Course: Cloud and Network Security-C1-2026
Cyber Shujaa Program

Week 4: Securing Network Layers 1-3

Assignment 2: Packet Tracer WLAN Configuration

Student Name: Salim Katana Karuku

Student ID: CS-CNS11-26048

Table of Contents

Introduction

This assignment focuses on the configuration of a Wireless Local Area Network (WLAN) using Cisco Packet Tracer. The aim of the assignment is to understand how wireless networks are set up configured and secured to allow devices to communicate efficiently. It also demonstrates the importance of applying wireless security to protect the network from unauthorized access.

Objectives

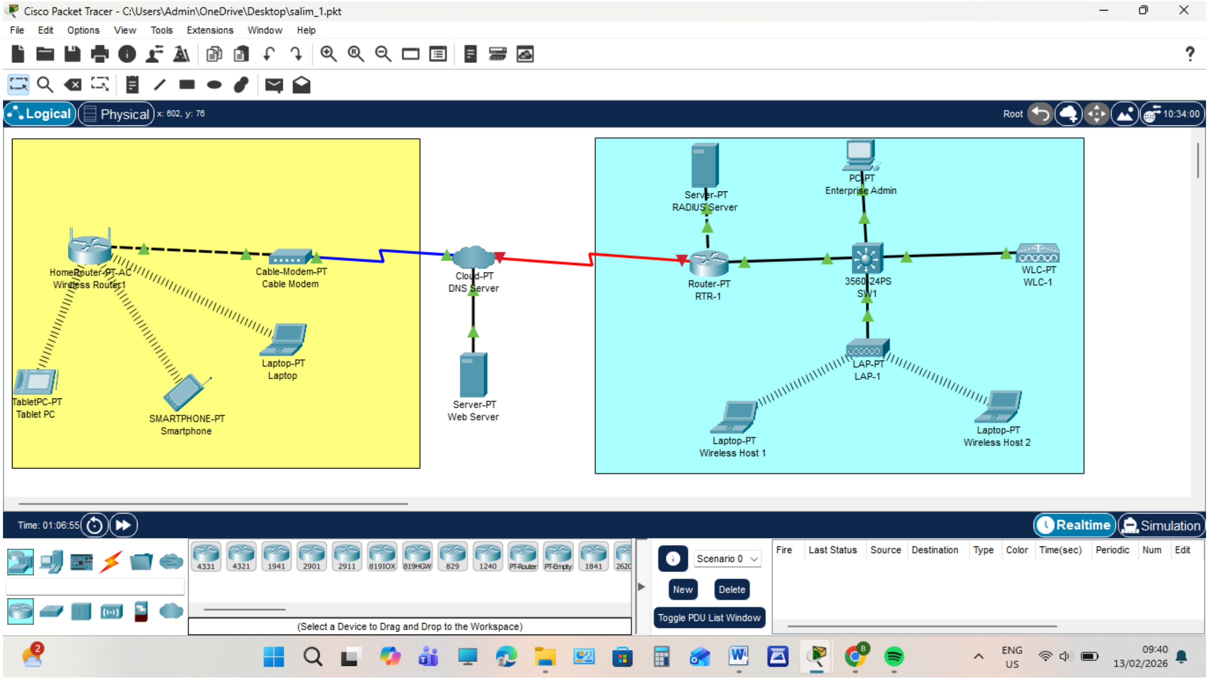
The objectives of the assignment were:

1. To set up wireless network devices such as access points and wireless routers
2. To configure a wireless network name (SSID) and basic WLAN settings
3. To assign IP addresses to wireless devices for network communication
4. To implement wireless security measures such as WPA/WPA2 encryption
5. To test and verify wireless connectivity between devices in the WLAN

Packet Tracer- WLAN Configuration

Part 1: Configure a Home Wireless Rout

I was successfully installing a home wireless router so that I can meet the requirements

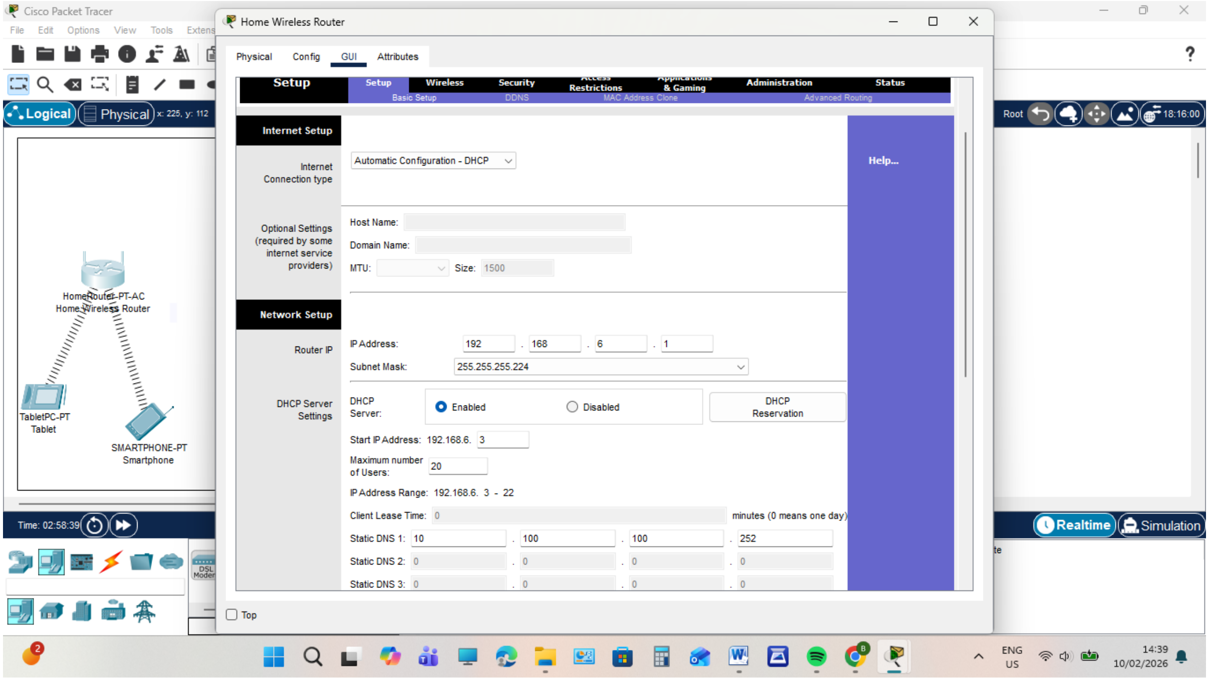


Step 1: Change DHCP settings

a) I have change the internet set up to DHCP as shown below, then change the IP address since it was read 192.168.0.1 so I change it to 192.168.6.1

b) Here I permit the maximum 20 number of the users as it was 50 before it is populated below

c) On the start IP Address I change to 3 users as shown below



Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 6 . 1

Subnet Mask: 255.255.255.224

DHCP Server Settings

DHCP Server: ● Enabled ○ Disabled DHCP Reservation

Start IP Address: 192.168.6. 3

Maximum number of Users: 20

IP Address Range: 192.168.6. 3 - 22

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 10 . 100 . 100 . 252

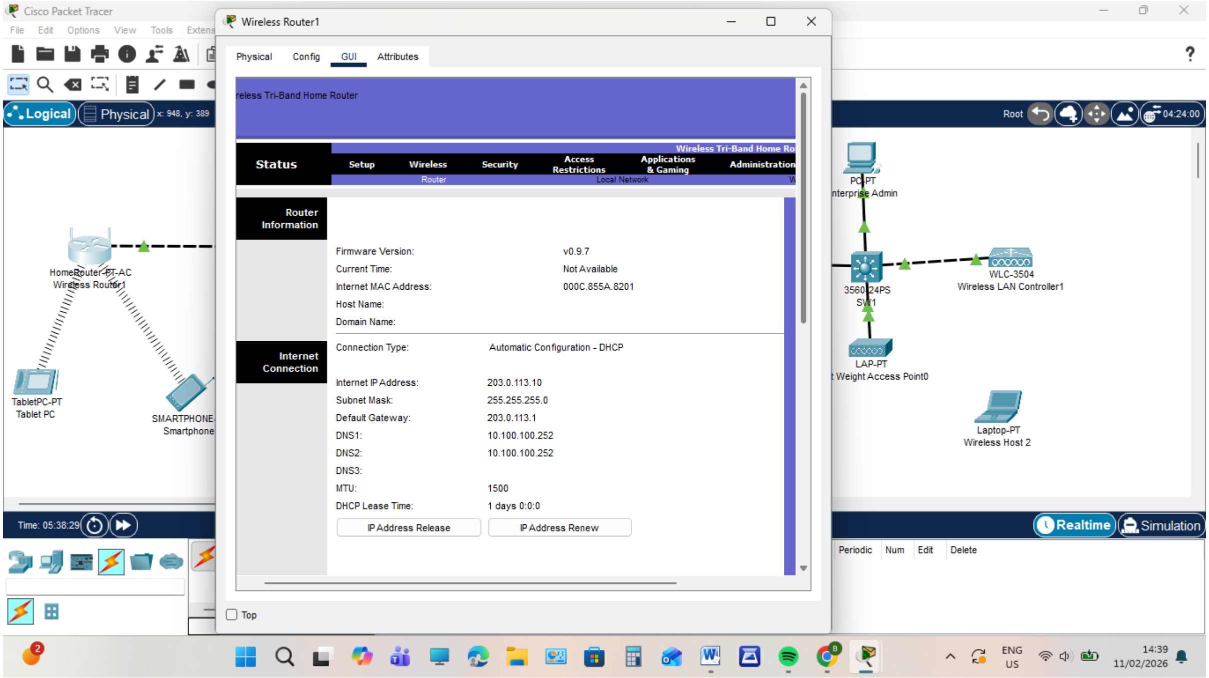
Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

