INDEX

EXPERIMENT 1

AIM:

To create a **wired Local Area Network (LAN)** setup in Cisco Packet Tracer, which includes a PC connected to a wireless router, which in turn is connected to a cable modem and ultimately to the Internet Cloud.

THEORY:

In networking, a wired LAN setup consists of various devices such as PCs, routers, and modems interconnected through cables. The router provides network connectivity to end devices like PCs and handles the routing of data packets. The cable modem facilitates communication with the Internet Service Provider (ISP) through the coaxial cable. Dynamic Host Configuration Protocol (DHCP) enables automatic IP address assignment to end devices.

PROCEDURE:

1. Start Cisco Packet Tracer and create a new project.
2. Add Network Devices:
   - From the 'End Devices' category, drag and drop a PC onto the workspace.
   - From the 'Network Devices' category, select and add a WRT300N wireless router.
   - From the 'WAN Emulation' category, add a Cable Modem to the workspace.
3. Rename Network Devices:
   - Click on each device and under the 'Config' tab, change the display name to the appropriate device type (e.g., PC, WirelessRouter0, CableModem1).
4. Cable the Devices:
   - Connect the PC to the Router using a copper straight-through cable.
   - Connect the Router's Internet interface to the Cable Modem using another copper straight-through cable.
   - Link the Cable Modem to the Cloud-PT using a coaxial cable.

5. Configure the PC:
   - Click on the PC and under the 'Desktop' tab, go to 'IP Configuration' to verify DHCP is enabled.

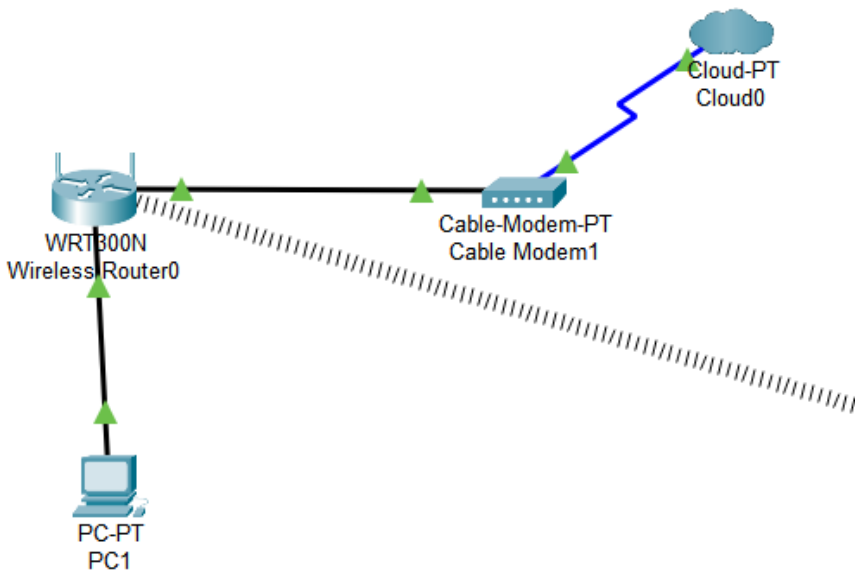
   - Use the 'Command Prompt' to issue an ipconfig /all command and confirm the PC has received an IP address within the 192.168.0.x range.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::204:9AFF:FE60:630B
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.102
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
```

6. Test connectivity by pinging the IP address of the Router.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Final Setup:



CONCLUSION:

In this experiment, a wired LAN was successfully created and configured in Cisco Packet Tracer. The PC was connected via Ethernet to the Wireless Router, which was in turn connected to a Cable Modem and the Internet Cloud. The PC received a dynamically assigned IP address from the router's DHCP server, and connectivity was verified through successful pinging of a test server. This setup demonstrates the fundamental aspects of a wired network and the process of dynamic IP address assignment.

EXPERIMENT 2

AIM:

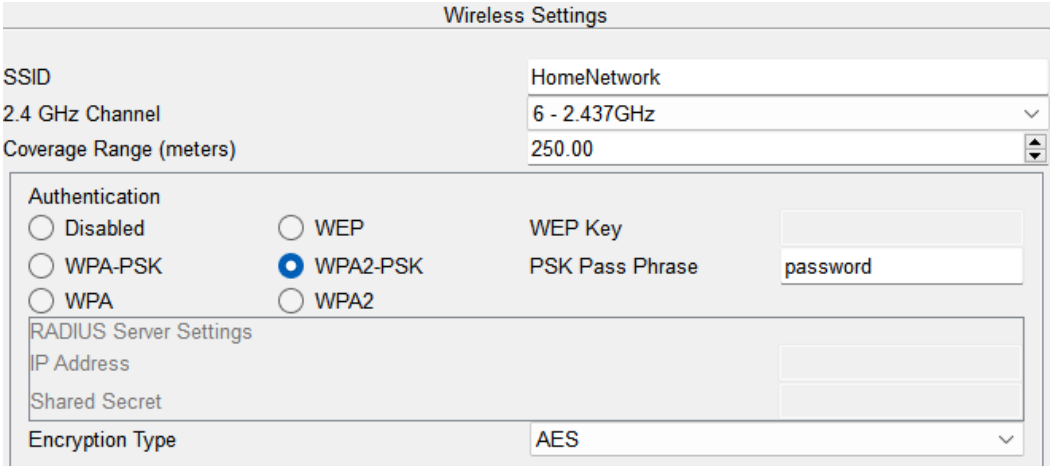
Create a wireless network topology in Cisco Packet Tracer, including a wireless router, wireless clients, and access points. Configure security settings and test connectivity.

THEORY:

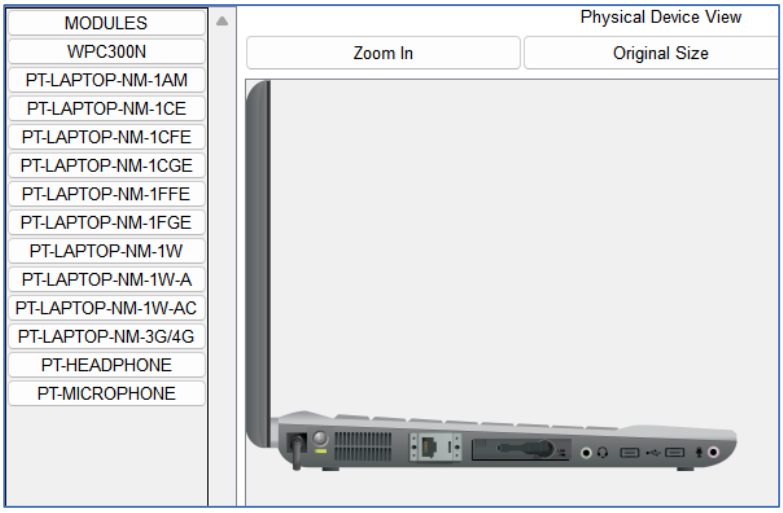
Wireless networking allows devices to connect to a network using radio waves instead of wires. The wireless router serves as an access point and provides IP addresses to the wireless clients. Security for wireless networks can be established using protocols such as WPA2-PSK to ensure that only authorized users can access the network. Testing connectivity through pinging ensures that network components are configured correctly and can communicate.

