Primer parcial de Redes

Parte 1: Conceptos y teoría

Ejercicio 1:

Ej:1 El mural representa un model OSI que es el modelo antiguo, y el explicado a continuación:

#	Capa OSI	Función Principal	Ejemplos/Protocolos
7	Aplicación	Interacción con el usuario y aplicaciones.	HTTP, FTP, SMTP, DNS
6	Presentación	Traducción de formatos, cifrado, compresión.	SSL/TLS, JPEG, MP3
5	Sesión	Establecimiento, gestión y cierre de sesiones.	NetBIOS, RPC
4	Transporte	Entrega fiable de datos, control de errores y flujo.	TCP, UDP
3	Red	Enrutamiento de paquetes, direccionamiento lógico.	IP, ICMP, OSPF, RIP
2	Enlace de Datos	Comunicación entre dispositivos del mismo segmento; control de acceso y errores.	Ethernet, PPP, HDLC
1	Física	Transmisión física de bits por el medio (señales, voltajes, conectores).	Cables, Wi-Fi, Bluetooth, fibra óptica

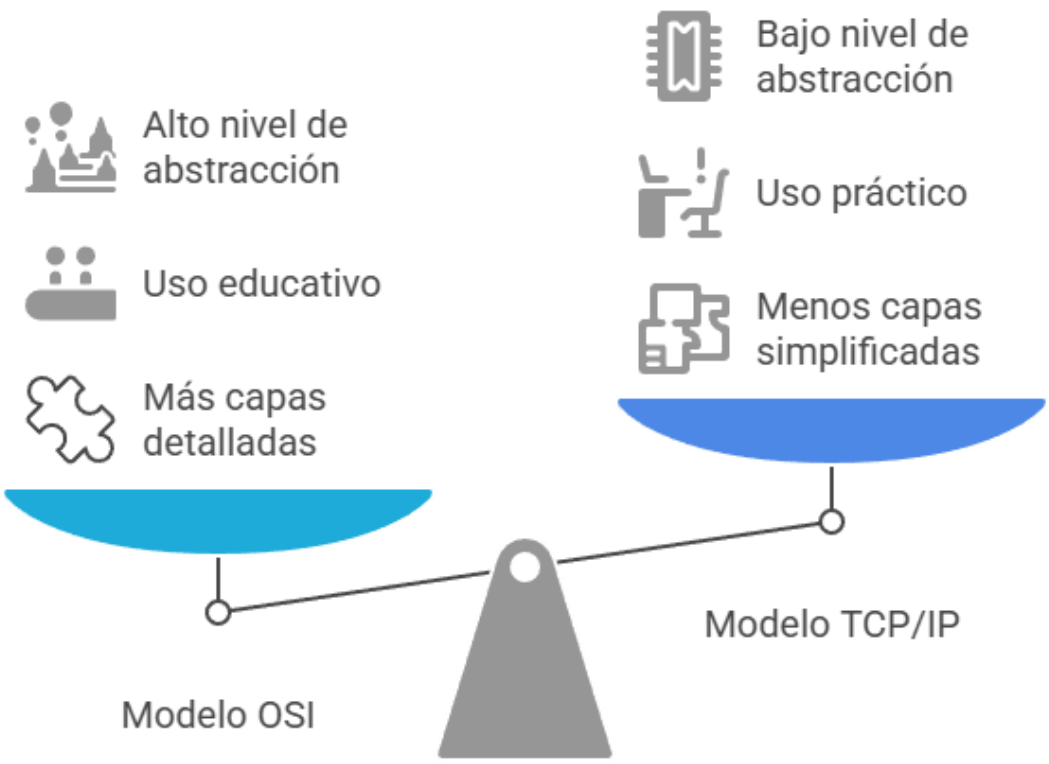
Por otra parte el modelo TCP/IP el cual se representa en la próxima tabla:

Nº	**Capa TCP/IP**	**Función Principal**	**Equivalente OSI**	**Ejemplos / Protocolos**
4	Aplicación	Servicios de red para aplicaciones del usuario final.	Capas 5, 6 y 7	HTTP, FTP, SMTP, DNS
3	Transporte	Comunicación entre procesos, entrega fiable o no fiable.	Capa 4	TCP, UDP
2	Internet	Direccionamiento lógico, enrutamiento entre redes.	Capa 3	IP, ICMP, ARP, IPv4/IPv6
1	Acceso a la red	Acceso físico al medio, tramas, control de transmisión.	Capas 1 y 2	Ethernet, Wi-Fi, MAC, PPP

