

## Laboratorio 5

Deivis J. Castro

### LABORATORIO: Entendiendo los Modelos OSI y TCP/IP

#### Paso 1: Diseño de la red en Packet Tracer

**1. Abrir Cisco Packet Tracer:** o Inicia Cisco Packet Tracer y selecciona un nuevo proyecto. Asegúrate de que el área de trabajo esté limpia para comenzar a diseñar la red.

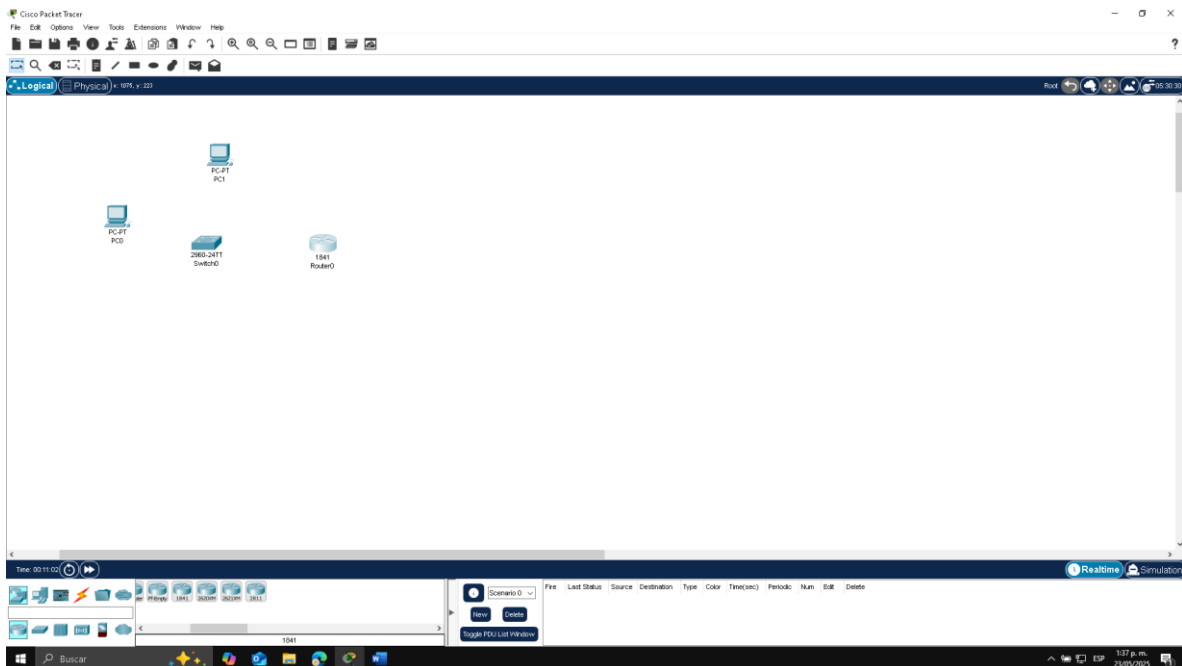
#### 2. Agregar dispositivos:

O En la parte inferior, selecciona los dispositivos necesarios desde la pestaña End Devices y Network Devices.

O Arrastra dos PCs desde la categoría de dispositivos finales (End Devices).

O Arrastra un Switch 2960 desde la categoría de switches.

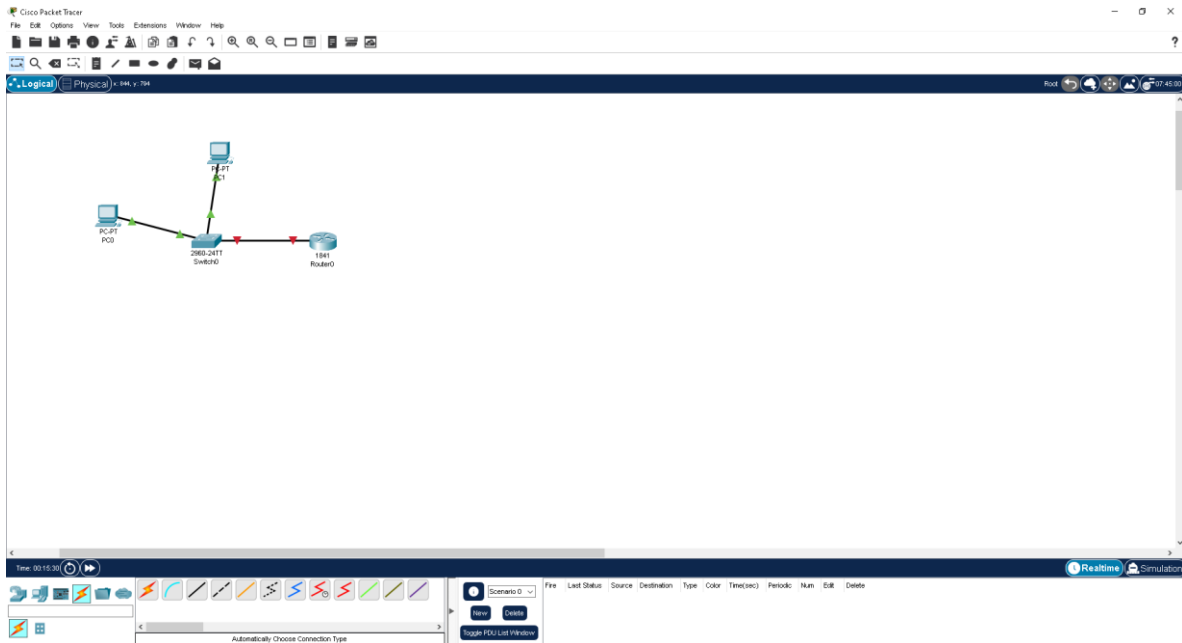
O Arrastra un Router 1841 desde la categoría de routers.



3. Conectar los dispositivos: o Haz clic en el ícono de conexión (que parece un rayo) y selecciona el tipo de cable **Copper Straight-Through**.

Conecta **PC1** al **Switch** y luego **PC2** al **Switch**.

Conecta el **Switch** al **Router** utilizando también el cable **Copper Straight-Through**.



#### 4. Verificar conexiones:

1. o Asegúrate de que las luces de los puertos en el Switch y Router estén encendidas (esto indica que los dispositivos están conectados correctamente).

