

Course: Cloud and Network Security – C2 – 2025.

Student: Luke Mbogo

Student No: cs-cns09-25076

Monday, July 16th, 2025.

Week 4 Assignment 2:

WLAN Configuration (Packet Tracer).

Contents

Introduction	3
Part 1: Configure a Home Wireless Router	3
Step 1: Change DHCP settings.....	3
Step 2: Configure the Wireless LAN.	4
Step 3: Configure security.	4
Step 4: Connect clients to the network.	5
Part 2: Configure a WLC Controller Network	7
Step 1: Configure VLAN interfaces.....	7
Step 2: Configure a DHCP scope for the wireless management network.....	9
Step 3: Configure the WLC with external server addresses.....	10
Step 4: Create the WLANs.....	11
Step 5: Configure the hosts to connect to the WLANs.	13
Step 6: Test connectivity.....	15
Summary.	15
Conclusion.....	16

Introduction

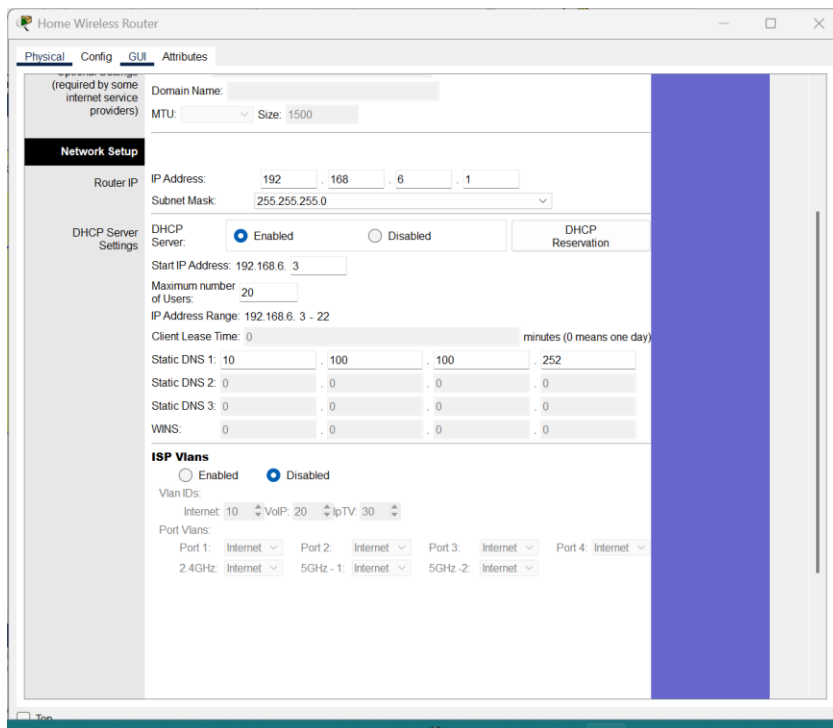
In this activity, I configured a wireless network using both a **home wireless router** and an **enterprise-level wireless LAN controller (WLC)**. The goal was to implement **WPA2-Personal** and **WPA2-Enterprise** wireless security configurations and ensure wireless devices could securely connect and communicate. The process included configuring DHCP settings, creating and securing SSIDs, and validating client connectivity through ping and web access. This assignment helped reinforce my understanding of wireless standards, VLANs, and security mechanisms used in real-world enterprise networks.

Part 1: Configure a Home Wireless Router

Step 1: Change DHCP settings.

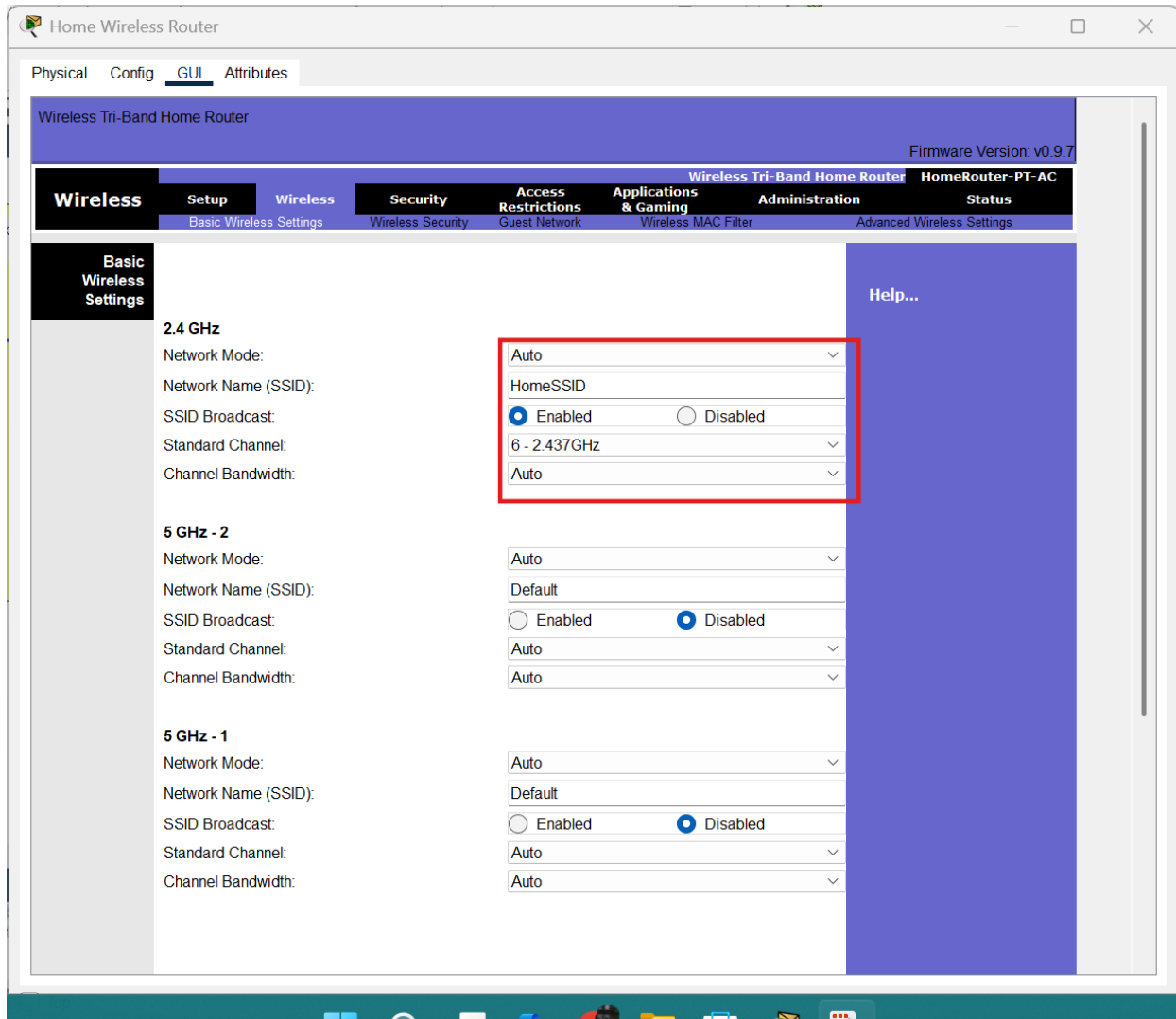
In this section, I set up a home wireless router to provide internet access and enhance network security. After accessing the router's GUI, I updated its IP and DHCP settings as per the Addressing Table. I limited the DHCP pool to 20 devices to prevent IP exhaustion and reduce the chances of unauthorized access.