Por ultimo, una comparativa entre ambos:

Aspecto	**Modelo OSI (7 capas)**	**Modelo TCP/IP (4 capas)**
Nº de capas	7	4
Desarrollo	Modelo teórico del ISO	Modelo práctico del Departamento de Defensa (DoD)
Uso actual	Referencia educativa y diagnóstica	Base real del funcionamiento de Internet
División de funciones	Muy detallada (capas separadas de sesión y presentación)	Más simplificada (agrupa funciones)
Nivel de abstracción	Alto – explicativo y preciso	Bajo – orientado a la implementación

Aspecto	Modelo OSI (7 capas)	Modelo TCP/IP (4 capas)
Protocolos reales	Menos directa	Alta – basado en protocolos reales (TCP/IP)
Facilidad para aprender	Más compleja pero ideal para enseñanza	Más sencilla y usada en la práctica



Comparando complejidad y aplicabilidad en redes.

Ejercicio 2

Pergamino	Descripción del Ritual	Protocolo Real
Mensajero Confiable	Realiza un saludo de tres pasos antes de enviar el mensaje, espera confirmación, y si no la recibe, reintenta el envío.	TCP (Transmission Control Protocol)

Pergamino	Descripción del Ritual	Protocolo Real
Mensajero Veloz	Envía mensajes continuamente sin confirmar si el receptor está listo o si recibió el mensaje. Prioriza velocidad sobre fiabilidad.	UDP (User Datagram Protocol)

Tabla de TCP

Aspecto	TCP – Mensajero Confiable
Tipo de conexión	Orientado a conexión (*Three-Way Handshake*)
Fiabilidad	Alta – garantiza entrega, orden y corrección de errores
Control de flujo	Sí
Control de congestión	Sí
Confirmación de recepción	Sí – cada segmento debe ser confirmado
Reenvío de datos perdidos	Sí – automático
Velocidad	Moderada – más lenta por control adicional
Orden de entrega	Asegurado
Uso común	HTTP/HTTPS, FTP, SMTP, correo electrónico, transferencia de archivos
Ventajas	- Entrega garantizada - Orden correcto - Corrección automática de errores
Desventajas	- Más lento - Mayor uso de recursos - Mayor complejidad