PROCEDURE:

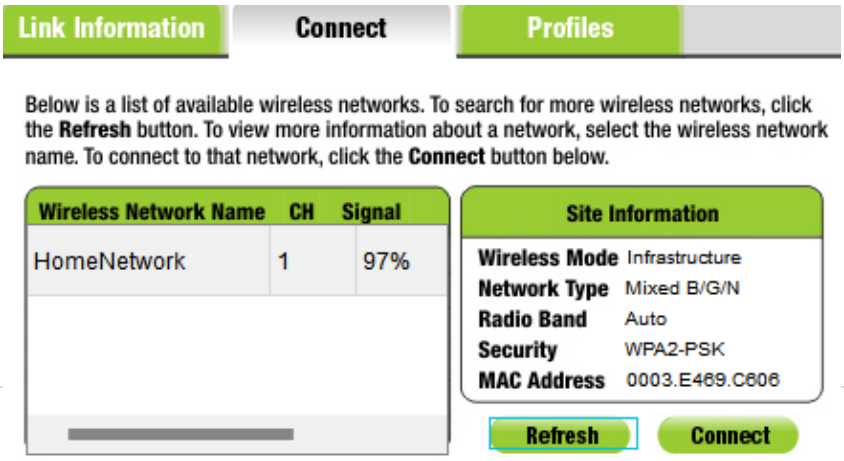
1. Open Cisco Packet Tracer and start a new project.
2. Build the Network:
   - From the 'End Devices' category, add a Laptop to the workspace.
   - From the 'Network Devices' category, select a WRT300N Wireless Router and place it in the workspace.
   - From the 'WAN Emulation' category, add a Cable Modem.
   - Finally, from the 'WAN Emulation' category, add the Cloud-PT to simulate internet connectivity.
3. Cabling:
   - Use a copper straight-through cable to connect the Wireless Router to the Cable Modem.
   - Attach a coaxial cable between the Cable Modem and the Cloud-PT to represent the connection to the Internet Service Provider.
4. Configure Wireless Security:
   - Click on the Wireless Router and navigate to the wireless settings.
   - Set up an SSID for the network, such as HomeNetwork.
   - Choose WPA2-PSK for security and set a strong passphrase.



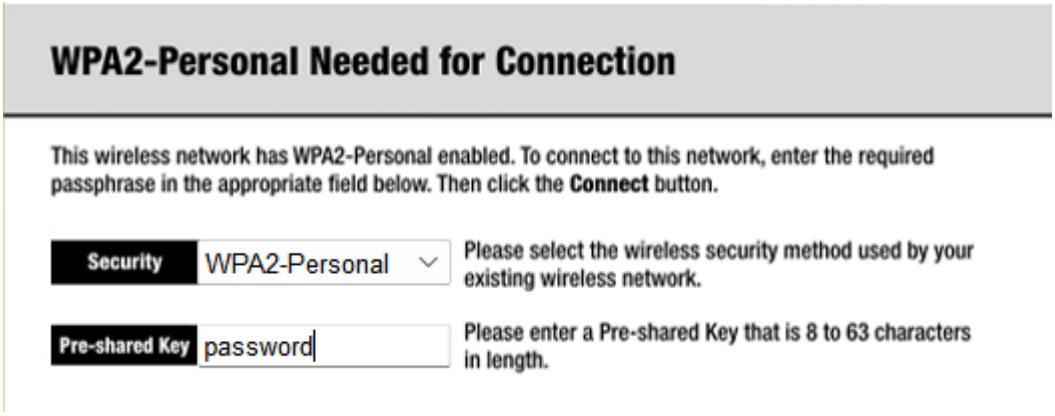
5. Prepare the Laptop for Wireless Connectivity:
   - Access the Laptop's physical tab.
   - Power off the Laptop, remove the Ethernet copper module, and replace it with a wireless WPC300N module.
   - Power on the Laptop to activate the wireless module.



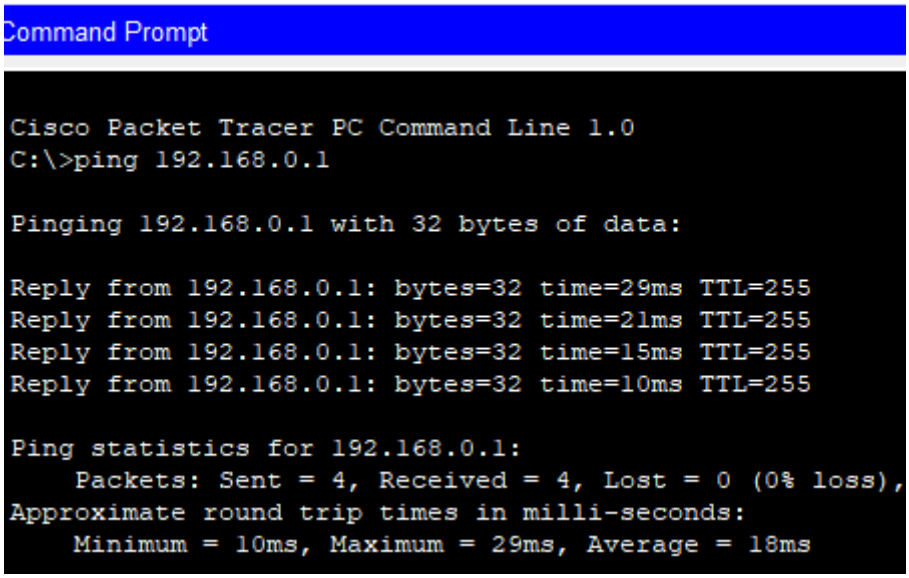
6. Connect the Laptop Wirelessly:
   - Click on the Laptop and go to the Desktop tab.
   - Open the PC Wireless application and search for available networks.



- Connect to the HomeNetwork SSID using the previously configured passphrase.

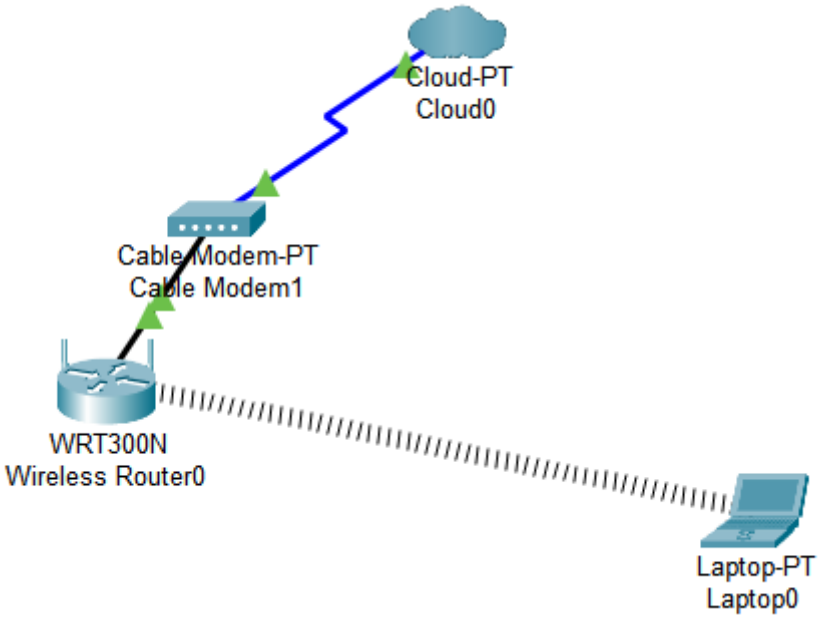


7. Verify Connectivity:
   - On the Laptop, open the Command Prompt and ping the Wireless Router's IP address to test connectivity. This will typically be 192.168.0.1.