To manage address distribution better, I set the DHCP pool to start from .3 of the LAN range. I then configured the router's internet interface to get its IP via DHCP and confirmed it successfully received an IP from the simulated ISP:



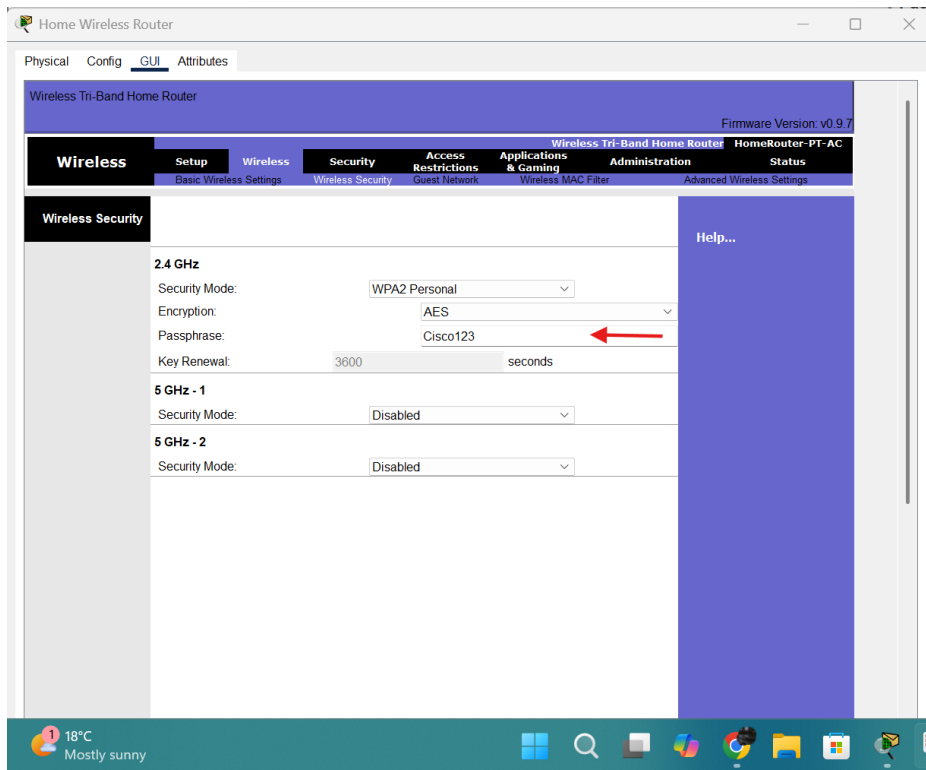
Step 2: Configure the Wireless LAN.

For the wireless setup, I configured the 2.4GHz interface with the SSID **HomeSSID** and set the channel to 6. I also ensured the SSID broadcast was enabled so that all wireless devices in the home could detect and connect to the network.



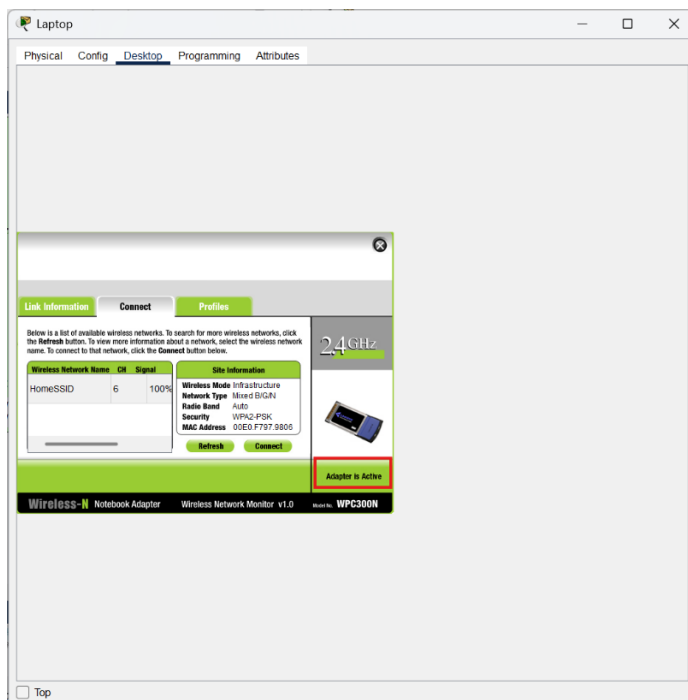
Step 3: Configure security.

To protect the wireless network, I enabled **WPA2-Personal** security on the 2.4GHz interface and set the passphrase to **Cisco123**, as provided in the Wireless LAN information. This type of encryption ensures that only users with the correct password can connect. Additionally, I updated the router's default admin password to improve access control and reduce the risk of unauthorized changes to the configuration. These steps help strengthen the overall security of the home network.

