

Laboratorio 5

Sesión #5 Modelos OSI y TCP/IP

Título del Laboratorio: Entendiendo los Modelos OSI y TCP/IP

Duración: 2 hora

Objetivos del Laboratorio:

1. Comprender y aplicar los principios de los modelos OSI y TCP/IP mediante la configuración y análisis de una red simulada en Cisco Packet Tracer.
2. Identificar y analizar el flujo de datos a través de las capas del modelo OSI y TCP/IP, utilizando herramientas de simulación de red y captura de paquetes como Wireshark dentro de Packet Tracer.
3. Demostrar la relación entre los dispositivos de red y los protocolos en diferentes capas de los modelos OSI y TCP/IP, correlacionando la teoría con la simulación práctica.

Materiales Necesarios:

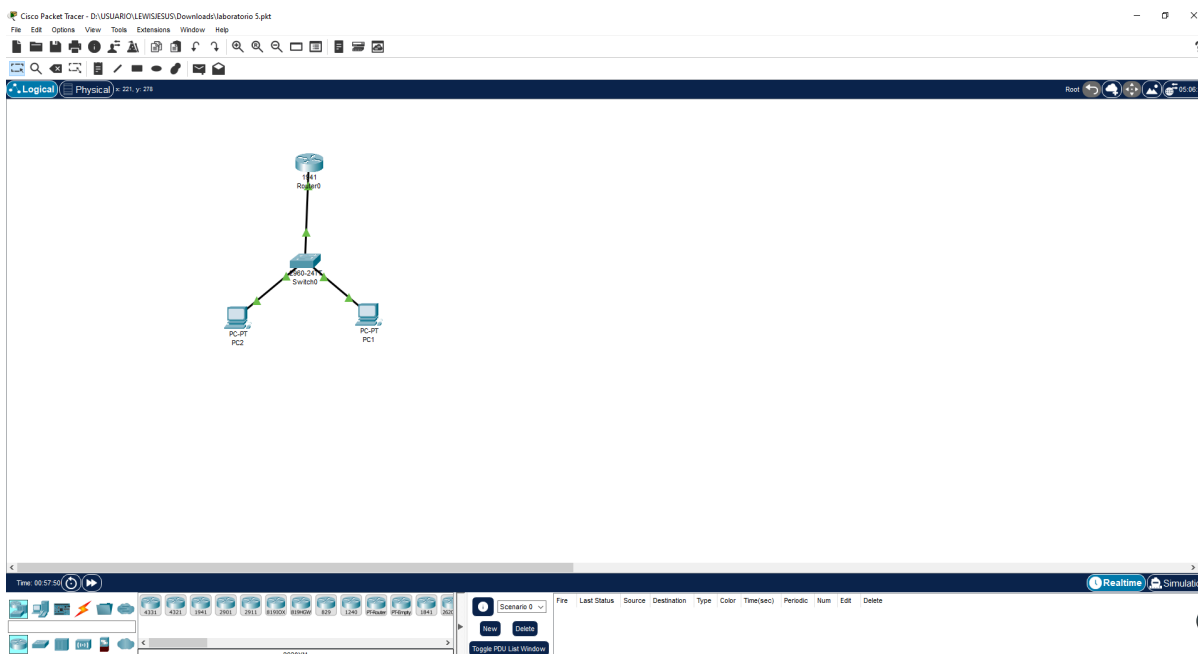
1. Utilizar GitHub como repositorio
2. Utilizar Academia Cisco
3. Computador
4. Acceso a internet

Estructura del Laboratorio:

El objetivo de este laboratorio es comprender el funcionamiento de las capas del Modelo OSI y el Modelo TCP/IP mediante la simulación de una red en Cisco Packet Tracer. Los estudiantes configurarán una red simple, observarán el tráfico que fluye entre los dispositivos y analizarán cómo los protocolos y dispositivos operan en diferentes capas.

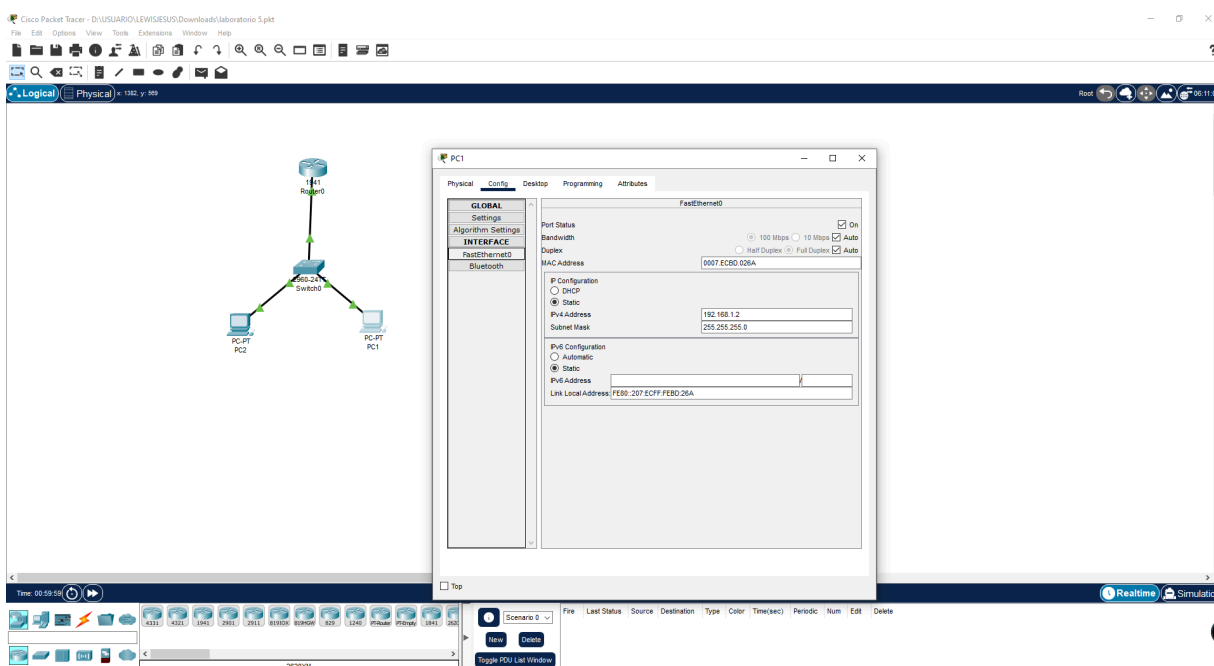
1. Parte 1: Configuración Básica de la Red en Packet Tracer