   - A successful response indicates that the wireless connection is established and functional.

Final Setup:



CONCLUSION:

This experiment successfully established a wireless LAN in Cisco Packet Tracer, demonstrating the setup and configuration of a wireless network topology. By replacing the Ethernet module with a wireless NIC on the laptop and configuring it to connect to the WRT300N wireless router, network connectivity was achieved without the use of physical cables. The implementation of WPA2-PSK security ensured that the wireless network was secured against unauthorized access. The successful ping to the router's IP address from the laptop verified that the wireless client could communicate effectively over the network, thus achieving the experiment's objectives.

EXPERIMENT 3

AIM:

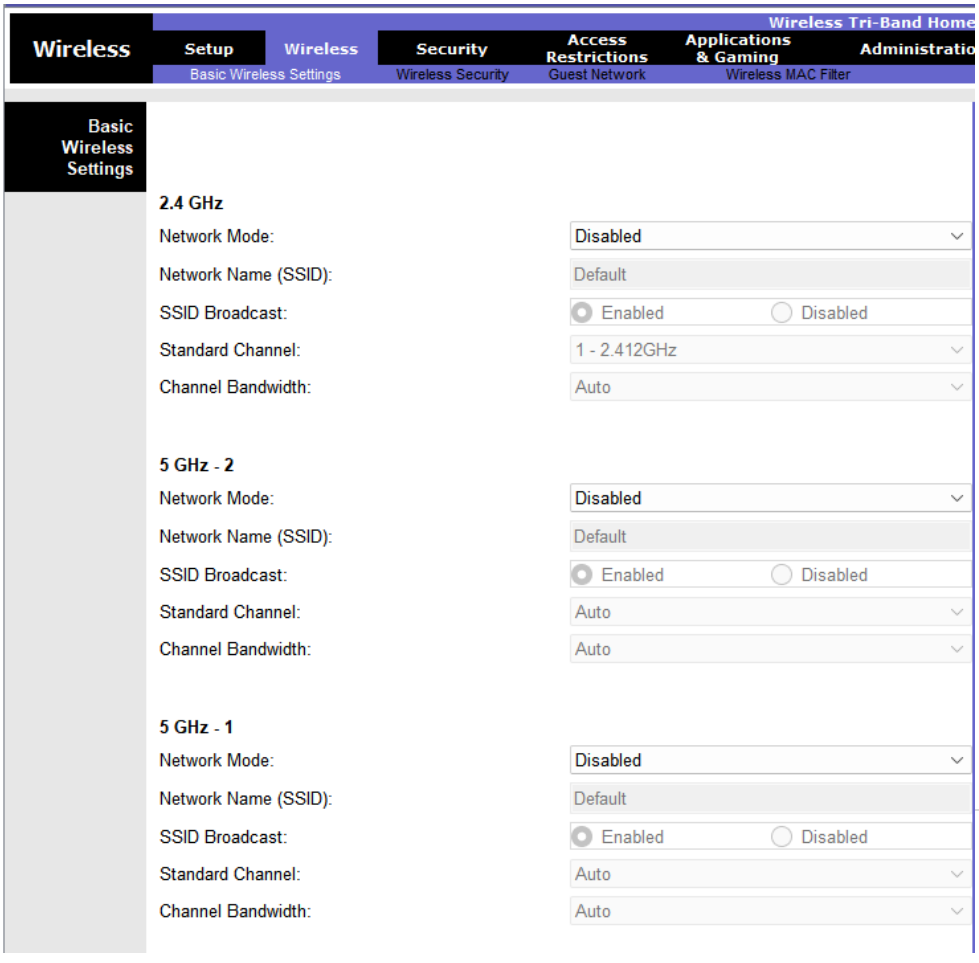
Set up a guest Wi-Fi network using a Cisco router in Packet Tracer, complete with a separate SSID and password for guest users.

THEORY:

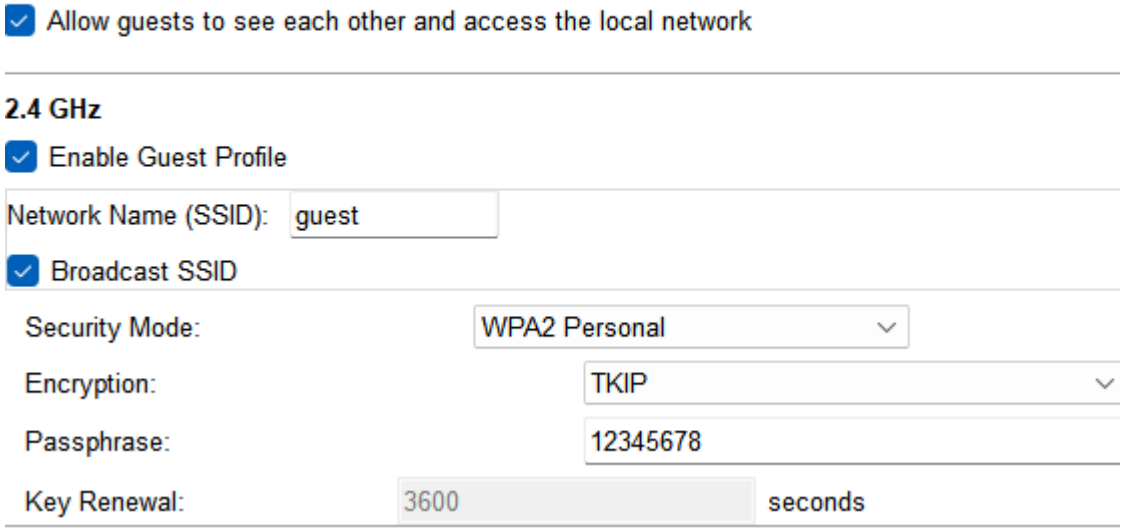
A guest Wi-Fi network is typically set up to provide internet access to visitors while keeping the main network secure. This is achieved by configuring a separate SSID with distinct security settings. By isolating the guest network, the primary network's integrity and security are maintained, and guests are prevented from accessing the organization's local network resources.