### Paso 2: Configuración de direcciones IP

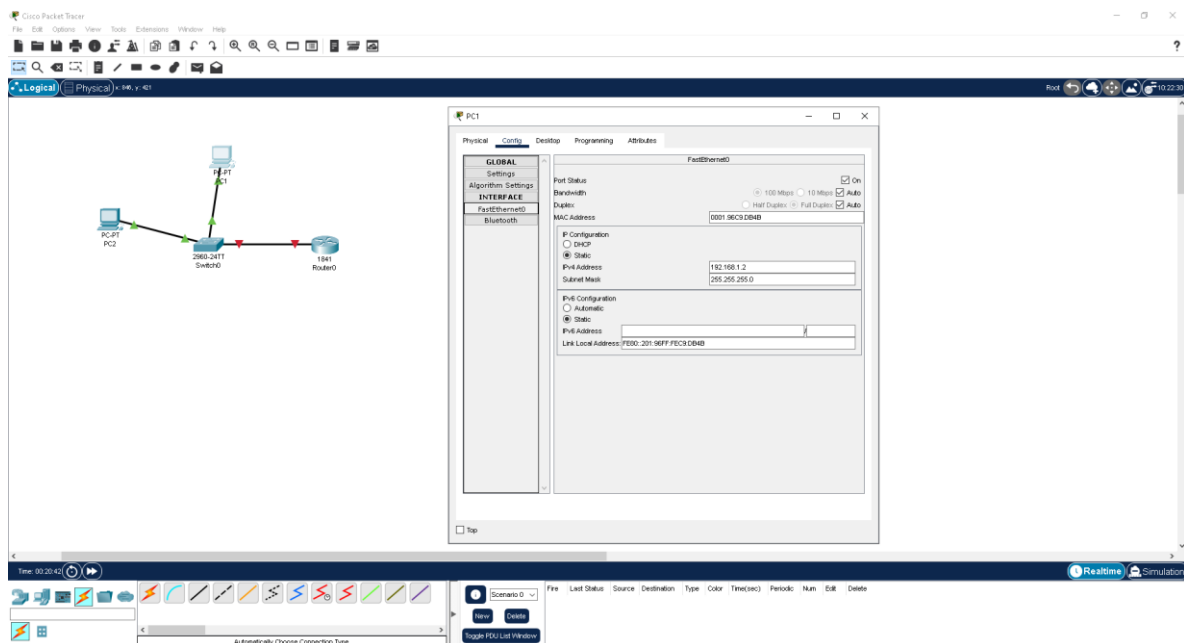
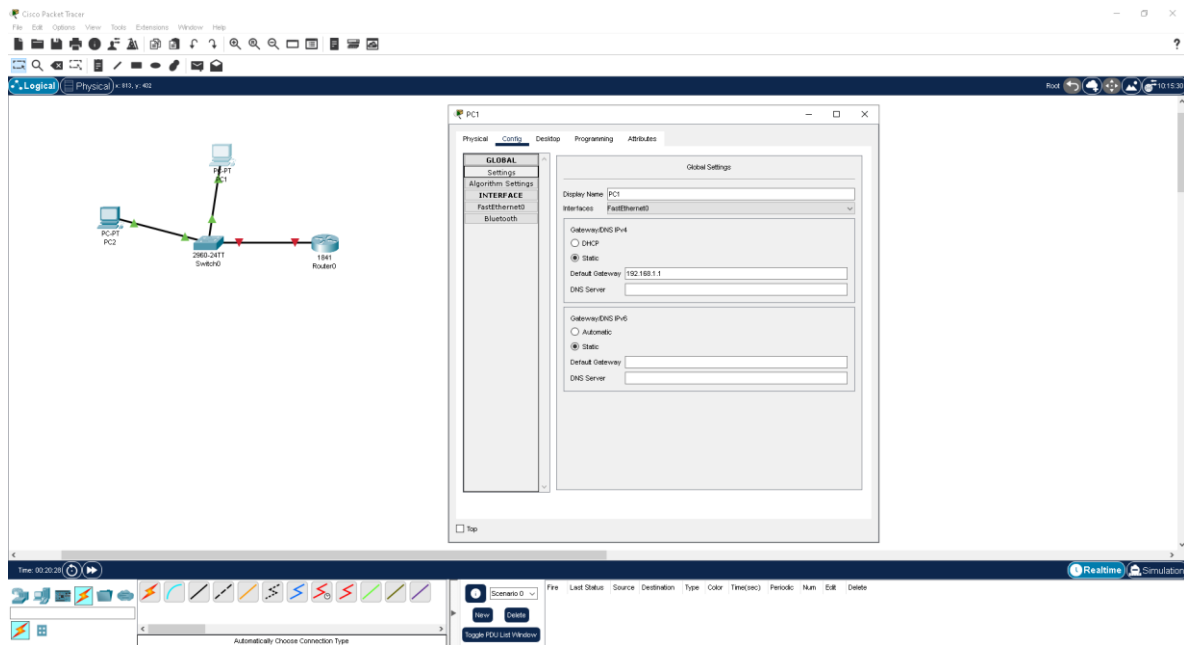
1. Configurar IP en PC1:

o Haz clic en **PC1** y selecciona la pestaña **Config**, luego elige **IP Configuration**.

