

Laboratorio #5

The image displays two screenshots of the Cisco Packet Tracer software interface, illustrating network configuration and testing in a laboratory setting.

Top Screenshot: The main workspace shows a network topology with a central 2961 Switch connected to a 1941 Router and seven PC-PT devices (PC1 through PC7). The right-hand pane is open to the configuration window for the 2961 Switch, specifically the GigabitEthernet0/0 interface. The configuration shows the interface is enabled, with a speed of 1000 Mbps, duplex of Full Duplex, and an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0. The Tx Ring Limit is set to 10. Below the configuration pane, the Equivalent IOS Commands are listed:

```
Router(config)# interface shutdown
Router(config-if)#
Router(config-if)#
ALINE0-5-CORRIG: Interface GigabitEthernet0/0, changed state to up
ALINE0-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0
Router(config-if)#
```

Bottom Screenshot: This screenshot shows the same network topology, but with the PC0 configuration window open. The Command Prompt window is active, displaying the results of a ping command from PC0 to the 192.168.1.7 IP address. The output shows successful connectivity with 4 packets sent and 4 received, 0% loss, and an approximate round trip time of 0ms. Below the Command Prompt, the PC0 configuration window shows the FastEthernet0 connection details, including the IP address 192.168.1.7 and the default gateway 192.168.1.1.

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x 100% y 684

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	4.390	Switch0
	4.390	Switch0
	4.390	Switch0
	6.389	—
Visible	6.390	Switch0
Visible	6.390	Switch0
Visible	6.390	Switch0
Visible	6.390	Switch0
Visible	6.390	Switch0
Visible	6.390	Switch0
Visible	6.390	Switch0

Reset Simulation Constant Delay Captured to: 6.390 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RFP, RPNg, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Scenario 0

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

Toggle PCUI List Window

Copper Straight-Through

Time: 00:31:18.630 PLAY CONTROLS

ESP LAA 7:02 p.m. 28/04/2025

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x 775 y 473

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	4.390	Switch0
	4.390	Switch0
	4.390	Switch0
	6.389	—
	6.390	Switch0
	6.390	Switch0
	6.390	Switch0
	6.390	Switch0
	6.390	Switch0
	6.390	Switch0
	6.390	Switch0
	6.390	Switch0
Visible	7.541	—

Reset Simulation Constant Delay Captured to: 7.541 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RFP, RPNg, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Scenario 0

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

Toggle PCUI List Window

Copper Straight-Through

Time: 00:31:11.781 PLAY CONTROLS

ESP LAA 7:02 p.m. 28/04/2025

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x 328 x 352

Time: 00:36:40

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::203:E4FF:FE53::1A3D
IPv6 Address...: 11
IPv6 Address...: 192.168.1.2
Subnet Mask...: 255.255.255.0
Default Gateway...: 11
0.0.0.0

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address...: 11
IPv6 Address...: 11
IPv6 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...: 0.0.0.0

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Internet Address      Physical Address      Type
192.168.1.1           0002.1677.cb01       dynamic
192.168.1.3           0030.f299.126e       dynamic
192.168.1.4           000c.cfa6.179e       dynamic
192.168.1.5           0007.ec11.40ea       dynamic
192.168.1.6           0040.0b89.48be       dynamic
192.168.1.7           0001.9754.2b15       dynamic

C:\>
```

Realtime Simulation

ESP LAA 7:09 p.m. 28/04/2025

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x 109 x 4

Time: 00:47:14.056

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
192.168.1.1 000c.cfa6.179e dynamic
192.168.1.5 0007.ec11.40ea dynamic
192.168.1.6 0040.0b89.48be dynamic
192.168.1.7 0001.9754.2b15 dynamic

C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Internet Address      Physical Address      Type
192.168.1.1           0002.1677.cb01       dynamic
192.168.1.3           0030.f299.126e       dynamic
192.168.1.4           000c.cfa6.179e       dynamic
192.168.1.5           0007.ec11.40ea       dynamic
192.168.1.6           0040.0b89.48be       dynamic
192.168.1.7           0001.9754.2b15       dynamic
192.168.1.8           0030.f299.126e       dynamic

C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.1.8:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:
```

Simulation Panel

Event List

Vis	Time(sec)	Last Device
6.672	-	-
6.672	-	-
6.673	-	Switch0
7.997	-	-
7.998	-	Switch0
7.998	-	Switch0
7.998	-	Switch0
7.998	-	Switch0
7.998	-	Switch0
7.998	-	Switch0
7.998	-	Switch0
Visible	8.696	-

