AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

Title:Exploring the Networks Lab File

Subject: Exploring the Networks
Course Code: IT307

Submitted by:
Name: RIJU KUMARI
Enrollment no.: A41105223228
Course: B. Tech. CSE (5th Semester)

Under the guidance of: Prof. Dr. Tejaswi Khanna

Amity University, Plot no. 48A, Knowledge Park III, Greater Noida, Uttar Pradesh-201308

<u>INDEX</u>

S.no.	Practical
1.	To observe TCP and UDP connections and ports using the netstat command in Cisco Packet Tracer.
2.	To examine and compare TCP and UDP packets using Wireshark.
3.	To examine and verify a device's default gateway in a network.
4.	To study and verify network connectivity using **Ping** and **Traceroute** using *ping* and *tracert* commands, and to display routing information using the *show ip route* command in Cisco Packet Tracer.
5.	To examine **ICMP (Internet Control Message Protocol) packets** by generating ping traffic and analyzing packet flow in Cisco Packet Tracer using the simulation mode
6.	To understand and perform **IPv4 Address Subnetting** by dividing a large network into smaller subnetworks for efficient utilization of IP addresses.
7.	To perform IPv4 subnetting and configure a router to enable communication between different subnets.

Practical - 1

Aim: To observe TCP and UDP connections and ports using the netstat command in Cisco Packet Tracer.

Network Topology:

We will use:

- 1 Server
- 2 PCs
- 1 Switch

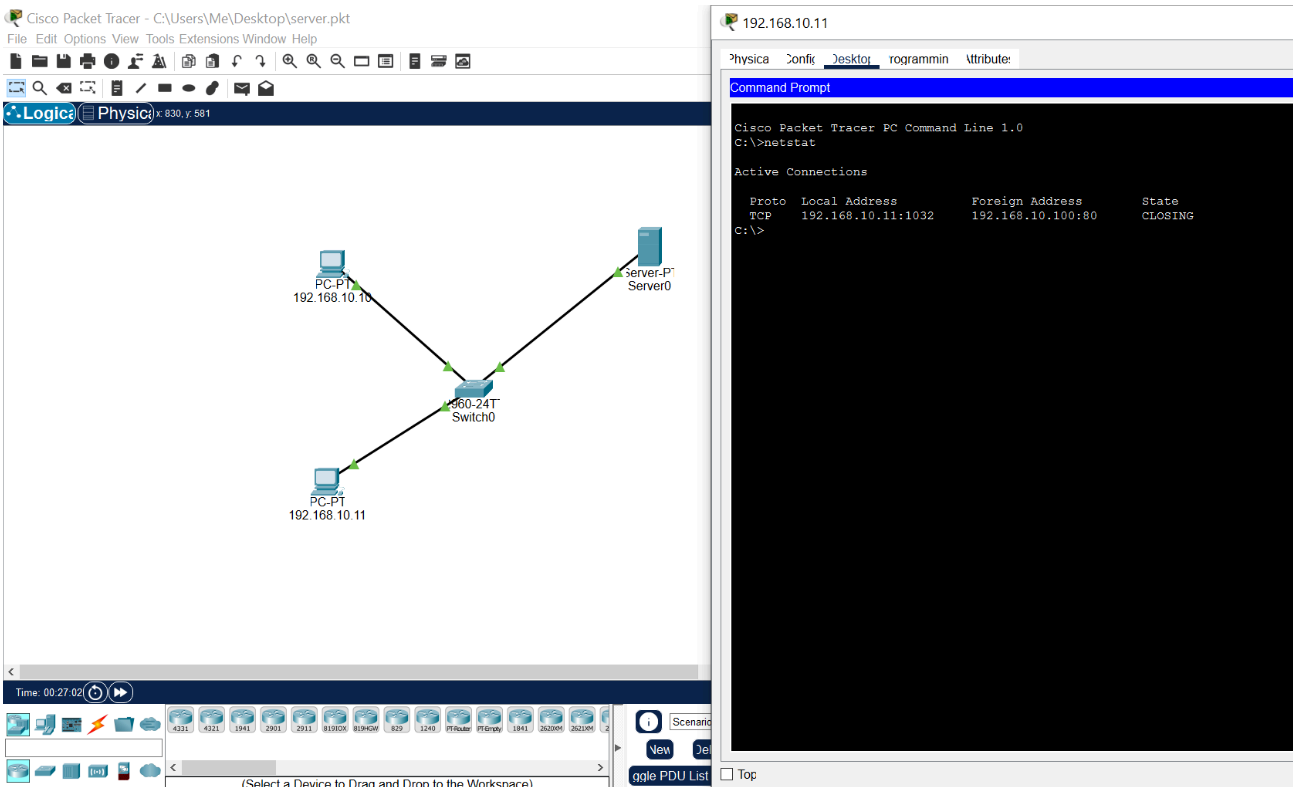
Network Setup

Device	IP Address	Subnet Mask
PC0	192.168.10.10	255.255.255.0
PC1	192.168.10.11	255.255.255.0
Server	192.168.10.100	255.255.255.0

Procedure

1. Open **Cisco Packet Tracer** and create a network with **2 PCs**, **1 Server**, and **1 Switch**.
2. Connect devices using **Copper Straight-Through** cables.
3. Assign IP addresses as shown above in network setup.
4. On the Server, enable **HTTP** service (TCP) and **DNS** service (UDP).
5. From PC0, open a web browser and go to http://192.168.10.100 to create TCP traffic.
6. From PC0, open **Command Prompt** and type netstat to view TCP and UDP connections.
7. Note the TCP connection to port **80** (HTTP).

Network setup and Output:



Result:

netstat displayed an active TCP connection to port 80 (HTTP), confirming TCP is connection-oriented.

Practical - 2

Aim: To examine and compare TCP and UDP packets using Wireshark.

Apparatus / Tools

- Wireshark (installed on PC)
- Internet connection / Local server

Theory

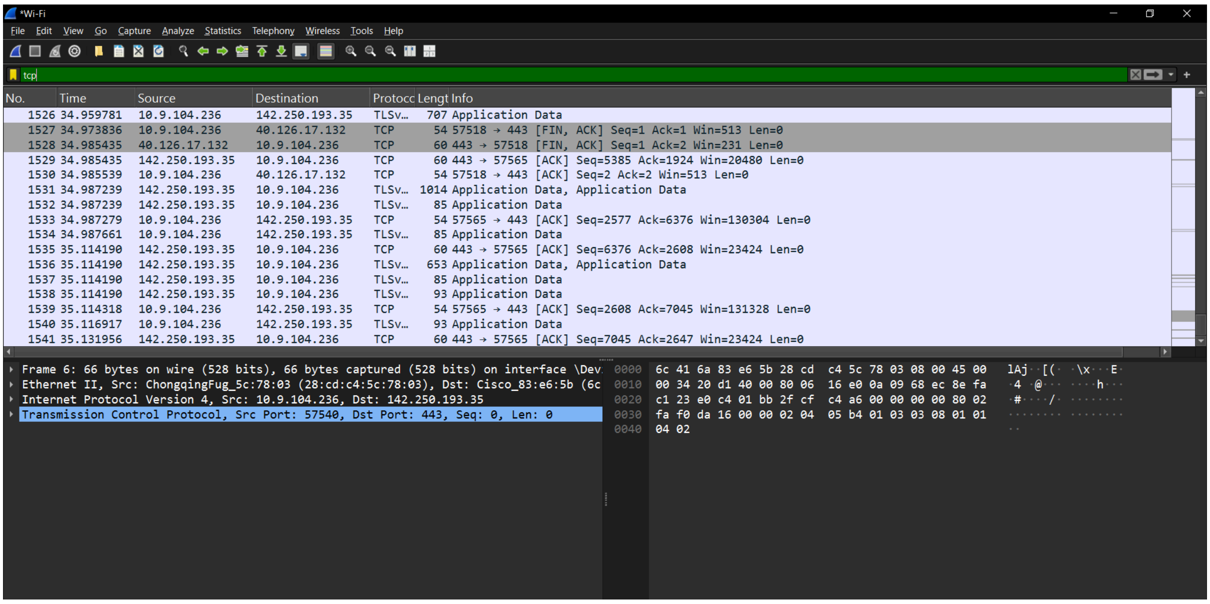
- **TCP (Transmission Control Protocol):** Connection-oriented, reliable protocol that uses acknowledgments, sequencing, and retransmissions.
- **UDP (User Datagram Protocol):** Connectionless, fast, lightweight protocol with no delivery guarantee.