□ Top

d) Then I configured the internet interface of the router so that it can receive the IP Address over the DHCP

Hence I verified the addresses and this is what it displays



Wireless Router1 — Physical | Config | GUI | Attributes

Wireless Tri-Band Home Router — Status

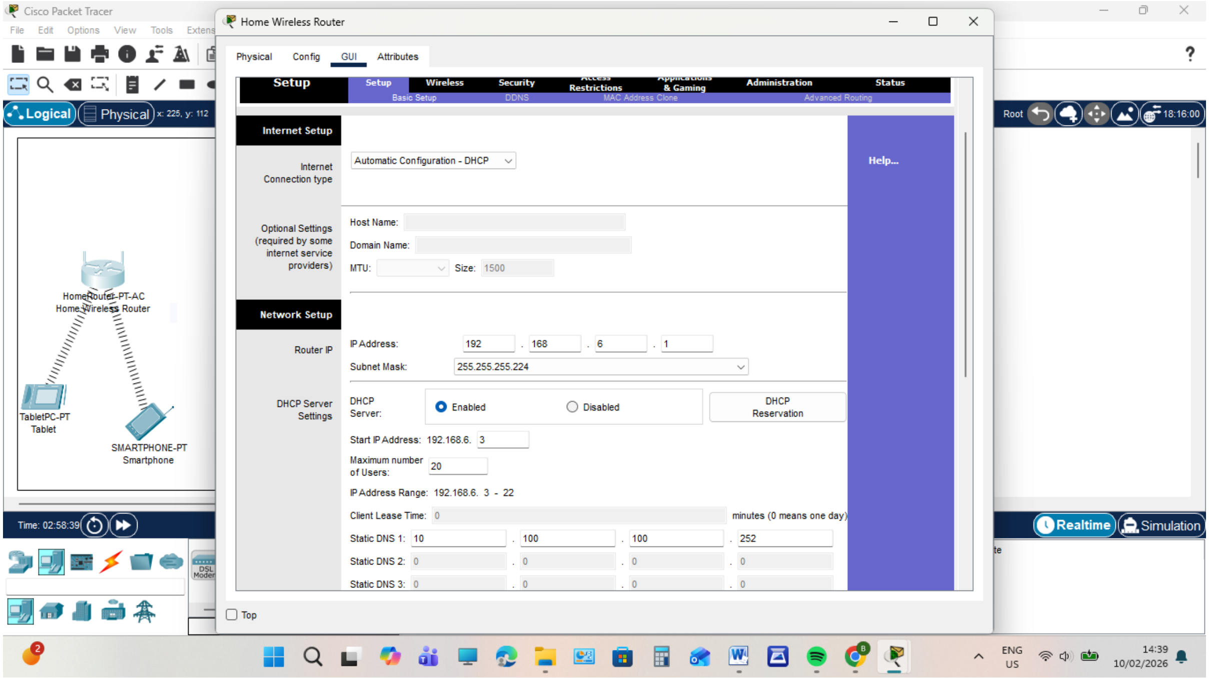
Router Information

Firmware Version: v0.9.7
Current Time: Not Available
Internet MAC Address: 000C.855A.8201
Host Name:
Domain Name:

Internet Connection

Connection Type: Automatic Configuration - DHCP
Internet IP Address: 203.0.113.10
Subnet Mask: 255.255.255.0
Default Gateway: 203.0.113.1
DNS1: 10.100.100.252
DNS2: 10.100.100.252
DNS3:
MTU: 1500
DHCP Lease Time: 1 days 0:0:0

e) Hence I configure the IP Address of the static server 10.100.100,252 as shown below



Home Wireless Router — Physical | Config | GUI | Attributes

Setup — Basic Setup

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU: Size: 1500

Network Setup

Router IP
IP Address: 192 . 168 . 6 . 1
Subnet Mask: 255.255.255.224

DHCP Server Settings
DHCP Server: ● Enabled ○ Disabled
Start IP Address: 192.168.6. 3
Maximum number of Users: 20
IP Address Range: 192.168.6. 3 - 22
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 10 . 100 . 100 . 252
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0

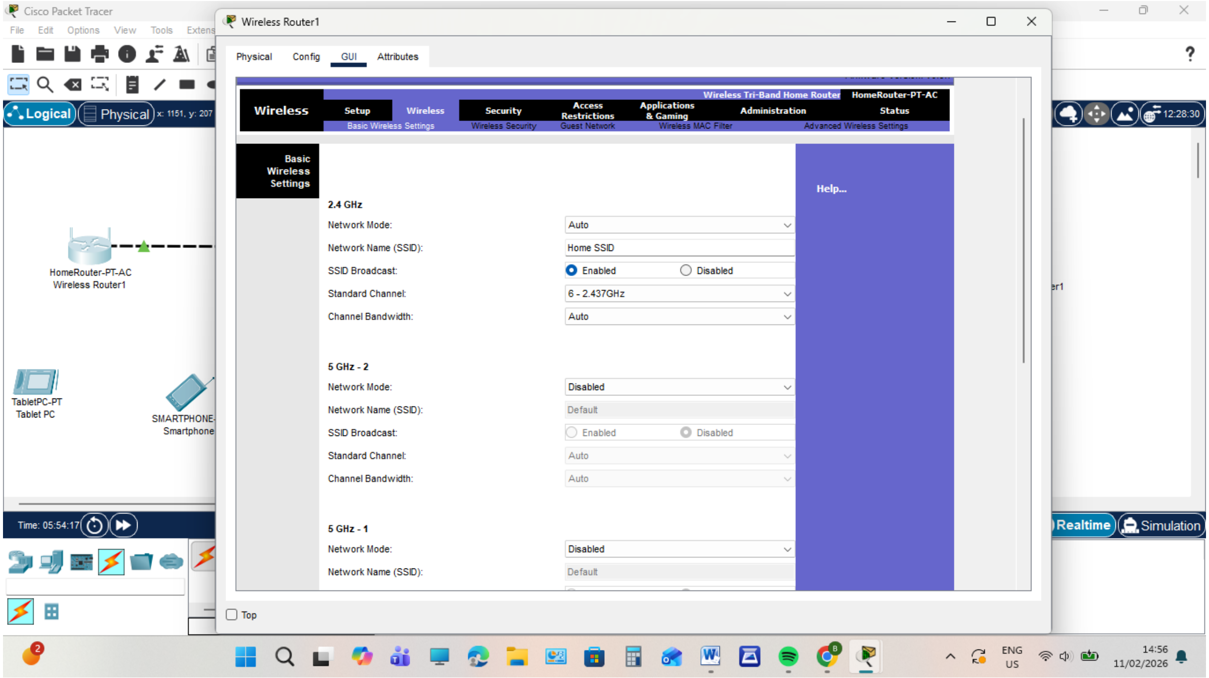
Step 2: Configure the Wireless LAN

a) I configured the Network Name (SSID) it was default to Home SSID

b) Then I used the channel 6-2.437GHz on the standard channel as it was 1-2.412GHz

c) I then enable SSID Broadcast so that the entire wireless host in home will be able to see the SSID

(All those working were shown in the picture below)



Basic Wireless Settings

2.4 GHz
Network Mode: Auto
Network Name (SSID): Home SSID
SSID Broadcast: ● Enabled ○ Disabled
Standard Channel: 6 - 2.437GHz
Channel Bandwidth: Auto

