

# ARQUITECTURA Y SISTEMAS OPERATIVOS

## Trabajo Práctico N° 3: Subredes, Puertos y otros.

Semana III – Sussini Patricio

---

### 1. Preparativos

---

En Windows:

```
Administrator: Command Prompt
Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::41fc:871d:1c71:fa99%4
    IPv4 Address. . . . . : 192.168.1.204
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8e15:52c8:7836:6ef2%5
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:2877:7aa:3456:ea27:4aa4:239a
    Link-local IPv6 Address . . . . . : fe80::3456:ea27:4aa4:239a%13
    Default Gateway . . . . . : ::
```

Y netstat -an me da una larga lista de puertos UDP y TCP abiertos con su estado.

## Parte 1: Subredes, Subnetting con CIDR

### 1- Usando "ipconfig"

```
IPv4 Address. . . . . : 192.168.1.204
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

### 2- Aplicación de CIDR:

- Con esa dirección IP puedo generar 4 subredes si cambio la máscara a "/26"
- En este caso cada subred podemos tener 62 hosts utilizables.
- Completa la siguiente tabla con los rangos de direcciones IP válidos para cada subred para el caso 192.168.1.0/26

Subnet	Dirección de red	Rango de hosts	Dirección de broadcast
1	• 192.168.1.0	192.168.1.1 - 192.168.1.62	192.168.1.63
2	• 192.168.1.64	192.168.1.65 - 192.168.1.126	192.168.1.127
3	• 192.168.1.128	192.168.1.129 - 192.168.1.190	192.168.1.191
4	• 192.168.1.192	192.168.1.193 - 192.168.1.254	192.168.1.255

## Parte 2: Exploración de puertos

### 1.

```
C:\Users\paddy>netstat -an

Active Connections

  Proto Local Address           Foreign Address         State
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING
  TCP    0.0.0.0:27036            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:38000            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:39000            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:49664            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:49665            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:49666            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:49667            0.0.0.0:0               LISTENING
  TCP    0.0.0.0:49668            0.0.0.0:0               LISTENING
```

### 2. Identifica al menos 3 servicios activos y en qué puertos están corriendo.

- a) SMB (server message block)
  - Puerto TCP 445. Usado para compartir archivos, impresoras y otros recursos en redes de Windows.
- b) RPC (remote procedure call)
  - Puerto TCP 135. Utilizado por servicios Windows para comunicación entre procesos.
- c) Steam (plataforma de juegos)
  - Puertos UDP/TCP 27036. Steam usa estos puertos para actualizaciones y multijugador para juegos comunicándose con sus servidores.

3. Algunos puertos son fijos porque sirven para conexiones que deber ser facilmente localizables. Para conexiones temporales o aplicaciones que estan descargando recursos en paralelo o aplicaciones que no necesitan un puerto conocido se usan puertos dinamicos.
4. El escaneo de puertos funciona enviando solicitudes a una serie de puertos en un sistema objetivo para determinar cuáles están abiertos, cerrados o bloqueados por un firewall. Cuando un puerto esta abierto, responde a la solicitud, mostrando que hay un servicio activo escuchando en ese puerto. Esto permite identificar qué aplicaciones se están ejecutando.

### Parte 3: Medición de latencia y ancho de banda

1-

```
C:\Users\paddy>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\paddy>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=32ms TTL=113
Reply from 8.8.8.8: bytes=32 time=30ms TTL=113
Reply from 8.8.8.8: bytes=32 time=32ms TTL=113
Reply from 8.8.8.8: bytes=32 time=31ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 32ms, Average = 31ms
```

- 2- Lo que principalmente influye es la distancia y ademas el medio por el cual se transmiten los datos.
- 3- La latencia afecta en aplicaciones en tiempo real, dañando la sincronizacion del mensaje y el receptor. Generando mala coordinaciones de recursos. En aplicaciones mas demandantes puede bajar tanto el rendimiento que deja de ser funcional
- 4- No, la latencia no tiene nada que ver con el ancho de banda. La mejor respuesta es un ejemplo practico, entre 100mb de internet "Starlink" o 20mb de internet "Gigared", que se diferencian en que usandolos para correr aplicaciones en linea como el juego Real Time "Rocket League", el proveedor de internet "Gigared" lo corre mucho mas fluido y es mucho mas jugable mientras que con "Starlink" la latencia y la perdida de paquetes es tal que no permite jugarlo. Sin embargo para descargar archivos grandes, donde la latencia no hace mucha diferencia, podemos encontrar mayor utilidad en "Starlink".

## Parte 4: Seguridad en HTTPS

- HTTPS es mucho mas seguro porque el mensaje en texto plano no se transmite, sino que se transmite encriptado, de una forma cuyo significado solo lo conocen ambas partes y no puede ser entendido por terceros. En cambio HTTP se transmite directamente en texto plano.

## Parte 5: VPN

- 1- Seguridad en redes publicas.
- 2- Privacidad y anonimato en linea.
- 3- Acceso a contenido geobloqueado.
- 4- Evitar restricciones institucionales.
- 5- Proteccion contra vigilancia masiva.

## Parte 6: Sockets

Un socket de redes es un punto de comunicación virtual entre dos dispositivos en una red, que permite el intercambio de datos. Funciona como un “extremo” de una conexión, y usa 3 puntos claves:

- Dirección IP
- Puerto
- Protocolo

Se usa en servidores, quienes crean un socket, lo asocia a un puerto y espera conexiones. Luego el cliente crea su propio socket y se conecta al socket del servidor usando su IP y puerto. Una vez establecido se genera el intercambio de datos.

---

*Resultados esperados*

---

Se han completado los 3 requerimientos arriba.