Department of Computer Science and Engineering,
Anna University, Chennai- 600025
CS23502– NETWORKS AND DATA COMMUNICATION
End Sem Practical
July- Oct 2026
Year/Sem/Batch : III/V/ N

22- 10- 2026

1. Packet tracer Tool

Connect two PCs with a crossover cable and verify connectivity using the ping command.

Steps:

1. Open Packet Tracer.
2. Drag and drop **two PCs** onto the workspace.
3. Connect them with a **crossover cable**.
4. Assign IP addresses:
5. PC1: 192.168.1.1 / 255.255.255.0
6. PC2: 192.168.1.2 / 255.255.255.0
7. Use the **Command Prompt** on PC1 and run:
8. ping 192.168.1.2
9. You should get successful replies.

Connect multiple PCs to a switch and ensure they can communicate.

Steps:

1. Place **1 switch** and **3 PCs** on the workspace.
2. Connect each PC to the switch using **copper straight-through cables**.
3. Assign IPs:
   - PC1: `192.168.10.1`
   - PC2: `192.168.10.2`
   - PC3: `192.168.10.3`
4. Ping each PC from the others.

Use a router to connect two different networks and allow communication between them.

Steps:

1. Place **1 router** and **2 PCs**.
2. Connect:
   - PC1 to Router's FastEthernet0/0
   - PC2 to Router's FastEthernet0/1
3. Assign IPs:
   - Router fa0/0: `192.168.1.1`
   - Router fa0/1: `192.168.2.1`
   - PC1: `192.168.1.2` (Gateway: `192.168.1.1`)
   - PC2: `192.168.2.2` (Gateway: `192.168.2.1`)
4. Use the CLI to enable router interfaces:

```
enable
configure terminal
interface fa0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface fa0/1
ip address 192.168.2.1 255.255.255.0
no shutdown
```

5. Test connectivity using ping.

Use a DHCP server to automatically assign IP addresses to clients.

Steps:

1. Place **1 DHCP server**, **1 switch**, and **2 PCs**.
2. Connect all devices to the switch.
3. Configure the DHCP server with:
   - IP: `192.168.100.1`
   - Subnet: `255.255.255.0`
   - Pool Range: `192.168.100.10 - 192.168.100.50`
   - Default Gateway: `192.168.100.1`
4. Set the PCs to get IP via **DHCP (automatic)**.
5. Verify the PCs receive IPs and can `ping` each other.

Access a web page hosted on a local web server.

Steps:

1. Place **1 web server**, **1 switch**, and **1 PC**.
2. Connect them via the switch.
3. Assign:
   - Web Server: `192.168.0.10`
   - PC: `192.168.0.2` (Gateway not needed in this LAN)
4. On the web server, configure the HTTP service (default is ON).
5. On the PC, open the **Web Browser** and enter:
6. `http://192.168.0.10`
7. You should see a test page.

Connect two LANs (representing two branch offices) using a **WAN link (serial connection)** between routers, and enable full communication between PCs in each LAN.

2. Wireshark

Capture TCP packets and observe connection establishment and termination

- Start a Wireshark capture on your active network interface (Wi-Fi or Ethernet).
- Generate some TCP traffic, for example by opening a website or connecting with `telnet`/`curl`.
- Filter with `tcp`, then find and identify:
    - **Connection establishment (three-way handshake):**
        1. Client sends `SYN`
        2. Server replies `SYN, ACK`
        3. Client sends `ACK`
    - **Connection termination (four-way handshake):**
        1. One side sends `FIN, ACK`
        2. The other side sends `ACK`
        3. The other side sends its own `FIN, ACK`
        4. The first side sends the final `ACK`

    Sometimes termination is abrupt, with a `RST` packet instead of a clean FIN exchange. Note this if you see it.

- Note the sequence numbers, acknowledgment numbers, flags, and window size in each packet. Right-click a packet and choose **Follow → TCP Stream** to view one whole connection.

2. Filter packets based on an IP address
Use display filters in the filter bar:

- `ip.addr == 192.168.1.5` (traffic to or from that address)
- `ip.src == 192.168.1.5` (only from)
- `ip.dst == 142.250.77.46` (only to)
- Combine them: `ip.addr == 142.250.77.46 && tcp`