Wireshark is a packet analyzer that captures and displays the details of TCP and UDP headers in real time.

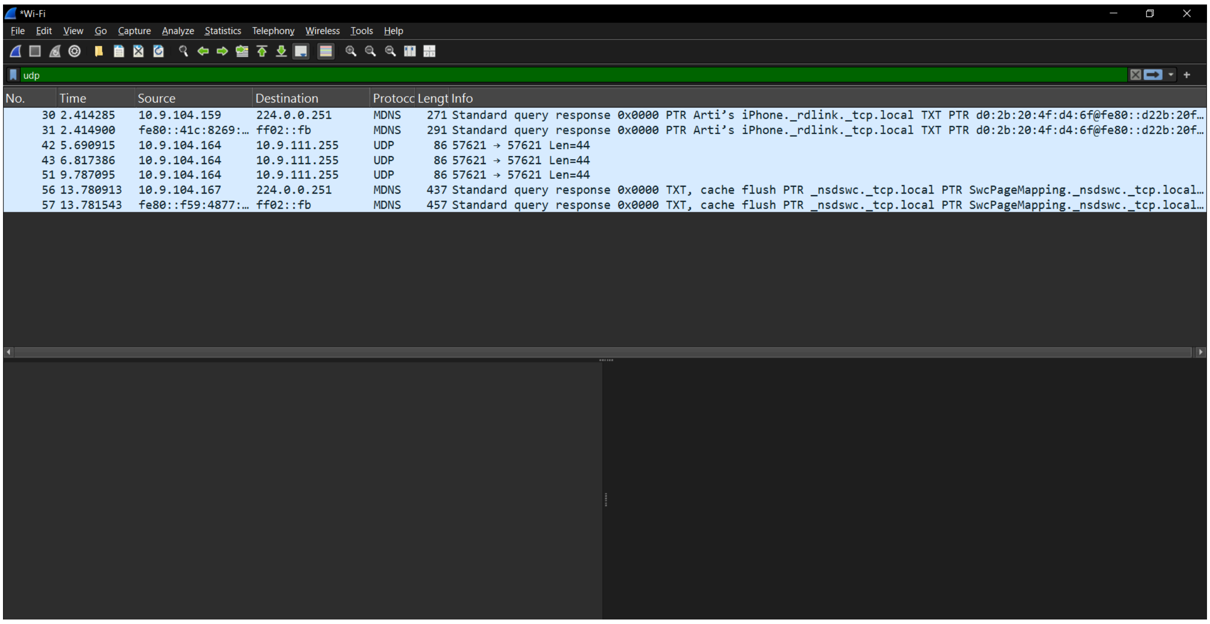
Procedure

1. Open **Wireshark** and start a capture on your active network interface.
2. **Generate TCP traffic:**
    - Open a web browser and visit any website (HTTP/HTTPS).
    - In Wireshark, apply the filter: ‘tcp’
    - Observe fields like **Source Port, Destination Port, Sequence Number, Acknowledgment, Flags (SYN, ACK, FIN)**.
3. **Generate UDP traffic:**
    - Open Command Prompt and use a DNS query: ‘nslookup www.google.com’
    - In Wireshark, apply the filter: ‘udp’
    - Observe fields like **Source Port, Destination Port, Length, Checksum**.
4. Stop the capture and compare the structure of TCP and UDP packets.

Observation in Wireshark:



TCP



UDP

Result: Using Wireshark, TCP packets were observed with handshake and acknowledgment fields, while UDP packets showed simple headers without connection setup. This confirms TCP is reliable and connection-oriented, whereas UDP is fast and connectionless.