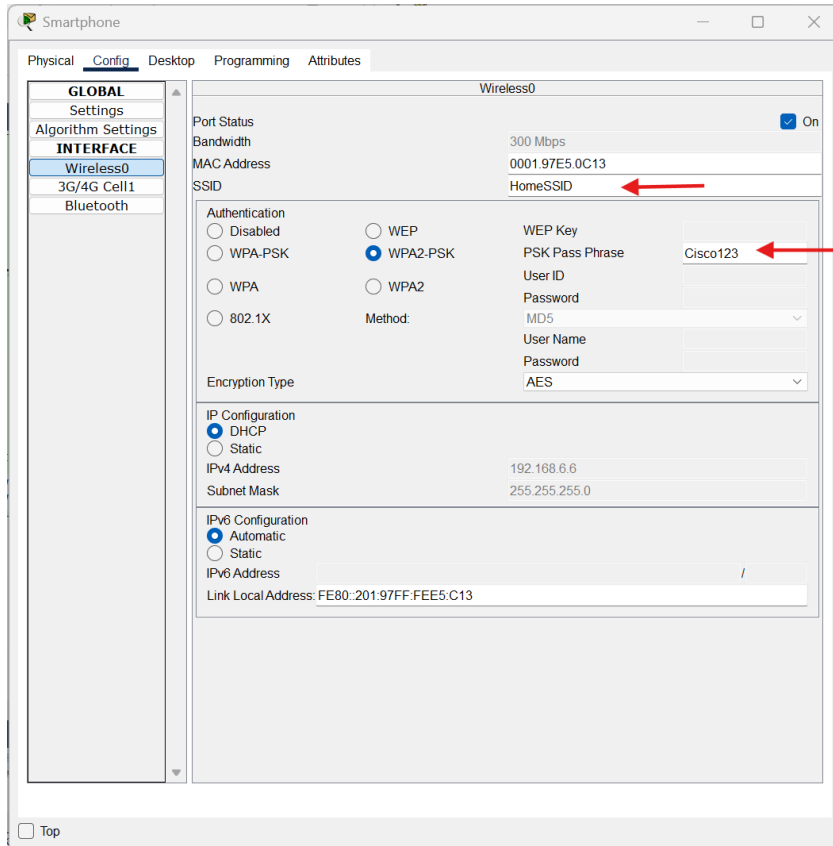


Step 4: Connect clients to the network.

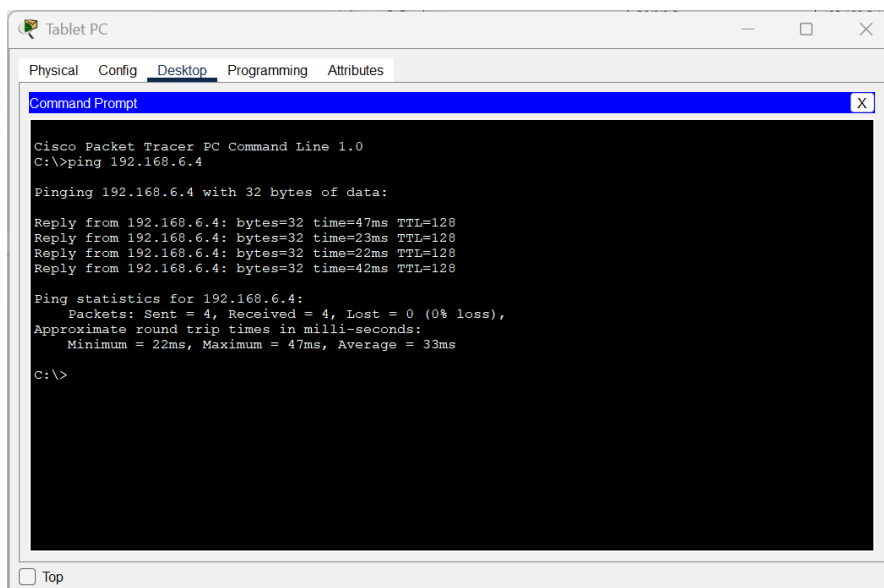
I connected the wireless devices (laptop, tablet, and smartphone) to the configured network HomeSSID using the correct passphrase (Cisco123). On the laptop, I used the PC Wireless app to select and join the network.



For the tablet and smartphone, I used the Config tab to set the SSID and security settings. After the connections were established, I verified connectivity by pinging between devices and successfully accessing the web server via its URL. This confirmed that the wireless configuration was working correctly and that the router was handling DHCP and routing as expected.



Ping Test



Part 2: Configure a WLC Controller Network

In the second part of the task, I worked on configuring the Wireless LAN Controller (WLC) to manage two separate wireless networks. One WLAN was secured using WPA2-PSK for simpler password-based access, while the other used WPA2-Enterprise for more secure, username-password-based authentication through a RADIUS server. I also set up SNMP settings for network monitoring and created a DHCP scope to support IP assignment for devices on the wireless management network.

Step 1: Configure VLAN interfaces.

To begin the enterprise WLAN setup, I accessed the WLC-1 management interface through a web browser using the provided admin credentials. I then created a new interface named **WLAN 2**, assigned to VLAN ID **2** on **Port 1**. The IP address for this interface was set to **192.168.2.254**, with a subnet mask of **255.255.255.0**. The default gateway and primary DHCP server were both pointed to the address of **RTR-1's subinterface G0/0/0.2**, ensuring proper routing and address assignment for devices on this VLAN.

The screenshot displays the Cisco Enterprise Admin web interface for configuring a WLAN interface. The browser address bar shows the URL `https://192.168.100.254/frameInterfaceEdit.html`. The interface is titled "Interfaces > Edit" and includes a "Web Browser" tab. The left sidebar shows the navigation menu with "Interfaces" selected. The main content area is divided into several sections:

- General Information:** Interface Name: WLAN 2, MAC Address: 00:0C:85:BA:1A:1C.
- Configuration:** Guest Lan, Quarantine, Quarantine Vlan Id (0), NAS-ID.
- Physical Information:** Port Number (1), Backup Port (0), Active Port (1), Enable Dynamic AP Management.
- Interface Address:** VLAN Identifier (2), IP Address (192.168.2.254), Netmask (255.255.255.0), Gateway (192.168.2.1).
- DHCP Information:** Primary DHCP Server (192.168.2.1), Secondary DHCP Server, DHCP Proxy Mode (Global), Enable DHCP Option 82.
- Access Control List:** ACL Name (none).