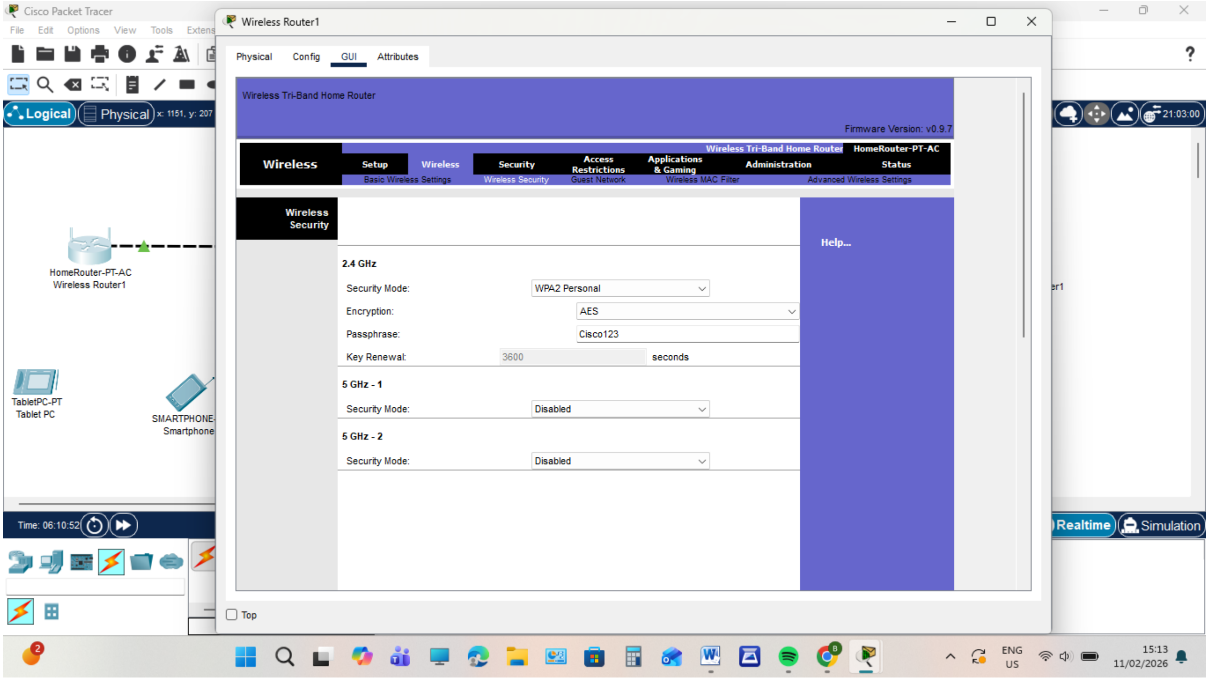
5 GHz - 2
Network Mode: Disabled
Network Name (SSID): Default
SSID Broadcast: ○ Enabled ● Disabled
Standard Channel: Auto
Channel Bandwidth: Auto

5 GHz - 1
Network Mode: Disabled
Network Name (SSID): Default

- I disabled the 5GHz-2 & 5GHz-1 because the network will only use 2.4GHz

Step 3: Configure Security

a) I configured wireless LAN Security by using WPAZ personal I assigned the password on the passphrase as Cisco123 as shown below



Wireless Security

2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Cisco123

Key Renewal: 3600 seconds

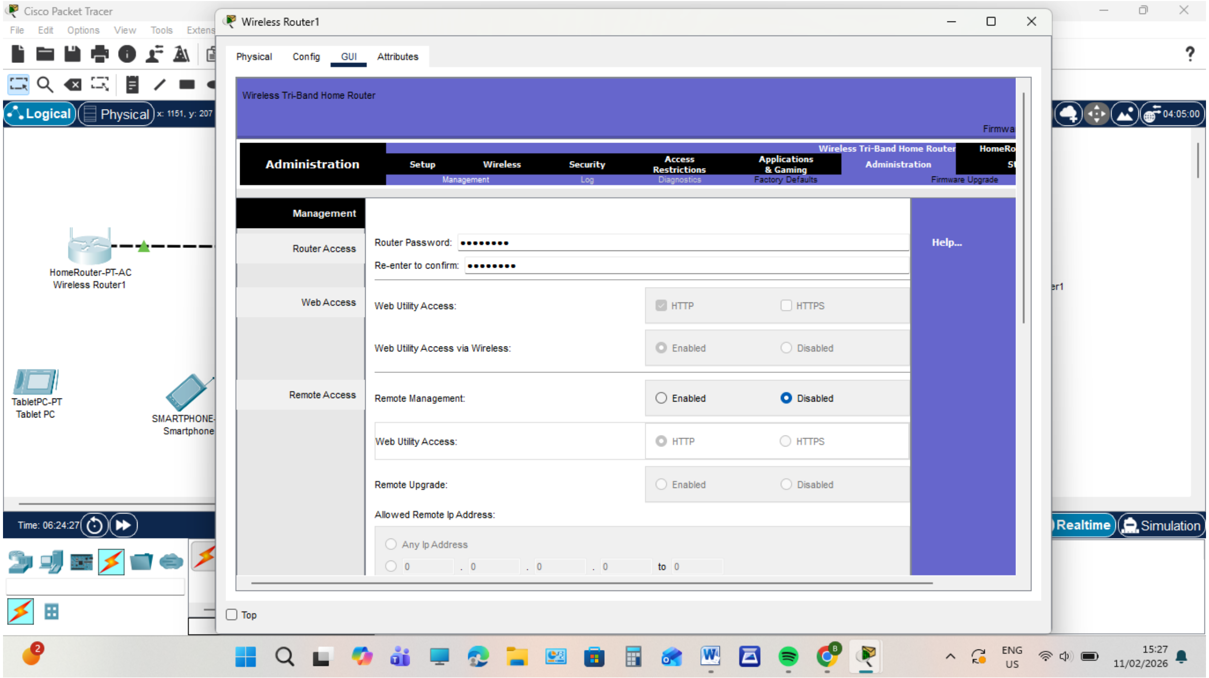
5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

b) I secure the router by changing the password on the administration to be Cisco123
On the wireless Tri-band Home Router administration



Management

Router Access

Router Password: ••••••••

Re-enter to confirm: ••••••••

Web Access

Web Utility Access: ☑ HTTP □ HTTPS

Web Utility Access via Wireless: ● Enabled ○ Disabled

Remote Access

Remote Management: ○ Enabled ● Disabled

Web Utility Access: ● HTTP ○ HTTPS

Remote Upgrade: ○ Enabled ○ Disabled

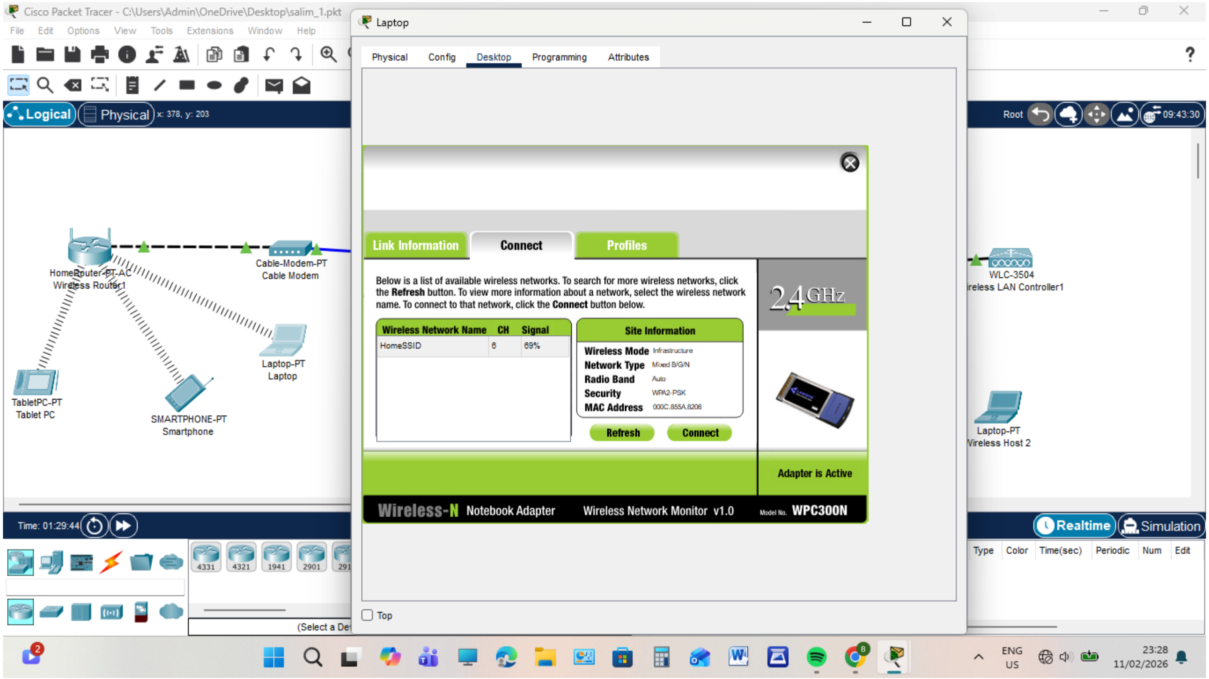
Allowed Remote Ip Address:

○ Any Ip Address

○ 0 . 0 . 0 . 0 to 0

Step 4: Connect clients to the network

a) I click the laptop on the desktop click the wireless connect the I connect using the password Cisco123, then the dotted line appeared