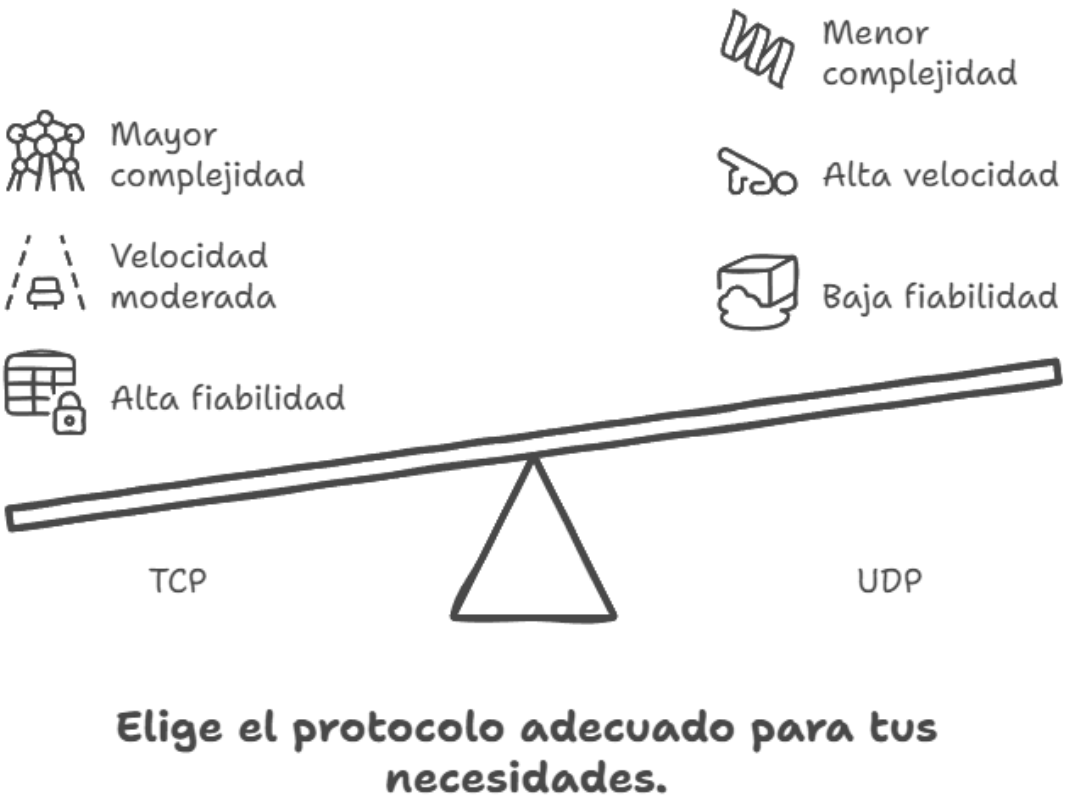
Tabla de UDP

Aspecto	**UDP – Mensajero Veloz**
Tipo de conexión	No orientado a conexión
Fiabilidad	Baja – no garantiza entrega ni orden
Control de flujo	No
Control de congestión	No
Confirmación de recepción	No – no espera confirmación del receptor
Reenvío de datos perdidos	No – no se reenvían datagramas perdidos
Velocidad	Alta – muy rápida, baja latencia
Orden de entrega	No garantizado
Uso común	Streaming, videollamadas, juegos online, DNS
Ventajas	- Muy rápido - Bajo consumo de recursos - Ideal para tiempo real
Desventajas	- Pérdida de datos posible - No garantiza orden - Sin control interno

Comparativa TCPvsUDP

Aspecto	**TCP**	**UDP**
Tipo de conexión	Orientado a conexión	No orientado a conexión
Fiabilidad	Alta – asegura entrega y orden	Baja – sin garantía de entrega ni orden
Control de flujo	Sí	No
Control de congestión	Sí	No
Velocidad	Moderada (por control y verificación)	Alta (mínima sobrecarga)
Reenvío automático	Sí	No

Aspecto	TCP	UDP
Confirmación de recepción	Sí	No
Orden de datos	Asegurado	No asegurado
Recursos y complejidad	Mayor uso de recursos y complejidad	Ligero y sencillo
Uso ideal	Web, correo, transferencia fiable de archivos	Streaming, juegos online, VoIP, DNS



Ejercicio 3

- Red base: 192.168.50.0
- Se necesita: dividir en 4 subredes de igual tamaño
- Es una dirección privada clase C (por defecto /24)

Sabemos que en una red clase C (/24 → 255.255.255.0) tenemos 256 direcciones posibles (2^8).

Para dividir en 4 subredes, necesitamos encontrar cuántos bits extra (de la parte de host) tomar prestados para crear subredes:

2^n ≥ 4 → n = 2 bits

La nueva máscara será:
/24 + 2 = /26 → **255.255.255.192**

En una subred /26, quedan 6 bits para hosts (porque 32 - 26 = 6):

2^6 = 64 direcciones por subred

- 2 reservadas (una para red, una para broadcast)

= 62 hosts utilizables por subred

Resultado final:

Elemento	**Valor**
Dirección base	192.168.50.0
Máscara utilizada	/26 → 255.255.255.192
Nº de subredes creadas	4 subredes
Direcciones por subred	64 (incluyendo red y broadcast)
Hosts utilizables por subred	62

Subredes resultantes:

Subred	**Rango de Hosts**	**Broadcast**
Subred 1	192.168.50.1 → 192.168.50.62	192.168.50.63
Subred 2	192.168.50.65 → 192.168.50.126	192.168.50.127
Subred 3	192.168.50.129 → 192.168.50.190	192.168.50.191
Subred 4	192.168.50.193 → 192.168.50.254	192.168.50.255

Para dividir la red 192.168.50.0/24 en 4 subredes de igual tamaño, los antiguos prestaron 2 bits

del campo de host, porque $2^2 = 4$ subredes. Esto cambió la máscara a /26 (255.255.255.192),

permitiendo 64 direcciones por subred. De esas, 62 son utilizables (se descartan la de red y

la de broadcast). Cada gremio recibe así una subred con su propio rango y aislamiento.

Ejercicio 4

Una tabla de enrutamiento es una base de datos interna de un router que contiene información sobre las rutas posibles hacia distintas redes. Cada entrada en la tabla indica:

- Red de destino (a qué lugar va el paquete)
- Máscara de subred (cuál es el tamaño del destino)
- Siguiente salto (la dirección del siguiente router)
- Interfaz de salida (por dónde sale el paquete)
- Métrica (prioridad o “coste” de la ruta)

Cuando un router recibe un paquete, consulta esta tabla para encontrar la mejor ruta disponible (usualmente la que tenga la métrica más baja o la coincidencia más específica) y lo reenvía por la interfaz correspondiente.