<u>Practical - 3</u>

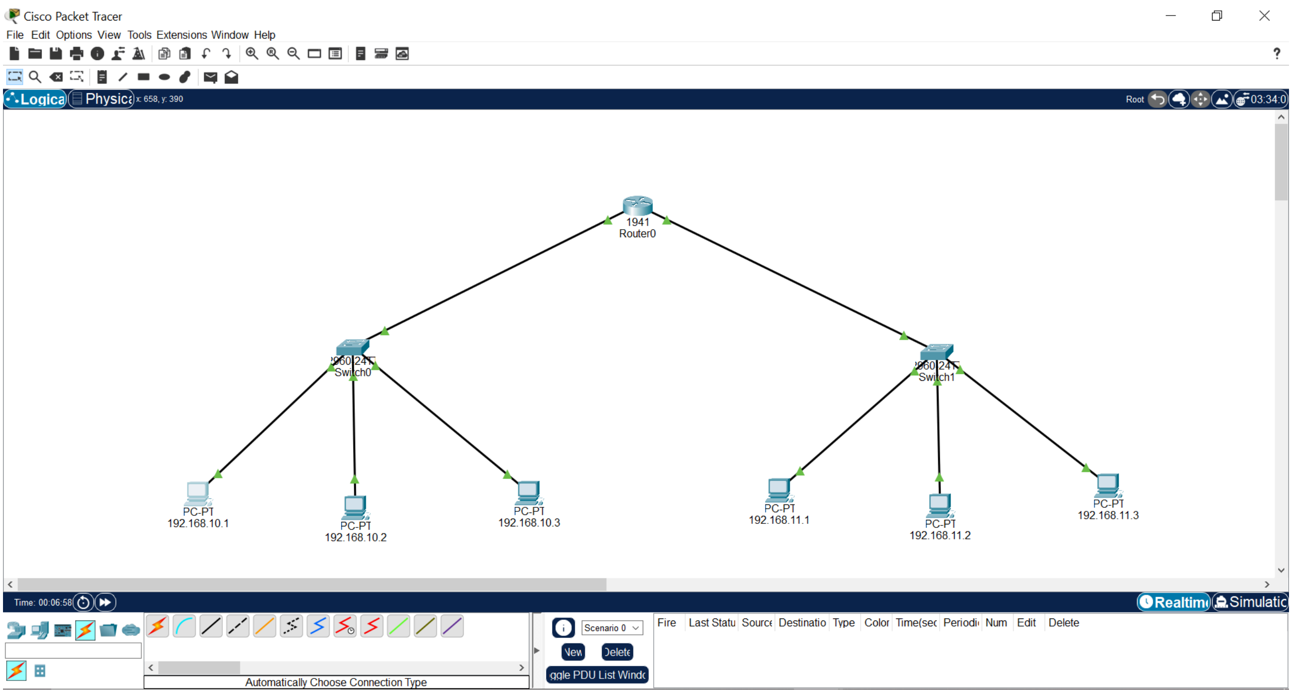
Aim: To examine and verify a device's default gateway in a network.

Network Topology Devices

- **1 Router** (gateway)
- **2 Switches** (Switch0, Switch1)
- **6 PCs** (PC0–PC5)
- Copper Straight-Through cables everywhere

Network Setup:

Device	IP Address	Subnet Mask	Default Gateway
PC0	192.168.10.1	255.255.255.0	192.168.10.100
PC1	192.168.10.2	255.255.255.0	192.168.10.100
PC2	192.168.10.3	255.255.255.0	192.168.10.100
PC3	192.168.11.1	255.255.255.0	192.168.11.100
PC4	192.168.11.2	255.255.255.0	192.168.11.100
PC5	192.168.11.3	255.255.255.0	192.168.11.100