Reset Simulation Constant Delay Captured to: 8.696 s

Play Controls

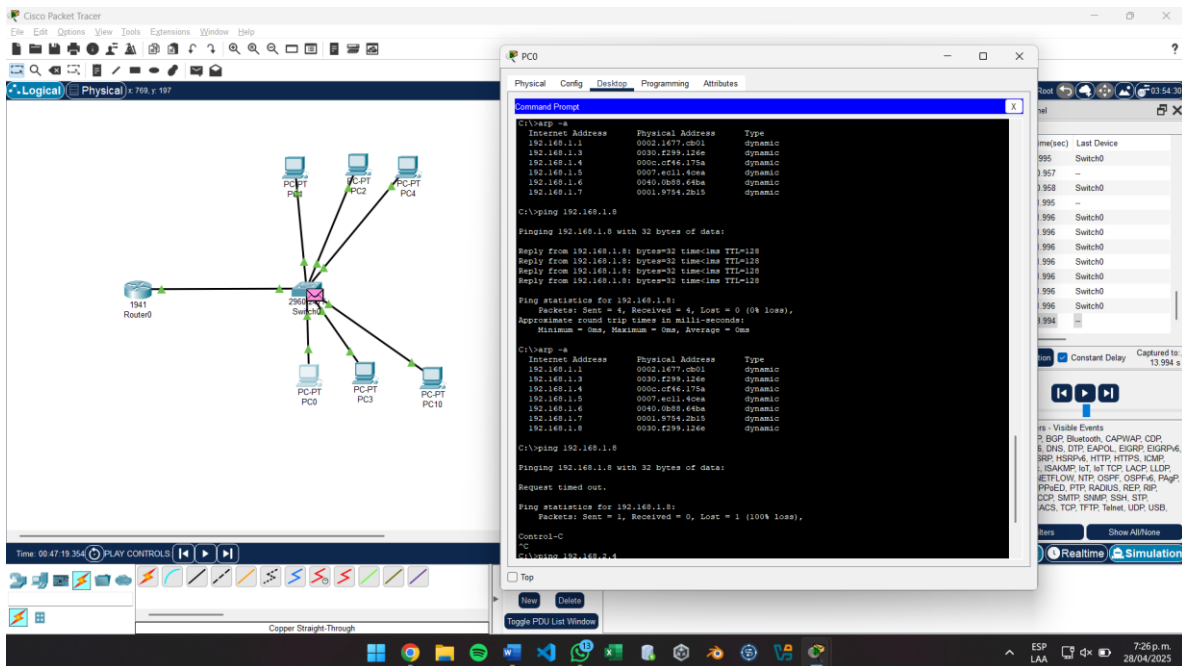
Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IOT, IOTv6, LACP, LLDP, Mosh, NTP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RSP, RRP, RTP, SCCP, SMTP, SNMP, SSH, SIP, Syslog, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

New List Realtime Simulation

ESP LAA 7:23 p.m. 28/04/2025



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 traceroute, ipconfig o ifconfig.

Parte 1: Modelo OSI y su Aplicación en Redes

- Investigación teórica:
 - 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	Capa de Aplicación	Interacción directa con el usuario. Proporciona servicios de red a aplicaciones.	HTTP, FTP, SMTP, DNS
6	Capa de Presentación	Traduce, cifra y comprime los datos.	SSL/TLS, JPEG, MPEG
5	Capa de Sesión	Establece, mantiene y finaliza sesiones de comunicación.	NetBIOS, PPTP
4	Capa de Transporte	Entrega confiable o no confiable de datos. Control de flujo y errores.	TCP, UDP
3	Capa de Red	Encaminamiento y direccionamiento lógico.	IP, ICMP, ARP, RIP, OSPF
2	Capa de Enlace de Datos	Entrega de tramas entre dispositivos en la misma red local.	Ethernet, PPP, Switches, MAC
1	Capa Física	Transmisión de bits a través del medio físico.	Cables, tarjetas de red, hubs, señales eléctricas

Parte 2: Protocolo TCP/IP y Captura de Paquetes

Simulación y captura de tráfico:

- Abre Wireshark en tu computadora y selecciona la interfaz de red activa.
- 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 trace route (Linux/Mac) para la misma dirección IP o dominio.
- Análisis del tráfico capturado:
 - 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.
 - Completa la siguiente tabla con el análisis de algunos de los paquetes capturados.

No. de Paquete	Protocolo	Capa OSI	Fuente	Destino	Puerto	Descripción
1	ICMP	Capa 3 (Red)	192.168.1.2	8.8.8.8	N/A	Solicitud ping enviada desde PC local a Google DNS
2	ICMP	Capa 3 (Red)	8.8.8.8	192.168.1.2	N/A	Respuesta ping desde Google DNS
3	TCP	Capa 4 (Transporte)	192.168.1.2	142.250.64.78	443 (HTTPS)	Conexión HTTPS iniciada al visitar un sitio web
4	UDP	Capa 4 (Transporte)	192.168.1.2	8.8.8.8	53 (DNS)	Consulta DNS para traducir google.com

Parte 3: Comparación entre OSI y TCP/IP

1. Investigación teórica:

- 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.

Capa OSI	Capa TCP/IP	Protocolos / Servicios Ejemplares
Aplicación	Aplicación	HTTP, FTP, SMTP, DNS
Presentación	Aplicación	SSL, TLS, codificación MIME
Sesión	Aplicación	NetBIOS, RPC
Transporte	Transporte	TCP, UDP
Red	Internet	IP, ICMP, ARP
Enlace de Datos + Física	Acceso a la Red	Ethernet, Wi-Fi, cables, hardware físico

2. Análisis práctico:

- 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

R% relación con los paquetes capturados

- Los **paquetes ICMP** pertenecen a la **capa de Internet** en TCP/IP y a la **capa de red** en OSI.

- Los paquetes **TCP y UDP** corresponden a la **capa de transporte** en ambos modelos.
- La dirección MAC observada en Wireshark es parte de la **capa de acceso a red** (TCP/IP) o **capa 2 en OSI**.
- La **capa física** no se ve en Wireshark directamente, ya que es el nivel eléctrico o de señal.

Parte 4: Evaluación de Conocimientos

1. Preguntas de repaso:

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

Respuesta: La **capa 4 (Transporte)**, mediante protocolos como TCP.

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

Respuesta: Los **switches** y **tarjetas de red (NIC)** operan principalmente en la **capa**

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

Respuesta: Observando si el paquete usa **TCP** o **UDP**, y revisando los **números de puerto** (como 80, 443, 53, etc.).

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

Respuesta:

- El modelo OSI tiene **7 capas**, mientras que el TCP/IP tiene **4 capas principales**.
- OSI es más teórico y detallado; TCP/IP está basado en protocolos reales usados en Internet.
- En TCP/IP, las capas de aplicación, presentación y sesión están combinadas en una sola capa.