1.1. Diseño de la red:

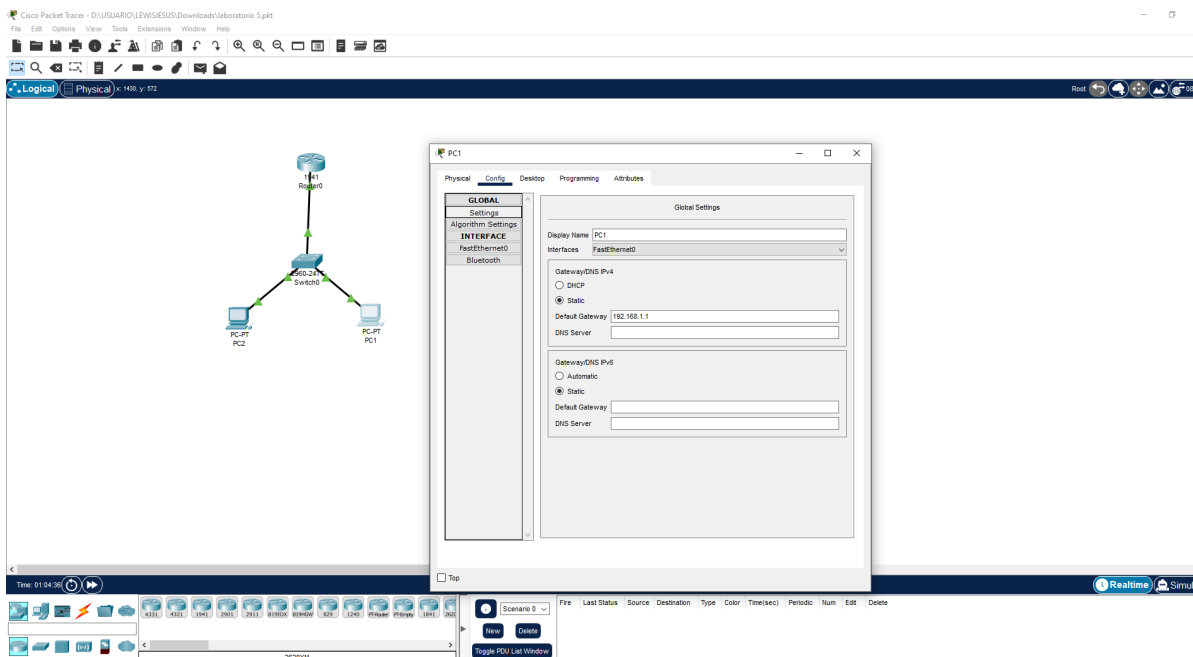


1.2. Configuración de las IPs:

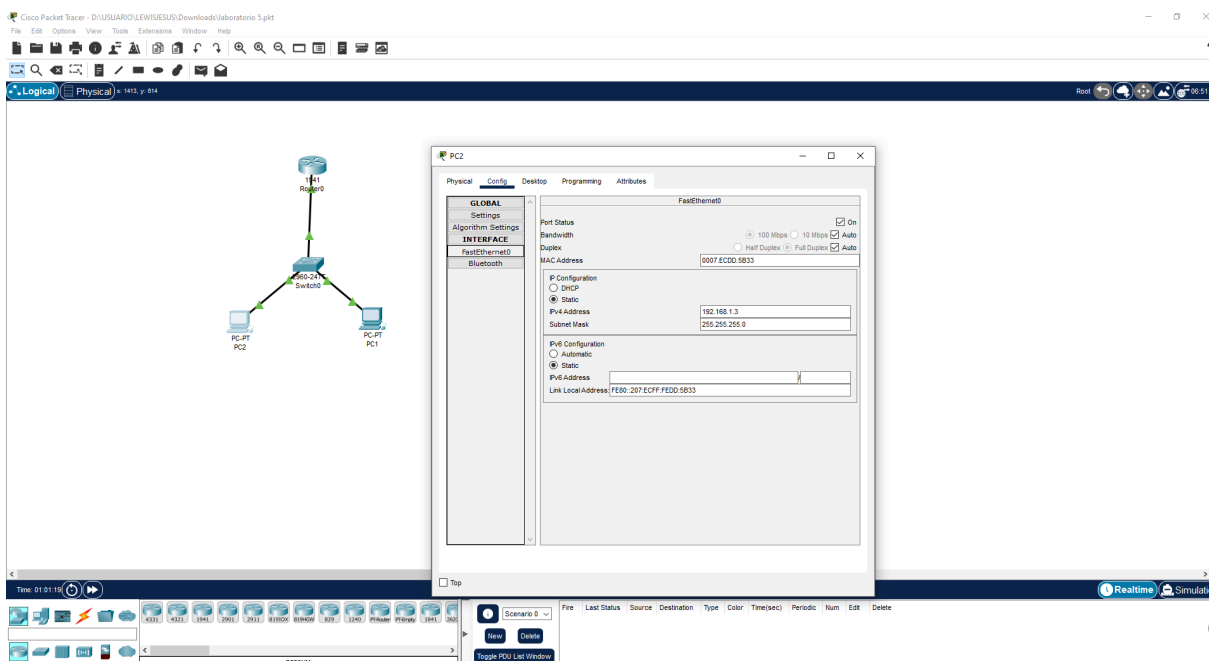
PC_1



Gateway



PC_2

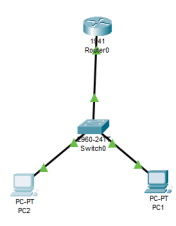


Gateway

Cisco Packet Tracer - D:\USUARIO\LEWIS\SUS\Downloads\laboratorio 5.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical 142 y 814



PC2

Global Settings

Display Name: PC2

Interfaces: FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway: 192.168.1.1

DNS Server:

Gateway/DNS IPv6

☐ Automatic

☒ Static

Default Gateway:

DNS Server:

Time: 01:02:30

Scenario 0

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

Toggle PDU List Window

2620M

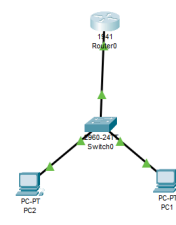
Realtime

Router

Cisco Packet Tracer - D:\USUARIO\LEWIS\SUS\Downloads\laboratorio 5.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical 885 y 410



Router0

Config

Global Settings

ROUTING

Static

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Port Status: ☒ On

Bandwidth: ☐ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address: 0000.3ED1.94D1