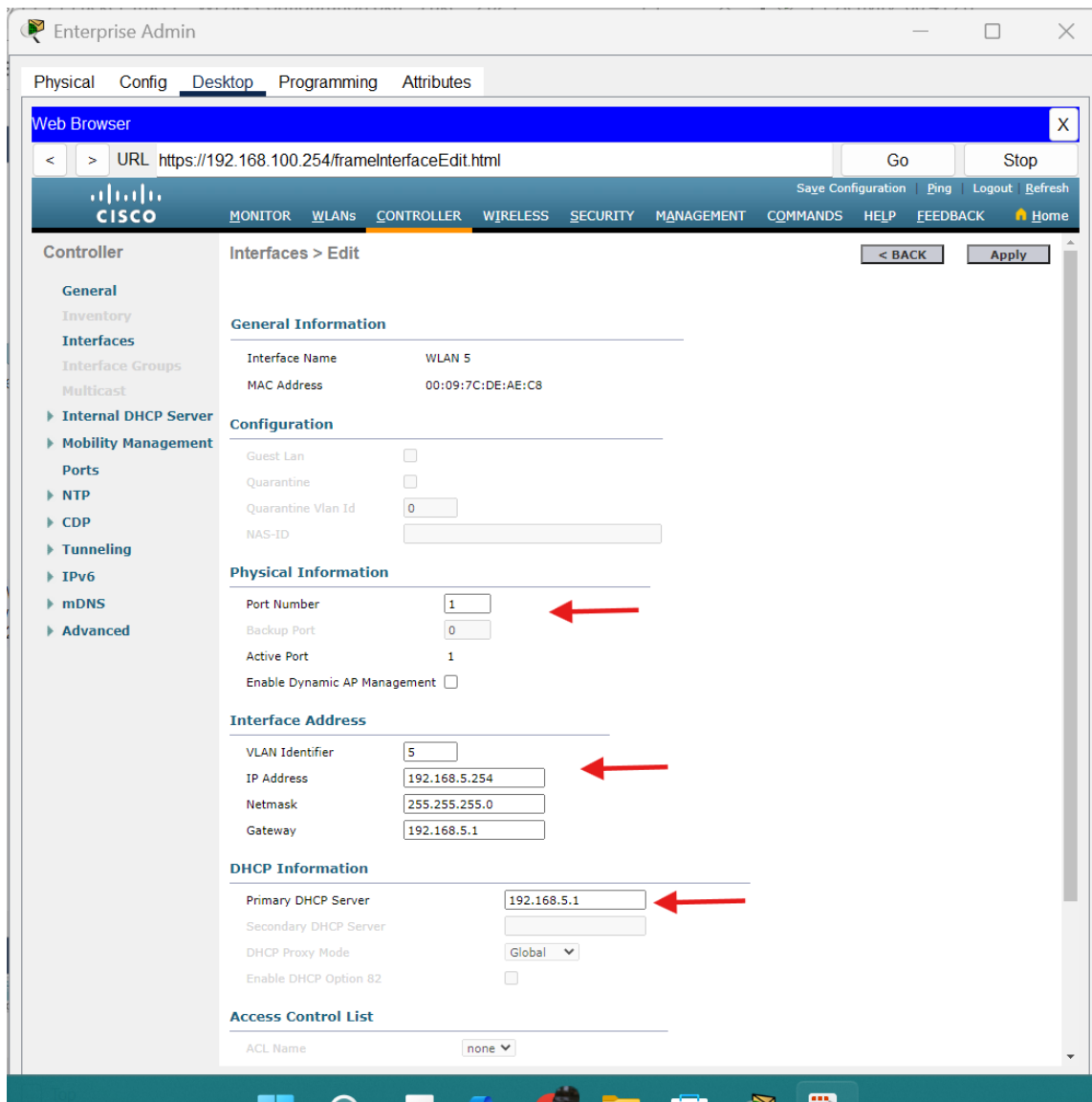
Red arrows highlight the Port Number (1), IP Address (192.168.2.254), and Primary DHCP Server (192.168.2.1) fields.

Next, I configured the second interface on the WLC named **WLAN 5**, assigned to **VLAN ID 5** on **Port 1**. Its IP address was set to **192.168.5.254** with a **255.255.255.0** subnet mask. Both the gateway and primary DHCP server were set to **RTR-1's subinterface G0/0/0.5**, ensuring that devices on this VLAN could communicate effectively with the rest of the network and receive IP configuration dynamically.

The screenshot shows the Cisco Enterprise Admin web interface for configuring a WLAN. The left sidebar lists various configuration categories, and the main area is titled 'Interfaces > Edit'. The configuration is for 'WLAN 5' with MAC address '00:09:7C:DE:AE:C8'. The 'Physical Information' section shows 'Port Number' set to 1. The 'Interface Address' section shows 'VLAN Identifier' set to 5, 'IP Address' set to 192.168.5.254, 'Netmask' set to 255.255.255.0, and 'Gateway' set to 192.168.5.1. The 'DHCP Information' section shows 'Primary DHCP Server' set to 192.168.5.1. Red arrows highlight these four fields.

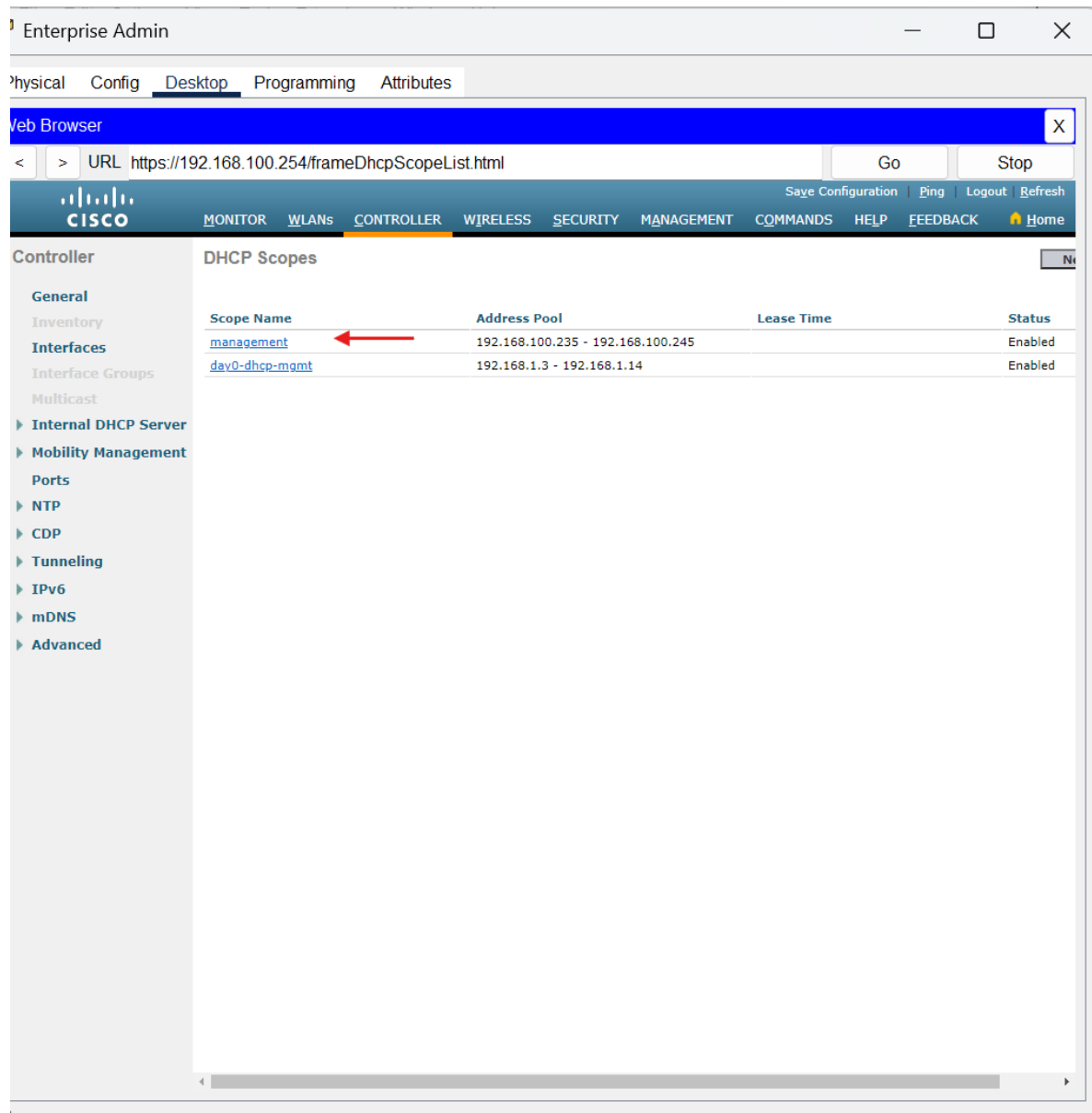
Section	Field	Value
General Information	Interface Name	WLAN 5
	MAC Address	00:09:7C:DE:AE:C8
Configuration	Guest Lan	<input type="checkbox"/>
	Quarantine	<input type="checkbox"/>
	Quarantine Vlan Id	0
	NAS-ID	
Physical Information	Port Number	1
	Backup Port	0
	Active Port	1
	Enable Dynamic AP Management	<input type="checkbox"/>
Interface Address	VLAN Identifier	5
	IP Address	192.168.5.254
	Netmask	255.255.255.0
	Gateway	192.168.5.1
DHCP Information	Primary DHCP Server	192.168.5.1
	Secondary DHCP Server	
	DHCP Proxy Mode	Global
	Enable DHCP Option 82	<input type="checkbox"/>
Access Control List	ACL Name	none

