# ARQUITECTURA Y SISTEMAS OPERATIVOS

## Actividad II: Puertos

### 1. ¿Qué es un puerto?

Un dispositivo en la red se identifica a través de su dirección IP. Sin embargo, dentro de un mismo dispositivo, múltiples aplicaciones pueden necesitar enviar y recibir información al mismo tiempo.

Para gestionar estos flujos de datos, los protocolos TCP y UDP de la Capa de Transporte utilizan el concepto de **puerto de red**.

Un puerto de red es un **punto de acceso lógico** en un dispositivo que permite la comunicación entre aplicaciones y servicios dentro de una red. **Se identifica mediante un número de 16 bits**, lo que permite 65.536 posibles valores (de 0 a 65535).

Aunque existen números de puerto comúnmente asociados a ciertos servicios, esta asignación no es fija y puede modificarse según la configuración.

Por convención:

- Puerto 80 suele utilizarse para servidores web con HTTP.
- Puerto 443 se usa comúnmente para conexiones seguras mediante HTTPS.

Analogía:

Imagina los puertos como si fueran oficinas en un edificio. El número del edificio es la IP y el número de cada oficina es el puerto. Cada oficina tiene una función específica por convención. Sin embargo, si el administrador decide reorganizar el edificio, podría asignar diferentes funciones a cada oficina. Lo mismo ocurre con los puertos en una red: pueden configurarse según la necesidad, pero seguir las convenciones facilita la comunicación.

**Rango de Puertos**

Los puertos están organizados en rangos según su uso:

1. **Puertos bien conocidos (0-1023):**
    - Reservados para servicios y protocolos comunes como HTTP (80), HTTPS (443), y FTP (21).
    - Ejemplo: Cuando escribes http://www.ejemplo.com en tu navegador, se usa automáticamente el puerto **80**.
2. **Puertos registrados (1024-49151):**

- Utilizados por aplicaciones específicas, como juegos o servicios personalizados.
- Ejemplo: Un juego online como Minecraft usa el puerto 25565 para permitir conexiones entre jugadores.

3. **Puertos dinámicos o privados (49152-65535):**
   - Asignados temporalmente por el sistema operativo para conexiones salientes. **Se usan de manera automática y cambian constantemente.**
   - Ejemplo: Cuando abres varias pestañas en tu navegador, cada una usa un puerto dinámico (es decir, no es fijo) diferente para comunicarse con los servidores web.

## 2. Relación entre puertos y aplicaciones

Cuando una aplicación necesita enviar información usando TCP o UDP, el sistema operativo gestiona la comunicación a través de dos tipos de puertos:

- Puerto de origen: Es el puerto que el sistema operativo asigna a la aplicación que envía el paquete.
- Puerto de destino: Es el puerto en el que la aplicación receptora está en escucha, esperando recibir datos, normalmente corriendo en un servidor remoto.

**Cómo funciona el envío de datos con puertos**

La aplicación emisora (cliente) inicia la comunicación. El sistema operativo le asigna un puerto de origen dinámico en el rango 49152-65535. Luego, envía el paquete a la IP del destino, en un **puerto de destino fijo asociado al servicio**.

La aplicación receptora (servidor) recibe el paquete. Está escuchando en un puerto específico, como 80 para HTTP o 53 para DNS. Procesa la solicitud y responde al puerto de origen del cliente.

**Ejemplo práctico con TCP (navegación web)**

Cuando un usuario visita https://www.google.com, su computadora envía un paquete a los servidores de Google:

Solicitud del cliente (desde la computadora del usuario):

192.168.1.50:52345 → 142.250.190.46:443 (TCP)

En este caso:

- 192.168.1.50 es la IP del usuario.

- 52345 es el puerto de origen, asignado dinámicamente.
- 142.250.190.46 es la IP del servidor de Google.
- 443 es el puerto de destino, donde Google escucha solicitudes HTTPS.
- Notar la notación estándar IP:Puerto

Respuesta del servidor (de vuelta al usuario):

142.250.190.46:443 → 192.168.1.50:52345 (TCP)

Ahora, el puerto de destino es 52345, porque la respuesta debe volver a la aplicación que inició la solicitud.