IP Configuration

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```

#LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router#enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
  
```

Time: 01:07:12

Scenario 0

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

Toggle PDU List Window

2620M

Realtime

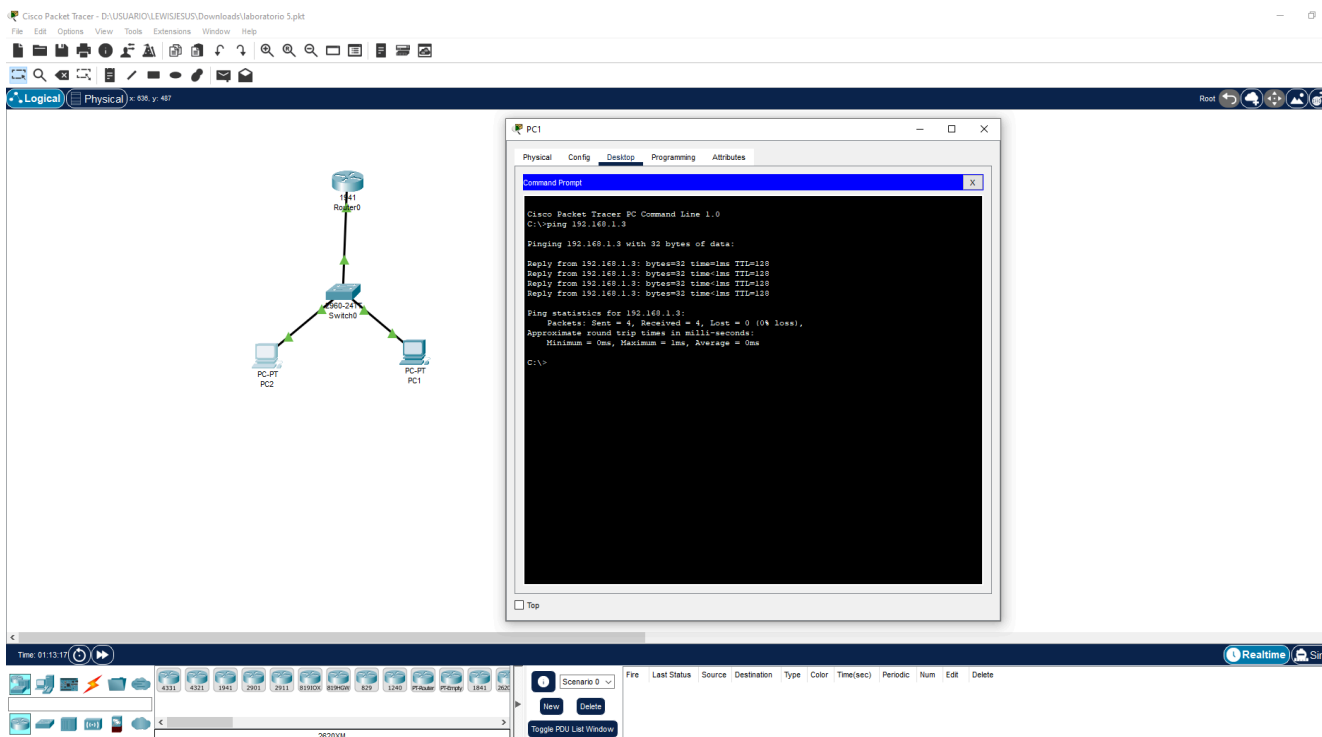
1.3. Verificación de conectividad:

Verifica que los PCs puedan hacer ping entre sí.

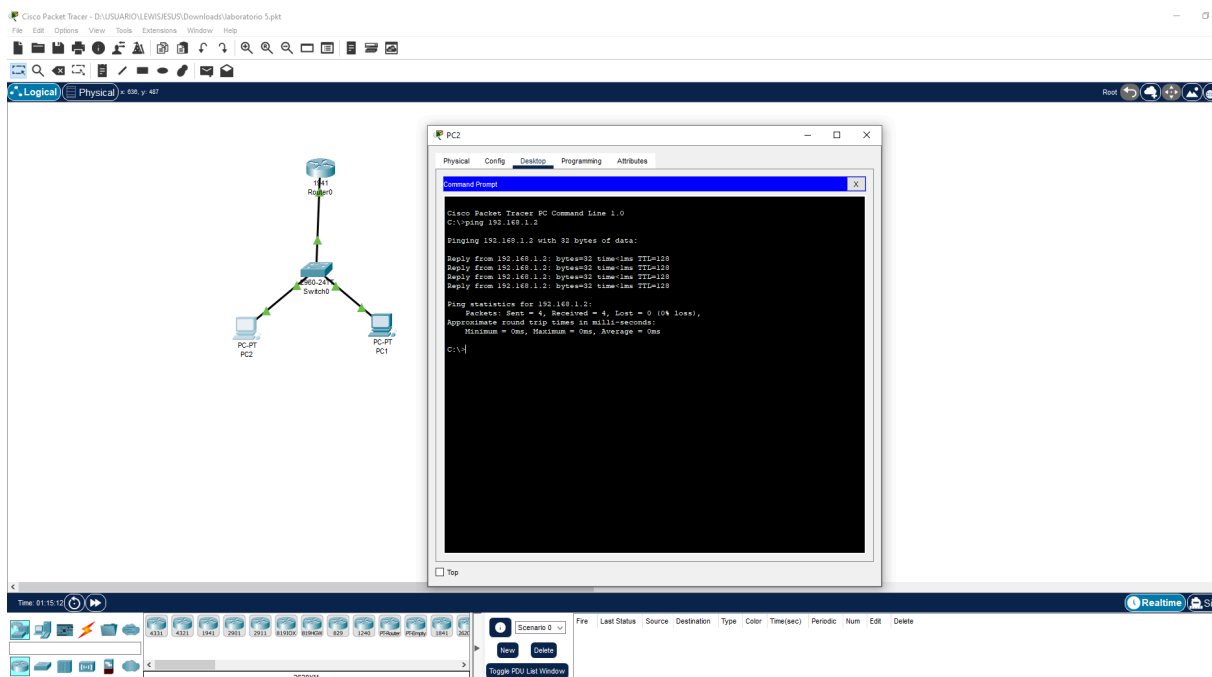
En PC1, abre la terminal y usa el comando: ping 192.168.1.3.

Asegúrate de que las respuestas sean exitosas.

PC1 a PC2

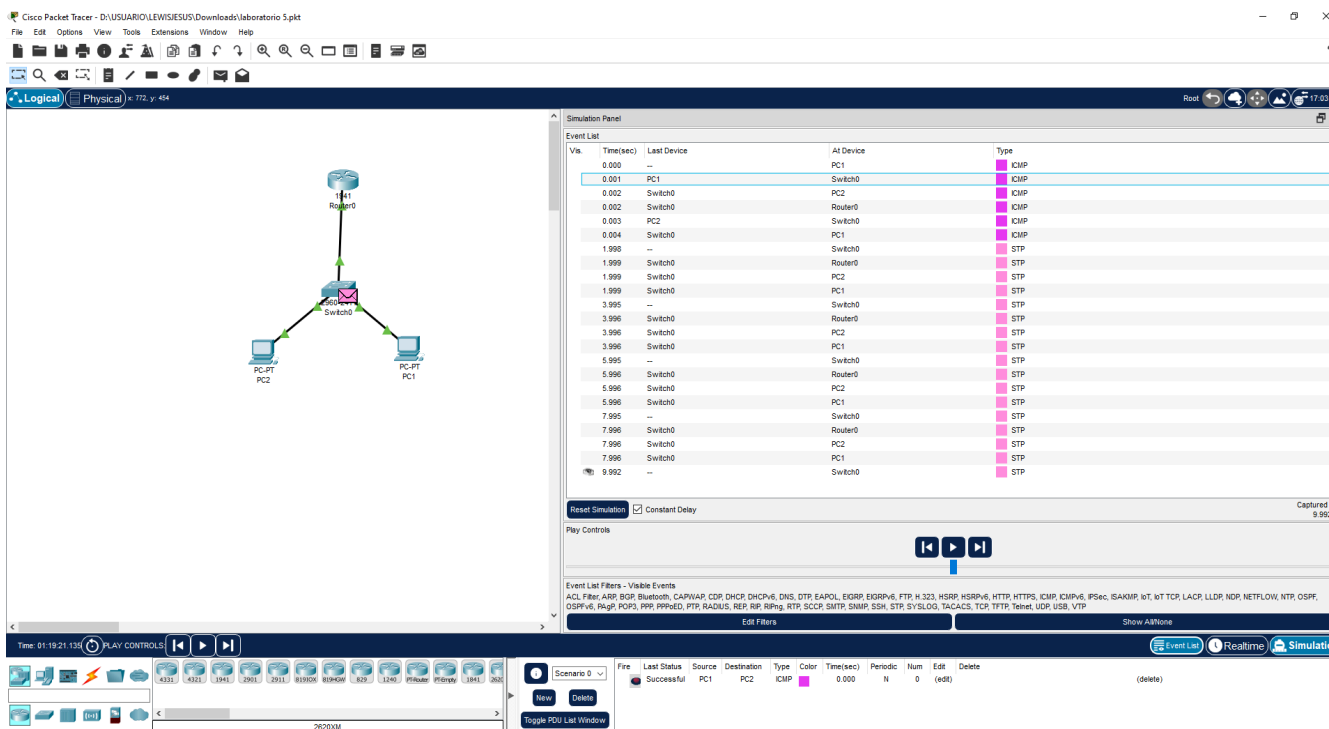


PC2 a PC1



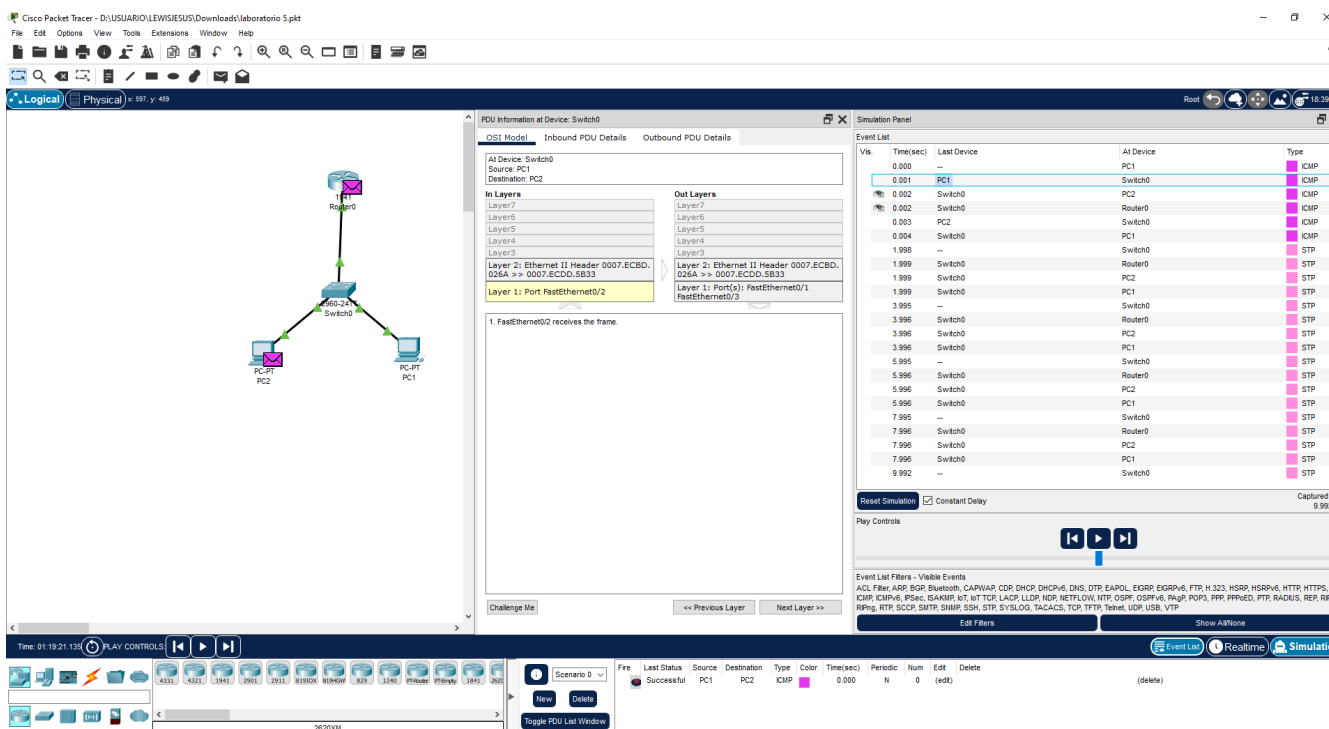
2. Parte 2: Análisis del Tráfico con Packet Tracer (Modelo OSI)

- 2.1. Simulación del tráfico:
- 2.2. Análisis del tráfico a través del modelo OSI:
- 2.3. Captura de un paquete:



The screenshot shows the Cisco Packet Tracer interface. On the left, a network topology is visible with a central switch connected to two PCs (PC-PT) and a router. The main panel displays the 'Event List' table, which records network events.

Time(sec)	Last Device	AI Device	Type
0.000	--	PC1	ICMP
0.001	PC1	Switch0	ICMP
0.002	Switch0	PC2	ICMP
0.002	Switch0	Router0	ICMP
0.003	PC2	Switch0	ICMP
0.004	Switch0	PC1	ICMP
1.998	--	Switch0	STP
1.999	Switch0	Router0	STP
1.999	Switch0	PC2	STP
3.995	--	Switch0	STP
3.996	Switch0	Router0	STP
3.996	Switch0	PC2	STP
3.996	Switch0	PC1	STP
5.995	--	Switch0	STP
5.996	Switch0	Router0	STP
5.996	Switch0	PC2	STP
5.996	Switch0	PC1	STP
7.995	--	Switch0	STP
7.996	Switch0	Router0	STP
7.996	Switch0	PC2	STP
7.996	Switch0	PC1	STP
9.992	--	Switch0	STP



The screenshot shows the Cisco Packet Tracer interface with the 'PDU Information at Device: Switch0' panel open. This panel displays the details of the current packet being processed by the switch, organized by the seven layers of the OSI model.

Layer	Details
Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	0007.EC0D.5B33
Layer 1	Port FastEthernet0/2

The 'Simulation Panel' on the right shows the event list, which is the same as in the first screenshot.

PDU Information at Device: PC2

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: PC2	Source: PC1	Destination: PC2
Layer 7	Layer 7	Layer 7
Layer 6	Layer 6	Layer 6
