

ACTIVIDAD I

1. FUNDAMENTOS DE REDES

1.1. ¿Por qué aprender redes en programación?

En las primeras etapas del desarrollo de software, las aplicaciones eran mayormente autónomas, enfocadas en procesar datos **localmente** y en la interacción con el usuario a través de bases de datos y pantallas simples. Sin embargo, el panorama actual ha cambiado radicalmente: las redes son ahora el núcleo de la funcionalidad de la mayoría de las aplicaciones, ya que permiten la interacción entre dispositivos, servicios y servidores distribuidos en todo el mundo.

El desarrollo de aplicaciones modernas se divide típicamente en dos componentes principales:

- **Cliente:** Es la parte visible de la aplicación que interactúa directamente con el usuario. Este "frontend" incluye aspectos como la interfaz gráfica, la experiencia de usuario y el diseño. Los desarrolladores especializados en esta área manejan tecnologías que permiten la comunicación con servidores remotos a través de sockets o llamadas API REST.
- **Servidor:** Es la parte oculta para el usuario, encargada del almacenamiento, procesamiento de datos y operaciones lógicas. Este "backend" suele incluir la gestión de bases de datos, desarrollo de APIs y la lógica que conecta con el cliente.

En este contexto, comprender redes no solo amplía el entendimiento del flujo de datos entre estos componentes, sino que también es fundamental para garantizar la funcionalidad, seguridad y eficiencia de las aplicaciones.

1.2. Conceptos clave

Al conectar un dispositivo a una red, este utiliza una **interfaz de red**, que puede ser cableada (Ethernet) o inalámbrica (Wi-Fi). Cada interfaz tiene identificadores específicos que la distinguen y permiten la comunicación con otros dispositivos.

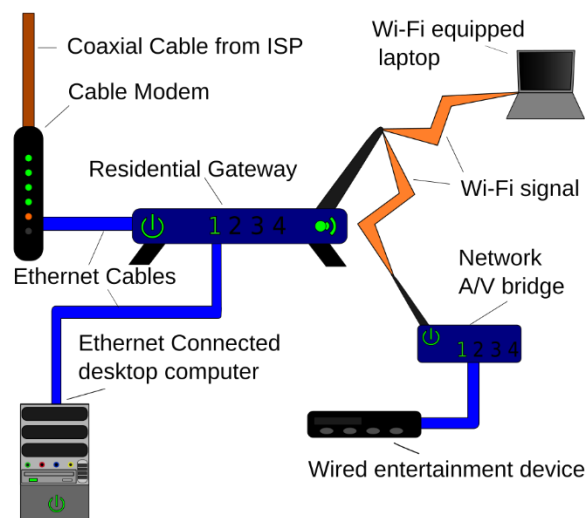
Los elementos clave son:

- **Nombre:** Identifica la interfaz según el sistema operativo y tipo de conexión (por ejemplo, eth0, wlan0, docker0).

- **Dirección MAC:** Un identificador único y permanente asignado al hardware por el fabricante.
- **Dirección IP:** La dirección que localiza al dispositivo dentro de la red, esencial para el envío y recepción de datos.

Además, se utiliza una **máscara de subred** para diferenciar entre direcciones IP de la red local y direcciones externas (internet). El **router** actúa como puerta de enlace, facilitando la conexión entre dispositivos de la red local y el mundo exterior.

En redes con muchas conexiones físicas, se emplean switches, dispositivos que interconectan los equipos dentro de una red local. Los routers domésticos suelen integrar un switch, visible en sus conectores Ethernet.



A continuación, profundizamos en estos conceptos.

1.2.1. Interfaz de red

Permite la conexión del dispositivo a la red. Puede ser:

- Física: Como una tarjeta de red Ethernet o un adaptador Wi-Fi.
- Virtual: Generada por el sistema operativo para conexiones específicas.

Cada interfaz cuenta con dos identificadores únicos:

- Dirección MAC: Permanente y asignada por el fabricante.
- Dirección IP: Variable y dependiente de la configuración de la red.

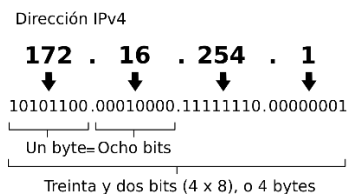
1.2.2. Dirección MAC

Es un identificador único de 48 bits expresado en formato hexadecimal (por ejemplo, 00:1A:2B:3C:4D:5E). Su función principal es identificar dispositivos dentro de redes locales, actuando como una "huella digital" del hardware.



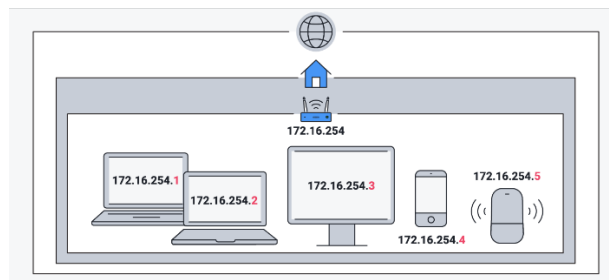
1.2.3. Dirección IP

Es un número dinámico (es decir, que puede cambiar con el tiempo o la configuración) que identifica al dispositivo en la red. Se expresa en formato decimal, dividido en cuatro octetos (por ejemplo, 192.168.1.10). Una dirección IP puede ser fija o dinámica y es esencial para la comunicación en redes locales e internet.