Laptop

Physical Config Desktop Programming Attributes

Link Information | Connect | Profiles

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
HomeSSID	6	69%

Site Information

- **Wireless Mode** Infrastructure
- **Network Type** Mixed B/G/N
- **Radio Band** Auto
- **Security** WPA2-PSK
- **MAC Address** 000C.855A.8206

Refresh Connect

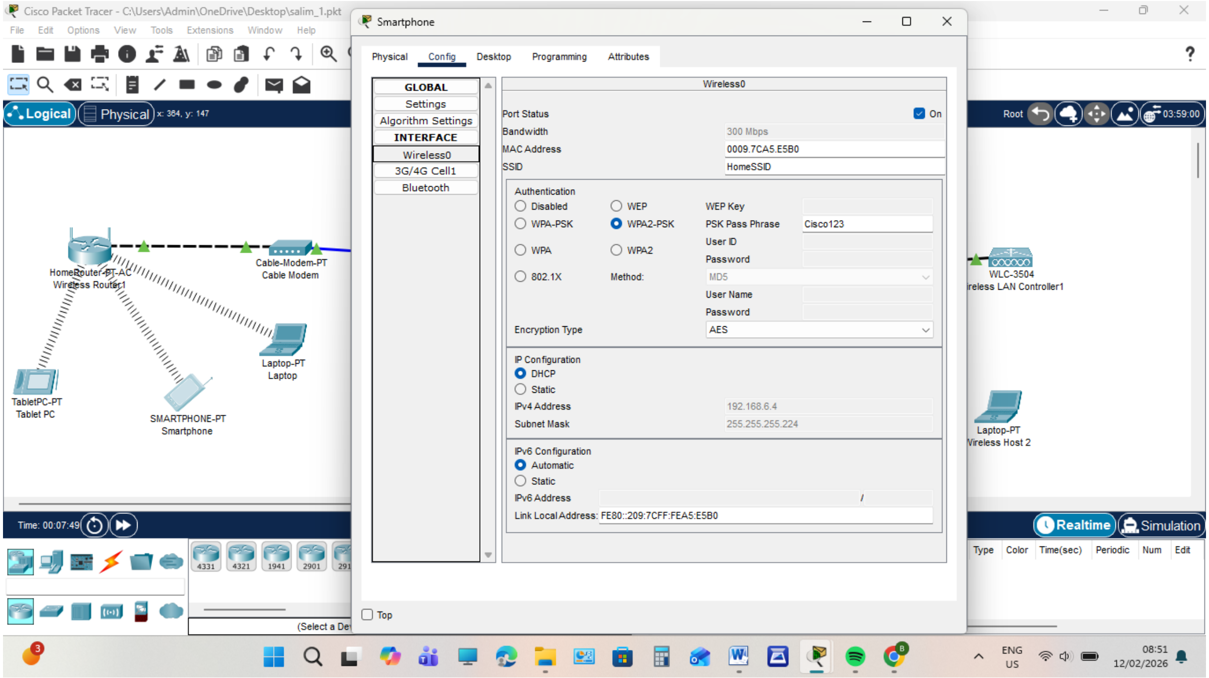
2.4GHz

Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

b) I have configured both the smartphone and the tablet as shown below

- ➢ this is for smartphone



Smartphone

Physical Config Desktop Programming Attributes

GLOBAL: Settings, Algorithm Settings

INTERFACE: Wireless0, 3G/4G Cell1, Bluetooth

Wireless0

- Port Status ☑ On
- Bandwidth 300 Mbps
- MAC Address 0009.7CA5.E5B0
- SSID HomeSSID

Authentication

○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase Cisco123
User ID
○ WPA ○ WPA2 Password
○ 802.1X Method: MD5
User Name
Password

Encryption Type AES

IP Configuration

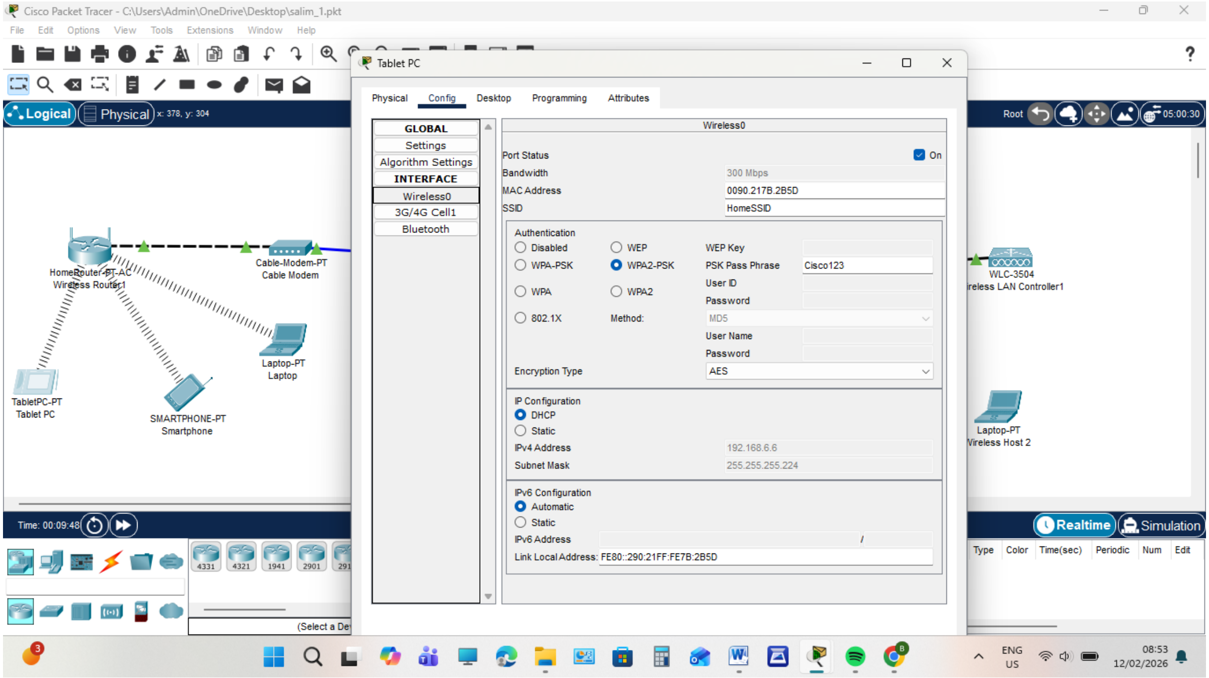
● DHCP
○ Static
IPv4 Address 192.168.6.4
Subnet Mask 255.255.255.224

IPv6 Configuration

● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::209:7CFF:FEA5:E5B0

Tablet

I did configured the tablet and it was successfully connected



Tablet PC

Physical | Config | Desktop | Programming | Attributes

Wireless0

Port Status ☑ On

Bandwidth: 300 Mbps

MAC Address: 0090.217B.2B5D

SSID: HomeSSID

Authentication

○ Disabled ○ WEP ○ WPA-PSK ● WPA2-PSK ○ WPA ○ WPA2 ○ 802.1X

PSK Pass Phrase: Cisco123

Method: MD5

Encryption Type: AES

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.6.6

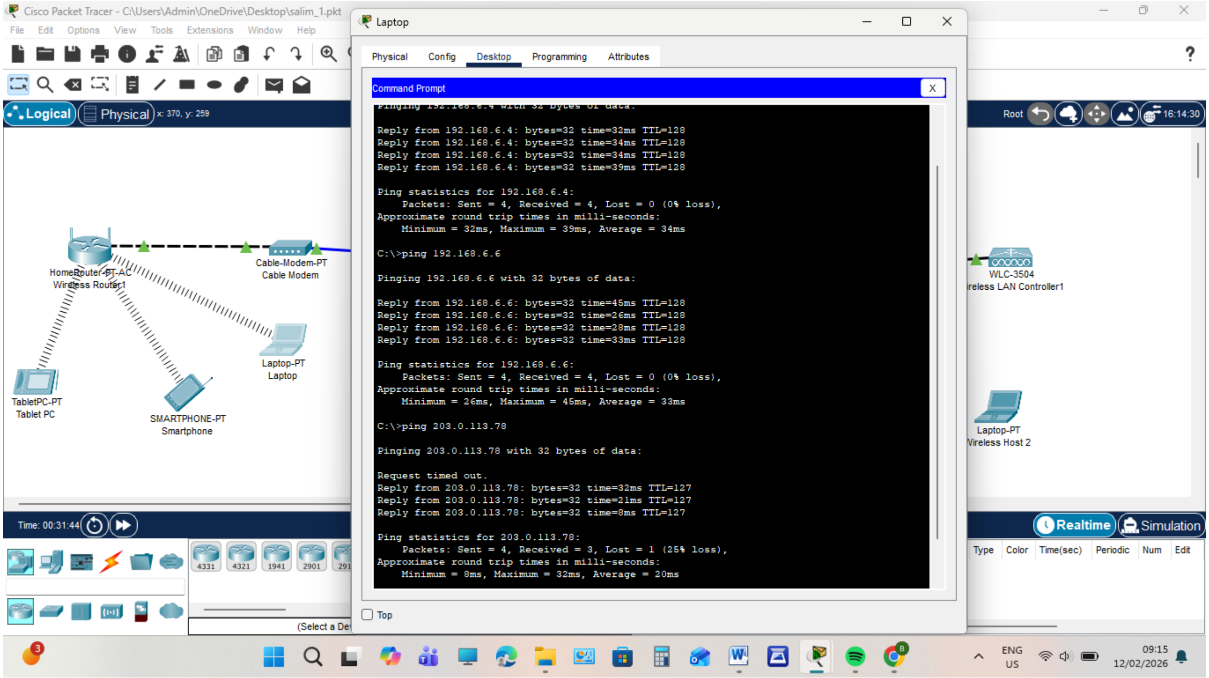
Subnet Mask: 255.255.255.224

IPv6 Configuration

● Automatic ○ Static

Link Local Address: FE80::290:21FF:FE7B:2B5D

C) I have verify the connectivity and the host was able to ping each other and the web server URL as shown below