Layer 5	Layer 5	Layer 5
Layer 4	Layer 4	Layer 4
Layer 3	Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.3 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 192.168.1.3, Dest. IP: 192.168.1.2 ICMP Message Type: 0
Layer 2	Layer 2: Ethernet II Header 0007.ECDD.0064 >> 0007.ECDD.006A	Layer 2: Ethernet II Header 0007.ECDD.006A >> 0007.ECDD.0064
Layer 1	Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Simulation Panel

Vis.	Time(sec)	Last Device	At Device	Type
0.000	—	PC1	PC1	ICMP
0.001	PC1	Switch0	Switch0	ICMP
0.002	Switch0	PC2	PC2	ICMP
0.003	PC2	Switch0	Switch0	ICMP
0.004	Switch0	PC1	PC1	ICMP
1.998	—	Switch0	Switch0	STP
1.999	Switch0	Router0	Router0	STP
1.999	Switch0	PC2	PC2	STP
1.999	Switch0	PC1	PC1	STP
3.995	—	Switch0	Switch0	STP
3.996	Switch0	Router0	Router0	STP
3.996	Switch0	PC2	PC2	STP
3.996	Switch0	PC1	PC1	STP
5.995	—	Switch0	Switch0	STP
5.996	Switch0	Router0	Router0	STP
5.996	Switch0	PC2	PC2	STP
5.996	Switch0	PC1	PC1	STP
7.995	—	Switch0	Switch0	STP
7.996	Switch0	Router0	Router0	STP
7.996	Switch0	PC2	PC2	STP
7.996	Switch0	PC1	PC1	STP
9.992	—	Switch0	Switch0	STP

Completa la siguiente tabla con la información del análisis del tráfico:

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:0007.ECDD.5B33	Resolución de IP a MAC

3. Parte 3: Modelo TCP/IP en Packet Tracer

3.1. Comparación de capas entre los modelos OSI y TCP/IP:

3.2. Verificación de la funcionalidad del modelo TCP/IP:

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

4. Parte 4: Evaluación de Conocimientos

Preguntas de repaso:

¿Qué dispositivos operan en la capa de enlace de datos en la simulación?

R//

Los switches operan principalmente en la capa 2 (enlace de datos) del modelo OSI, manejando direcciones MAC y frames Ethernet.

¿Qué protocolos de la capa de transporte observaste en el tráfico?

R//

En la captura se puede observar:

- **ICMP (aunque técnicamente ICMP pertenece a la capa de red, no de transporte)**
- **En la lista de filtros disponibles en la parte inferior se mencionan protocolos de capa de transporte como TCP y UDP**

¿Cómo se dividen las capas de los modelos OSI y TCP/IP al analizar un paquete ICMP?

R//

Al analizar un paquete ICMP:

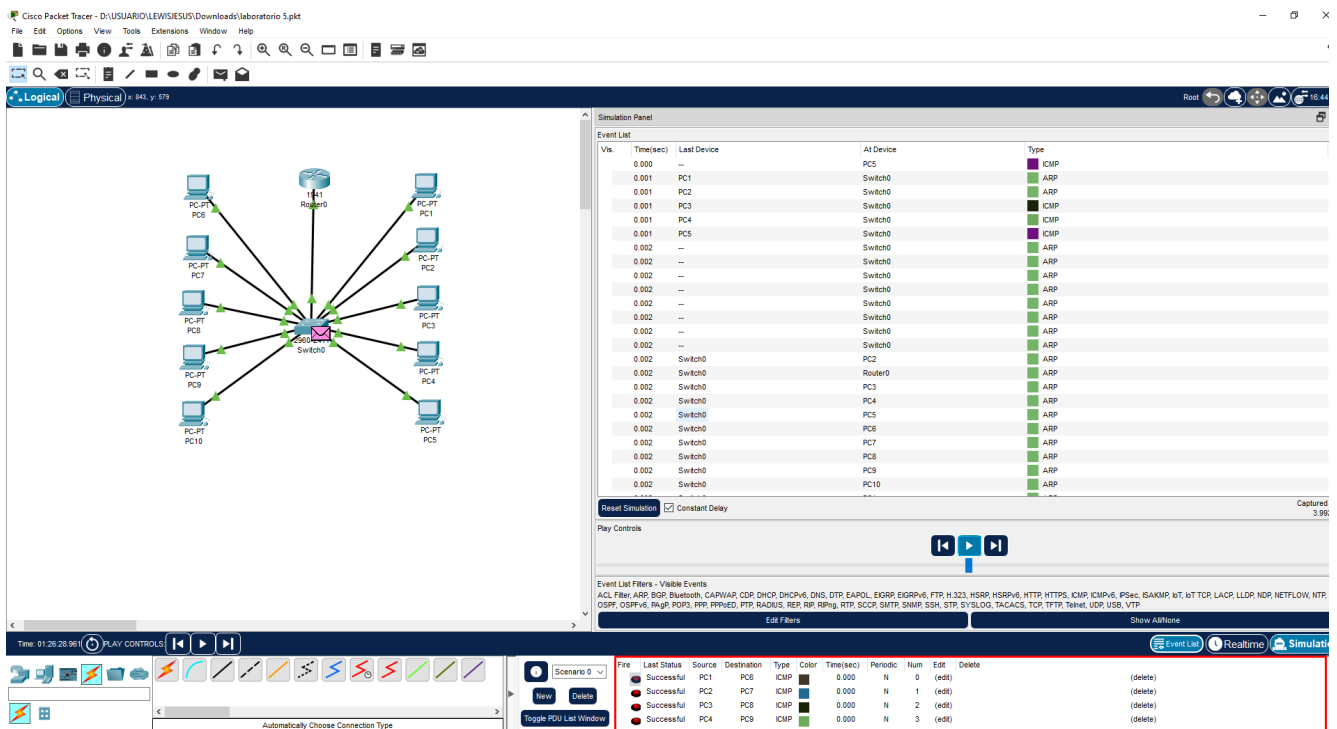
Modelo OSI:

- **Capa 7-5** (Aplicación, Presentación, Sesión): No aplica para ICMP