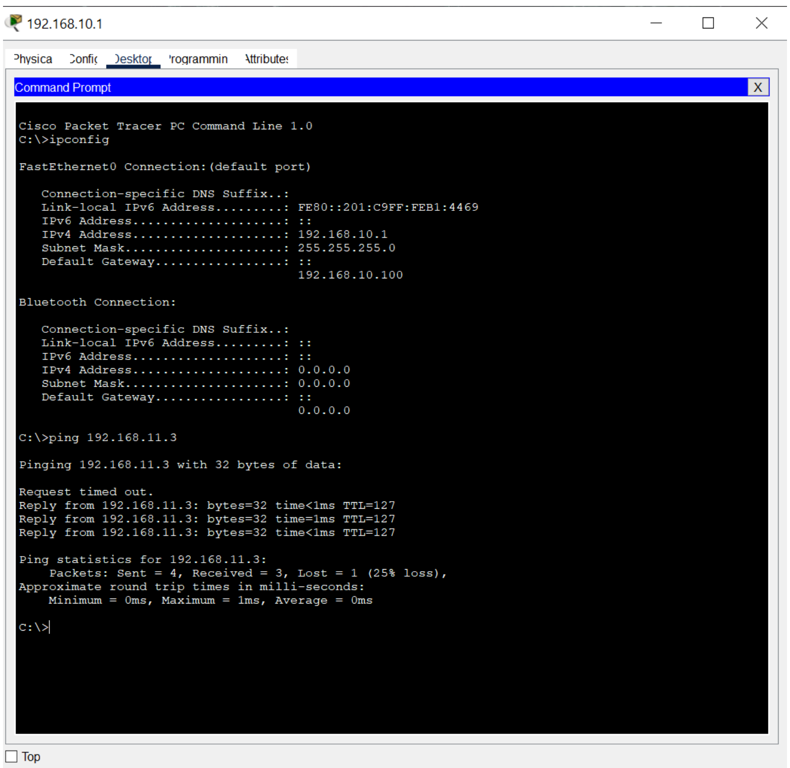
Procedure:

1. Open Cisco Packet Tracer and create the topology as shown in the network setup diagram:
    - 1 Router connected to Switch0 and Switch1
    - 3 PCs (PC0–PC2) connected to Switch0
    - 3 PCs (PC3–PC5) connected to Switch1
2. Use Copper Straight-Through cables for all connections.
3. **Configure Router (Gateway)**:
    - On Router

      → FastEthernet0/0 → Assign IP: 192.168.10.100, Subnet: 255.255.255.0
      →FastEthernet0/1 → Assign IP: 192.168.11.100, Subnet: 255.255.255.0

    - Turn **Port Status: On**.
4. Assign IP & Gateway to each PC according to the network setup.
5. **Verify the Gateway:**
    - On any PC(connected to Switch0) → Desktop → Command Prompt: Enter: ipconfig→ping 192.168.11.1

Output:



Result: All PCs successfully pinged through the router,confirming the gateway worked.

<u>Practical - 4</u>

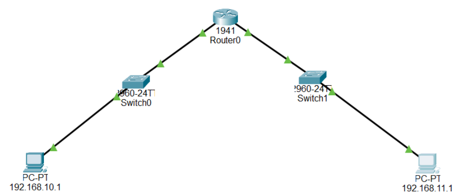
Aim: To study and verify network connectivity using **Ping** and **Traceroute** using *ping* and *tracert* commands, and to display routing information using the *show ip route* command in Cisco Packet Tracer.

Network Topology Devices

- **1 Router** (gateway)
- **2 Switches** (Switch0, Switch1)
- **2 PCs** (PC0, PC1)
- Copper Straight-Through cables everywhere

Network Setup:

Device	IP Address	Subnet Mask	Default Gateway
PC0	192.168.10.1	255.255.255.0	192.168.10.100
PC1	192.168.11.1	255.255.255.0	192.168.11.100



Procedure:
1. Open Cisco Packet Tracer and create a new project.
2. Place the required devices from the device list:

- 2 PCs
- 2 Switches
- 1 Router
- Copper Straight-through cables

3. Connect the devices using cables:

- Connect **PC0** → **Switch0** using a Straight-through cable
- Connect **Switch0** → **Router0 (G0/0)** using a Straight-through cable
- Connect **Router0 (G0/1)** → **Switch1** using a Straight-through cable
- Connect **Switch1** → **PC1** using a Straight-through cable

4. Assign IP addresses to PCs:

- Open **PC0 → Desktop → IP Configuration**
  - IP: 192.168.10.1
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.100
- Open **PC1 → Desktop → IP Configuration**
  - IP: 192.168.11.1
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.11.100

5. Configure Router Interfaces:

Select router → CLI tab

Enter the following commands:

```
enable
configure terminal
interface g0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface g0/1
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
end
```