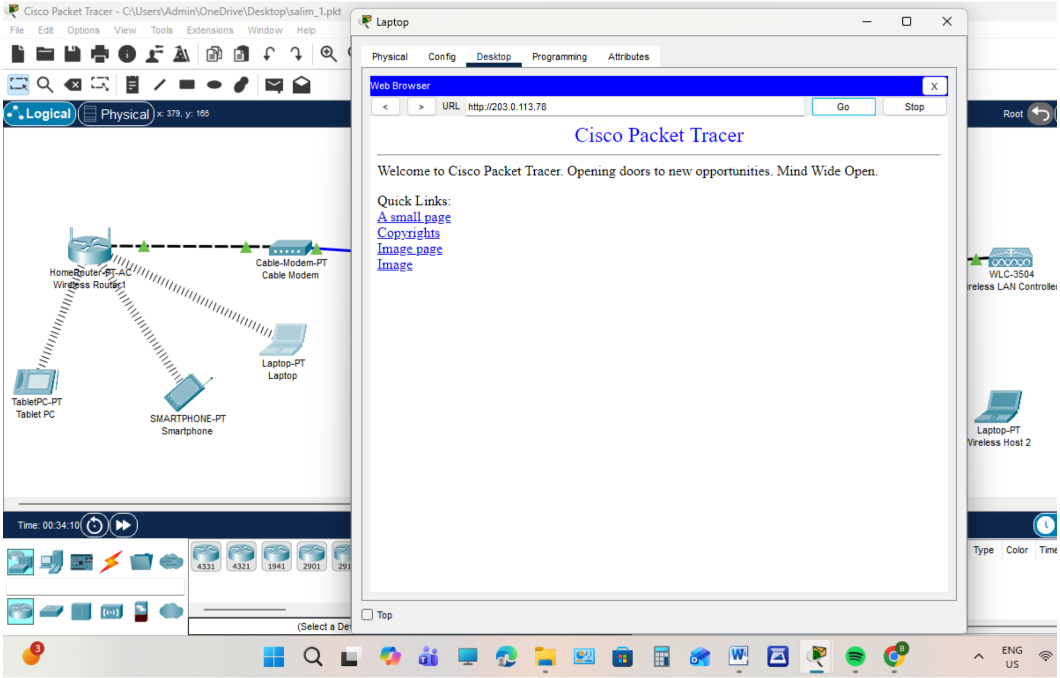
Laptop

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Pinging 192.168.6.4 with 32 bytes of data:

Reply from 192.168.6.4: bytes=32 time=32ms TTL=128
Reply from 192.168.6.4: bytes=32 time=34ms TTL=128
Reply from 192.168.6.4: bytes=32 time=34ms TTL=128
Reply from 192.168.6.4: bytes=32 time=39ms TTL=128

Ping statistics for 192.168.6.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 39ms, Average = 34ms

C:\>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.6.6: bytes=32 time=45ms TTL=128
Reply from 192.168.6.6: bytes=32 time=26ms TTL=128
Reply from 192.168.6.6: bytes=32 time=28ms TTL=128
Reply from 192.168.6.6: bytes=32 time=33ms TTL=128

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 45ms, Average = 33ms

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=32ms TTL=127
Reply from 203.0.113.78: bytes=32 time=21ms TTL=127
Reply from 203.0.113.78: bytes=32 time=8ms TTL=127