o Asigna la siguiente dirección IP: ▪ Dirección IP: 192.168.1.2

Máscara de Subred: 255.255.255.0

- Gateway predeterminado: 192.168.1.1

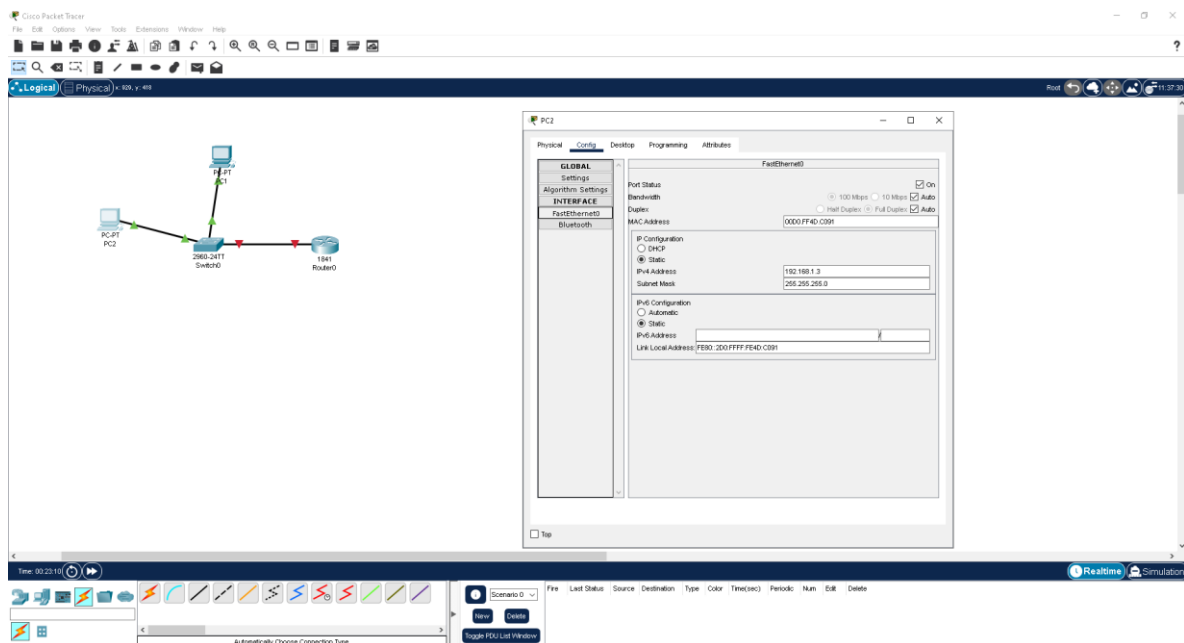
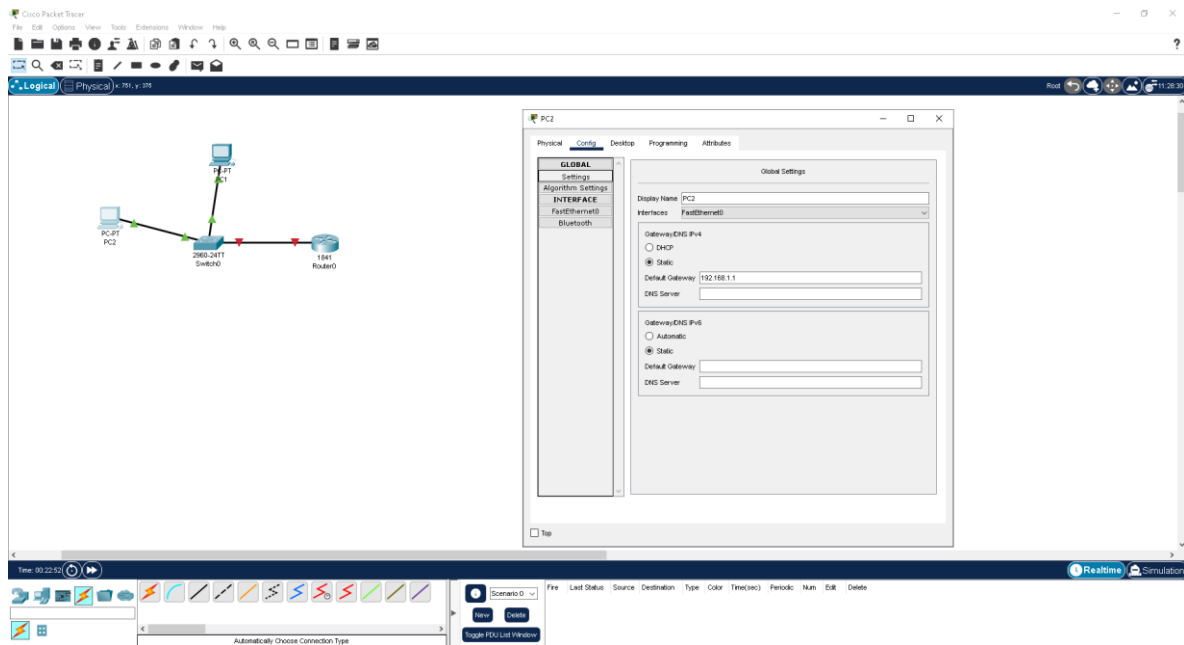