6. Check Router Routing Table:

```
show ip route
```

7. Test connectivity using Ping:
On **PC1**, open Command Prompt and type:

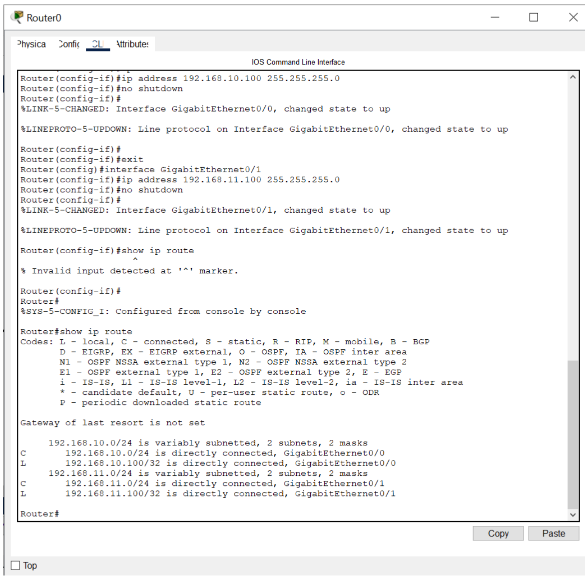
```
ping 192.168.10.1
```

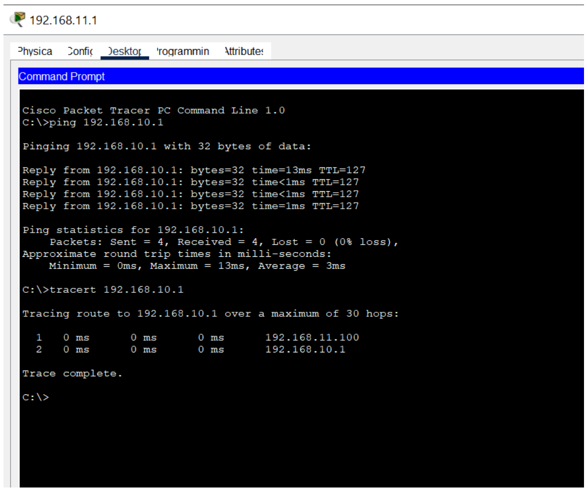
8. Use Traceroute to view network path:
On **PC1**, type:

```
tracert 192.168.10.1
```

9. Observe results—successful ping replies and traceroute hop display confirm correct routing.

Output:





Result:

Ping and traceroute were successfully executed between PC1 and PC2 through the router and switch.

The show ip route command displayed the connected networks, proving that routing and connectivity worked correctly.

Practical - 5

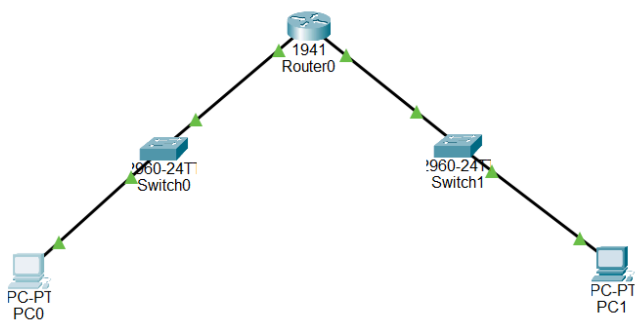
Aim: To examine **ICMP (Internet Control Message Protocol) packets** by generating ping traffic and analyzing packet flow in Cisco Packet Tracer using the simulation mode.

Network Topology Devices

Components	Quantity
PCs	2
Switch	1
Router	1
Copper straight-through cables	As required

Network Setup

Device	Interface	IP Address	Subnet Mask	Gateway
PC0	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.10	255.255.255.0	192.168.2.1
Router	G0/0	192.168.1.1	255.255.255.0	–
Router	G0/1	192.168.2.1	255.255.255.0	–



Procedure

Step 1: Create Network Topology

1. Open **Cisco Packet Tracer**
2. Drag 2 PCs, 1 Router, and 1 Switch.
3. Connect:
   - PC0 → Switch (straight-through)
   - PC1 → Switch (straight-through)
   - Switch → Router interface G0/0 and G0/1

Step 2: Configure IP Addresses

On PC0

Desktop → IP Configuration:

```
IP: 192.168.1.10
Mask: 255.255.255.0
Gateway: 192.168.1.1
```