Next, I configured the second interface on the WLC named **WLAN 5**, assigned to **VLAN ID 5** on **Port 1**. Its IP address was set to **192.168.5.254** with a **255.255.255.0** subnet mask. Both the gateway and primary DHCP server were set to **RTR-1's subinterface G0/0/0.5**, ensuring that devices on this VLAN could communicate effectively with the rest of the network and receive IP configuration dynamically.



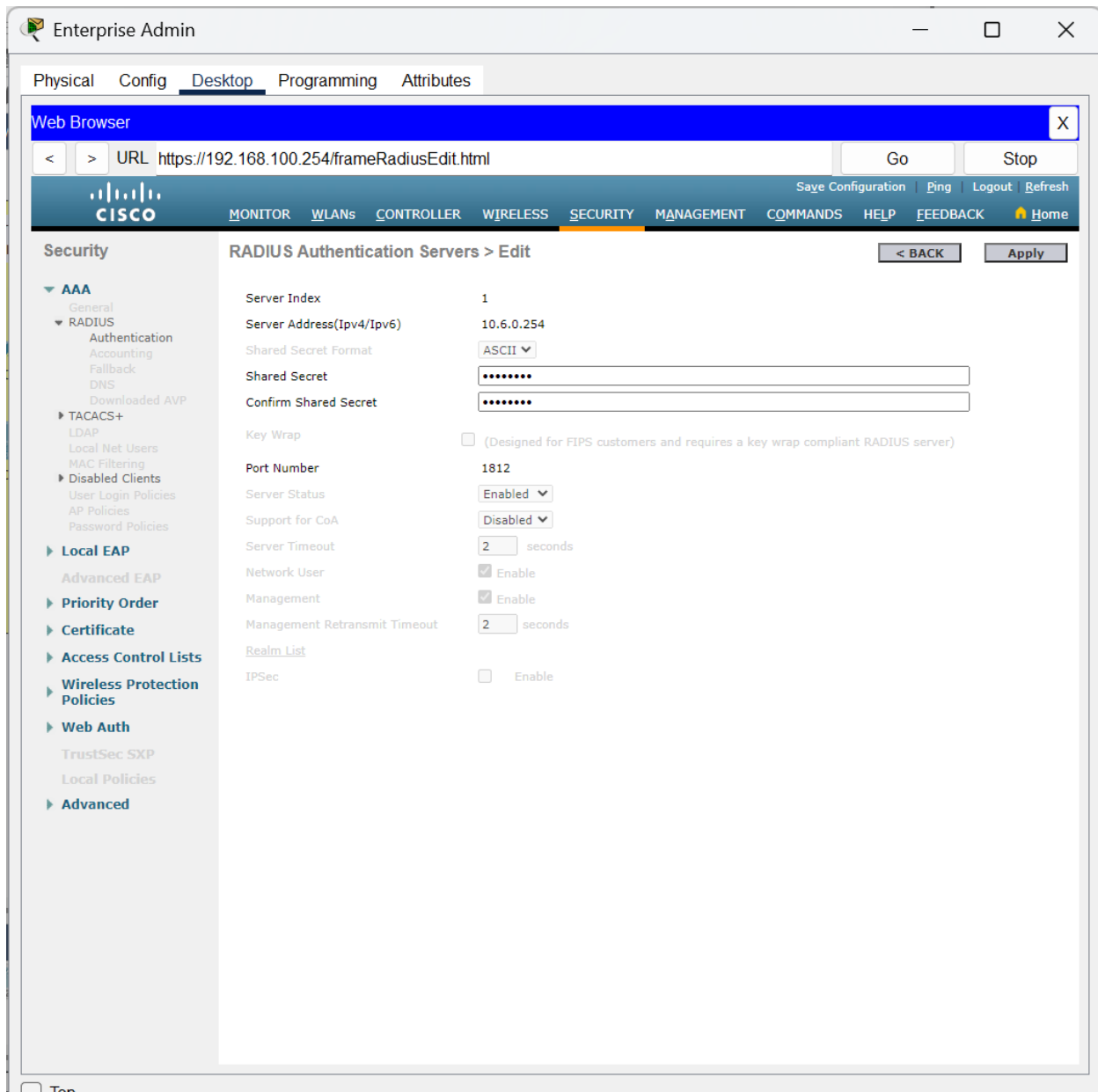
Step 2: Configure a DHCP scope for the wireless management network.

I proceeded to set up and enable an internal DHCP scope on the WLC named **"management"**. This scope was configured to serve addresses within the **192.168.100.0/24** network, specifically from **192.168.100.235** to **192.168.100.245**. The default gateway for this pool was set as **192.168.100.1**, allowing wireless management devices to obtain IPs automatically and communicate effectively.