PROCEDURE:

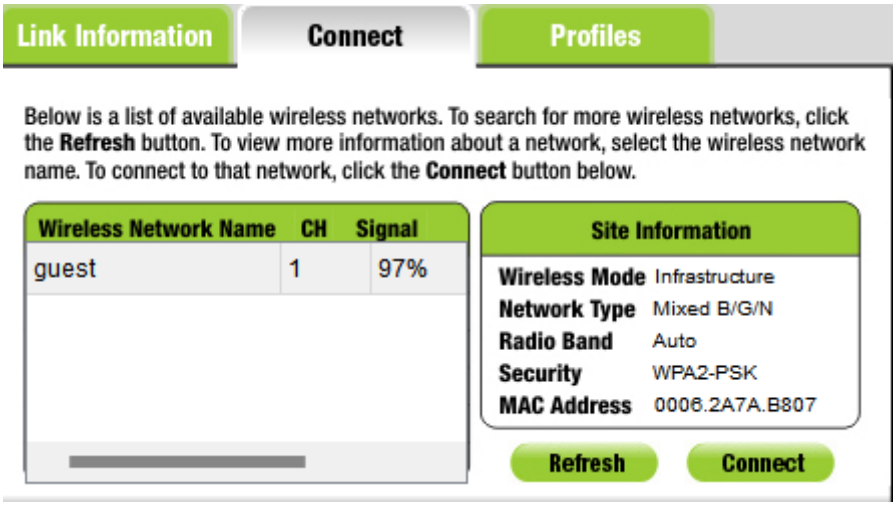
1. Open Cisco Packet Tracer and select the existing network project with the WRT300N wireless router.
2. Configure the Wireless Router for Guest Access:
   - Click on the wireless router and access the GUI setup.
   - Navigate to the 'Wireless' tab.
   - For each frequency band (2.4GHz, 5GHz-1, and 5GHz-2), change the network mode to 'Disabled' and save the settings.



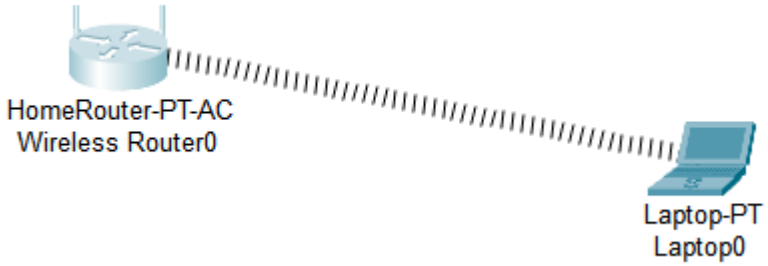
- Go to the 'Guest Network' tab.
- Enable 'Allow guests to see each other and access the local network'.
- For any one frequency band (e.g., 2.4GHz), enable the 'Guest Profile'.
- Set the SSID to 'GUEST'.
- Ensure 'Broadcast SSID' is ticked so the SSID can be seen by devices searching for Wi-Fi networks.
- Configure security by setting a WPA2 passkey, ensuring it is strong and unique.



3. Connect the Laptop to the Guest Network:
   - Click on the laptop, and under the 'Desktop' tab, navigate to the 'IP Wireless' application.
   - Search for the 'GUEST' Wi-Fi network.
   - Connect to it using the previously set WPA2 passkey.



Final Setup:



CONCLUSION:

The guest Wi-Fi network was successfully established on the Cisco router within Packet Tracer. The network was configured with a unique SSID and WPA2 passkey, distinct from the main network, to provide secure internet access to guests. The router was adjusted to prevent guests from accessing the main network while allowing visibility and connectivity among guest devices. The successful connection of a laptop to the guest network and the ability to access the internet verified the functionality of the guest Wi-Fi setup. This experiment highlights the importance of providing controlled network access to guests while securing internal resources.

EXPERIMENT 4

AIM:

Implement VLANs in a Wi-Fi network within Cisco Packet Tracer, ensuring that different VLANs cannot communicate with each other.

THEORY:

VLANs are used to segment a larger network into smaller, isolated networks at the data link layer of the OSI model. This isolation enhances network security and performance by limiting broadcast domains. In a Wi-Fi network, VLANs can be associated with different SSIDs to segregate traffic for various user groups, departments, or types of devices.

PROCEDURE:

1. Launch Cisco Packet Tracer and open the network project with the wireless router configured.
2. Create VLANs on the Wireless Router:
   - Access the wireless router's CLI or GUI, depending on the available options in Packet Tracer.
   - Enter the configuration mode and create multiple VLANs, assigning them unique IDs (e.g., VLAN 10, VLAN 20).
   - Assign each VLAN a separate subnet to ensure communication is isolated (e.g., VLAN 10 - 192.168.10.0/24, VLAN 20 - 192.168.20.0/24).
   - Create SSIDs corresponding to each VLAN, ensuring that each SSID is mapped to the appropriate VLAN.
3. Configure Wi-Fi Clients:
   - For each Wi-Fi client (like laptops or PCs with wireless capability), connect to the corresponding SSID associated with the VLAN it should belong to.
   - Verify that each client receives an IP address within the correct VLAN subnet via DHCP or manual configuration.
4. Verify VLAN Isolation:
   - Use the command prompt on each client to ping devices within the same VLAN to confirm intra-VLAN communication.
   - Attempt to ping devices on a different VLAN to ensure that inter-VLAN communication is not possible.

CONCLUSION:

The experiment successfully established multiple VLANs within a Wi-Fi network in Cisco Packet Tracer. Each VLAN was appropriately configured with a unique subnet and associated SSID. Tests confirmed that devices on the same VLAN could communicate with each other, while devices on separate VLANs were unable to do so, thus achieving the goal of network segmentation and security through VLAN implementation.

EXPERIMENT 5

AIM:

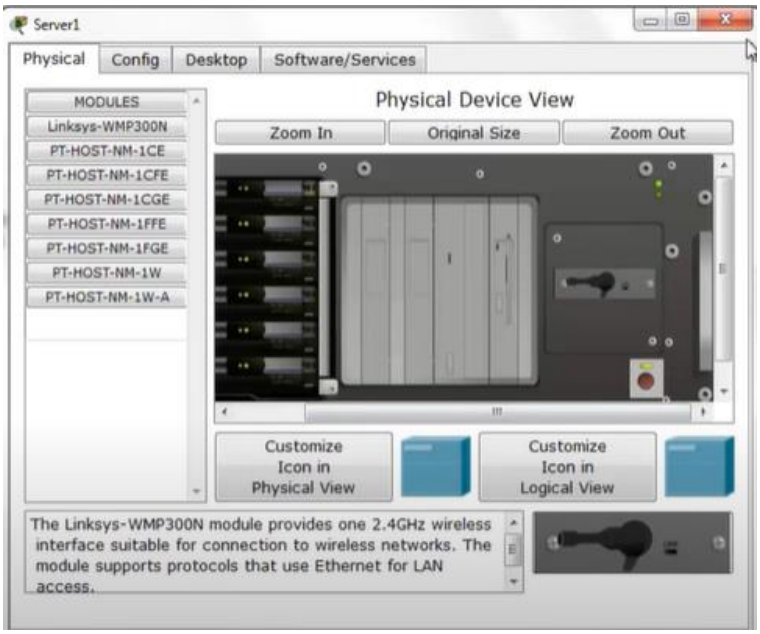
Set up a Cisco wireless network with a DHCP server to automatically assign IP addresses to wireless clients.

THEORY:

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on IP networks to automatically assign IP addresses and other communication parameters to devices (clients) on the network. This facilitates easy administration of network addresses and is scalable for large networks where manual assignment of IP addresses would be impractical.