Como se puede interpretar del enunciado, las flechas talladas son el enrutamiento estático y las móviles, el enrutamiento dinámico.

Aquí tenemos una comparación entre estos dos:

Aspecto	**Enrutamiento Estático**	**Enrutamiento Dinámico**
Configuración	Manual – el administrador define las rutas	Automática – los routers intercambian información
Actualización	No cambia a menos que se modifique manualmente	Se adapta automáticamente a los cambios de la red

Aspecto	Enrutamiento Estático	Enrutamiento Dinámico
Recursos del sistema	Menor consumo (sin cálculos ni protocolos adicionales)	Mayor uso de CPU/RAM por protocolos de enrutamiento
Complejidad	Fácil en redes pequeñas	Ideal para redes grandes y dinámicas
Tolerancia a fallos	Baja – no se detectan caídas automáticamente	Alta – redirige el tráfico si una ruta falla
Ejemplos	Rutas fijas configuradas por el usuario	Protocolos como RIP, OSPF, EIGRP

Ambos se usan según el tamaño y la necesidad de flexibiliad de la red.

Ejercicio 5

La historia representa el mecanismo de NAT (Network Address Translation), específicamente el tipo NAT con Sobrecarga, también conocido como PAT (Port Address Translation).

¿Qué es NAT?

NAT es una técnica que permite que múltiples dispositivos dentro de una red privada accedan a Internet utilizando una única dirección IP pública. El router (el "guardián") actúa como intermediario:

- Cuando un dispositivo interno envía datos a Internet, el router reemplaza su IP privada con su propia IP pública (la máscara única).
- Además, asigna un número de puerto único para identificar a cada conexión.
- Cuando llega la respuesta desde el exterior, el router consulta su tabla NAT para saber a qué dispositivo interno reenviar la respuesta correctamente.

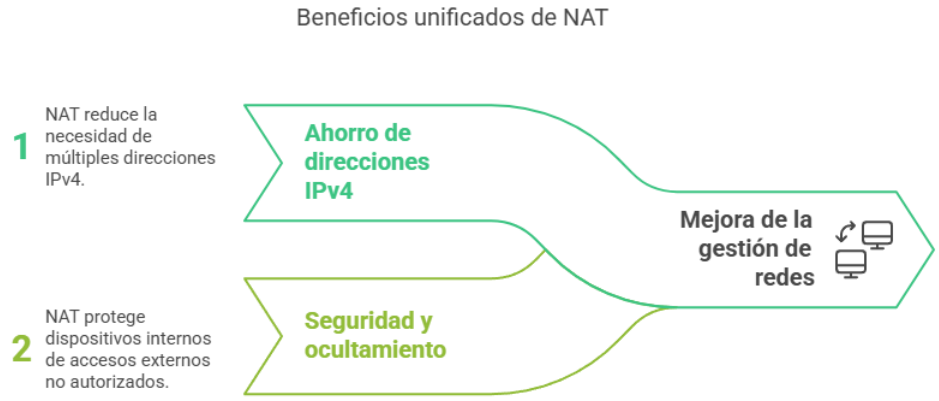
Ejemplo de como funciona:

Dispositivo Interno	**IP Privada**	**Puerto Interno**	**IP Pública del Router (NAT)**	**Puerto Asignado**
PC1	192.168.1.10	1234	203.0.113.5	40001
PC2	192.168.1.20	1234	203.0.113.5	40002