2. Configurar IP en PC2: o Repite los mismos pasos para **PC2**, asignando:

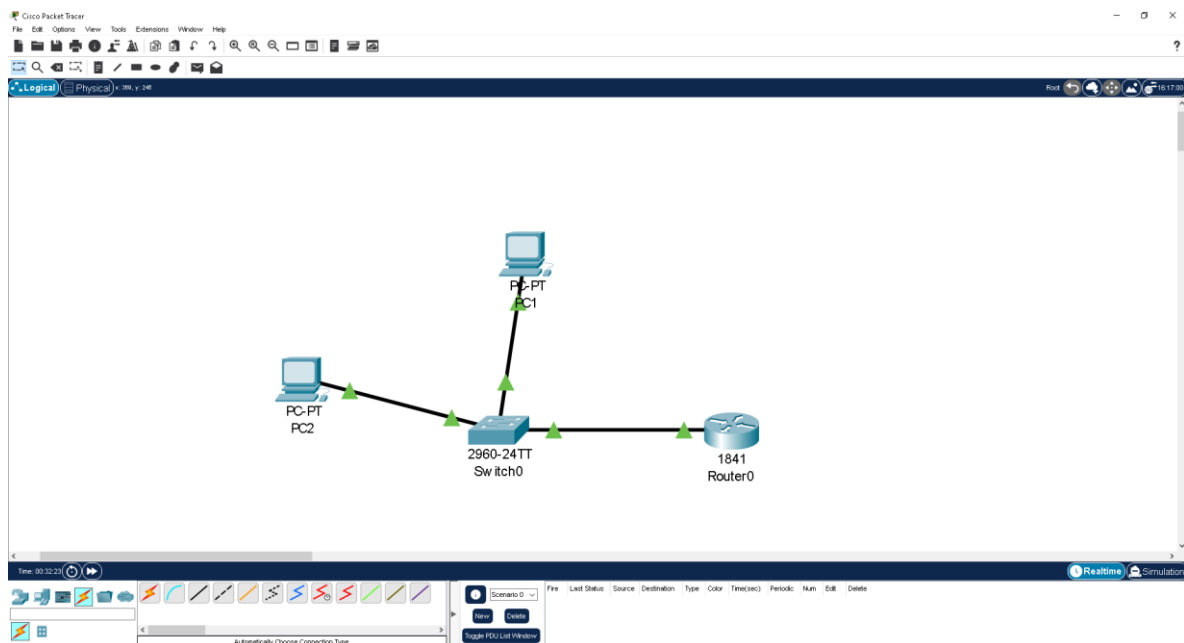
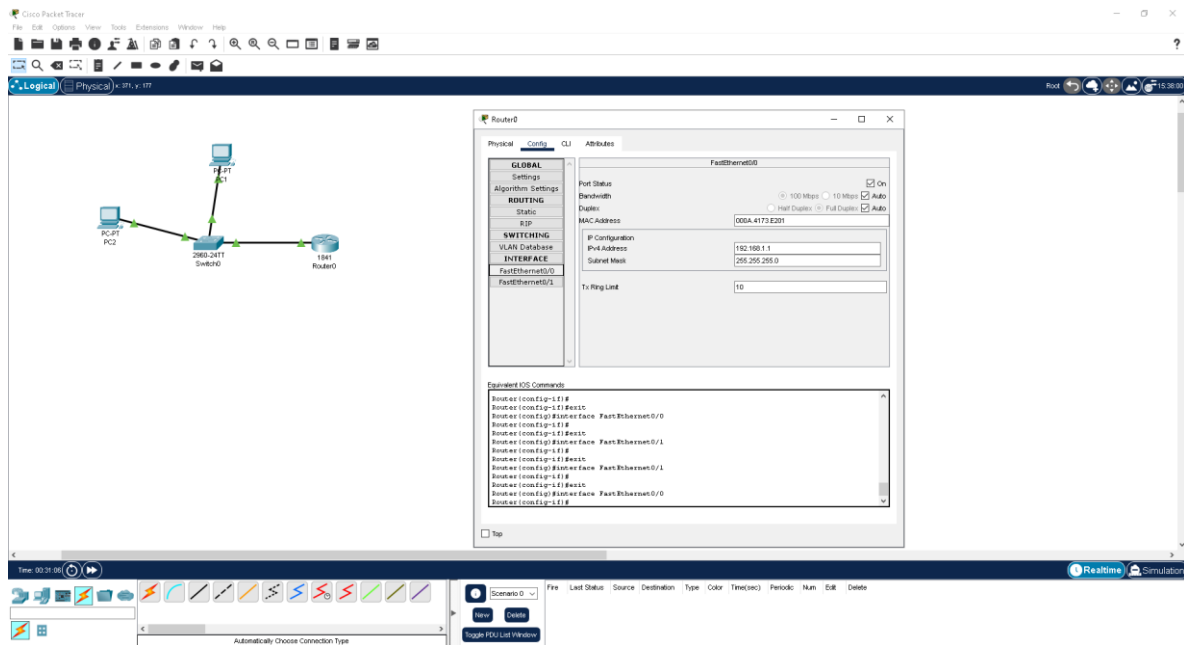
Dirección IP: 192.168.1.3

Máscara de Subred: 255.255.255.0

Gateway predeterminado: 192.168.1.1



3. Configurar IP en el Router: o Haz clic en el **Router**, selecciona la pestaña **Config**.
- o Selecciona la interfaz **GigabitEthernet0/0** y activa la interfaz marcando la opción **On**.
- o Asigna la siguiente IP a la interfaz G0/0:  
Dirección IP: 192.168.1.1  
Máscara de Subred: 255.255.255.0
- o Haz clic en **Save** o simplemente cierra la ventana del Router para aplicar los cambios.



### Paso 3: Verificación de conectividad

1. **Realizar pruebas de conectividad con ping:** o En PC1, abre la terminal seleccionando la pestaña **Desktop** y luego **Command Prompt**.

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical 180 v.30

PC1

PC-PT PC2

2960-24TT Switch0

1841 Router0

PC1 Configuration:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection (default port)
    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: FE80::201:94FF:FECD:D84B
    IPv4 Address. . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: 192.168.1.1

Bluetooth Connection:
    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: 
    IPv6 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: 0.0.0.0

C:\>ipconfig/all
Invalid Command.

C:\>ipconfig /all

FastEthernet0 Connection (default port)
    Connection-specific DNS Suffix...: 
    Physical Address. . . . .: 0001.96C9.3D4B
    Link-local IPv6 Address . . . . .: FE80::201:94FF:FECD:D84B
    IPv4 Address. . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: 192.168.1.1
```

Time 00:30:32

RealTime Simulation

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical 180 v.30

PC1

PC-PT PC2

2960-24TT Switch0

1841 Router0

PC1 Configuration:

```
C:\>ipconfig /all

FastEthernet0 Connection (default port)
    Connection-specific DNS Suffix...: 
    Physical Address. . . . .: 0001.96C9.3D4B
    Link-local IPv6 Address . . . . .: FE80::201:94FF:FECD:D84B
    IPv4 Address. . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: 192.168.1.1

DHCP Server . . . . .: 0.0.0.0
DHCPv6 Server . . . . .: 0.0.0.0
DHCPv6 Client DUID . . . . .: 00-01-00-01-0C-7D-9D-66-08-01-96-C9-18-4B
DHCP Server . . . . .: 0.0.0.0

Bluetooth Connection:
    Connection-specific DNS Suffix...: 
    Physical Address. . . . .: 000D.70A2.8BAA
    Link-local IPv6 Address . . . . .: 

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

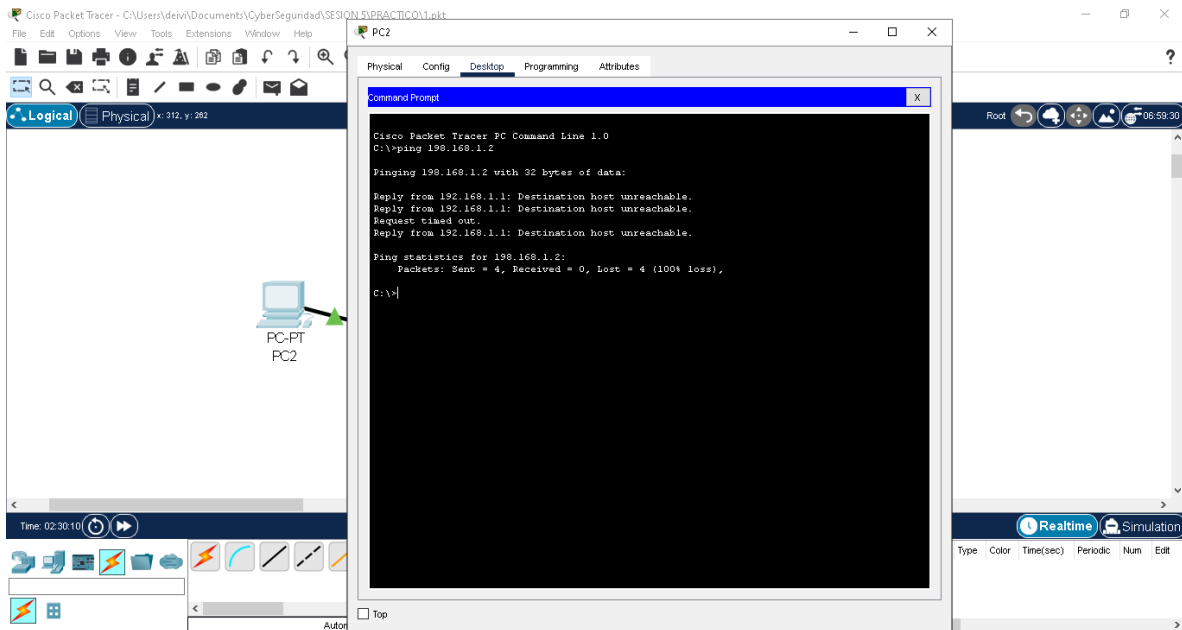
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Time 00:37:36