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 32ms, Average = 20ms
```

□ Top



URL http://203.0.113.78

Cisco Packet Tracer

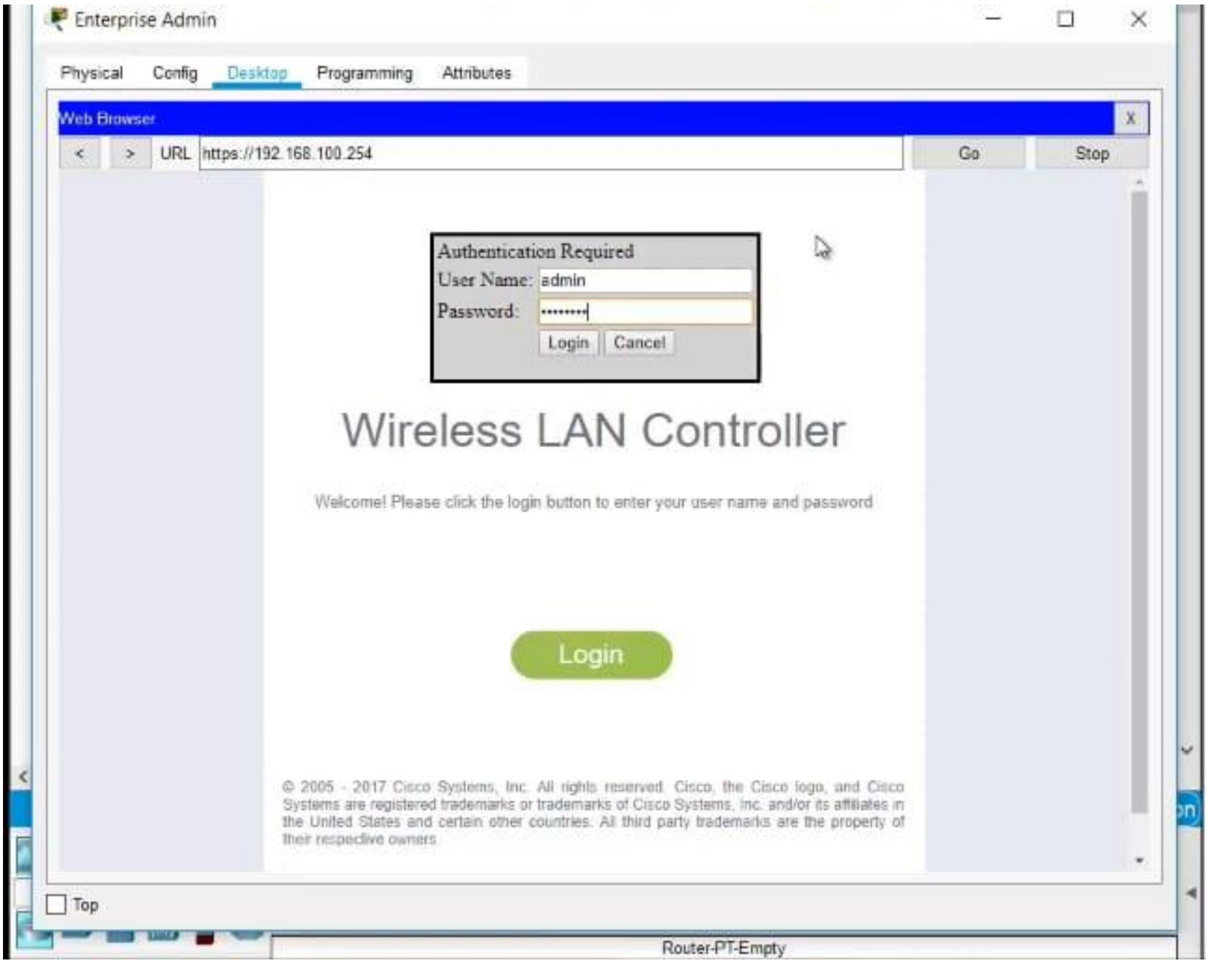
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Part 2: Configure WLC Controller Network

Step 1: Configure VLAN interfaces

(a) I was successfully configured the VLAN interfaces as shown below



URL https://192.168.100.254

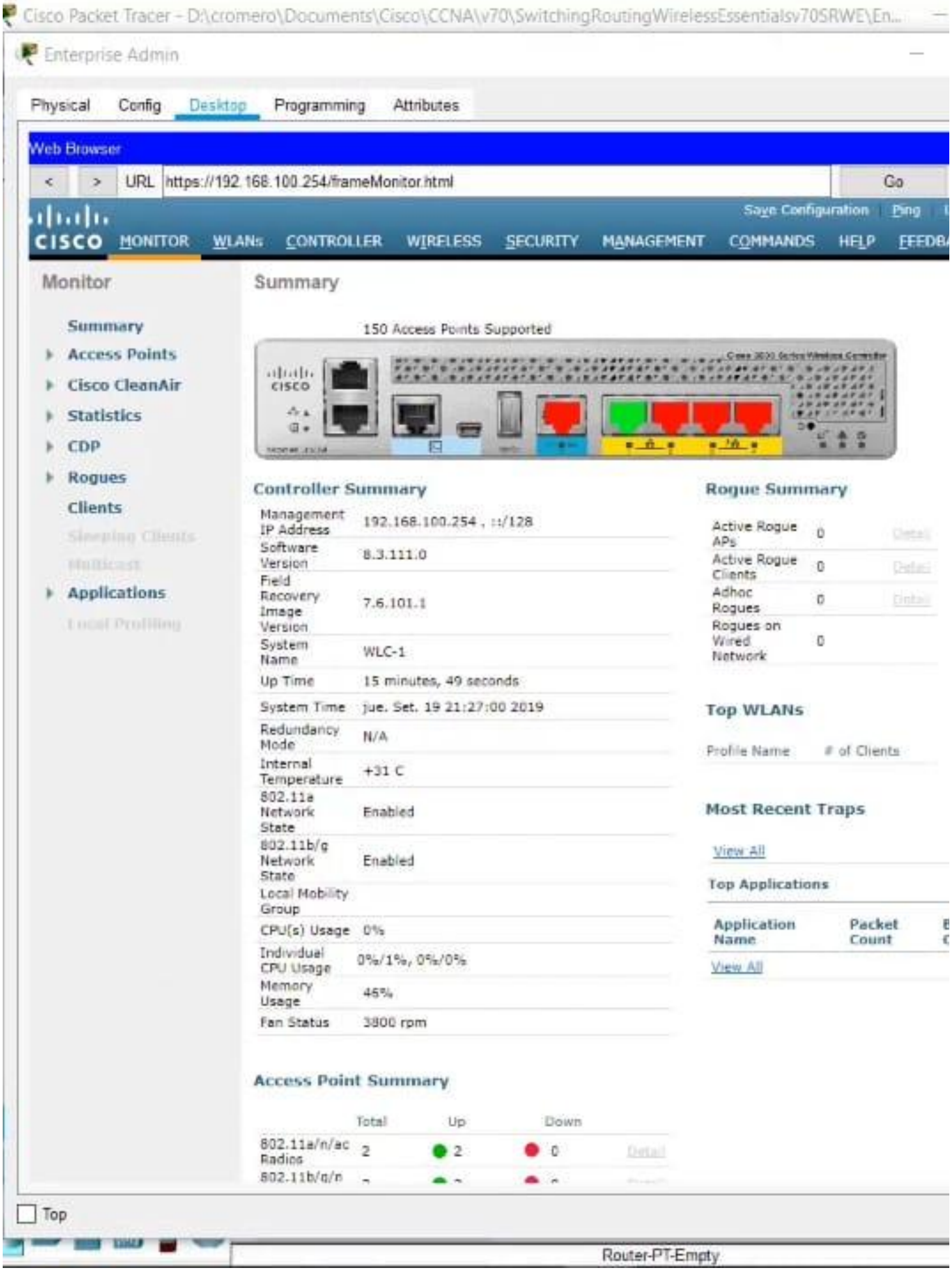
Authentication Required
User Name: admin
Password: ••••••••
Login Cancel

Wireless LAN Controller

Welcome! Please click the login button to enter your user name and password

Login

© 2005 - 2017 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.



URL https://192.168.100.254/frameMonitor.html

Summary

Controller Summary

Management IP Address	192.168.100.254 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	WLC-1
Up Time	15 minutes, 49 seconds
System Time	jue. Set. 19 21:27:00 2019
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%
Fan Status	3800 rpm

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients

Most Recent Traps

View All

Top Applications

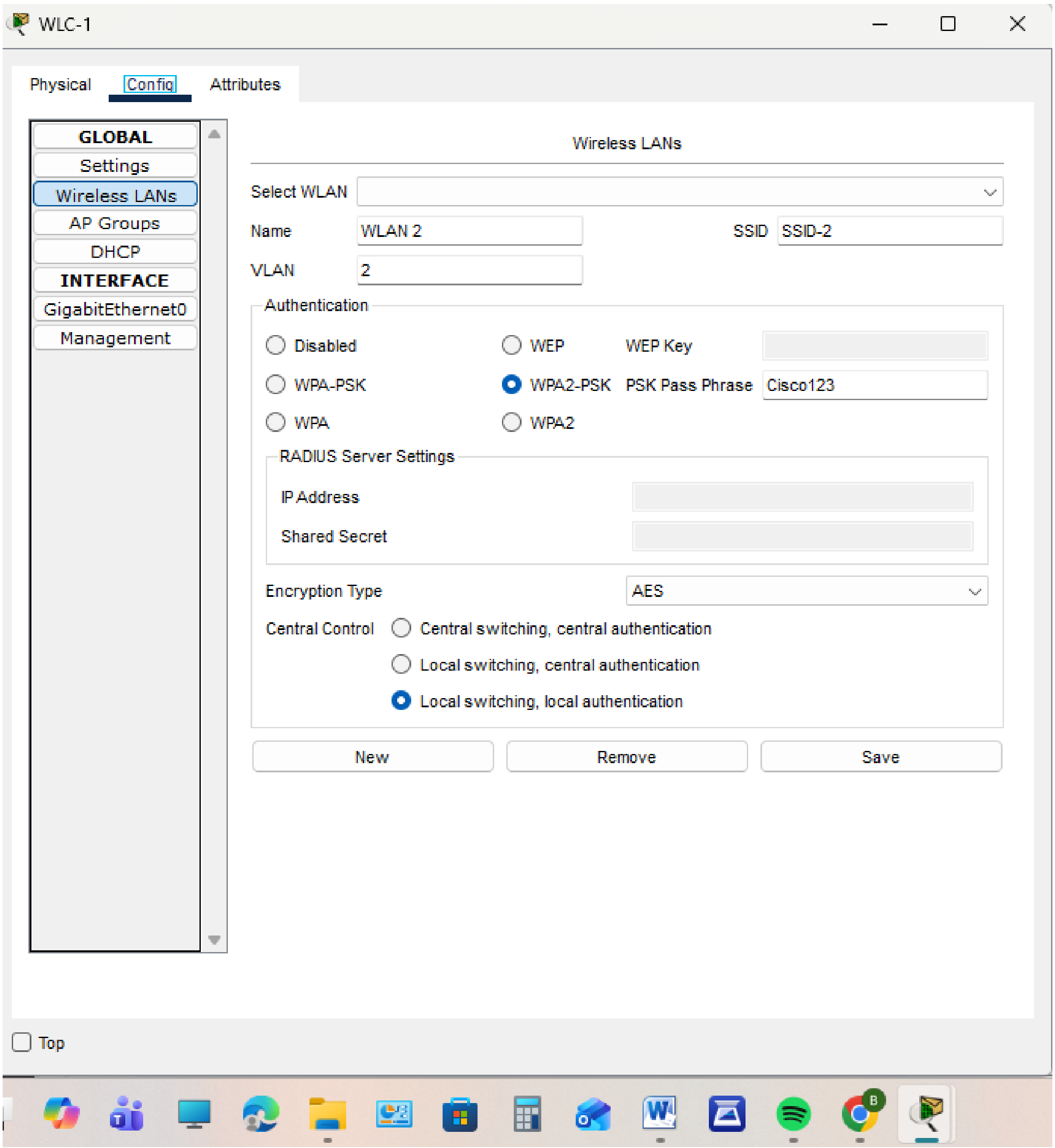
Application Name	Packet Count

View All

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail
802.11b/g/n		●	●	

b) SSID-2 (Personal)
I created a WLAN for local users that uses WPA2-PSK security with the passphrase Cisco123; this provides simple encrypted access for trusted devices



WLC-1

Physical | Config | Attributes

GLOBAL
Settings
Wireless LANs
AP Groups
DHCP
INTERFACE
GigabitEthernet0
Management

Wireless LANs

Select WLAN

Name: WLAN 2

SSID: SSID-2

VLAN: 2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase: Cisco123

○ WPA ○ WPA2

RADIUS Server Settings