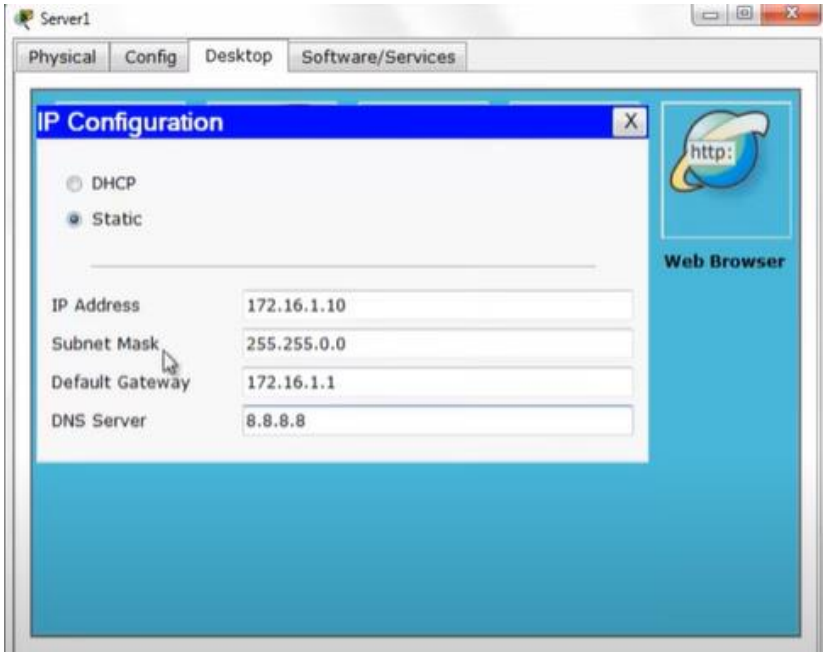
PROCEDURE:

1. Open Cisco Packet Tracer to begin a new or existing project.
2. Add and Configure the Server:
   - Place a physical server into the workspace.
   - Add a wireless network module to the server and toggle the power to initialize it.

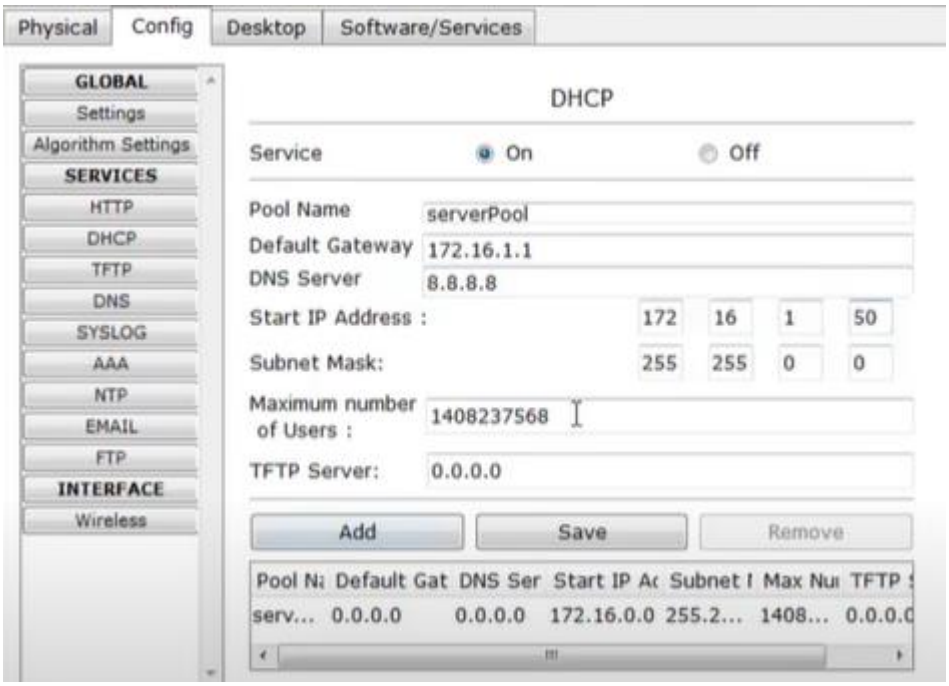


   - Set the server's IP configuration to a static IP address:
     - IP address: 172.16.1.10
     - Subnet Mask: 255.255.0.0

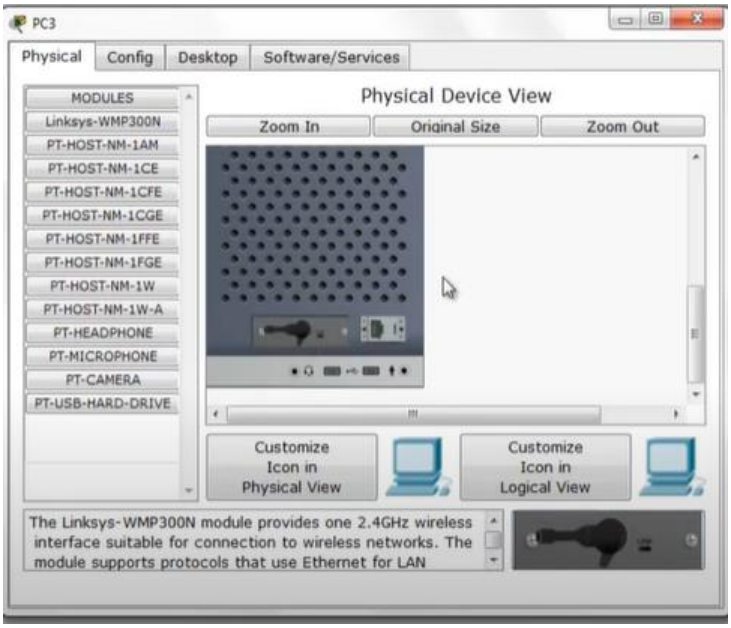
- Default Gateway: 172.16.1.1
- Preferred DNS server: 8.8.8.8



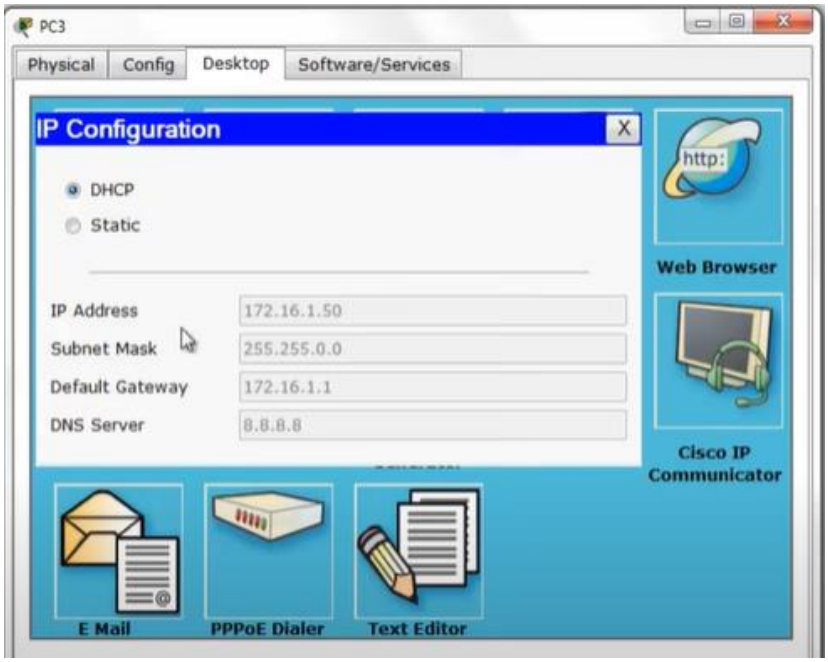
- Configure the server's DHCP service:
  - Navigate to the 'Config' tab and select the 'DHCP' setting.