RealTime Simulation

## VERIFICAR CONECTIVAD DEL PC2 AL PC1



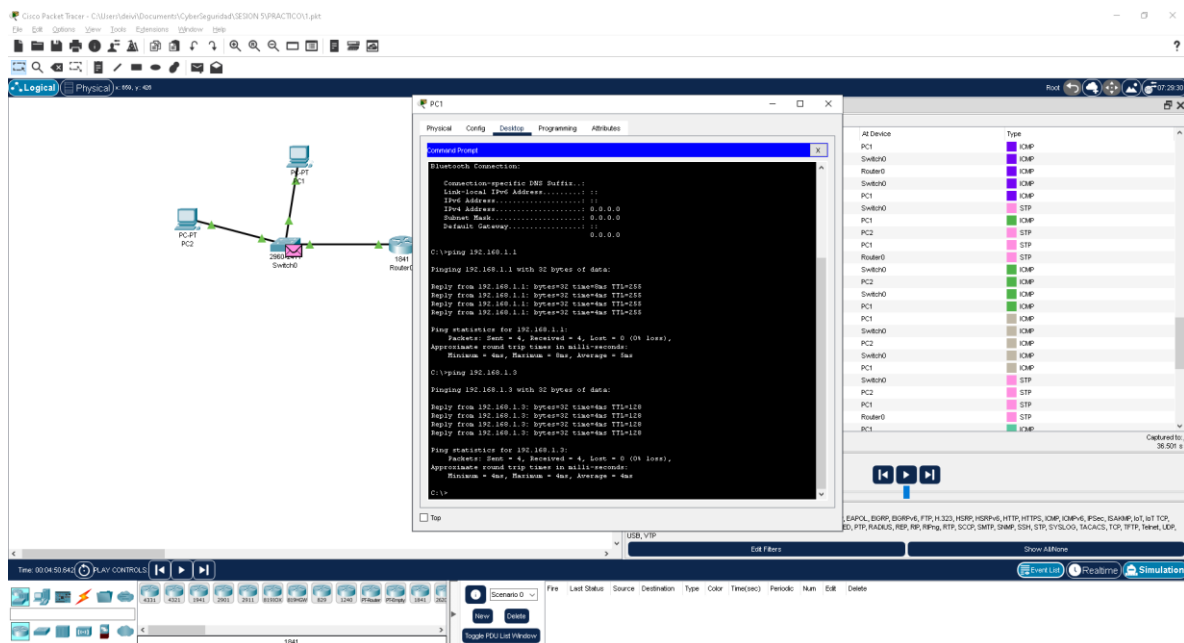
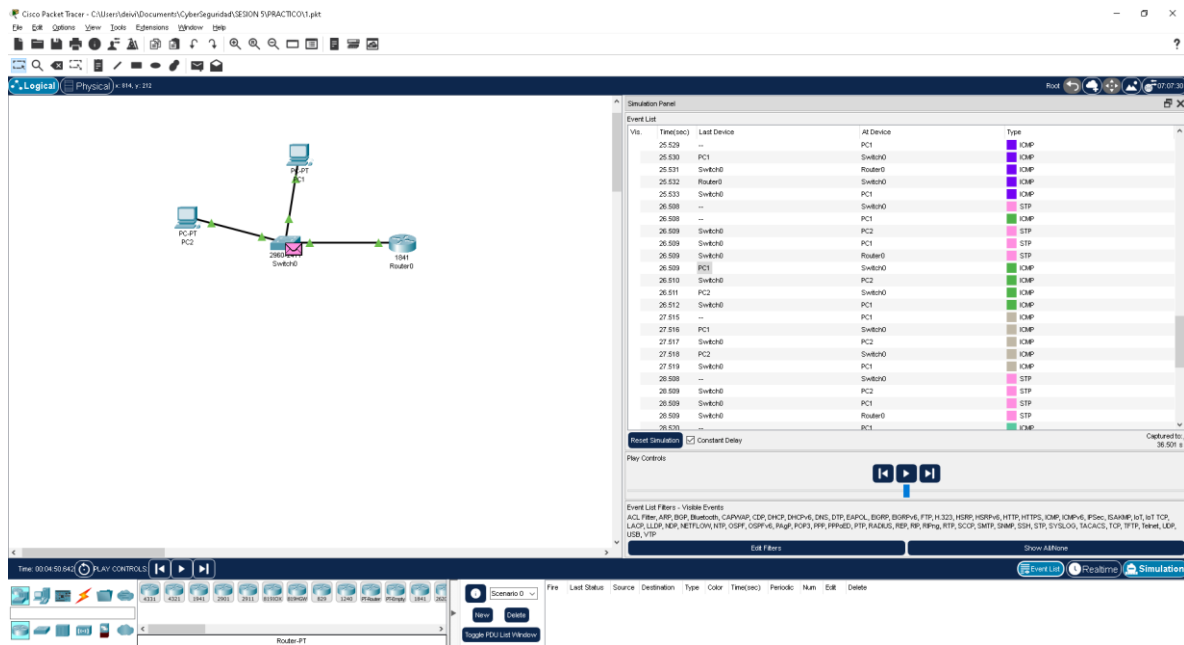
### Paso 4: Uso del modo de simulación para analizar el tráfico

#### 1. Activar el modo de simulación:

- o En la esquina inferior derecha de Packet Tracer, selecciona el modo **Simulación**.
- o Esto permitirá ver cómo los paquetes viajan por la red paso a paso.