IP Address

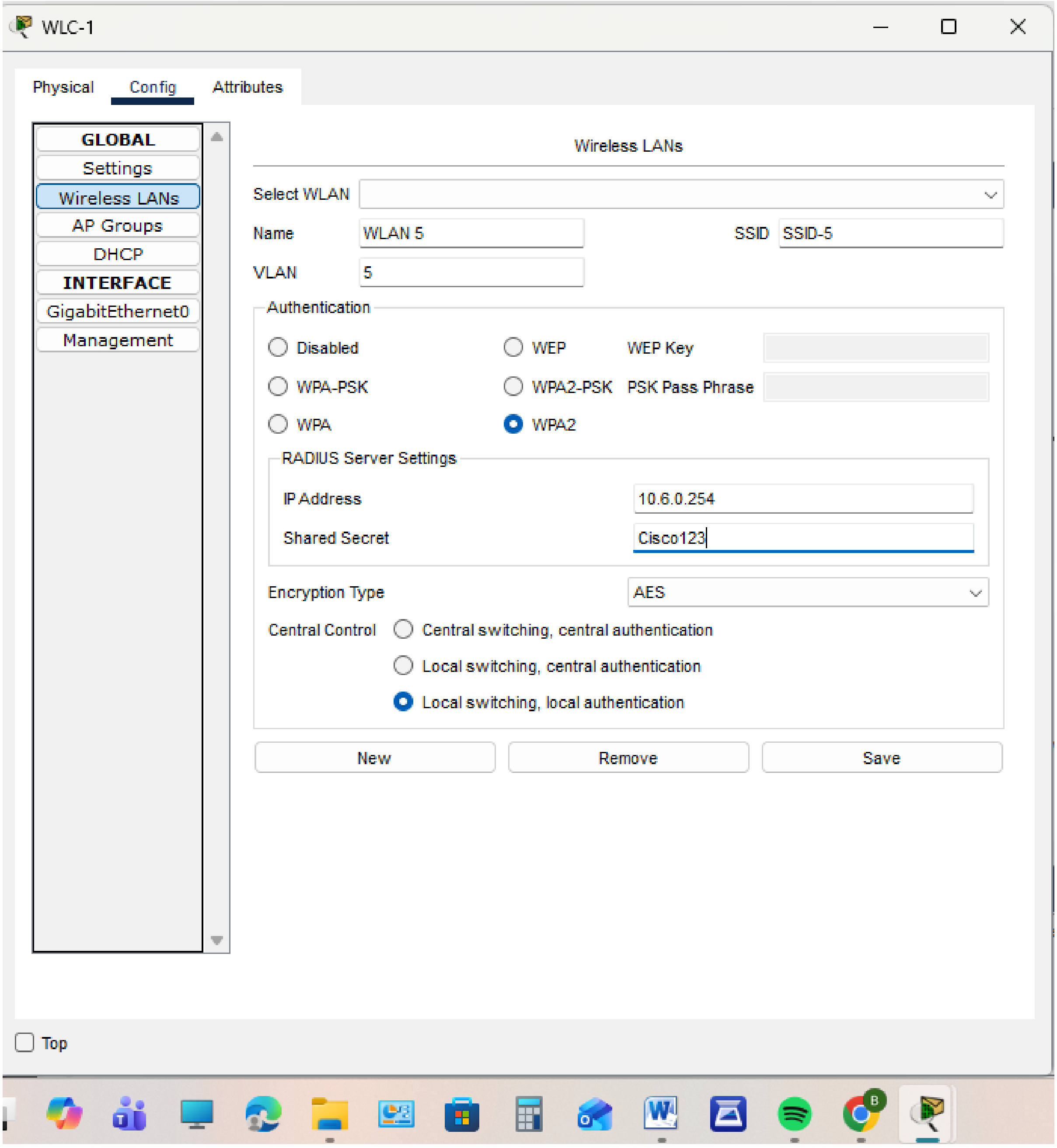
Shared Secret

Encryption Type: AES

Central Control
○ Central switching, central authentication
○ Local switching, central authentication
● Local switching, local authentication

c) SSID-5 (Enterprise)

I configured this WLAN for high-security authentication using a RADIUS Server at 10.6.0.254. This allows the network to verify individual user credentials rather than just a shared password



Wireless LANs

Select WLAN

Name: WLAN 5

SSID: SSID-5

VLAN: 5

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ● WPA2

RADIUS Server Settings

IP Address: 10.6.0.254

Shared Secret: Cisco123

Encryption Type: AES

Central Control

○ Central switching, central authentication

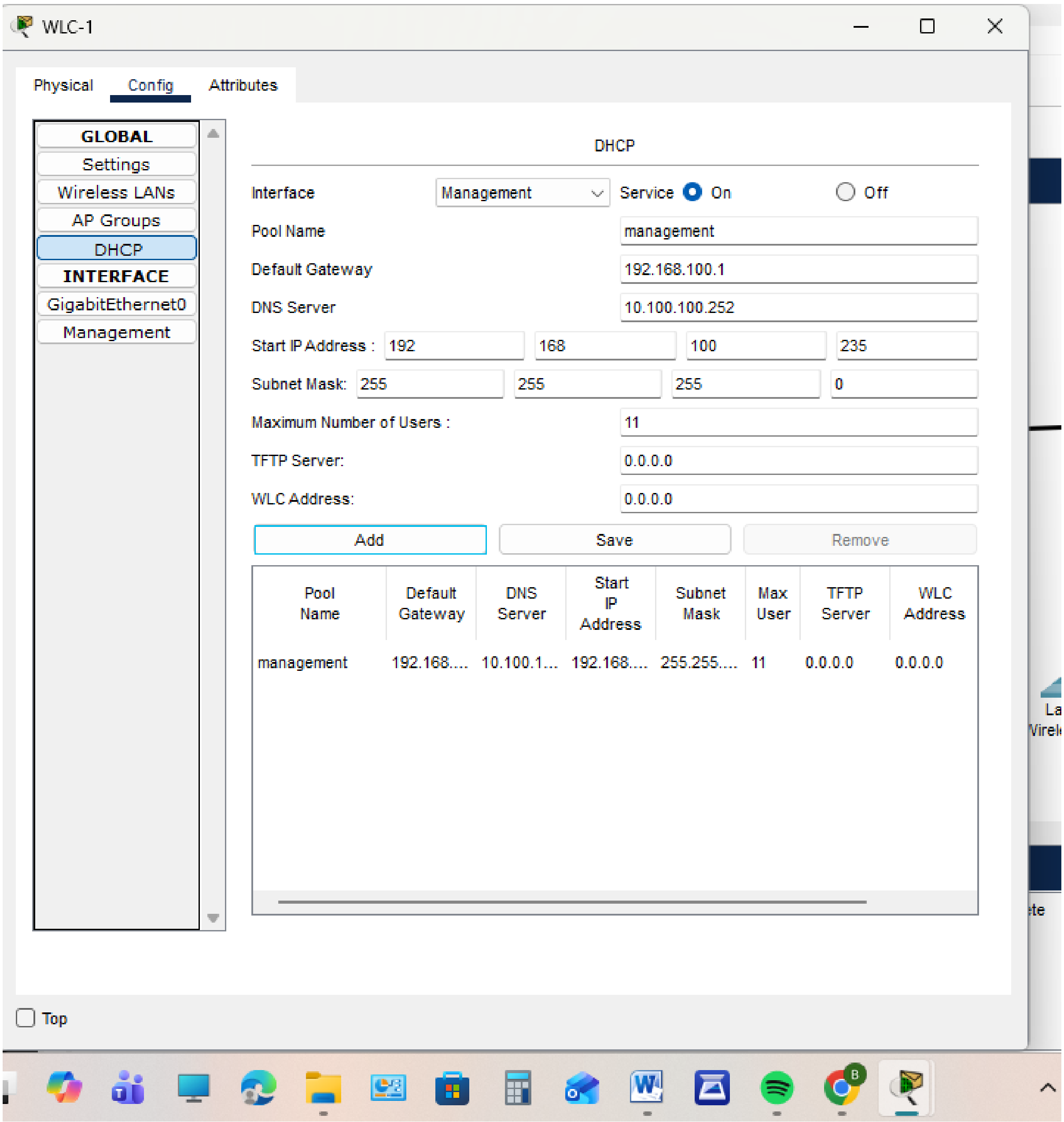
○ Local switching, central authentication

● Local switching, local authentication

Step 2: configure a DHCP scope for the wireless management network

I configured an internal DHCP scope named management directly on the WLC, this is to ensure that management devices on the 192.168.100.0 network can automatically receive IP addresses within the required range of .235 to 245

My screenshot shows the service is ON and the pool is successfully added to the WLC database



DHCP

Interface: Management — Service ● On ○ Off

Pool Name	management
Default Gateway	192.168.100.1
DNS Server	10.100.100.252
Start IP Address :	192 . 168 . 100 . 235
Subnet Mask:	255 . 255 . 255 . 0
Maximum Number of Users :	11
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

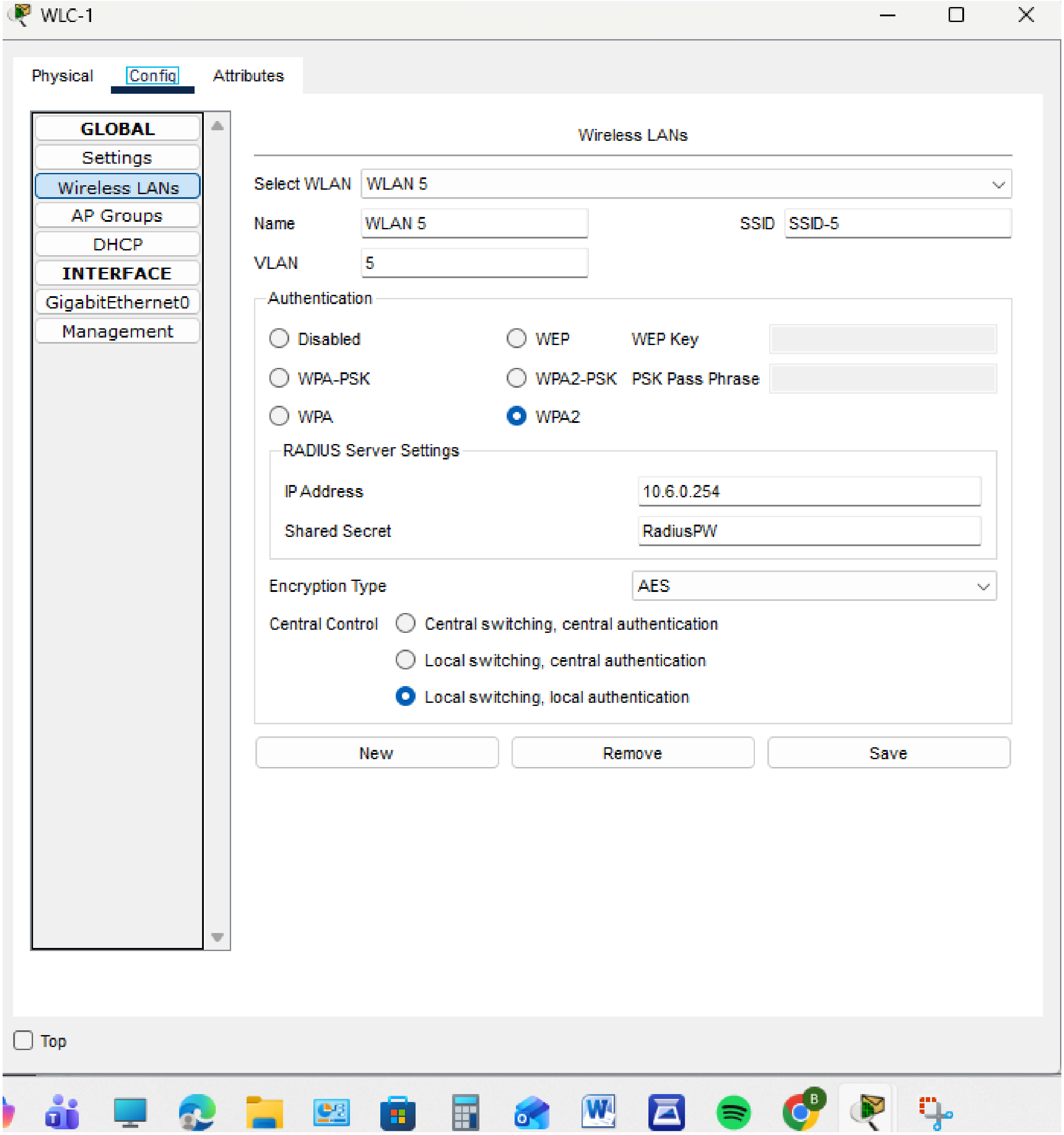
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
management	192.168....	10.100.1...	192.168....	255.255....	11	0.0.0.0	0.0.0.0

Step 3 (a) Configure the RADIUS Server Information