  - Set the Default Gateway to 172.16.1.1 and the DNS server to 8.8.8.8.
  - Define the starting IP address range for DHCP clients as 172.16.1.50.



3. Set Up Wireless Clients:
   - Place a PC on the workspace.
   - Replace the PC's Ethernet module with a wireless module and power cycle the PC to activate the changes.

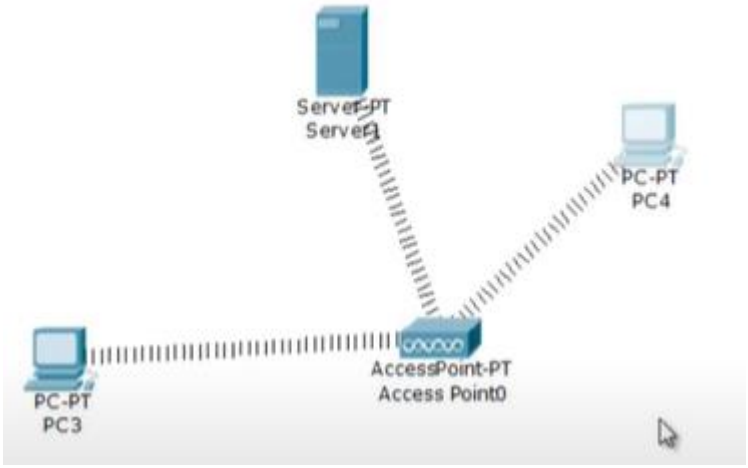


4. Connect the Access Point:
   - Add an access point to the workspace, which should automatically link to the PC.
5. Verify DHCP Configuration on the Client:
   - On the PC, navigate to the 'Desktop' tab and then to 'IP Configuration'.
   - The PC should display IP settings assigned by the server's DHCP service.



6. Expand the Network:
    - Additional PCs can now be added and equipped with wireless modules. Each will automatically receive network configurations from the DHCP server upon connecting to the network.

Final Setup:



CONCLUSION:

This experiment demonstrated the effective setup of a wireless network with an integrated DHCP server within Cisco Packet Tracer. The DHCP server was appropriately configured to automatically provide IP addresses and networking parameters to wireless clients. The successful automatic retrieval of IP settings by the client PCs upon joining the network verified the DHCP server's functionality.

EXPERIMENT 6

AIM:

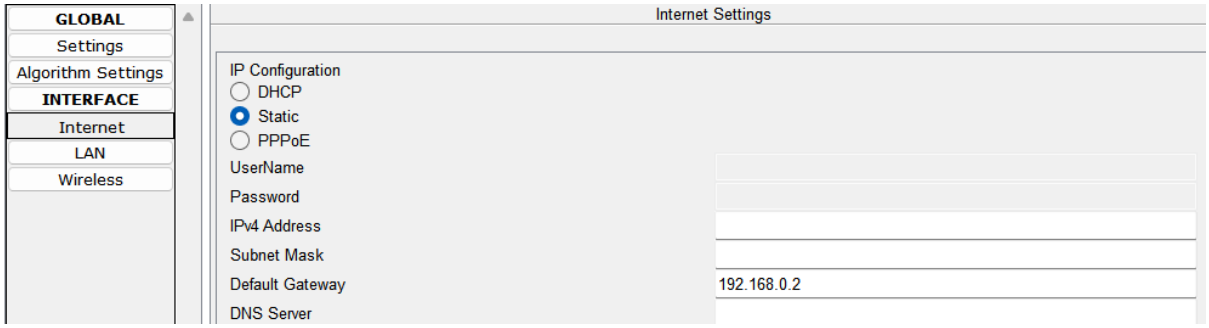
Configure a wireless router in Packet Tracer to act as a repeater, extending the range of an existing Wi-Fi network.

THEORY:

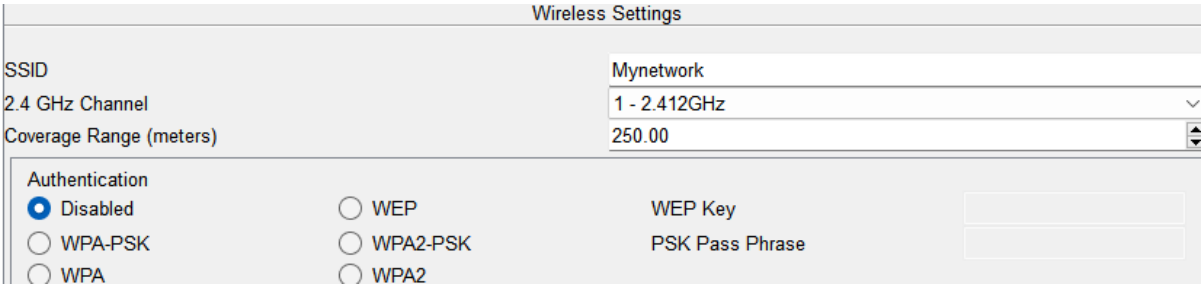
A repeater is used to extend the coverage area of a wireless network by receiving the wireless signal from a primary router and retransmitting it. This setup is particularly useful in areas where the primary router's signal is weak or does not reach. While Packet Tracer does not emulate the radio wave propagation and signal strength, the concept of network extension through a repeater can still be simulated.

PROCEDURE:

1. Open the Cisco Packet Tracer environment and set up the initial network with one wireless router (WRT300N Wireless Router0) connected to the internet.
2. Add a Secondary Router:
   - Place a second wireless router (WRT300N Wireless Router1) to act as the repeater.
   - Connect the secondary router's Ethernet port to the primary router's Internet port using a straight-through Ethernet cable.
3. Configure the Secondary Router (Repeater):
   - Access the configuration settings of the secondary router.
   - Set the default gateway to the IP address of the primary router (192.168.0.2).



   - Ensure that the SSID and security settings match those of the primary router to simulate the wireless repeater functionality.

