LAB 9 : Wireless Network Setup & Packet Analysis using Cisco Packet Tracer:

➢ Objectives:

1. To configure wireless router and connect laptops via Wi-Fi.
2. To analyze packet flow in wireless communication.

➢ Software Requirement:

- Cisco Packet Tracer (any recent version)
- Windows/Linux PC

➢ Theory:

1. Wireless Networks:

A **Wireless Network (WLAN)** allows devices to communicate without physical cables, using radio waves. The main components include:

Key Components:

1. **Access Point (AP) / Wireless Router:**
    - Acts as a central hub for wireless devices.
    - Broadcasts the **SSID (network name)**.
    - Can manage security (WPA2/WPA3) and assign IP addresses via DHCP.
2. **Wireless Clients:**
    - Devices like laptops, smartphones, IoT devices that connect to the WLAN.
3. **Router / Gateway:**
    - Connects the WLAN to other networks or the internet.
4. **DHCP Server:**
    - Assigns IP addresses automatically to devices joining the network.

Steps to Set Up a Wireless Network:

1. **Placing the Access Point:**
    - Choose a central location to ensure even coverage.
    - Avoid obstacles like thick walls or metal objects that interfere with signals.
2. **Configuring the SSID (Network Name):**
    - Set a recognizable SSID for easy identification.

    - Example: Office_WiFi or HomeNetwork.
3. **Setting Security:**
    - Use **WPA2** or **WPA3** encryption.
    - Set a strong password to prevent unauthorized access.
4. **IP Address Assignment (DHCP):**
    - Enable DHCP on the router or AP so devices automatically receive:
        - IP Address
        - Subnet Mask
        - Default Gateway
        - DNS Server
5. **Connecting Devices:**
    - Search for the SSID on the device.
    - Enter the password and obtain an IP address via DHCP.
6. **Testing Connectivity:**
    - Use `ping` commands to check if devices can communicate with each other or with the gateway.
    - Ensure internet access if required.

2. Packet Analysis

Packet Analysis is the process of capturing and inspecting network traffic to monitor, troubleshoot, or secure a wireless network.

Key Concepts:

1. **Packets:**
    - Basic units of data transmitted over a network.
    - Each packet contains:
        - **Header:** Source & destination IP, protocol type, sequence info.
        - **Payload:** Actual data being sent.
2. **Protocols in Wireless Networks:**
    - **802.11 (Wi-Fi)**: Wireless networking standard.
    - **TCP/IP**: Manages communication between devices.
    - **DHCP**: Assigns IP addresses.
    - **ARP**: Resolves MAC addresses.
3. **Tools for Packet Analysis:**
    - **Wireshark**: Captures live network traffic and displays detailed packet info.
    - **tcpdump**: Command-line tool for packet capture.
    - **Aircrack-ng**: Can analyze Wi-Fi traffic and security.

Steps for Packet Analysis:

1. **Capturing Packets:**
    - Put the network interface in **promiscuous mode** to capture all packets.

   - Use tools like Wireshark to start capturing traffic on the wireless interface.

2. **Filtering Traffic:**
   - Filter packets by:
     - IP address (`ip.addr == 192.168.1.5`)
     - Protocol (`tcp`, `udp`, `icmp`)
     - Port number (`tcp.port == 80`)
3. **Analyzing Packets:**
   - Examine headers for:
     - Source and destination MAC and IP addresses.
     - Protocol type and sequence numbers.
     - Errors or dropped packets.
   - Analyze payloads if not encrypted (e.g., HTTP vs HTTPS).
4. **Security & Troubleshooting:**
   - Detect unauthorized devices.
   - Check for packet loss, latency, or network congestion.
   - Identify suspicious activity like ARP spoofing or rogue access points.

3. Wireless Network Setup + Packet Analysis Example

Imagine a small office network:

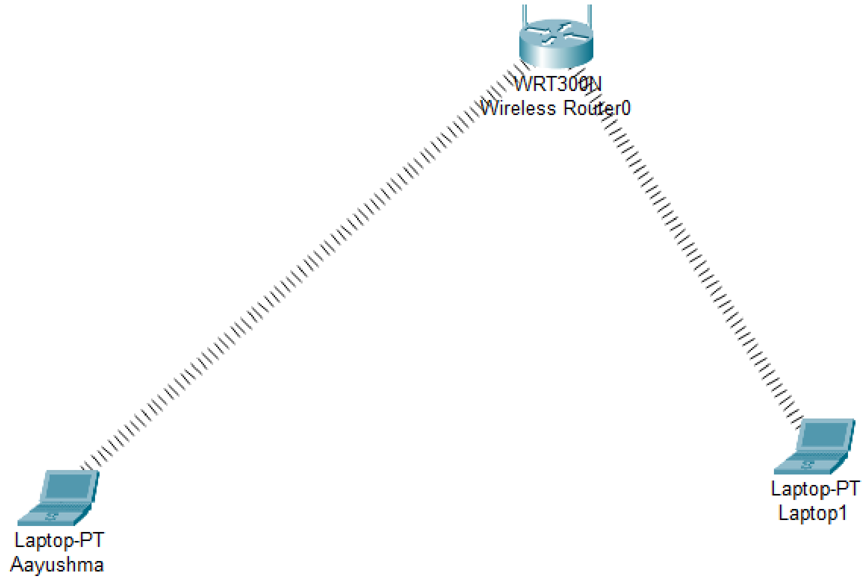
- **AP:** WRT300N router
- **SSID:** `OfficeWiFi`
- **Security:** WPA2, strong password
- **DHCP:** Enabled

Packet Analysis Steps:

1. Connect a laptop to the Wi-Fi network.
2. Open Wireshark → select Wi-Fi interface → start capture.
3. Ping the server → ICMP packets appear.
4. Check TCP packets → verify data from client to server.
5. Detect any unauthorized device → check MAC addresses.

➢ Network Topology:

Wireless Router 0↔Aayushma, Laptop1 (Wireless connection)



➢ Steps:Wireless Router Configuration

Step 1: Basic Setup

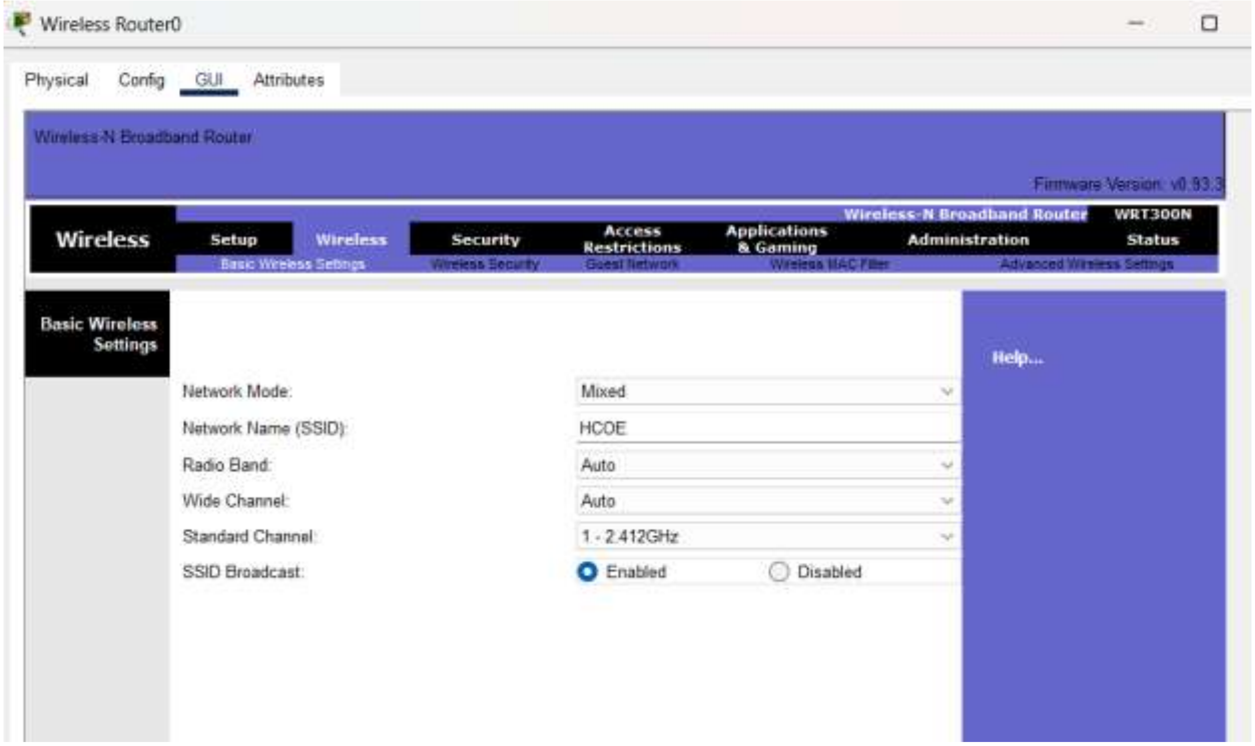
- Click on the Wireless Router.
- Go to GUI → Setup.
- Configure the following:
    - o IP Address: 192.168.0.1
    - o Subnet Mask: 255.255.255.0
    - o DHCP Server: Enabled