1.2.4. Máscara de subred

Es una herramienta que define qué direcciones IP pertenecen a la red local. Por ejemplo, 255.255.255.0 (o /24) es una máscara común en redes domésticas. Esta máscara, por ejemplo, indica que los 3 primeros números serán iguales en nuestra red, y el último número es el que determinará el dispositivo.



1.2.5. Gateway o puerta de enlace

El dispositivo que conecta la red local con redes externas, generalmente un **router**, que realiza la función de **NAT** (Network Address Translation) para compartir una dirección IP pública entre varios dispositivos locales.

1.2.6. Host

Es cualquier dispositivo conectado a una red, como una computadora, servidor, teléfono o impresora, con capacidad de enviar o recibir datos.

1.2.7. Router

Es el dispositivo central en una red local, encargado de conectar la red con internet, realizar NAT, gestionar redes Wi-Fi y asignar direcciones IP mediante DHCP. Además, puede incluir un **switch** para conexiones físicas.



1.3. Actividad Práctica

Observa las características de las interfaces de red de tu computadora, utilizando la consola:

- En Linux: Usa el comando ``ip addr show``.
- En Windows: Usa el comando ``ipconfig``.

Por ejemplo, en Windows, podemos tener este resultado:

Adaptador de LAN inalámbrica Wi-Fi:

Dirección IPv4: 192.168.1.10

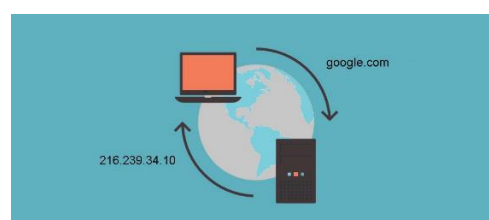
Máscara de subred: 255.255.255.0

Puerta de enlace predeterminada: 192.168.1.1 (la IP de nuestro router)

2. SERVICIOS COMUNES

2.1. DNS (Domain Name System)


El DNS traduce nombres de dominio (como `www.google.com`) en direcciones IP comprensibles para los dispositivos (por ejemplo, `8.8.8.8`). Este servicio es esencial para la navegación web y es gestionado por servidores DNS remotos.



2.2. DHCP (Dynamic Host Configuration Protocol)

El DHCP asigna automáticamente direcciones IP y parámetros de red a los dispositivos. Por ejemplo, al conectarte a una red Wi-Fi, el servidor DHCP (normalmente el router) asigna una dirección IP, junto con información como la máscara de subred, puerta de enlace y DNS.

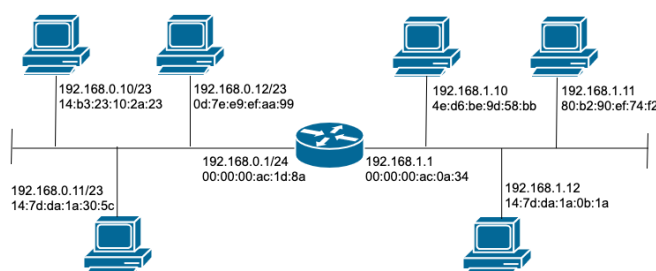
El DHCP evita que tengamos que configurar cada dispositivo de manera manual (aunque podríamos hacerlo en caso de necesitarlo). Va entregando IP distintas a los dispositivos a medida que se van vinculando, por lo que se evita también el problema de IP repetida, que no permite una conexión adecuada.



Dirección IP	192.168.0.15
Máscara de subred	255.255.255.0
Puerta de enlace	192.168.0.254
DNS preferido	80.58.0.33
DNS alternativo	80.58.32.97

2.2. ARP (Address Resolution Protocol)

Este protocolo asocia direcciones IP con direcciones MAC en una red local, permitiendo la comunicación efectiva entre dispositivos. Por ejemplo, cuando un equipo envía datos a otro, el ARP identifica la dirección MAC correspondiente a la IP destino.



2.2. Actividad Práctica

Explora la relación entre MAC e IP en tu red local:

1. Escribe ``arp -a`` en la terminal.

Verás una lista de dispositivos conectados con sus direcciones IP y MAC. Probablemente el primero de ellos sea el router.

```
C:\Users\diego>arp -a

Interfaz: 192.168.1.10 --- 0x8
Dirección de Internet      Dirección física      Tipo
192.168.1.1                44-65-7f-62-61-23    dinámico
192.168.1.255              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
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

2. Prueba conectividad con el comando `ping` seguido de algunas de las direcciones IP listadas en el punto anterior.

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

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 4ms, Media = 3ms

C:\Users\diego>
```

PING significa **Packet Internet Groper** (en español, *Sondeador de Paquetes en Internet*). Es una herramienta de red que se utiliza para probar la conectividad entre dispositivos dentro de una red. Funciona enviando paquetes de solicitud de eco ICMP (Internet Control Message Protocol) a un dispositivo destino y midiendo el tiempo que tarda en recibir una respuesta.

Si hay conexión, obtendrás como respuesta paquetes de eco indicando el tiempo que ha tardado el envío y la devolución, en milisegundos. Un tiempo bajo, indica una baja latencia, es decir que la interacción con el dispositivo remoto será más ágil.