- **Capa 4 (Transporte)**: No aplica directamente (ICMP no usa puertos)
- **Capa 3 (Red)**: Aquí opera ICMP, junto con las direcciones IP (en la imagen se ven 192.168.1.2 y 192.168.1.3)
- **Capa 2 (Enlace de datos)**: Frame Ethernet con direcciones MAC
- **Capa 1 (Física)**: Señales eléctricas por el cable (no visible directamente)

Modelo TCP/IP:

- **Capa de Aplicación:** No aplica para ICMP
- **Capa de Transporte:** No aplica directamente
- **Capa de Internet:** Aquí opera ICMP
- **Capa de Acceso a la Red:** Corresponde al encapsulamiento Ethernet

Completa el laboratorio diseñando una red de 10 computadores y realice el mismo procedimiento de cada computador con todos, se debe tener en cuenta que todos los pcs deben estar en la misma red.



5. Lista de Verificación Ejemplo:

1. Revisar en la academia cisco los conceptos.
2. Subir un documento pdf al repositorio GitHub con las actividades realizadas

Actividad Complementaria

Laboratorio Práctico: Entendiendo los Modelos OSI y TCP/IP

Objetivo:

El objetivo de este laboratorio es familiarizarse con los modelos de referencia OSI y TCP/IP, sus capas y cómo se aplican en las redes modernas. Los estudiantes identificarán funciones clave en cada capa y las correlacionarán con dispositivos de red y protocolos.

Materiales necesarios:

- Un switch o enrutador básico.
- Computadoras con acceso a la red local.
- Acceso a Internet (opcional para simulaciones).
- Software de captura de paquetes (Wireshark) instalado en las máquinas.
- Herramientas de línea de comandos como `ping`, `tracert` o `tracert`, `ipconfig` o `ifconfig`.

Parte 1: Modelo OSI y su Aplicación en Redes

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.

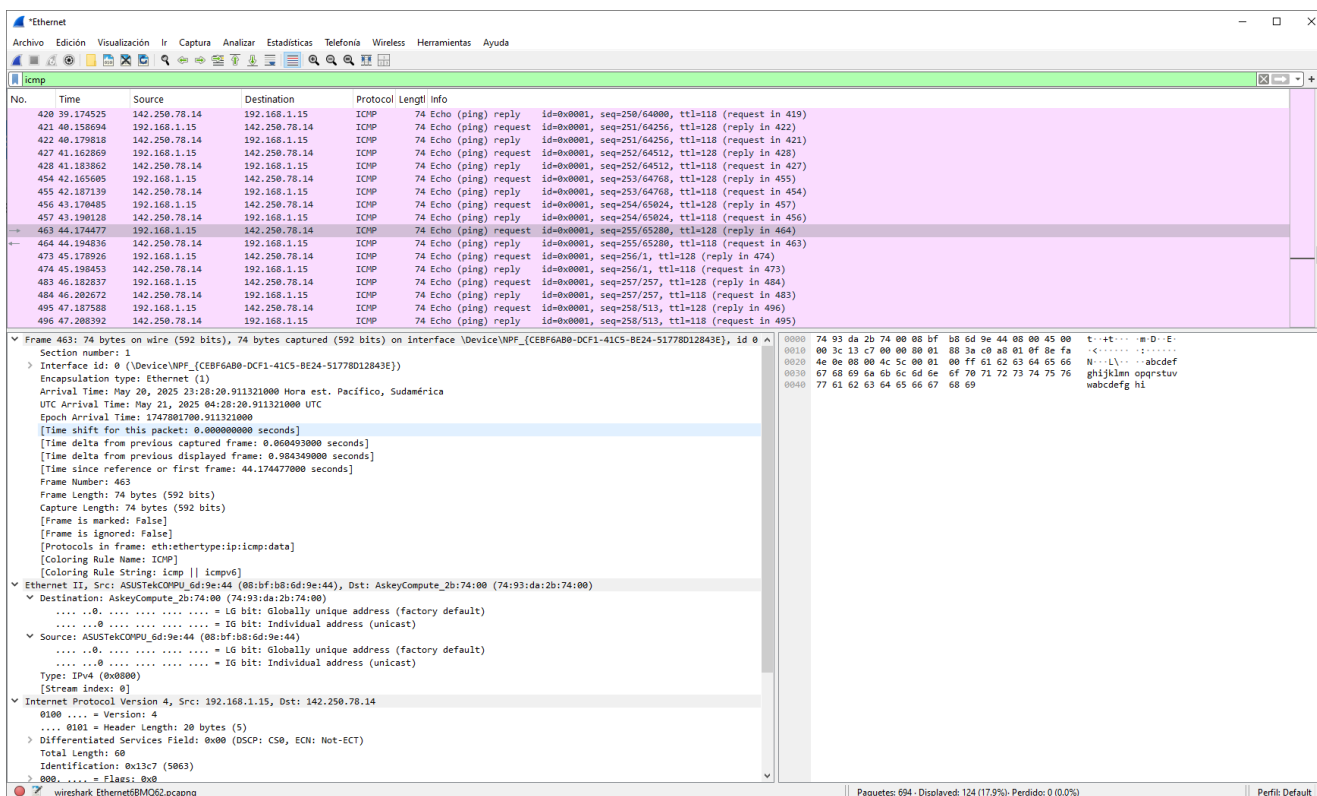
Dispositivo	Capa del Modelo OSI	Justificación / Función Principal
Computadora	Capa 7 – Aplicación	Ejecuta aplicaciones de red e interactúa directamente con el usuario.
Servidor	Capa 7 – Aplicación	Proporciona servicios de red (web, correo, DNS, etc.).
Router	Capa 3 – Red	Enruta paquetes entre redes diferentes 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.

Parte 2: Protocolo TCP/IP y Captura de Paquetes

1. Simulación y captura de tráfico:

- o Abre **Wireshark** en tu computadora y selecciona la interfaz de red activa.
- o Inicia una captura de paquetes mientras realizas las siguientes tareas en otra terminal o consola:
 - Ejecuta el comando `ping` hacia un servidor o una dirección IP (ejemplo: `ping google.com` o `ping 8.8.8.8`).
 - Ejecuta el comando `tracert` (Windows) o `traceroute` (Linux/Mac) para la misma dirección IP o dominio.

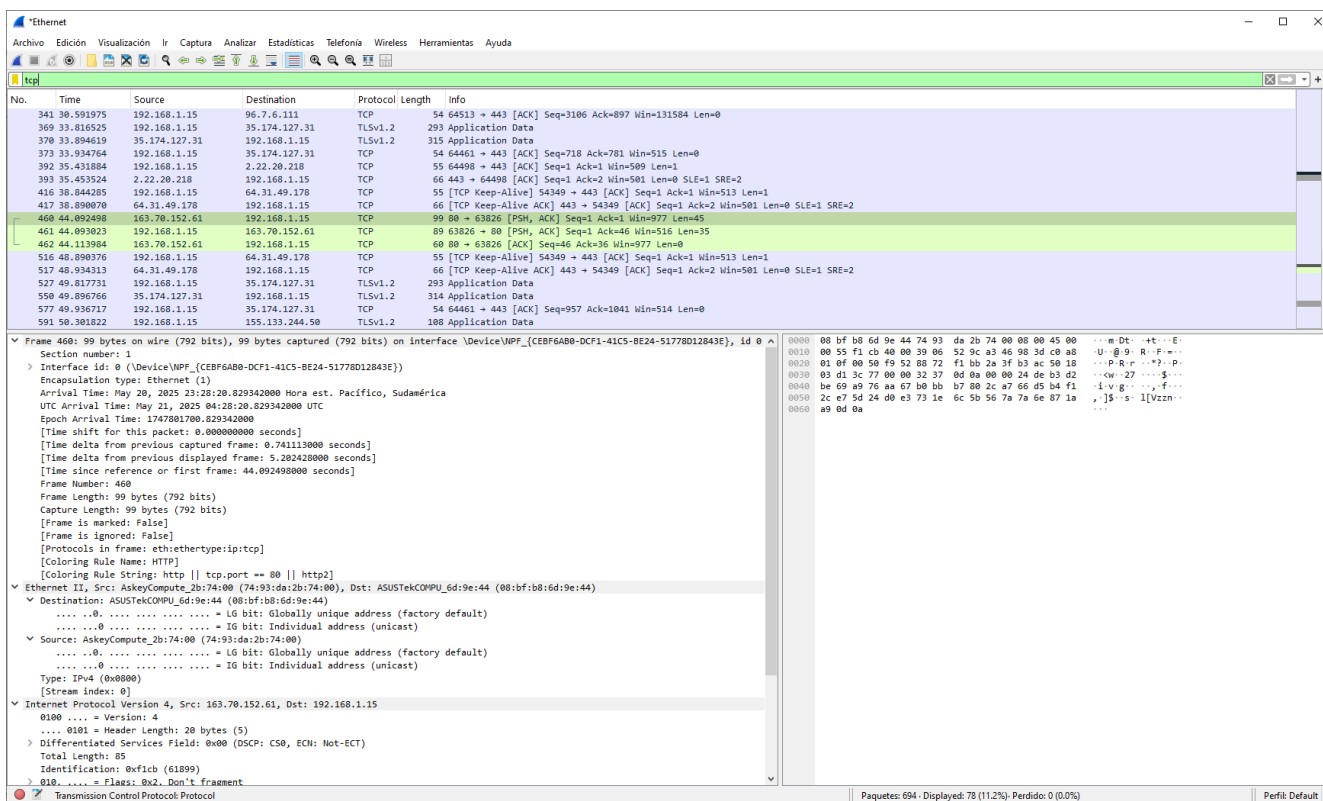
ICMP



The screenshot displays the Wireshark interface with a capture of ICMP traffic. The packet list shows a series of ping requests and replies. Packet 463 is selected, showing the following details:

- Ethernet II, Src: ASUSTEKCOMPU_6d9e44 (08:bf:b8:6d:9e:44), Dst: AskeyCompute_2b:74:00 (74:93:da:2b:74:00)**
 - Destination: AskeyCompute_2b:74:00 (74:93:da:2b:74:00)
 - ...0 ... = LG bit: Globally unique address (factory default)
 - ...0 ... = IG bit: Individual address (unicast)
 - Source: ASUSTEKCOMPU_6d9e44 (08:bf:b8:6d:9e:44)
 - ...0 ... = LG bit: Globally unique address (factory default)
 - ...0 ... = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
 - [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.1.15, Dst: 142.250.78.14**
 - 0100 ... = Version: 4
 - ...0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x13c7 (5063)
 - 0000 ... = Flags: 0x0

TCP



The image shows a Wireshark capture of TCP traffic. The top pane displays a list of packets, with packet 460 selected. The middle pane shows the details of packet 460, which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
341	30.591975	192.168.1.15	96.7.6.111	TCP	54	64513 → 443 [ACK] Seq=3106 Ack=897 Win=131584 Len=0
369	33.816525	192.168.1.15	35.174.127.31	TLSv1.2	293	Application Data
370	33.894619	35.174.127.31	192.168.1.15	TLSv1.2	315	Application Data
373	33.934764	192.168.1.15	35.174.127.31	TCP	54	64461 → 443 [ACK] Seq=718 Ack=781 Win=515 Len=0
392	35.431884	192.168.1.15	2.22.20.218	TCP	55	64499 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1
393	35.453524	2.22.20.218	192.168.1.15	TCP	66	443 → 64498 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
416	38.844285	192.168.1.15	64.31.49.178	TCP	55	[TCP Keep-Alive] 54349 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1
417	38.890870	64.31.49.178	192.168.1.15	TCP	66	[TCP Keep-Alive ACK] 443 → 54349 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
460	44.092498	163.70.152.61	192.168.1.15	TCP	99	80 → 63826 [PSH, ACK] Seq=1 Ack=1 Win=977 Len=45