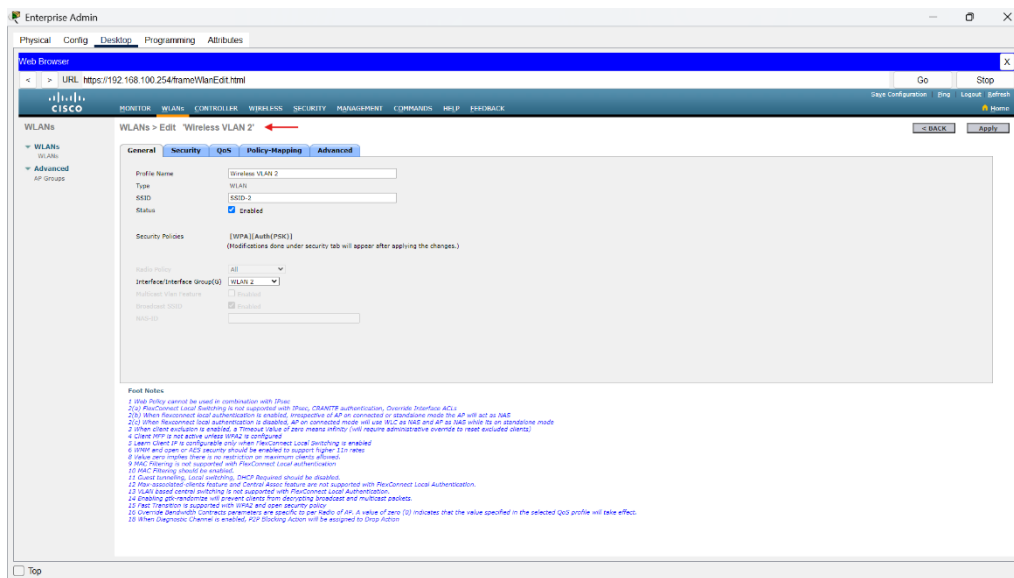
Step 3: Configure the WLC with external server addresses.

To support enterprise-level authentication and monitoring, I configured the WLC to use an external **RADIUS server** at IP **10.6.0.254** with the shared secret "**RadiusPW**", assigned to **Server Index 1**. Additionally, I enabled SNMP logging by setting up the **SNMP server** on the same IP, using "**WLAN**" as the community name. This ensures both authentication and network monitoring functions are properly supported.

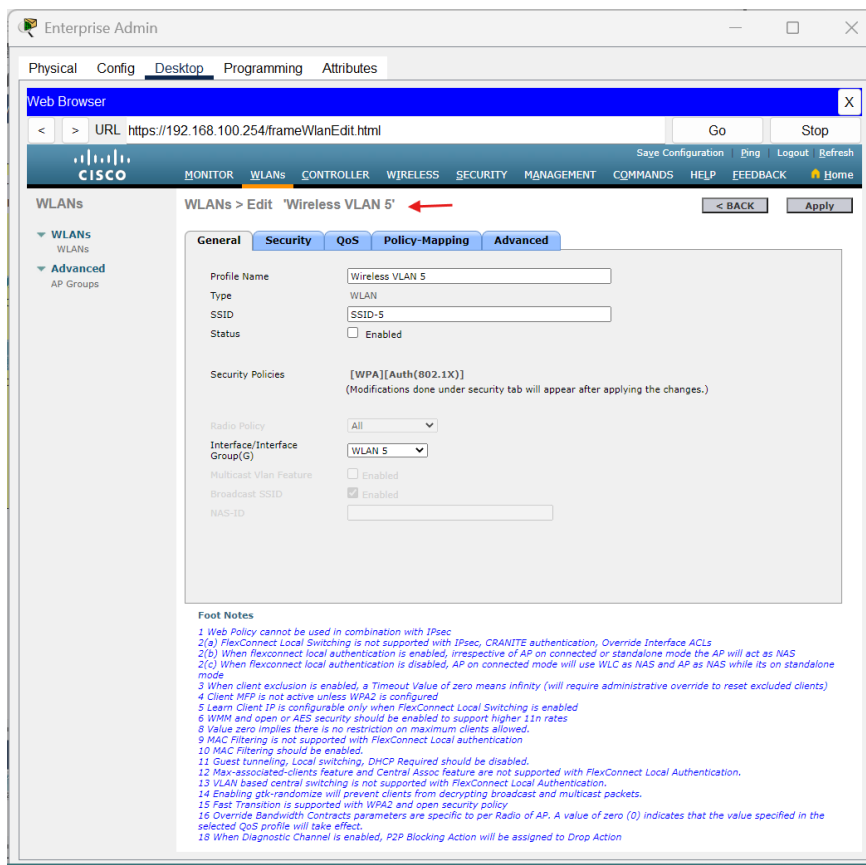


Step 4: Create the WLANs.

To set up the first wireless network, I created a WLAN profile named **"Wireless VLAN 2"** with the SSID **"SSID-2"**. This network uses **WPA2-PSK** security with the passphrase **"Cisco123"** and is linked to **Interface WLAN 2** (VLAN 2). Under the **Advanced > FlexConnect** tab, I enabled both **Local Switching** and **Local Authentication** to allow remote APs to operate independently of the WLC if needed.