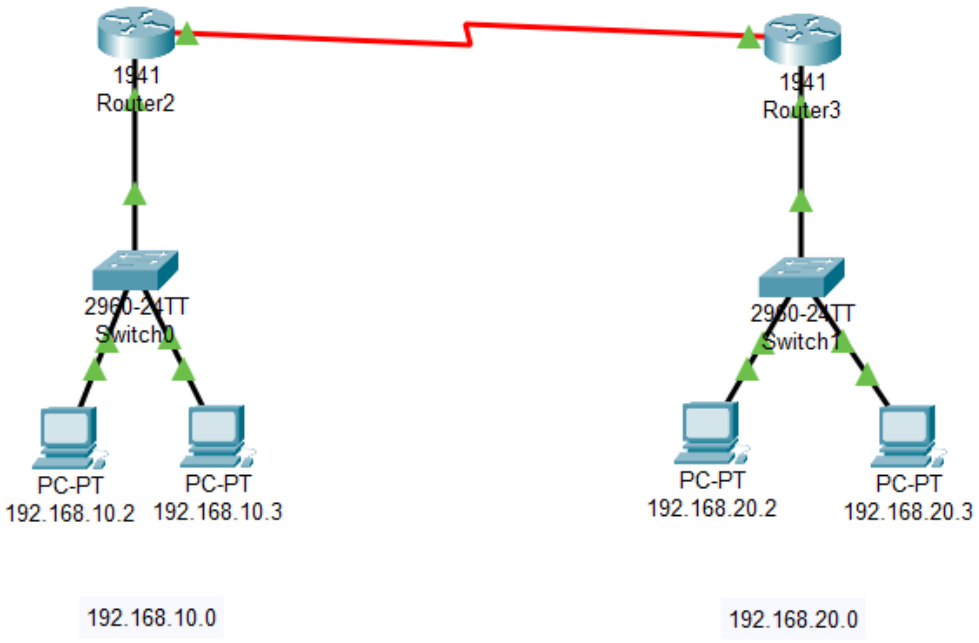
Beneficios de NAT para redes actuales

1. Ahorro de direcciones IPv4 públicas
   NAT permite que decenas o cientos de dispositivos privados compartan una sola IP pública, lo cual es fundamental ante la escasez de direcciones IPv4.

2. Seguridad y ocultamiento
   Los dispositivos internos no son visibles directamente desde el exterior, lo que aporta una capa extra de seguridad frente a accesos no autorizados.



Ejercicio 6



En esta práctica se ha simulado la interconexión directa entre dos redes locales independientes (Ciudad A y Ciudad B), mediante un enlace serial punto a punto entre dos routers Cisco 1941. El objetivo es permitir la comunicación entre ambas redes usando direccionamiento IP en diferentes subredes, configuración de rutas estáticas y encapsulación adecuada para el enlace WAN.

A diferencia de una versión anterior, en esta implementación no se ha utilizado una nube intermedia. La conexión entre los routers se ha establecido directamente mediante un cable serial, con encapsulación PPP y subred independiente en el enlace.

Dispositivos utilizados

- 2 Routers Cisco 1941 (Router2 y Router3)
- 2 Switches Cisco 2960
- 4 PCs (dos por red local)
- Cableado de cobre directo para LAN
- Cable serial DCE/DTE para conexión directa entre routers

Direccionamiento IP

Ciudad A (Red 192.168.10.0/24)

- Router2 (G0/0): 192.168.10.1
- PC0: 192.168.10.2
- PC1: 192.168.10.3
- Gateway en PCs: 192.168.10.1

Ciudad B (Red 192.168.20.0/24)

- Router3 (G0/0): 192.168.20.1
- PC2: 192.168.20.2
- PC3: 192.168.20.3
- Gateway en PCs: 192.168.20.1

Enlace WAN punto a punto (Red 192.168.30.0/30)

- Router2 (Serial0/1/0): 192.168.30.1

- Router3 (Serial0/1/0): 192.168.30.2

Configuración de los dispositivos

Router2

bash

CopiarEditar

```
hostname Router2
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown

interface Serial0/1/0
 ip address 192.168.30.1 255.255.255.252
 encapsulation ppp
 clock rate 64000
 no shutdown

ip route 192.168.20.0 255.255.255.0 192.168.30.2
```

Router3

bash

CopiarEditar

```
hostname Router3
interface GigabitEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 no shutdown

interface Serial0/1/0
 ip address 192.168.30.2 255.255.255.252
```

encapsulation ppp

no shutdown

ip route 192.168.10.0 255.255.255.0 192.168.30.1

El comando clock rate solo se aplica en el router que tiene el cable DCE (puede verificarse con show controllers serial 0/1/0).