**Ejemplo con UDP (consulta DNS)**

Cuando una computadora necesita resolver un dominio (www.ejemplo.com), envía un paquete UDP a un servidor DNS:

Solicitud del cliente: 192.168.1.50:53000 → 8.8.8.8:53 (UDP)

En este caso:

- 53000 es un puerto de origen dinámico.
- 53 es el puerto de destino, donde el servidor DNS escucha solicitudes.

Respuesta del servidor: 8.8.8.8:53 → 192.168.1.50:53000 (UDP)

El servidor DNS responde desde su puerto 53 al puerto de origen del cliente (53000).

**Práctica Propuesta**

Con netstat -aon en Windows o netstat -lntu en Linux podemos ver una lista de los puertos que se están utilizando actualmente, con su protocolo, la ip remota, el número de proceso y el estado, por ejemplo:

```
C:\Users\diego>netstat -aon

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1272
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9232
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       8104
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1004
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       908
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2544
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2724
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3864
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       980
  TCP    127.0.0.1:24830        0.0.0.0:0              LISTENING       4448
  TCP    192.168.1.13:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.1.13:7680      192.168.1.11:49629     TIME_WAIT       0
  TCP    192.168.1.13:7680      192.168.1.11:49630     TIME_WAIT       0
  TCP    192.168.1.13:7680      192.168.1.11:49631     TIME_WAIT       0
  TCP    192.168.1.13:49415     172.172.255.216:443    ESTABLISHED     5096
  TCP    192.168.1.13:53570     64.233.190.188:5228    ESTABLISHED     2136
  TCP    192.168.1.13:54094     172.172.255.216:443    ESTABLISHED     8400
  TCP    192.168.1.13:54096     31.13.94.52:5222       ESTABLISHED     9748
  TCP    192.168.1.13:54145     142.250.0.188:5228     ESTABLISHED     9748
  TCP    192.168.1.13:54964     52.111.225.6:443       ESTABLISHED     17280
  TCP    192.168.1.13:55229     23.196.15.58:443       CLOSE_WAIT      9904
  TCP    192.168.1.13:55230     23.196.15.58:443       CLOSE_WAIT      9904
```

Podemos observar en este caso varias conexiones establecidas con el puerto remoto 443, el cual, como mencionamos anteriormente, es utilizado por servidores HTTPS. Esto indica que dichas conexiones corresponden, probablemente, a las pestañas abiertas en el navegador.

Por otro lado, las conexiones con estado LISTENING representan puertos abiertos en la computadora, utilizados por el sistema operativo para diversos servicios. Desde una perspectiva de seguridad, sería recomendable cerrar aquellos que no sean estrictamente necesarios. Sin embargo, dado que el router no tiene puertos abiertos al exterior, el riesgo de exposición es menor.

## 3. Preguntas de reflexión

**¿Cada pestaña del navegador usa uno o varios puertos?**

Cada pestaña abierta en el navegador generalmente utiliza un **puerto dinámico único** para cada conexión que realiza. Por ejemplo:

- Si abres dos pestañas para visitar diferentes sitios web, cada una usará un puerto dinámico distinto (como **49155** y **49156**) para comunicarse con los servidores correspondientes.
- Sin embargo, si ambas pestañas cargan contenido del mismo servidor (como imágenes o videos), pueden reutilizar el mismo puerto dinámico para optimizar las conexiones.

**¿Qué relación tienen los puertos con la Capa de Transporte?**

Los puertos son una parte fundamental de la **Capa 4 (Transporte)** del modelo OSI. Esta capa se encarga de establecer y gestionar las comunicaciones entre aplicaciones en dispositivos diferentes. Los protocolos **TCP** y **UDP** usan los puertos para identificar qué aplicación o servicio debe recibir los datos.