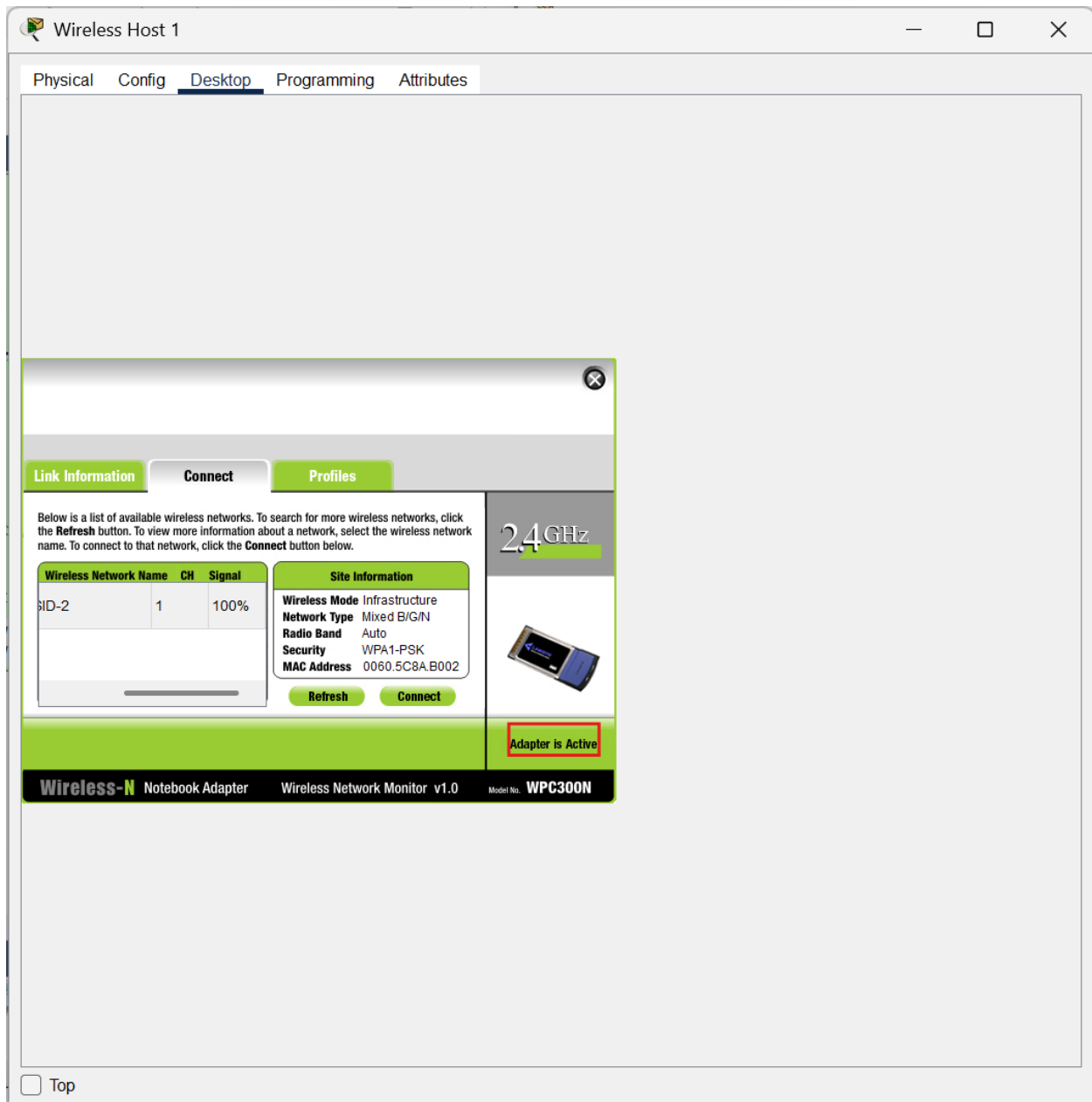


I created a second WLAN named **"Wireless VLAN 5"** using the SSID **"SSID-5"**, linked to **Interface WLAN 5** (VLAN 5). This network was secured with **WPA2-Enterprise (802.1x)**, and configured to use the **RADIUS server** for user authentication. Just like the previous WLAN, I enabled **FlexConnect Local Switching** and **FlexConnect Local Authentication** in the Advanced settings to ensure proper handling by access points.

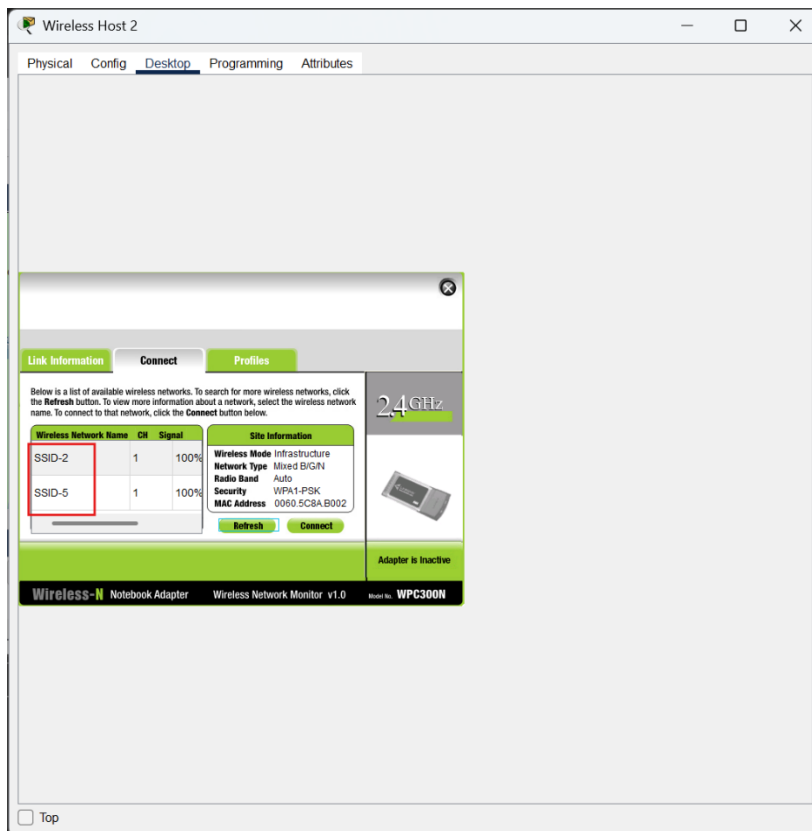


Step 5: Configure the hosts to connect to the WLANs.

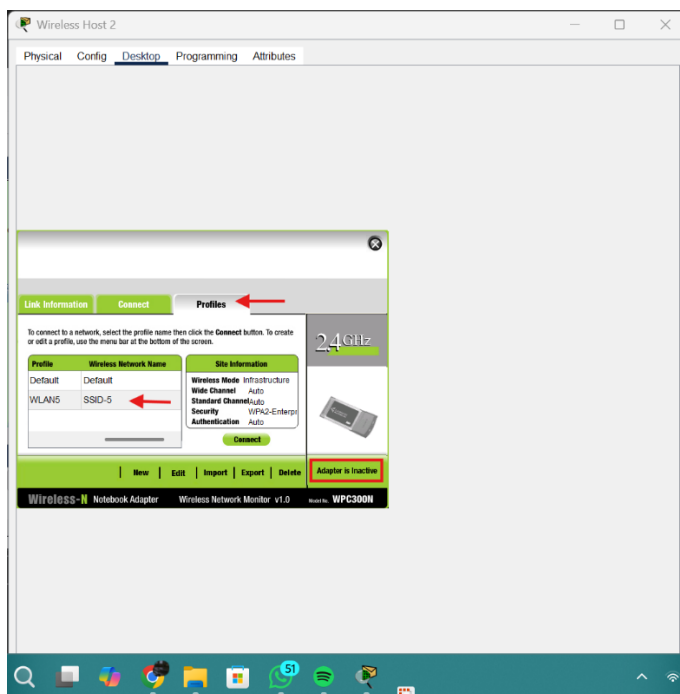
Using the **PC Wireless app**, I configured **Wireless Host 1** to connect to **SSID-2**, which corresponds to **Wireless VLAN 2**. I entered the **WPA2-PSK passphrase (Cisco123)** provided earlier and confirmed that the host successfully joined the network.



