type: rsa
|_ Public Key bits: 1024
|_ Signature Algorithm: sha1WithRSAEncryption
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-08T23:48:47
|_ MD5: a0a4:4cc9:9e84:b26f:9e63:9f9e:d229:dee0
|_ SHA-1: b023:8c54:7a90:5bfa:119c:4e8b:acca:eacf:3649:1fff6
|_ http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
|_ http-title: Welcome to XAMPP
|_ Requested resource was https://192.168.5.174/dashboard/
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: A0:36:BC:97:86:D2 (ASUSTek Computer)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_se:
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (86%), Microso:
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 1.067 days (since Mon Mar 31 15:41:40 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE
HOP RTT ADDRESS
1 3.09 ms 192.168.5.174
```

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

```
C:\Windows\System32>netstat -anob

Conexiones activas

    Proto  Dirección local          Dirección remota          Estado      PID
    TCP    0.0.0.0:135              0.0.0.0:0                LISTENING   1728
    RpcEptMapper
    [svchost.exe]
    TCP    0.0.0.0:445              0.0.0.0:0                LISTENING   4
    No se puede obtener información de propiedad
    TCP    0.0.0.0:902              0.0.0.0:0                LISTENING   6896
    [vmware-authd.exe]
    TCP    0.0.0.0:912              0.0.0.0:0                LISTENING   6896
    [vmware-authd.exe]
    TCP    0.0.0.0:3306             0.0.0.0:0                LISTENING   6736
    [mysqld.exe]
    TCP    0.0.0.0:5040             0.0.0.0:0                LISTENING   11040
    CDPSvc
    [svchost.exe]
    TCP    0.0.0.0:7275             0.0.0.0:0                LISTENING   8964
    [java.exe]
    TCP    0.0.0.0:8060             0.0.0.0:0                LISTENING   8964
    [java.exe]
    TCP    0.0.0.0:8061             0.0.0.0:0                LISTENING   8964

    [postgres.exe]
    UDP    [:::]:64168             *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::50a2:c8c2:789e:bec0%17]:1900 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::50a2:c8c2:789e:bec0%17]:64167 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::729e:c7b0:a3f1:f20c%11]:1900 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::729e:c7b0:a3f1:f20c%11]:64164 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::87a6:621b:6cb9:d870%14]:1900 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::87a6:621b:6cb9:d870%14]:64165 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::b45d:acfb:f1d4:3083%16]:1900 *:.*                     7896
    SSDPSRV
    [svchost.exe]
    UDP    [fe80::b45d:acfb:f1d4:3083%16]:64166 *:.*                     7896
    SSDPSRV
    [svchost.exe]

C:\Windows\System32>
```

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