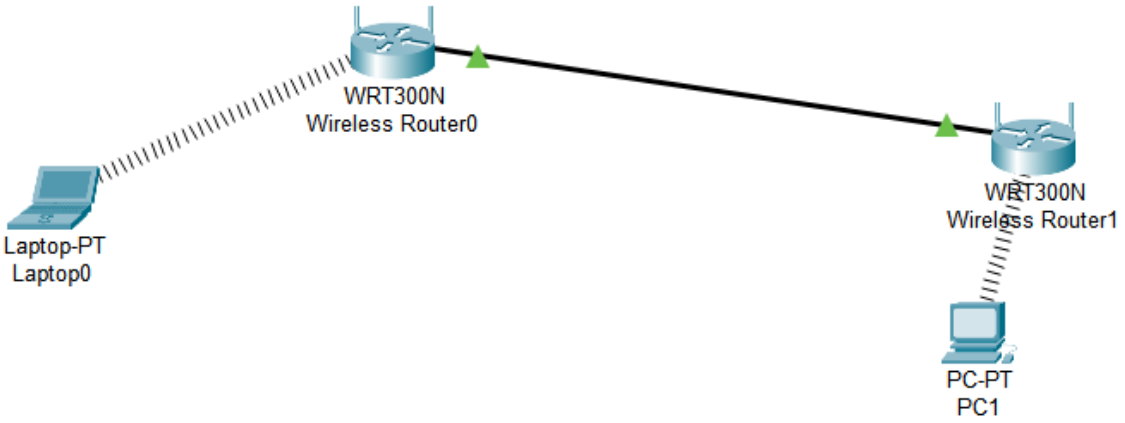


4. Prepare the Laptop for Wireless Connectivity:
   - Add a laptop to the workspace and insert a wireless module.
   - Connect the Laptop to the Secondary Router:
   - Connect the laptop wirelessly to the SSID broadcasted by the secondary router.
5. Test the Configuration:
   - Use the command prompt on the laptop to ping the IP address of the primary router (192.168.0.2 in this case).

```
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=5ms TTL=128
Reply from 192.168.0.2: bytes=32 time=7ms TTL=128
Reply from 192.168.0.2: bytes=32 time=9ms TTL=128
Reply from 192.168.0.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 9ms, Average = 7ms
```

   - Confirm that the responses received indicate successful communication through the secondary router, which acts as the repeater.

Final Setup:



CONCLUSION:

This experiment successfully demonstrated the setup of a wireless router configured as a repeater within Cisco Packet Tracer. The additional router was integrated into the existing network, intending to extend its Wi-Fi coverage. The careful configuration of network settings, including IP addressing and default gateways, was key to creating a seamless network extension. Through this exercise, we've reinforced the concept that a repeater serves as an intermediary to bolster the wireless signal, ensuring broader network accessibility while maintaining a single cohesive network.

EXPERIMENT 7

AIM:

Implement wireless security mechanisms, including WPA2-PSK, WPA2-Enterprise, and MAC address filtering on a Cisco wireless network in Packet Tracer.

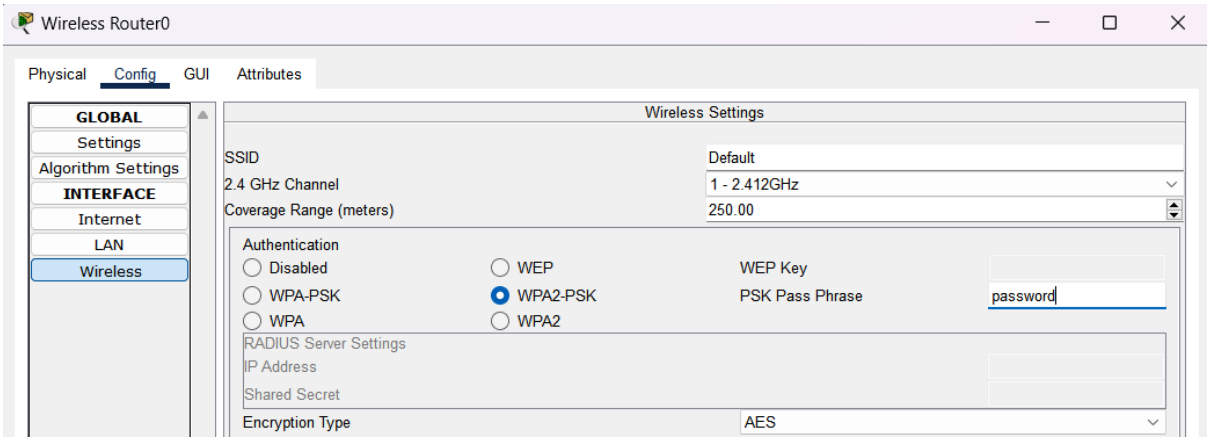
THEORY:

Wireless networks are susceptible to unauthorized access and eavesdropping. Therefore, robust security mechanisms are crucial. WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) is a common security protocol that uses a pre-shared key for authentication. WPA2-Enterprise provides a higher security level by using a RADIUS server to manage individual user authentication. MAC address filtering adds an additional security layer by restricting network access to devices with specific MAC addresses.

PROCEDURE:

1. Setup the Network:
   - Add a wireless router and a server (to act as a RADIUS server for WPA2-Enterprise) to the Packet Tracer workspace.
   - Add a PC and other wireless clients that will connect to the network.

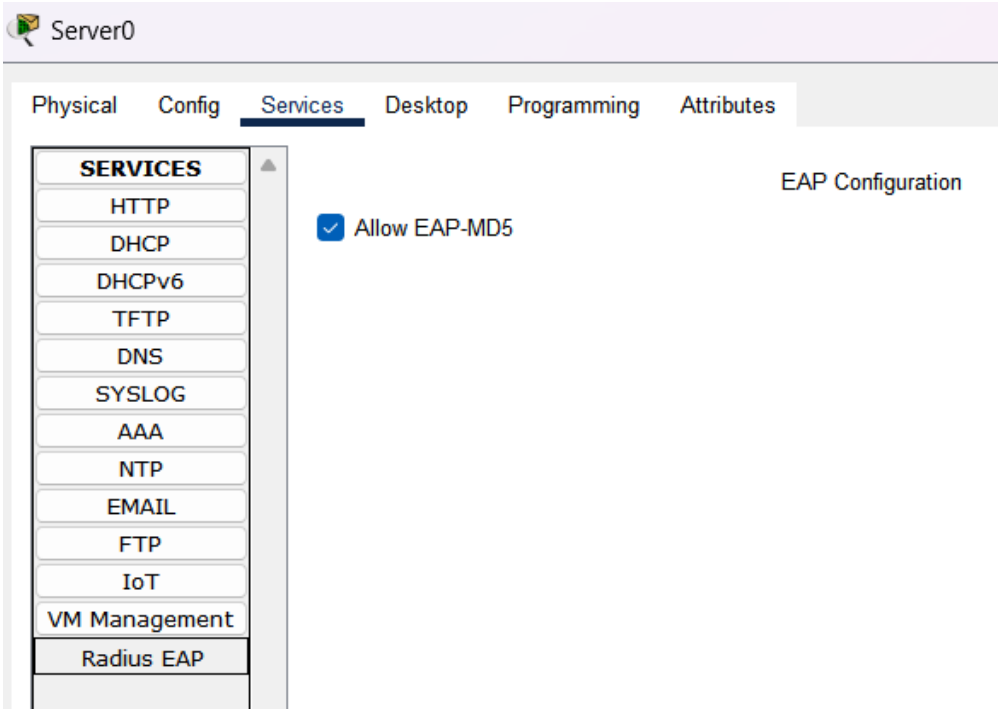
2. Configure WPA2-PSK:
   - Access the wireless router's GUI.
   - Navigate to the security settings and select WPA2-PSK.