461	44.093023	192.168.1.15	163.70.152.61	TCP	89	63826 → 80 [PSH, ACK] Seq=1 Ack=46 Win=516 Len=35
462	44.113984	163.70.152.61	192.168.1.15	TCP	60	80 → 63826 [ACK] Seq=46 Ack=36 Win=977 Len=0
516	48.890376	192.168.1.15	64.31.49.178	TCP	55	[TCP Keep-Alive] 54349 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1
517	48.934313	64.31.49.178	192.168.1.15	TCP	66	[TCP Keep-Alive ACK] 443 → 54349 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
527	49.817731	192.168.1.15	35.174.127.31	TLSv1.2	293	Application Data
550	49.890766	35.174.127.31	192.168.1.15	TLSv1.2	314	Application Data
577	49.936717	192.168.1.15	35.174.127.31	TCP	54	64461 → 443 [ACK] Seq=957 Ack=1841 Win=514 Len=0
591	50.301822	192.168.1.15	155.133.244.50	TLSv1.2	108	Application Data

Packet 460 Details:

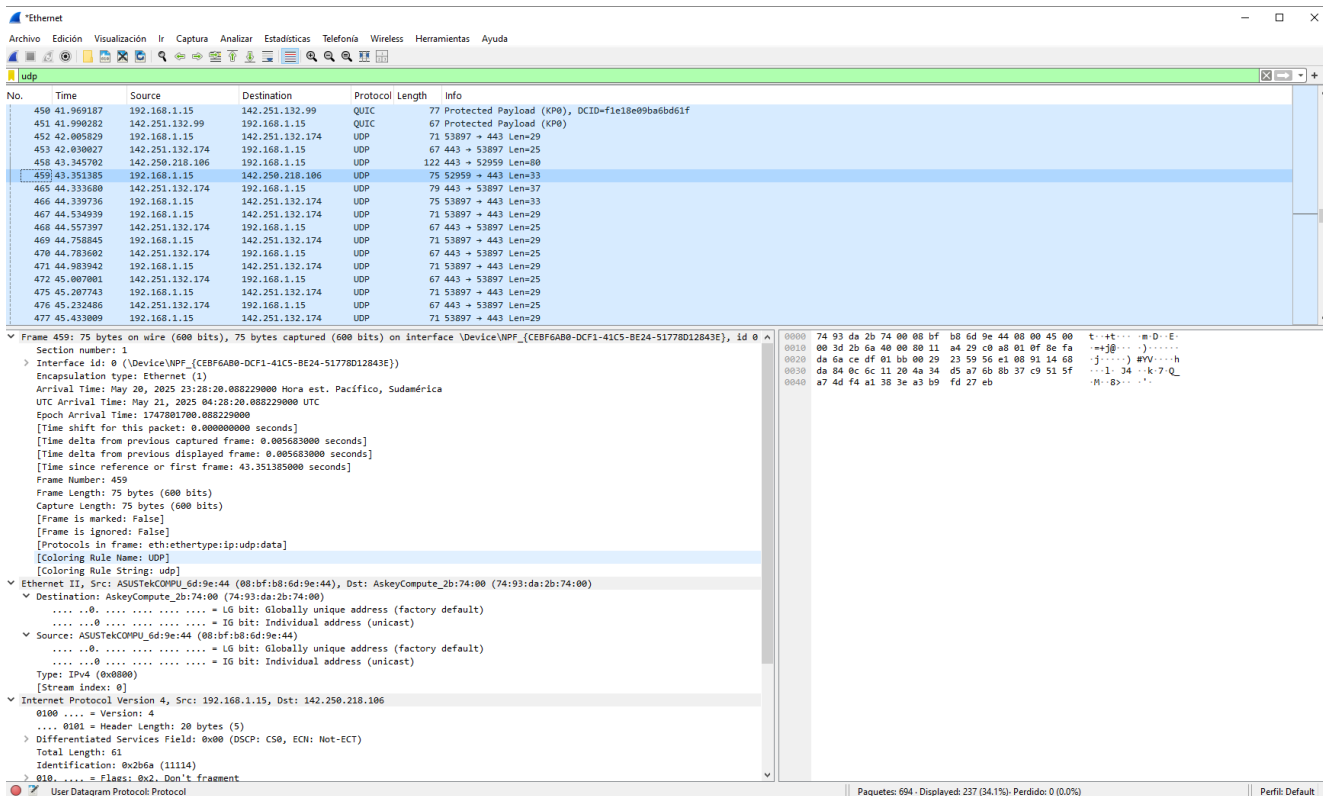
- Frame 460: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{CEBF6A80-DCF1-41C5-BE24-51778D12843E}, id 0
- Section number: 1
- Interface id: 0 (\Device\NPF_{CEBF6A80-DCF1-41C5-BE24-51778D12843E})
- Encapsulation type: Ethernet (1)
- Arrival Time: May 20, 2025 23:28:20.829342000 Hora est. Pacifico, Sudamérica
- UTC Arrival Time: May 21, 2025 04:28:20.829342000 UTC
- Epoch Arrival Time: 1747881700.829342000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.741138000 seconds]
- [Time delta from previous displayed frame: 5.202428000 seconds]
- [Time since reference or first frame: 44.092498000 seconds]
- Frame Number: 460
- Frame Length: 99 bytes (792 bits)
- Capture Length: 99 bytes (792 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: ethertype:ip:tcp]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: AskyCompute_2b:74:00 (74:93:da:2b:74:00), Dst: ASUSTekCOMPU_6d:9e:44 (08:bf:b8:6d:9e:44)
- Destination: ASUSTekCOMPU_6d:9e:44 (08:bf:b8:6d:9e:44)
- ...0. = LG bit: Globally unique address (factory default)
- ...0. = IG bit: Individual address (unicast)
- Source: AskyCompute_2b:74:00 (74:93:da:2b:74:00)
- ...0. = LG bit: Globally unique address (factory default)
- ...0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 163.70.152.61, Dst: 192.168.1.15
- 0100 = Version: 4
-0001 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 85
- Identification: 0xf1cb (61899)
- 010. = Flags: 0x2. Don't fragment
- Transmission Control Protocol Protocol

Raw Data:

```

0000  08 bf b8 6d 9e 44 74 93 da 2b 74 00 08 00 45 00  ...mDt: +t...E
0010  00 55 f1 cb 40 00 39 06 52 9c a3 46 98 3d c0 a8  ...U@9: R:F...
0020  01 0f 00 50 f9 52 88 72 f1 bb 2a 3f b3 ac 50 18  ...P.R.r...?..P
0030  03 d1 3c 77 00 00 32 37 0d 0a 00 00 24 de b3 d2  ...Qv.27...$...
0040  be 69 a9 76 aa 67 b0 bb b7 80 2c a7 66 d5 b4 f1  ...i.v.g...f...
0050  2c e7 5d 24 d0 e3 73 1e 6c 5b 56 7a 7a 6e 87 1a  ...J's'..l[Vzzn...
0060  a9 6d 0a
  
```

UDP



The image shows a Wireshark capture of UDP traffic. The top pane displays a list of packets, with packet 459 selected. The middle pane shows the details of packet 459, which is a QUIC packet. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
450	41.969187	192.168.1.15	142.251.132.99	QUIC	77	Protected Payload (QP0), DCID=f1e18e9ba6bd61f
451	41.990282	142.251.132.99	192.168.1.15	QUIC	67	Protected Payload (QP0)
452	42.005829	192.168.1.15	142.251.132.174	UDP	71	53897 → 443 Len=29
453	42.030827	142.251.132.174	192.168.1.15	UDP	67	443 → 53897 Len=25
458	43.345792	142.250.218.106	192.168.1.15	UDP	122	443 → 52959 Len=80
459	43.351385	192.168.1.15	142.250.218.106	UDP	75	52959 → 443 Len=33
465	44.333680	142.251.132.174	192.168.1.15	UDP	79	443 → 53897 Len=37
466	44.339736	192.168.1.15	142.251.132.174	UDP	75	53897 → 443 Len=33
467	44.334939	192.168.1.15	142.251.132.174	UDP	71	53897 → 443 Len=29
468	44.357397	142.251.132.174	192.168.1.15	UDP	67	443 → 53897 Len=25
469	44.758845	192.168.1.15	142.251.132.174	UDP	71	53897 → 443 Len=29
470	44.783602	142.251.132.174	192.168.1.15	UDP	67	443 → 53897 Len=25
471	44.983942	192.168.1.15	142.251.132.174	UDP	71	53897 → 443 Len=29
472	45.007901	142.251.132.174	192.168.1.15	UDP	67	443 → 53897 Len=25
475	45.207743	192.168.1.15	142.251.132.174	UDP	71	53897 → 443 Len=29
476	45.232486	142.251.132.174	192.168.1.15	UDP	67	443 → 53897 Len=25
477	45.433909	192.168.1.15	142.251.132.174	UDP	71	53897 → 443 Len=29

Packet 459 Details:

- Frame 459: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{CEBF6A80-DCF1-41C5-BE24-51778D12843E}, id 0
- Section number: 1
- Interface id: 0 (\Device\NPF_{CEBF6A80-DCF1-41C5-BE24-51778D12843E})
- Encapsulation type: Ethernet (1)
- Arrival Time: May 20, 2025 23:28:20.888229000 Hora est. Pacifico, Sudamérica
- UTC Arrival Time: May 21, 2025 04:28:20.888229000 UTC
- Epoch Arrival Time: 1747881700.888229000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.005683000 seconds]
- [Time delta from previous displayed frame: 0.005683000 seconds]
- [Time since reference or first frame: 43.351385000 seconds]
- Frame Number: 459
- Frame Length: 75 bytes (600 bits)
- Capture Length: 75 bytes (600 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: ethertype:ip:udp:data]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]
- Ethernet II, Src: ASUSTekCOMPU_6d:9e:44 (08:bf:b8:6d:9e:44), Dst: AskyCompute_2b:74:00 (74:93:da:2b:74:00)
- Destination: AskyCompute_2b:74:00 (74:93:da:2b:74:00)
- ...0. = LG bit: Globally unique address (factory default)
- ...0. = IG bit: Individual address (unicast)
- Source: ASUSTekCOMPU_6d:9e:44 (08:bf:b8:6d:9e:44)
- ...0. = LG bit: Globally unique address (factory default)
- ...0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.1.15, Dst: 142.250.218.106
- 0100 = Version: 4
-0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 61
- Identification: 0x2b6a (11114)
- 010. = Flags: 0x2. Don't fragment
- User Datagram Protocol Protocol

Raw Data:

```

0000  74 93 da 2b 74 00 08 bf b8 6d 9e 44 08 00 45 00  t:~t... mD:E:
0010  00 3d 2b 6a 40 00 00 11 a4 29 c0 a8 01 0f 8e fa  ...+@... ).....
0020  da 6a ce df 01 bb 00 29 23 59 56 e1 08 91 14 68  ...j.....)vV...h
0030  da 04 0c 6c 11 29 4a 34 d5 a7 6d 8b 37 c9 51 5f  ...l.34..k7-Q...
0040  a7 4d f4 a1 38 3e a3 b9 fd 27 eb
  
```

2. Análisis del tráfico capturado:

- o Detén la captura de Wireshark y analiza los paquetes capturados.
 - Identifica los paquetes ICMP correspondientes a los comandos `ping` y `tracert`.
 - Localiza los paquetes de la capa de transporte (TCP o UDP) y determina qué puerto y protocolo están usando.
 - Describe qué capas del modelo OSI están presentes en los paquetes capturados y qué información puedes ver de cada una de ellas.
- o Completa la siguiente tabla con el análisis de algunos de los paquetes capturados.

No. de Paquete	Protocolo	Capa OSI	Fuente	Destino	Puerto	Descripción
463	ICMP	3 (Capa de Red)	192.168.1.15	142.250.78.14		Echo (ping) request id=0x0001, seq=255/65280, ttl=128 (reply in 464)
460	TCP	4 (Transporte de datos)	163.70.152.61 cc	192.168.1.15	80	63826 [PSH, ACK] Seq=1 Ack=1 Win=977 Len=45
459	UDP	4 (Transporte de datos)	43.351385	192.168.1.15	52959	443 Len=33

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
7. Aplicación	Interfaces de usuario, servicios de red	4. Aplicación	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP, SNMP, Telnet, SSH
6. Presentación	Traducción de datos, cifrado, compresión	<i>(Incluida en Aplicación)</i>	TLS/SSL, JPEG, MPEG, ASCII, EBCDIC, GIF
5. Sesión	Control de sesiones, establecimiento y terminación	<i>(Incluida en Aplicación)</i>	RPC, NetBIOS, PPTP
4. Transporte	Comunicación extremo a extremo, control de flujo y errores	3. Transporte	TCP, UDP
3. Red	Enrutamiento de datos entre dispositivos y redes	2. Internet	IP, ICMP, IGMP, ARP, RARP, Ipsec
2. Enlace de datos	Control de acceso al medio, detección de errores	1. Acceso a la red	Ethernet, Wi-Fi (IEEE 802.11), PPP, Frame Relay, ATM, HDLC

1. Física	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
------------------	---	-----------------------------------	--

2. 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.

Parte 4: Evaluación de Conocimientos

1. Preguntas de repaso:

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

R//

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?

R//

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?

R//

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).
- ¿Cuáles son las diferencias clave entre los modelos OSI y TCP/IP?

R//

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