

# TRABAJO PRÁCTICO

*Subredes, puertos y otros*

Alumno: Ignacio Figueroa

Tecnicatura Universitaria en Programación – UTN

Materia: AySO

Comisión: 7

## Objetivos

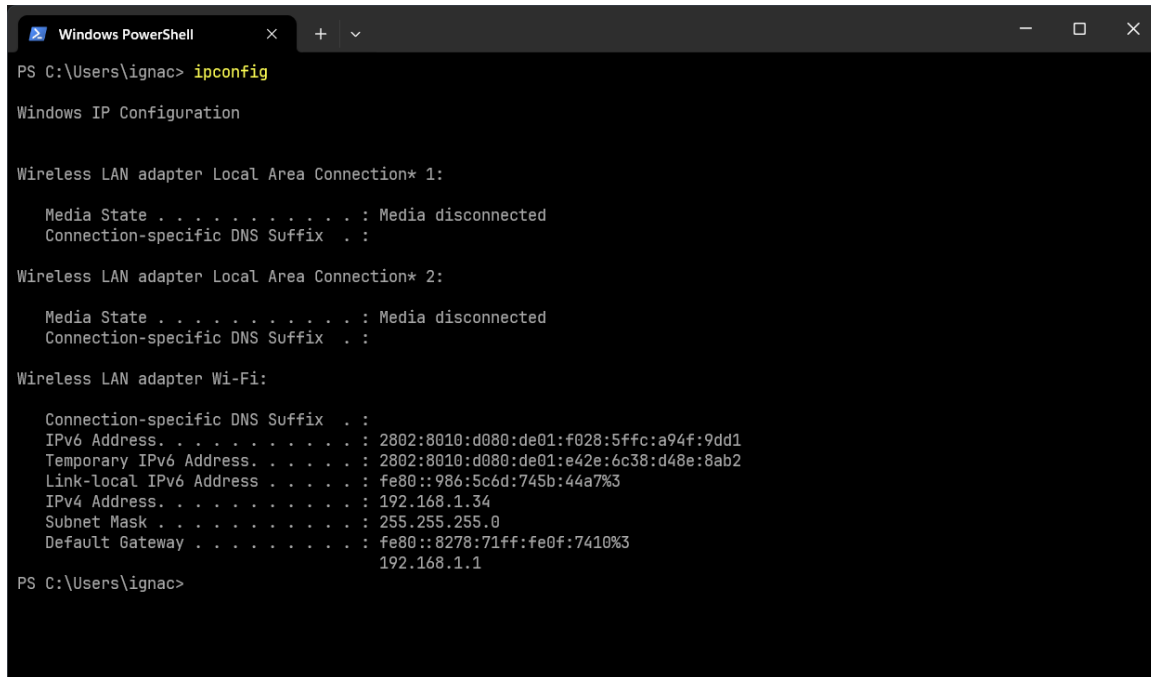
Comprender los conceptos básicos de:

- Subredes y Subnetting con CIDR
- Puertos
- Zonificación DNS
- Latencia vs. Ancho de Banda
- HTTPS
- VPN
- Sockets

## Desarrollo

### Parte 1: Subredes, Subnetting con CIDR

#### 1. Encuentra tu dirección IP local y la máscara de subred



```

Windows PowerShell
PS C:\Users\ignac> ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2802:8010:d080:de01:f028:5ffc:a94f:9dd1
    Temporary IPv6 Address. . . . . : 2802:8010:d080:de01:e42e:6c38:d48e:8ab2
    Link-local IPv6 Address . . . . . : fe80::986:5c6d:745b:44a7%3
    IPv4 Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::8278:71ff:fe0f:7410%3
                                192.168.1.1

PS C:\Users\ignac>
  
```

#### 2. Aplicación de CIDR

IP Base: 192.168.1.34

Mascara: 255.255.255.0

Formato CIDR equivalente: /24



- **¿Cuántas subredes se generan al cambiar de /24 a /26?**
  - Se ganan 2 bits para subneteo ( $26 - 24 = 2$ )
  - $2^2 = 4 = 4$  subredes posibles 
- **¿Cuántos hosts por subred?**
  - En una /26 hay  $2^{16} = 65536$  direcciones totales
  - Restando red y broadcast:  $65536 - 2 = 65534$  hosts válidos 

Tabla de subredes con /26

Subred	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

Identifica al menos tres servicios activos y en qué puertos están corriendo:

Acá van tres ejemplos de servicios que están activos en mi sistema y los puertos en los que están escuchando.