Step 2: Wireless Configuration

- Go to Wireless → Basic Wireless Settings.
- Configure the following parameters:
    - o Network Mode: Mixed
    - o Network Name (SSID): HCOE

o Channel: Auto

• Click **Save Settings**



Network Mode: Mixed

Network Name (SSID): HCOE

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ● Enabled ○ Disabled

Step 3: Wireless Security

• Go to Wireless → Wireless Security.

• Configure the following:

o Security Mode: WPA2-Personal

o Encryption: AES

o Passphrase: hcoe@123

• Click **Save Settings**

➢ Steps: Laptop Configuration

Step 1: Check Physical Wireless Adapter (If Needed)

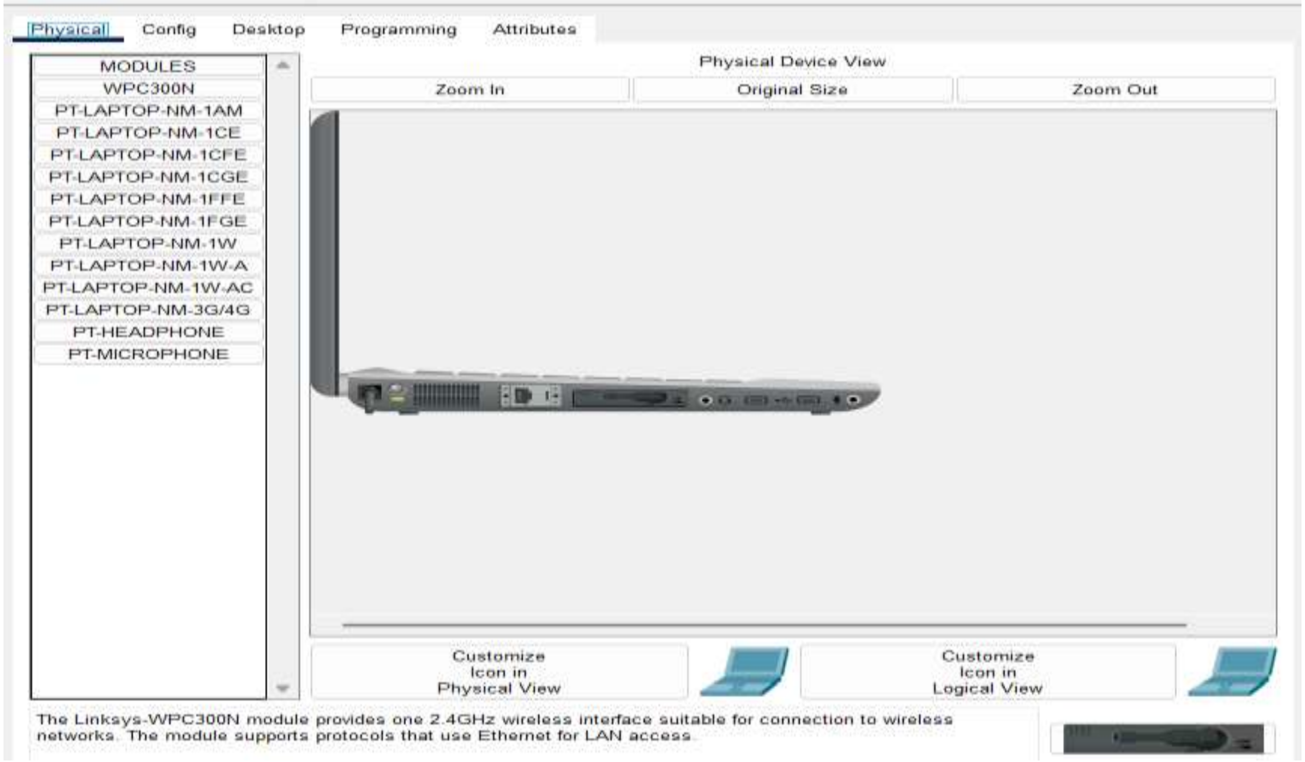
• Click on the Laptop

• Go to the Physical tab.