#### 2. Generar tráfico con ping:

- o Desde **PC1**, ejecuta de nuevo el comando ping 192.168.1.3 para enviar paquetes ICMP a **PC2**.
- o Packet Tracer comenzará a capturar el tráfico entre los dispositivos.



### 3. Observar el flujo de paquetes:

o Paso a paso, puedes observar cómo los paquetes viajan desde **PC1** a **PC2** a través del Switch y el Router.

o Haz clic en el botón **Capture/Forward** para ver cómo los paquetes se mueven por la red.

o En cada paso, podrás ver cómo los datos se encapsulan y desencapsulan a medida que atraviesan las capas del modelo OSI.



Cisco Packet Tracer - C:\Users\deva\Documents\CyberSecurity\SESSION 5\PRAC\TC01.pkt  
 File Edit Options View Tools Extensions Window Help

Logical Physical 1941 v. 10

**PDU Information at Device: Switch0**  
**INSTRUMENT** Inbound PDU Details Outbound PDU Details

At Device: Switch0  
 Source: PC1  
 Destination: 192.168.1.3

**In Layers**  
 Layer 7  
 Layer 6  
 Layer 5  
 Layer 4  
 Layer 3  
 Layer 2: Ethernet II Header  
 0001.80C9.DB4B >> 000C.FF4D.C091  
**Layer 1: Port FastEthernet0/2**

**Out Layers**  
 Layer 7  
 Layer 6  
 Layer 5  
 Layer 4  
 Layer 3  
 Layer 2: Ethernet II Header  
 0001.80C9.DB4B >> 000C.FF4D.C091  
**Layer 1: Port(G): FastEthernet0/2**

1. FastEthernet0/2 receives the frame.

Challenge Me << Previous Layer Next Layer >>

Event List  
 Vis Time(sec) Last Device  
 25.529 -

At Device	Type
PC1	ICMP
Switch0	ICMP
Router0	ICMP
Switch0	ICMP
PC1	ICMP
Switch0	STP
PC1	ICMP
PC2	STP
PC1	STP
Router0	STP
Switch0	ICMP
PC2	ICMP
Switch0	STP
PC1	ICMP
Switch0	STP
PC2	STP
PC1	STP
Router0	STP
PC1	STP

Captured to: 36.901 s

Time: 00:04:59.640 PLAY CONTROLS

Scenario 0 v. 1  
 New Delete  
 Apply PDU List Filter

File Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

Cisco Packet Tracer - C:\Users\deva\Documents\CyberSecurity\SESSION 5\PRAC\TC01.pkt  
 File Edit Options View Tools Extensions Window Help

Logical Physical 1941 v. 48

**PDU Information at Device: Switch0**  
**INSTRUMENT** Inbound PDU Details Outbound PDU Details

At Device: Switch0  
 Source: PC1  
 Destination: 192.168.1.1

**In Layers**  
 Layer 7  
 Layer 6  
 Layer 5  
 Layer 4  
 Layer 3  
 Layer 2: Ethernet II Header 000A.4173.E201 >> 0001.96C9.DB4B  
**Layer 1: Port FastEthernet0/3**

**Out Layers**  
 Layer 7  
 Layer 6  
 Layer 5  
 Layer 4  
 Layer 3  
 Layer 2: Ethernet II Header 000A.4173.E201 >> 0001.96C9.DB4B  
**Layer 1: Port(G): FastEthernet0/3**

1. FastEthernet0/3 receives the frame.

Challenge Me << Previous Layer Next Layer >>

Event List  
 Vis Time(sec) Last Device  
 24.598 Switch0

At Device	Type
PC1	STP
Router0	STP
PC1	ICMP
Switch0	ICMP
Router0	ICMP
Switch0	ICMP
PC1	ICMP
PC1	ICMP
Switch0	STP
PC1	ICMP
Switch0	ICMP
PC2	STP
PC1	STP
Router0	STP
Switch0	ICMP
PC2	ICMP
Switch0	ICMP
PC1	ICMP
Switch0	ICMP
PC2	ICMP

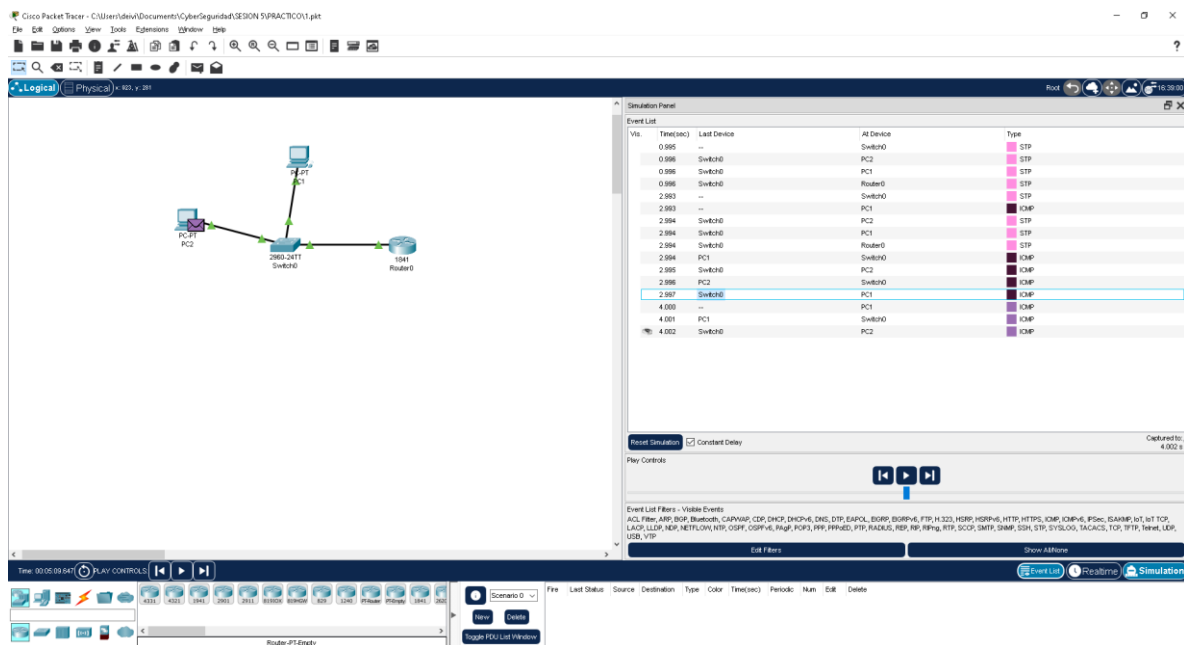
Captured to: 41.512 s

Time: 00:04:55.650 PLAY CONTROLS

Scenario 0 v. 1  
 New Delete  
 Apply PDU List Filter

File Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete





## Paso 5: Análisis del tráfico en el modelo OSI

1. Inspección de paquetes: o Haz clic en uno de los paquetes que aparece en la simulación para abrir la ventana de análisis del paquete.