Puerto	Protocolo	Estado	Servicio posible
135	TCP	LISTENING	<b>RPC (Remote Procedure Call).</b> Usado por Windows para comunicación entre procesos.
445	TCP	LISTENING	<b>SMB (Server Message Block).</b> Utilizado para compartir archivos/impresoras en red.
5353	UDP	*	<b>mDNS (Multicast DNS),</b> usado por servicios como AirPlay o

			descubrimiento de dispositivos en red local.
--	--	--	--

¿Por qué algunos servicios usan puertos fijos y otros puertos dinámicos?

- Algunos servicios usan puertos fijos asignados por IANA para funciones estándar, mientras que los puertos dinámicos los asigna el sistema operativo temporalmente para conexiones salientes y evitar conflictos.

¿Cómo funciona el escaneo de puertos y qué puede revelar?

- Un escaneo de puertos envía paquetes para detectar puertos abiertos, cerrados o filtrados, revelando servicios activos, posibles vulnerabilidades, sistema operativo y versiones de software, sin permiso puede considerarse actividad maliciosa.

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

```
Windows PowerShell
PS C:\Users\ignac> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=16ms TTL=64
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms 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 = 5ms, Maximum = 16ms, Average = 8ms
PS C:\Users\ignac> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=43ms TTL=119
Reply from 8.8.8.8: bytes=32 time=64ms TTL=119
Reply from 8.8.8.8: bytes=32 time=11ms TTL=119
Reply from 8.8.8.8: bytes=32 time=10ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 64ms, Average = 32ms
PS C:\Users\ignac>
```

**Medición de latencia:**

Realicédos pruebas con el comando ping

- ping 192.168.1.1 (router)
  - Latencia promedio: 8ms
  - Mínimo: 5ms | Máximo: 16ms
- ping 8.8.8.8 (Servidor de Google en Internet)
  - Latencia promedio: 32ms
  - Mínimo: 10sm | Máximo: 64ms

### **Comparación y análisis:**

- La latencia hacia el router es mucho menor que la latencia hacia un servidor en Internet. Esto se debe a que el router está físicamente cerca mientras que el servidor 8.8.8.8 está geográficamente mas lejos y se accede a través de varios nodos en Internet.
- Factores como la calidad del proveedor de Internet, congestión de red o el tipo de conexión, wi-fi o cable, también influyen

### **Impacto de la latencia en aplicaciones en tiempo real:**

Una latencia baja y estable es fundamental para aplicaciones como por ejemplo juegos en línea, con latencias mayores a 100ms pueden generar el famoso lag, lo que perjudica la experiencia. Otro ejemplo son las videollamadas, alta latencia provoca retrasos y superposiciones de voces, etc. Y por último un ejemplo mas moderno sería el streaming en vivo, al requerir respuestas en tiempo real, la latencia influye directamente en la fluidez.

### **¿Ubicación remota = menos ancho de banda?**

No necesariamente, una mayor latencia por distancia no significa automáticamente menos ancho de banda. El ancho de banda es la cantidad de datos que se pueden transferir por segundo, y la latencia es el tiempo que tardan en llegar los datos.

Es posible tener alta latencia, pero buen ancho de banda y también tener baja latencia, pero bajo ancho de banda.

## **Parte 4: Seguridad en HTTPS**

HTTPS es mas seguro que HTTP porque cifra los datos entre cliente y servidor usando TLS, evitando que terceros puedan espiar o modificar información.

## **Parte 5: VPN**

Una VPN es útil para proteger datos en redes públicas, acceder a contenido restringido geográficamente o mantener la privacidad ocultando la IP original

## **Parte 6: Sockets**

Un socket es un punto de comunicación entre dos dispositivos, TCP se usa cuando requiere conexión confiable, como web o correo, y UDP cuándo se prioriza velocidad sobre fiabilidad, como streaming o juegos.