• Verify if the Wireless Network Adapter is installed (WPC300N Wireless Card).

• If not installed, drag and drop a Wireless Network Adapter into the laptop.

• Ensure the adapter is powered on (green light).

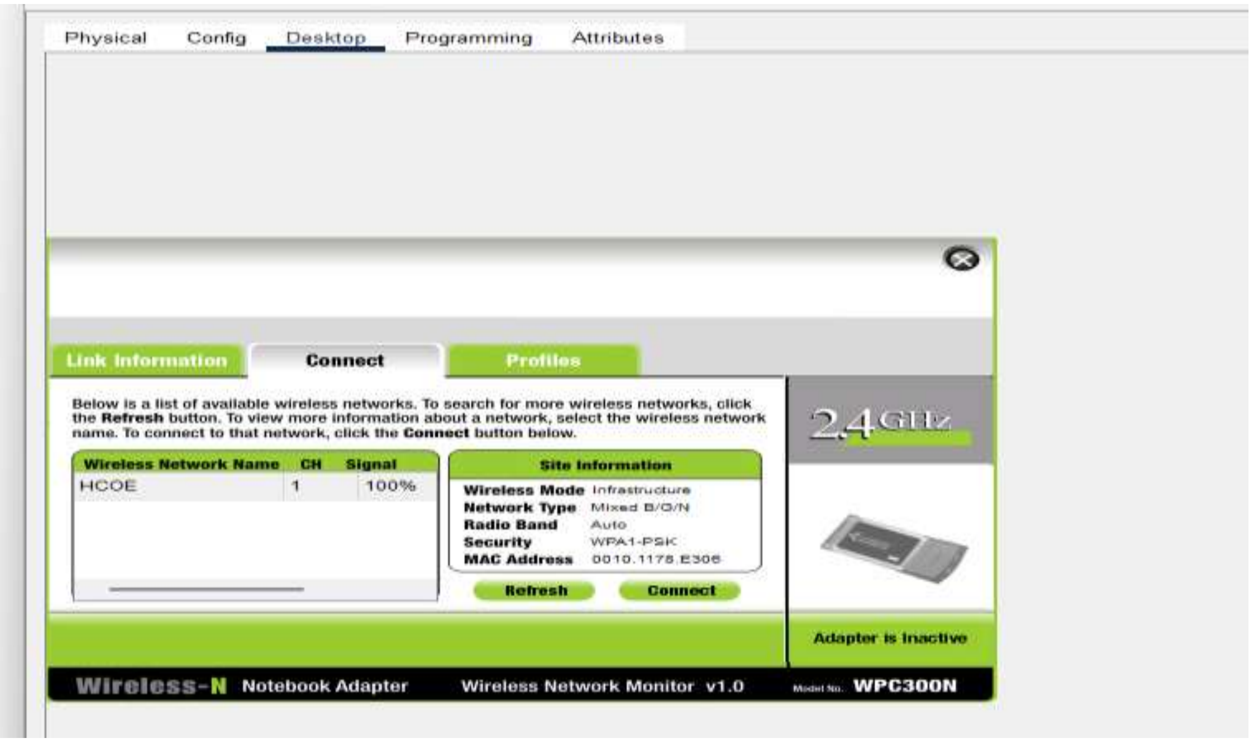


MODULES
- WPC300N
- PT-LAPTOP-NM-1AM
- PT-LAPTOP-NM-1CE
- PT-LAPTOP-NM-1CFE
- PT-LAPTOP-NM-1CGE
- PT-LAPTOP-NM-1FFE
- PT-LAPTOP-NM-1FGE
- PT-LAPTOP-NM-1W
- PT-LAPTOP-NM-1W-A
- PT-LAPTOP-NM-1W-AC
- PT-LAPTOP-NM-3G/4G
- PT-HEADPHONE
- PT-MICROPHONE

The Linksys-WPC300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

Step 2: Accessing Wireless Network

- Go to Desktop → PC Wireless.
- Click on Connect to a Network.