On PC1

```
IP: 192.168.2.10
Mask: 255.255.255.0
Gateway: 192.168.2.1
```

Step 3: Configure Router

Open CLI:

```
Router> enable
Router# configure terminal
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface g0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

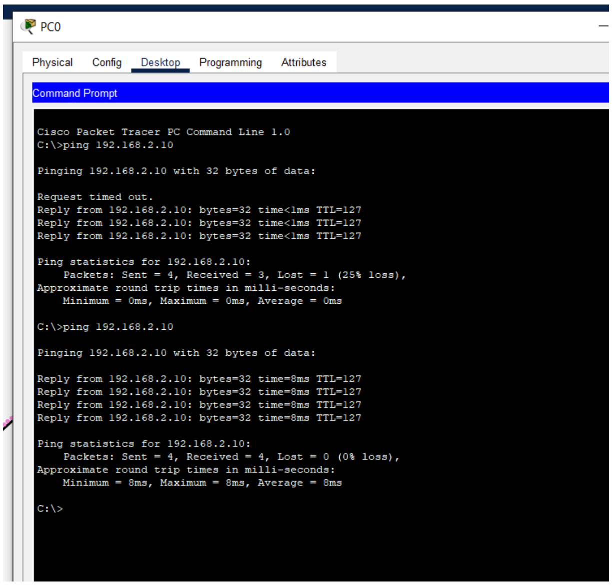
Step 4: Use Simulation Mode to Observe ICMP Packets

1. Click **Simulation Mode** (bottom right)
2. Select **ICMP** from the Event Filters

   On **PC1**, open Command Prompt: `ping 192.168.2.10`

3. Observe the packet movement frame-by-frame.
4. Click **Play** or **Capture/Forward** to view each stage.

Output:



On Simulation Screen

- ICMP **Echo Request** packet travels **PC0** →**Switch** →**Router**→**Switch** →**PC1**
- ICMP **Echo Reply** packet returns **PC1** →**Switch** → **Router** →**Switch** →**PC0**
- Packet type is shown as ICMP with colored arrows

Result: ICMP packet behavior was successfully examined. The Echo Request and Echo Reply packets were visualized during transmission across the router using simulation mode in Cisco Packet Tracer.

Practical-6

Aim: To understand and perform **IPv4 Address Subnetting** by dividing a large network into smaller subnetworks for efficient utilization of IP addresses.

Theory: Subnetting is the process of dividing a single large IP network into multiple smaller logical networks. It helps in:

- Better network management
- Improved security
- Reduced broadcast traffic
- Efficient usage of IP addresses

IPv4 addresses include **Network Portion + Host Portion**, determined by the Subnet Mask.

Given Problem

Network Address: **192.168.1.0 /24**
Requirement: **4 Subnets**

Steps to Calculate Subnets

Step 1: Determine number of bits to borrow

To create 4 subnets:

```
2^n ≥ 4
n = 2 bits
```

So borrow **2 bits** from the host portion.

Step 2: New Subnet Mask

Original mask: /24
Borrowed 2 bits: /24 + 2 = **/26**

Subnet mask for /26 = **255.255.255.192**

Step 3: Calculate Subnet Increment

Formula:`256 − 192 = 64`

Therefore, each subnet increases by 64.

Step 4: Create Subnet Table

Subnet No.	Network ID	First Usable Host	Last Usable Host	Broadcast Address
1	192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127
3	192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191
4	192.168.1.192	192.168.1.193	192.168.1.254	192.168.1.255

Example Host Assignment

Device	IP Address	Subnet Mask	Gateway
PC1	192.168.1.10	255.255.255.192	192.168.1.1
PC2	192.168.1.50	255.255.255.192	192.168.1.1
PC3	192.168.1.70	255.255.255.192	192.168.1.65
PC4	192.168.1.130	255.255.255.192	192.168.1.129

Result

Subnetting for the network **192.168.1.0/24** was successfully performed. Four subnets were created with a subnet mask of **255.255.255.192 (/26)**, and the Network ID, Broadcast address, and valid host ranges were calculated.

Conclusion

Subnetting divides a large network into smaller networks, improving IP utilization, security, and performance.

Practical-7

Aim: To perform IPv4 subnetting and configure a router to enable communication between different subnets.

Network Topology Devices

Components	Quantity
Router	1
Switches	**2**
PCs	4
Copper straight-through cables	As required

Network Address Information

Given Network: **192.168.10.0 /24**
Required: **4 Subnets**

Subnetting Calculation

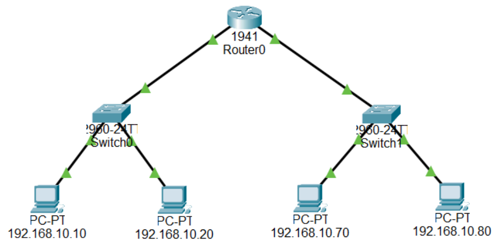
Borrow bits: $2^n \ge 4 \rightarrow n = 2$ bits

New Prefix:

```
/24 + 2 = /26
Subnet Mask = 255.255.255.192
Increment = 64
```

Subnet Table & Network Setup

Subnet	Network ID	First Host	Last Host	Broadcast Address
1	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63
2	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
3	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
4	192.168.10.192	192.168.10.193	192.168.10.254	192.168.10.255



IP Address Assignment

Device	IP Address	Subnet Mask	Default Gateway
PC1	192.168.10.10	255.255.255.192	192.168.10.1
PC2	192.168.10.20	255.255.255.192	192.168.10.1
PC3	192.168.10.70	255.255.255.192	192.168.10.65
PC4	192.168.10.80	255.255.255.192	192.168.10.65
Router G0/0	192.168.10.1	255.255.255.192	—
Router G0/1	192.168.10.65	255.255.255.192	—

Procedure

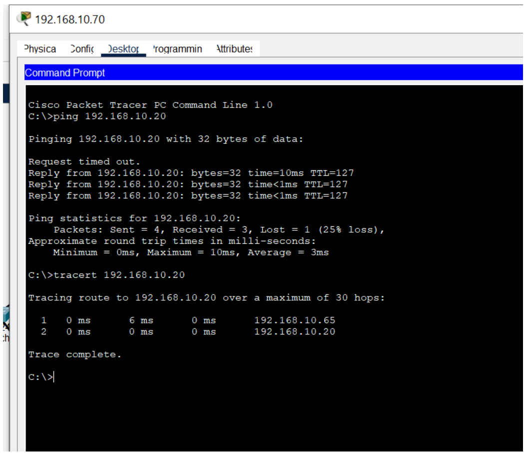
1. Subnet the given network (192.168.10.0/24) into 4 subnets.
2. Create the network topology using: 1 Router, **2 Switches**, and 4 PCs.
3. Connect PC1 & PC2 to Switch 1, and PC3 & PC4 to Switch 2.
4. Connect both switches to the router using straight-through cables.
5. Assign IP addresses to PCs according to subnet table.
6. Open router CLI and configure router interfaces:

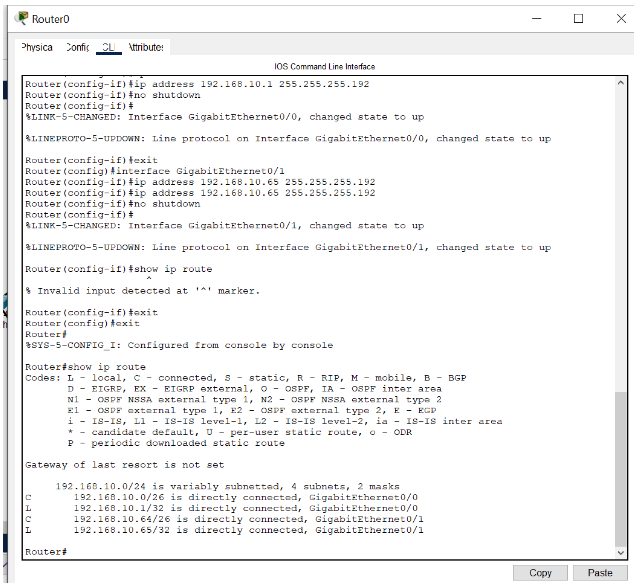
```
Router> enable

Router# configure terminal

Router(config)# interface g0/0

Router(config-if)# ip address 192.168.10.1
255.255.255.192
```

```
Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface g0/1

Router(config-if)# ip address 192.168.10.65
255.255.255.192

Router(config-if)# no shutdown
```

7. Verify router routing table: `Router# show ip route`
8. Test communication: On PC3 using *ping 192.168.10.20*

Output:





Result: Subnetting was successfully implemented and router interfaces were configured. Devices from different subnets communicated successfully through the router.