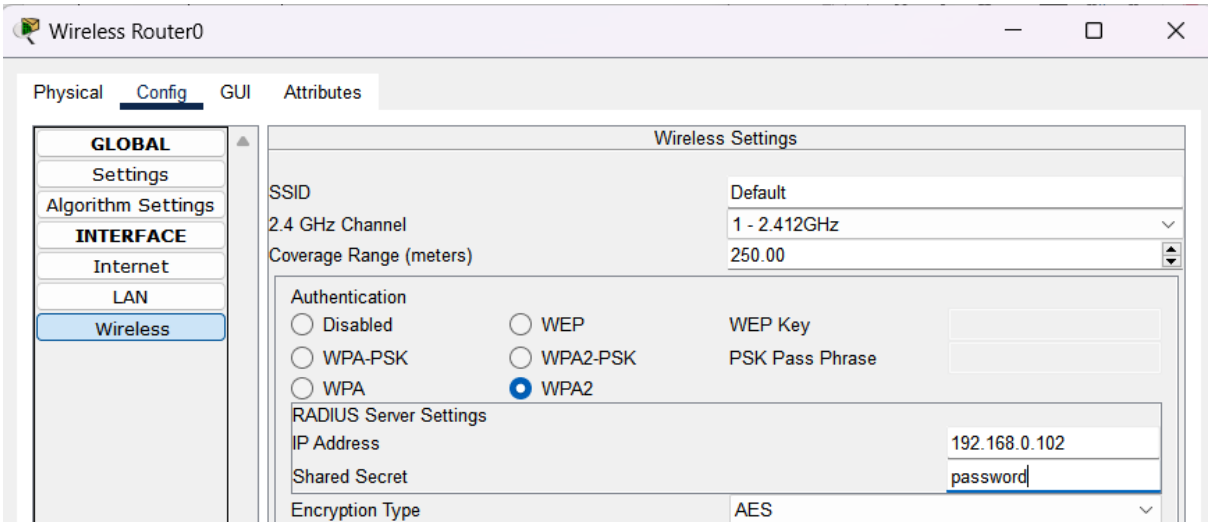
   - Set a strong pre-shared key.

3. Configure WPA2-Enterprise:

- In the RADIUS server settings on the router, input the IP address of the server, and set the shared secret.

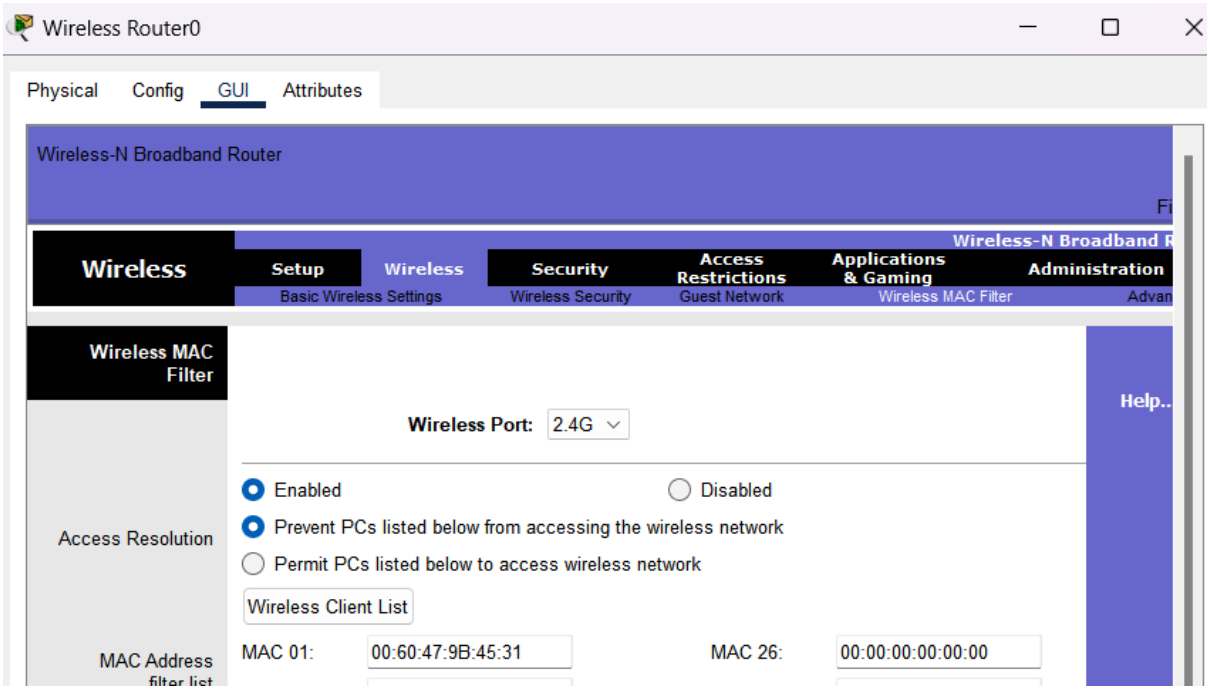


- On the server, configure the RADIUS service with the corresponding shared secret and add the router as a client.



4. Configure MAC Address Filtering:

- In the router's MAC address filtering settings, add the MAC addresses of the devices you want to allow on the network.



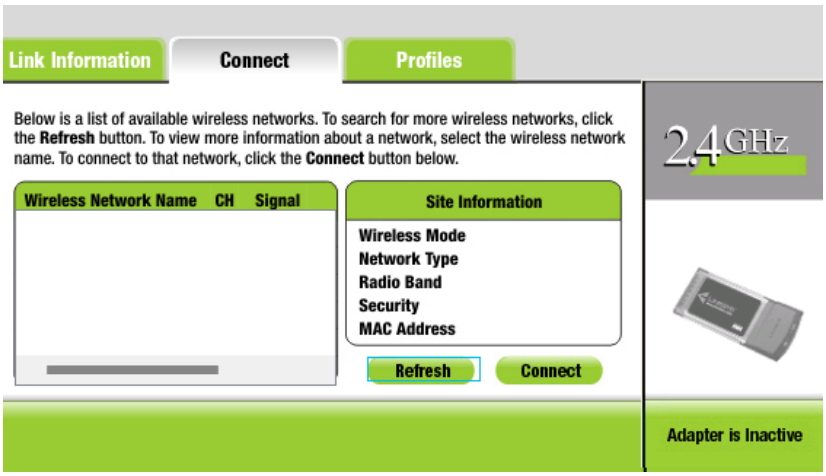
- Enable the filter and choose to deny or allow access based on the list.

5. Connect and Test Clients:

   - Configure wireless clients to connect using WPA2-PSK or WPA2-Enterprise as appropriate

   - Verify connectivity by connecting to the network and attempting to access network resources.

6. Validate Security Settings:
   Attempt to connect with a client not listed in the MAC address filter to ensure it is denied access.



CONCLUSION:

This experiment demonstrated the implementation of essential wireless security mechanisms within a simulated Cisco network environment. By successfully configuring WPA2-PSK and WPA2-Enterprise, the network now benefits from two robust layers of authentication. Additionally, MAC address filtering has been employed to control device access further. These security measures collectively enhance the network's integrity and resilience against unauthorized access, aligning with best practices for wireless network security.