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
HCOE	1	100%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA1-PSK
MAC Address	0010.1178.E306

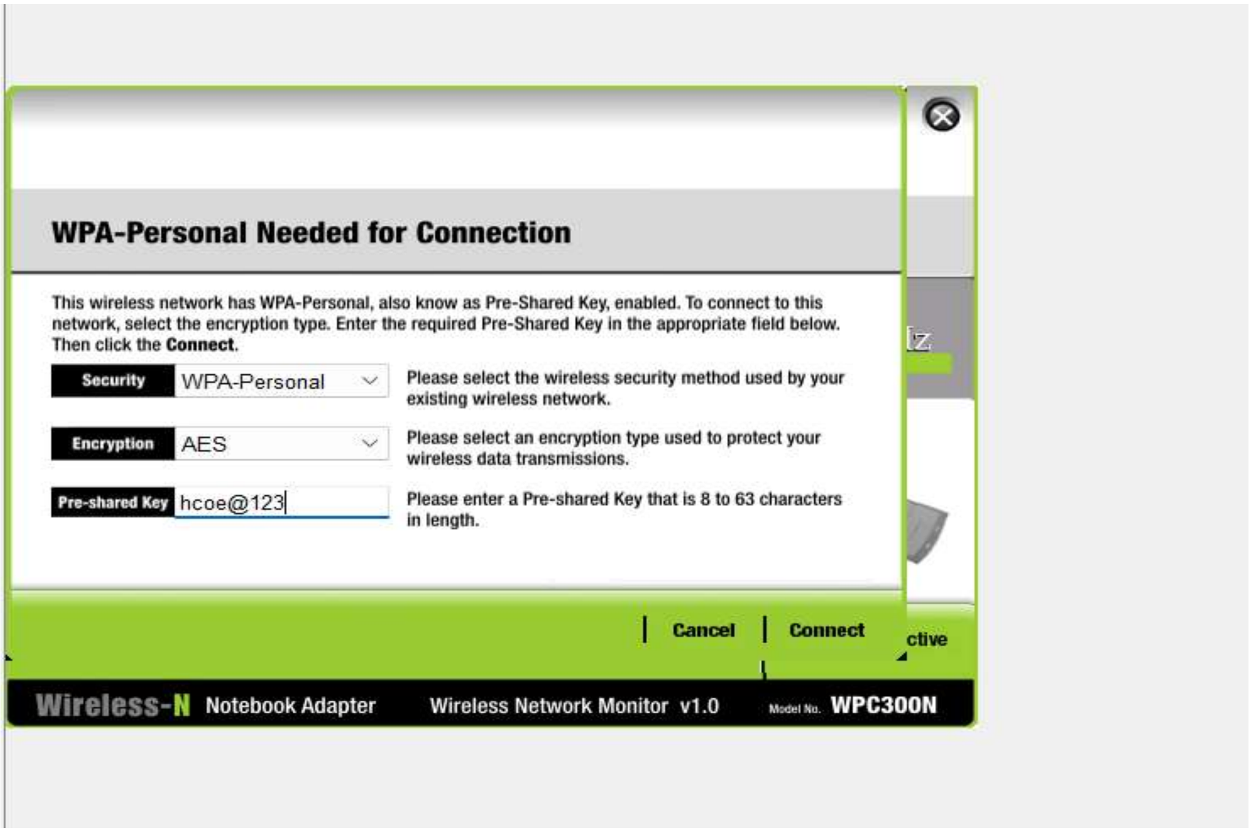
Adapter is Inactive

Step 3: Selecting the Network

- From the list of available networks, select the SSID: HCOE.
- Click Connect.

Step 4: Entering Security Details

- Enter the Passphrase: hcoe@123.
- Ensure the connection shows Successful or Connected.