o Packet Tracer mostrará la información de las diferentes capas del paquete, desde la capa física hasta la capa de aplicación.

o Observa cómo el paquete ICMP se encapsula con la dirección MAC en la capa 2, la dirección IP en la capa 3, y cómo viaja por la red.

2. Relación con el modelo OSI: o A medida que los paquetes avanzan, podrás identificar cómo se procesan en cada capa del modelo OSI: ▪ **Capa 1 (Física):** Los datos se transmiten a través de los cables.

- **Capa 2 (Enlace de Datos):** El Switch utiliza las direcciones MAC para reenviar el paquete.
- **Capa 3 (Red):** El Router utiliza direcciones IP para dirigir los paquetes.
- **Capa 4 (Transporte):** El protocolo ICMP es manejado a nivel de transporte, enviando paquetes de control.
- **Capas 5-7:** Las capas superiores se encargan de la sesión y presentación de la información, aunque en el caso de ping, no se usa aplicación específica aparte del protocolo ICMP.

3. Completar la tabla de análisis: o Completa la siguiente tabla basándote en los resultados del análisis de los paquetes capturados:

No. de Paquete	Protocolo	Capa OSI	Fuente IP	Destino IP	Descripción
1	ICMP	3 RED	192.168.1.2	192.168.1.3	Ping de PC1 a PC2
2	ARP	2 (Enlace de Datos)	192.168.1.2	DEST ADDR:00D0.FF4D.C091	Resolución de IP a MAC


### Paso 6: Comparación entre OSI y TCP/IP

1. Identificación de capas en el modelo TCP/IP:

o Al analizar los paquetes ICMP, observa cómo las capas del modelo TCP/IP también están presentes.

o La capa de transporte en TCP/IP (en este caso, ICMP) corresponde a las capas 3 y 4 del modelo OSI.

Modelo OSI	Modelo TCP/IP	Análisis para ICMP
<b>7. Aplicación</b>	<b>4. Aplicación</b>	<i>ICMP no es un protocolo de aplicación (no transporta datos de usuario).</i>
<b>6. Presentación</b>		<i>No aplica.</i>
<b>5. Sesión</b>		<i>No aplica.</i>
<b>4. Transporte</b>	<b>3. Transporte</b>	<i>ICMP no usa TCP/UDP (opera directamente sobre IP).</i>
<b>3. Red</b>	<b>2. Internet</b>	<input checked="" type="checkbox"/> <b>ICMP pertenece aquí</b> (se encapsula en paquetes IP, sin puertos).
<b>2. Enlace</b>	<b>1. Acceso a Red</b>	<input checked="" type="checkbox"/> <b>Ethernet/Frame (MAC)</b> encapsula el paquete IP que lleva ICMP.

<b>1. Física</b>		 <b>Bits</b> (transmisión eléctrica/óptica del frame).
------------------	--	---

2. Completar la tabla de comparación: o Completa la siguiente tabla con las capas equivalentes entre los modelos OSI y TCP/IP:

<b>Modelo OSI</b>	<b>Función Principal</b>	<b>Modelo TCP/IP</b>	<b>Protocolos Comunes</b>
<b>7. Aplicación</b>	Interfaces de usuario, servicios de red	<b>4. Aplicación</b>	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP, SNMP, Telnet, SSH
<b>6. Presentación</b>	Traducción de datos, cifrado, compresión	<i>(Incluida en Aplicación)</i>	TLS/SSL, JPEG, MPEG, ASCII, EBCDIC, GIF
<b>5. Sesión</b>	Control de sesiones, establecimiento y terminación	<i>(Incluida en Aplicación)</i>	RPC, NetBIOS, PPTP
<b>4. Transporte</b>	Comunicación extremo a extremo, control de flujo y errores	<b>3. Transporte</b>	TCP, UDP
<b>3. Red</b>	Enrutamiento de datos entre dispositivos y redes	<b>2. Internet</b>	IP, ICMP, IGMP, ARP, RARP, Ipsec
<b>2. Enlace de datos</b>	Control de acceso al medio, detección de errores	<b>1. Acceso a la red</b>	Ethernet, Wi-Fi (IEEE 802.11), PPP, Frame Relay, ATM, HDLC
<b>1. Física</b>	Transmisión de bits a través del medio físico	<i>(Incluida en Acceso a red)</i>	RJ-45, cables UTP/STP, fibra óptica, RS-232, DSL, módems, señales eléctricas/ópticas

## Actividad Complementaria

### Laboratorio Práctico: Entendiendo los Modelos OSI y TCP/IP

#### 1. Investigación teórica:

o Realiza una breve investigación sobre las 7 capas del Modelo OSI y completa la siguiente tabla, describiendo la función principal de cada capa y ejemplos de dispositivos y protocolos utilizados en ellas.

Capa	Nombre de la Capa	Función Principal	Protocolos / Dispositivos
7	Aplicación	Provee servicios de red directamente al usuario o aplicación.	Protocolos: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP Dispositivos: PC, servidor web
6	Presentación	Traduce, cifra o comprime los datos para la capa de aplicación.	Protocolos: TLS/SSL, JPEG, GIF, MPEG, ASCII, EBCDIC Dispositivos: PC, servidor de medios
5	Sesión	Establece, mantiene y termina sesiones entre aplicaciones.	Protocolos: NetBIOS, RPC, PPTP Dispositivos: Gateway, servidor de aplicaciones
4	Transporte	Controla el flujo de datos, asegura entrega y maneja errores extremos a extremo.	Protocolos: TCP, UDP Dispositivos: Gateway, firewall, balanceadores de carga
3	Red	Determina la ruta de los datos, direccionamiento lógico y enrutamiento.	Protocolos: IP, ICMP, IGMP, IPsec, ARP Dispositivos: Router
2	Enlace de Datos	Proporciona transmisión libre de errores entre nodos conectados directamente.	Protocolos: Ethernet, Wi-Fi (IEEE 802.11), PPP, Frame Relay Dispositivos: Switch, bridge
1	Física	Transmite bits a través del medio físico (señales eléctricas, ópticas o de radio).	Protocolos: RS-232, DSL, IEEE 802.3 Dispositivos: Cable UTP, módem, hub, tarjetas NIC

## 2. Asociación de capas con dispositivos:

o Con base en la infraestructura de la red a la que están conectadas las computadoras (incluyendo routers, switches y computadoras), asocia cada dispositivo con la capa del Modelo OSI que mejor se corresponda con su función principal.