While attempting to connect **Wireless Host 2** to **SSID-5** (Wireless VLAN 5), the network was visible and detected, but the connection consistently failed despite entering the correct **WPA2-Enterprise credentials (userWLAN5 / userW5pass)**. This may have been caused by a configuration issue or a known Packet Tracer limitation affecting 802.1x authentication.

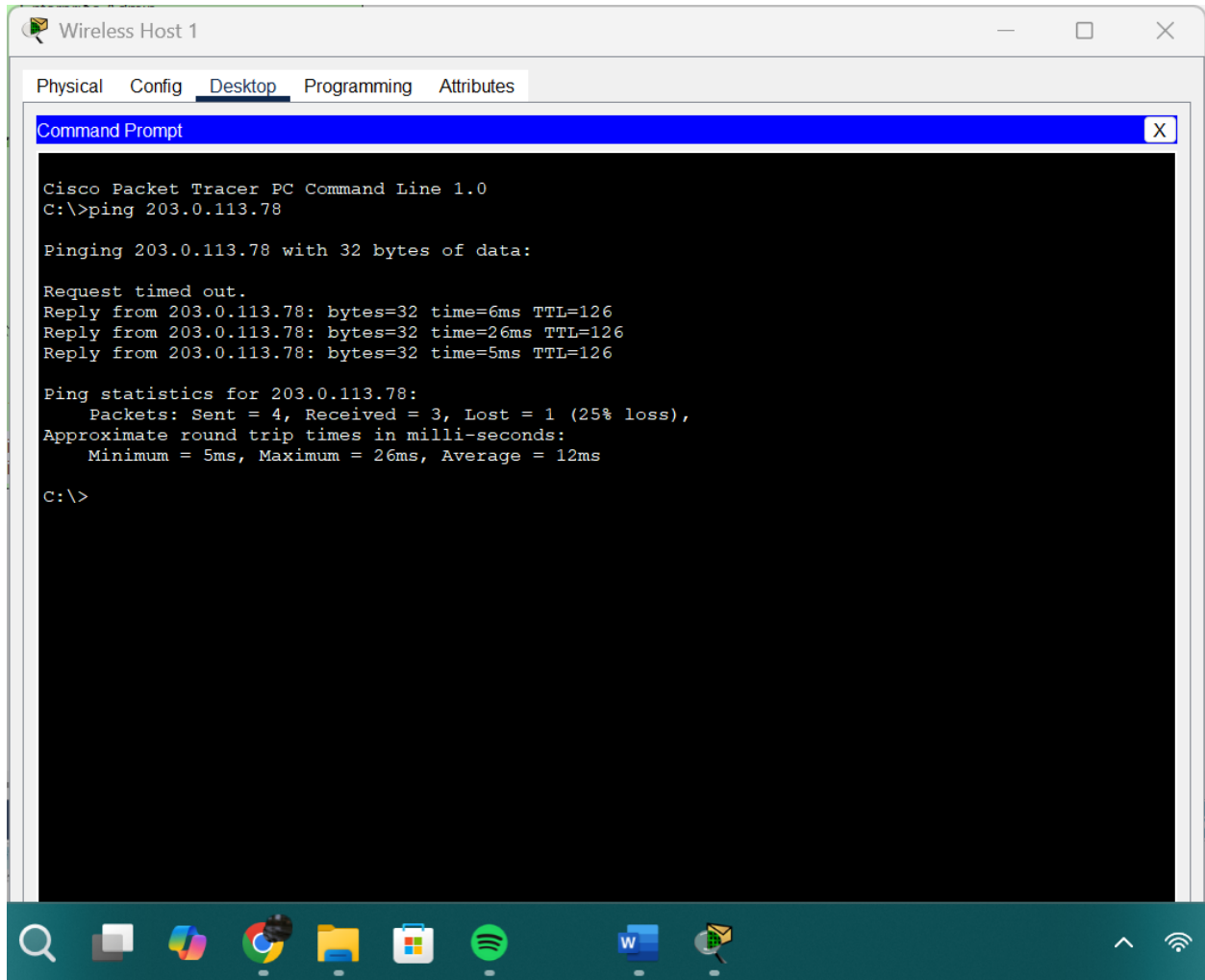


I successfully created a profile for **SSID-5** with the correct WPA2-Enterprise credentials. However, the profile failed to establish a connection. Despite multiple attempts, the host remained disconnected, possibly due to a simulation limitation or misconfiguration.



Step 6: Test connectivity.

I tested connectivity for the device connected to **WLAN VLAN 2**, and both pinging the web server and accessing it via its URL were successful. This confirmed that the configuration for **WLAN 2** was functioning correctly.



The screenshot shows a Cisco Packet Tracer PC Command Line window for 'Wireless Host 1'. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with 'Desktop' selected. The Command Prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Request timed out.
Reply from 203.0.113.78: bytes=32 time=6ms TTL=126
Reply from 203.0.113.78: bytes=32 time=26ms TTL=126
Reply from 203.0.113.78: bytes=32 time=5ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 26ms, Average = 12ms

C:\>
```

Summary.

In this assignment, I configured both a **Home Wireless Router** and an **Enterprise Wireless LAN Controller (WLC)** to support wireless connectivity using **WPA2-Personal** and **WPA2-Enterprise** security modes. The devices used included:

- **Wireless Router** (Home Router)
- **WLC-1** (Wireless LAN Controller)
- **Enterprise Admin PC**

- **Wireless Host 1** (connected to VLAN 2)
- **Wireless Host 2** (attempted to connect to VLAN 5)
- **Tablet** and **Smartphone** (connected to HomeSSID)
- **Web Server** (used to test connectivity via ping and URL)

The tasks involved setting up SSIDs, DHCP scopes, VLAN interfaces, security credentials, and confirming successful connections. While **Wireless Host 1** connected and communicated successfully, **Wireless Host 2** faced issues connecting to the Enterprise WLAN, possibly due to simulation or profile errors.

Conclusion.

This activity gave me a hands-on understanding of how to set up and secure both home and enterprise wireless networks. I was able to configure DHCP, set up SSIDs with different authentication methods, and connect multiple wireless clients. Through this, I strengthened my grasp of concepts like VLANs, WPA2 security, DHCP scopes, and RADIUS authentication. Although I faced challenges connecting one of the enterprise clients, troubleshooting it helped me understand possible real-world issues in WLAN deployment. Overall, this task improved my confidence in configuring wireless infrastructure and highlighted the importance of planning, accuracy, and verification in network setup.