WPA-Personal Needed for Connection

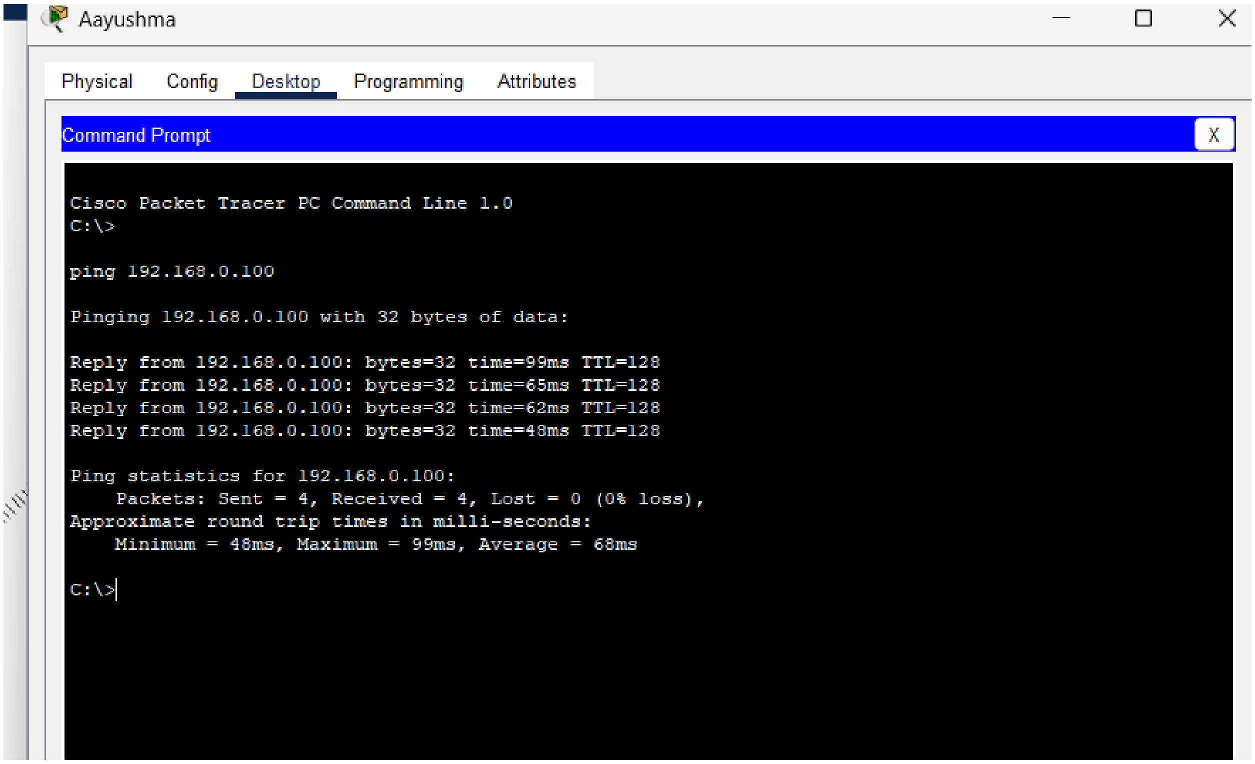
This wireless network has WPA-Personal, also know as Pre-Shared Key, enabled. To connect to this network, select the encryption type. Enter the required Pre-Shared Key in the appropriate field below. Then click the **Connect**.

Security	WPA-Personal	Please select the wireless security method used by your existing wireless network.
Encryption	AES	Please select an encryption type used to protect your wireless data transmissions.
Pre-shared Key	hcoe@123	Please enter a Pre-shared Key that is 8 to 63 characters in length.

Step 5: Verifying Connectivity

- Go to Desktop → IP Configuration.
- Ensure the laptop has received an IP Address automatically from the router
- Test connectivity using Command Prompt:

  ping 192.168.0.100 (to check connection to the router)



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

ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=99ms TTL=128
Reply from 192.168.0.100: bytes=32 time=65ms TTL=128
Reply from 192.168.0.100: bytes=32 time=62ms TTL=128
Reply from 192.168.0.100: bytes=32 time=48ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 99ms, Average = 68ms

C:\>
```

➢ Result:

The wireless network in Cisco Packet Tracer was successfully set up using a WRT300N router with IP 192.168.0.1, subnet mask 255.255.255.0, and an active DHCP server. A wireless network with SSID "HCOE" was secured with WPA2-Personal, AES encryption, and the passphrase "hcoe@123", allowing Aayushma and Laptop1 to connect automatically via their WPC300N adapters and receive IP addresses from DHCP. Network connectivity was confirmed with successful ping tests to the gateway (192.168.0.100) showing 0% packet loss.

➢ Discussion and Conclusion:

In this lab, we set up a wireless network to enable devices to communicate without physical cables, providing mobility and reducing setup costs. We configured the router to act as both an Access Point and a DHCP server, allowing it to connect clients and manage the network efficiently. The network was identified using the SSID "HCOE," and performance was ensured by setting the router to Mixed mode on the 2.4 GHz band. We also secured the network with WPA2-Personal encryption to protect data from unauthorized access. Using Packet Tracer’s Simulation Mode, we were able to visualize packet flow and troubleshoot connectivity issues effectively. Overall, we observed that while wireless networks are flexible and convenient, they can be limited by signal interference and range compared to wired networks.