Dispositivo	Capa del Modelo OSI	Justificación / Función Principal
Computadora	Capa 7 – Aplicación	Ejecuta aplicaciones de red e interactúa directamente con el usuario.
Servidor	Capa 7 – Aplicación	Proporciona servicios de red (web, correo, DNS, etc.).
Router	Capa 3 – Red	Enruta paquetes entre redes diferentes usando direcciones IP.
Switch (gestionado)	Capa 2 – Enlace de Datos	Envía tramas entre dispositivos dentro de la misma red local usando direcciones MAC.
Switch (capa 3)	Capa 3 – Red	Realiza funciones de encaminamiento además de las de un switch tradicional.
Hub	Capa 1 – Física	Repite señales eléctricas sin procesar información, transmite bits.
Tarjeta de red (NIC)	Capas 1 y 2 – Física / Enlace	Se encarga de la conexión física y direccionamiento MAC para la comunicación local.
Firewall	Capa 3/4 – Red / Transporte	Filtra tráfico basado en IP (capa 3) y puertos/protocolos como TCP/UDP (capa 4).
Punto de acceso (Wi-Fi)	Capa 2 – Enlace de Datos	Gestiona la comunicación inalámbrica dentro de una red local.
Módem	Capa 1 – Física	Modula y demodula señales para permitir la transmisión de datos sobre medios como líneas telefónicas o coaxiales.

## 1. Simulación y captura de tráfico:

o Abre **Wireshark** en tu computadora y selecciona la interfaz de red activa.





### Parte 3: Comparación entre OSI y TCP/IP

#### 1. Investigación teórica:

o Investiga el modelo **TCP/IP** y compáralo con el modelo OSI. Completa la siguiente tabla mostrando las capas equivalentes en ambos modelos y algunos ejemplos de protocolos o servicios en cada una.

Modelo OSI	Función Principal	Modelo TCP/IP	Protocolos Comunes
<b>7. Aplicación</b>	Interfaces de usuario, servicios de red	<b>4. Aplicación</b>	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP, SNMP, Telnet, SSH
<b>6. Presentación</b>	Traducción de datos, cifrado, compresión	<i>(Incluida en Aplicación)</i>	TLS/SSL, JPEG, MPEG, ASCII, EBCDIC, GIF
<b>5. Sesión</b>	Control de sesiones, establecimiento y terminación	<i>(Incluida en Aplicación)</i>	RPC, NetBIOS, PPTP
<b>4. Transporte</b>	Comunicación extremo a extremo, control de flujo y errores	<b>3. Transporte</b>	TCP, UDP
<b>3. Red</b>	Enrutamiento de datos entre dispositivos y redes	<b>2. Internet</b>	IP, ICMP, IGMP, ARP, RARP, Ipsec
<b>2. Enlace de datos</b>	Control de acceso al medio, detección de errores	<b>1. Acceso a la red</b>	Ethernet, Wi-Fi (IEEE 802.11), PPP, Frame Relay, ATM, HDLC
<b>1. Física</b>	Transmisión de bits a través del medio físico	<i>(Incluida en Acceso a red)</i>	RJ-45, cables UTP/STP, fibra óptica, RS-232, DSL, módems, señales eléctricas/ópticas

#### Análisis práctico:

o Analiza los paquetes capturados en la **Parte 2** e indica cómo las capas del modelo TCP/IP se corresponden con las capas del modelo OSI.

- ¿Qué capa del modelo OSI se encarga de la entrega confiable de datos

#### Capa 4 – Transporte

Esta capa garantiza la entrega confiable de datos entre dispositivos extremos de la red.

Utiliza protocolos como TCP (Transmission Control Protocol), que asegura que los datos lleguen completos, en orden y sin errores mediante el uso de confirmaciones (ACK) y retransmisiones si es necesario.

o ¿Qué dispositivos de red operan en la capa 2 del modelo OSI

#### Capa 2 – Enlace de Datos

Dispositivos que operan en esta capa:

Switches (no gestionados o de capa 2): Redirigen tramas de datos basadas en direcciones MAC.

Bridges (puentes): Conectan segmentos de red y filtran tráfico por direcciones MAC.

Tarjetas de red (NIC): Funcionan parcialmente en capa 2 para el direccionamiento de tramas.

#### o ¿Cómo puedes identificar la capa de transporte (capa 4) al analizar un paquete capturado en Wireshark?

En **Wireshark**, puedes identificar la capa de transporte observando:

- El **protocolo** usado: busca **TCP** o **UDP** en la columna “Protocol”.
- El **número de puerto**: cada segmento tendrá un puerto de origen y destino (por ejemplo, puerto 80 para HTTP, 443 para HTTPS, 53 para DNS).
- Los **campos del encabezado** de capa 4, como:
  - Número de puerto de origen/destino.
  - Número de secuencia y confirmación (en TCP).
  - Indicadores de control (SYN, ACK, FIN en TCP).

o ¿Cuáles son las diferencias clave entre los modelos OSI y TCP/IP

<b>Aspecto</b>	<b>Modelo OSI</b>	<b>Modelo TCP/IP</b>
<b>Número de capas</b>	7 capas	4 capas
<b>Estructura</b>	Conceptual y detallada	Práctico y orientado a implementación
<b>Separación de funciones</b>	Cada capa tiene funciones específicas bien definidas	Algunas capas combinan varias funciones
<b>Uso real</b>	Modelo de referencia	Arquitectura usada en Internet
<b>Desarrollo</b>	Por ISO (Organización Internacional de Normalización)	Por el Departamento de Defensa de EE.UU.
<b>Capa de sesión y presentación</b>	Existen de forma independiente	Están integradas en la capa de aplicación