**¿Qué es el escaneo de puertos?**

El escaneo de puertos es una técnica utilizada para descubrir qué puertos están abiertos en un dispositivo. Esto permite identificar qué servicios están disponibles o funcionando.

**Usos comunes:**

- **Administradores de red:** Utilizan escáners de puertos para asegurarse de que solo los servicios necesarios estén disponibles y proteger la red contra posibles amenazas.

- **Hackers:** Pueden usar el escaneo de puertos para encontrar vulnerabilidades en un sistema y explotarlas.

**Ejemplo sencillo:** Es como tocar las puertas de un vecindario para ver cuáles responden. Si una puerta está abierta, podrías entrar (o al menos saber que alguien está allí).

**Herramientas comunes:**

- **Nmap:** Una herramienta popular para escanear puertos y mapear redes.

**Relación con NAT (Network Address Translation)**

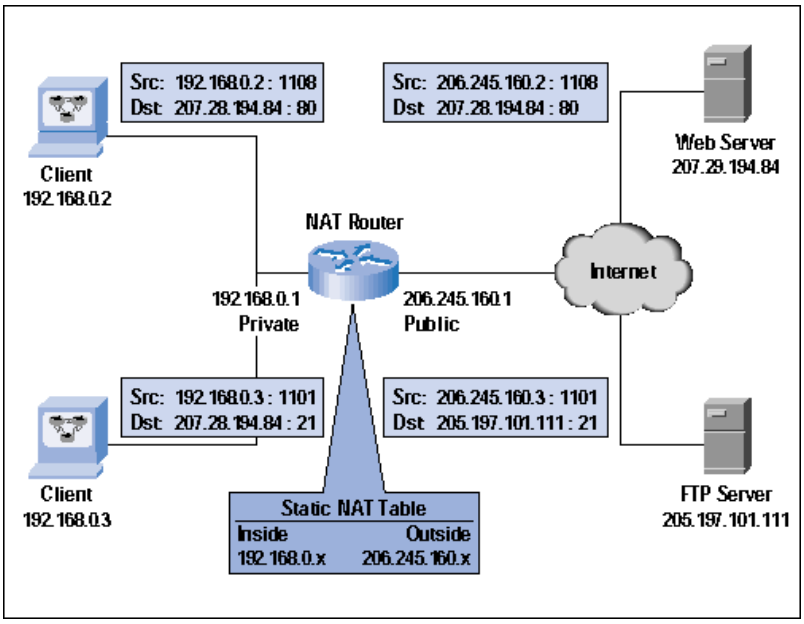
NAT es un protocolo que permite que todos los dispositivos en tu red local (con IP privadas) compartan una sola dirección IP pública para acceder a internet.

**Ejemplo sencillo:** Tienes tres dispositivos en casa:

- Laptop (IP privada: 192.168.1.10)
- Teléfono (IP privada: 192.168.1.20)
- Consola (IP privada: 192.168.1.30)

Cuando todos se conectan a internet, NAT traduce sus IP privadas a la misma IP pública del router (por ejemplo 203.0.113.42). Las conexiones se diferencian usando puertos dinámicos a la salida del router:

- Laptop: IP pública 203.0.113.42 : puerto 49155
- Teléfono: IP pública 203.0.113.42 : puerto 49156
- Consola: IP pública 203.0.113.42 : puerto 49157



**¿Qué significa abrir un puerto en un router?**

Abrir un puerto significa configurar el router para que permita el acceso a un servicio específico desde internet. Esto es necesario, por ejemplo, cuando quieres alojar un servidor de videojuegos o compartir archivos desde tu computadora.

**Ejemplo práctico:** Quieres jugar Minecraft con tus amigos y alojar el servidor en tu PC. Debes abrir el puerto **25565** en tu router y redirigirlo a la IP privada de tu computadora para que puedan conectarse desde internet.

Si quisieras saber cual es la IP Pública con la que accedes a internet, podrías entrar a la página https://whatismyipaddress.com/ .

Podemos usar herramientas en línea como https://www.canyouseeme.org/ para verificar si tenemos puertos abiertos en nuestro router.