Verificación de conectividad

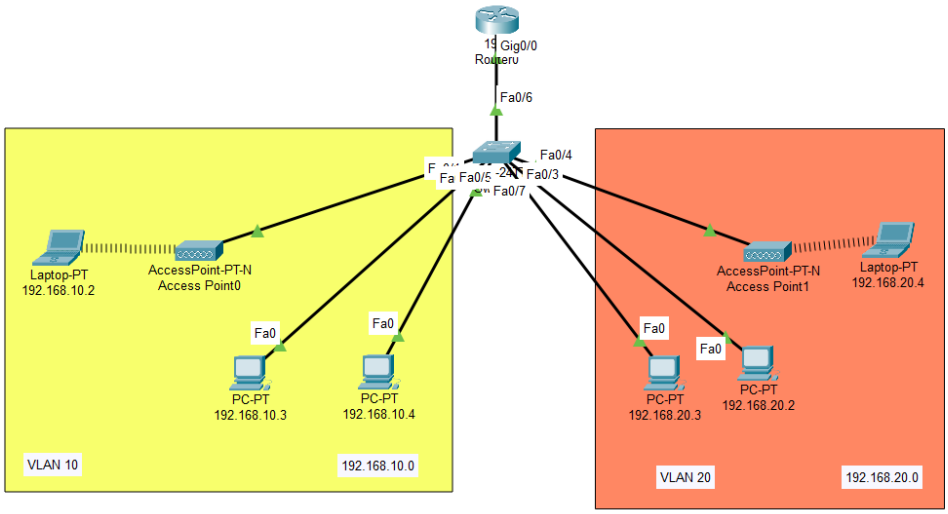
Se realizaron pruebas de conectividad mediante ping desde un PC de la red de Ciudad A a un PC de la red de Ciudad B. Las pruebas resultaron exitosas, confirmando que:

- Los routers están correctamente configurados con direcciones IP válidas.
- La encapsulación PPP está habilitada en ambos extremos.
- Las rutas estáticas permiten el reenvío de paquetes entre subredes.
- El enlace serial está operativo y el protocolo de capa 2 ha sido establecido correctamente.

Conclusión

Este ejercicio ha demostrado la implementación de una conexión directa entre dos routers usando enlaces seriales, con subred independiente y encapsulación PPP. La red resultante permite la comunicación entre dispositivos de diferentes redes LAN mediante enrutamiento estático, sin la necesidad de dispositivos intermedios como nubes o switches de capa 3. Esta topología representa un ejemplo funcional y eficiente de red punto a punto en entornos académicos o de laboratorio.

Ejercicio 6



En esta práctica se ha diseñado una red que simula la coexistencia de dos comunidades virtuales (VLAN 10 y VLAN 20) aisladas entre sí a nivel de capa 2, pero interconectadas mediante un router configurado como gateway utilizando la técnica **router-on-a-stick**. La solución permite mantener la segmentación lógica de la red al tiempo que se facilita la comunicación entre ambas VLANs.

Dispositivos utilizados

- 1 Router Cisco 1941 (Router0)
- 1 Switch Cisco 2960
- 2 Access Points inalámbricos
- 2 Laptops inalámbricas (una por VLAN)
- 4 PCs cableados (dos por VLAN)
- Cableado de cobre directo para conexiones cableadas
- Conectividad inalámbrica para los portátiles

Topología implementada

VLAN 10 – Subred 192.168.10.0/24 (zona amarilla)

- **Router0 (subinterfaz G0/0.10):** 192.168.10.1
- **PC1:** 192.168.10.3

- **PC2:** 192.168.10.4
- **Laptop1:** 192.168.10.2 (conectada vía Access Point0)
- **Gateway para todos los dispositivos:** 192.168.10.1

VLAN 20 – Subred 192.168.20.0/24 (zona roja)

- **Router0 (subinterfaz G0/0.20):** 192.168.20.1
- **PC3:** 192.168.20.2
- **PC4:** 192.168.20.3
- **Laptop2:** 192.168.20.4 (conectada vía Access Point1)
- **Gateway para todos los dispositivos:** 192.168.20.1

Verificación de conectividad

Se realizaron pruebas de ping entre equipos dentro de la misma VLAN (intra-VLAN), así como entre equipos de diferentes VLANs (inter-VLAN). Las pruebas resultaron exitosas, confirmando que:

- La segmentación lógica por VLAN se mantiene correctamente.
- La comunicación entre VLANs se logra mediante el router configurado con subinterfaces.

Conclusión

Esta práctica ha demostrado cómo aplicar el concepto de **router-on-a-stick** para permitir el enrutamiento entre VLANs en una red de capa 2. Se han aplicado técnicas de configuración de VLANs, subinterfaces, trunking y gateways predeterminados, permitiendo una topología escalable y segmentada, adecuada para redes corporativas o académicas con requerimientos de aislamiento lógico y conectividad controlada.