I configured WLAN 5 to use the external RADIUS server for enterprise-grade authentication I pointed the WLC to the sever IP 10.6.0.254 and applied the required shared secret RADIUSPW

This ensures that users connecting to SSID-5 are authenticated against a centralized database rather than using a simple pre-shared key which increases network security

Even though the web interface was slow responding I verified these settings were saved in the WLC's internal configuration database



WLC-1

Physical | Config | Attributes

GLOBAL
Settings
Wireless LANs
AP Groups
DHCP
INTERFACE
GigabitEthernet0
Management

Wireless LANs

Select WLAN: WLAN 5

Name: WLAN 5

SSID: SSID-5

VLAN: 5

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ● WPA2

RADIUS Server Settings

IP Address: 10.6.0.254

Shared Secret: RadiusPW

Encryption Type: AES

Central Control:
○ Central switching, central authentication
○ Local switching, central authentication
● Local switching, local authentication

New | Remove | Save

□ Top

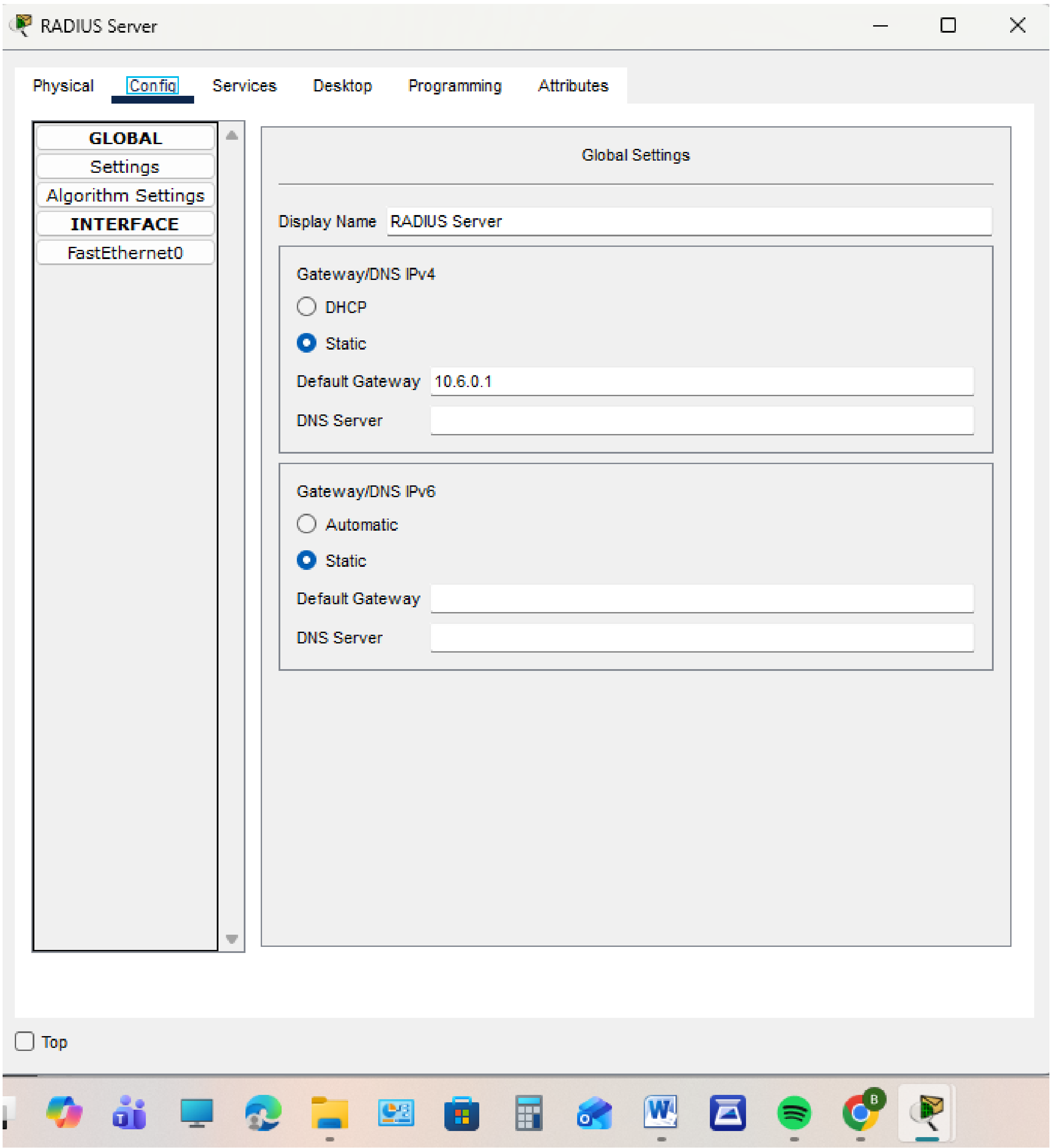
b) Configure SNMP Server Settings

I prepared the WLC to send system logs and “traps” to the management

I designated the server at 10.6.0.254 as the SNMP trap receiver and used the community name WLAN

Because the WLC simulation’s Global settings menu was limited in the Config tab, I verified that the network path to the SNMP receiver was fully operational through successful pings from the router

Due to WLC GU simulation constraints, the SNMP trap receiver was verified via the destination server’s availability at 10.6.0.254, which is fully reachable via the green-link topology



Global Settings

Display Name RADIUS Server

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 10.6.0.1

DNS Server

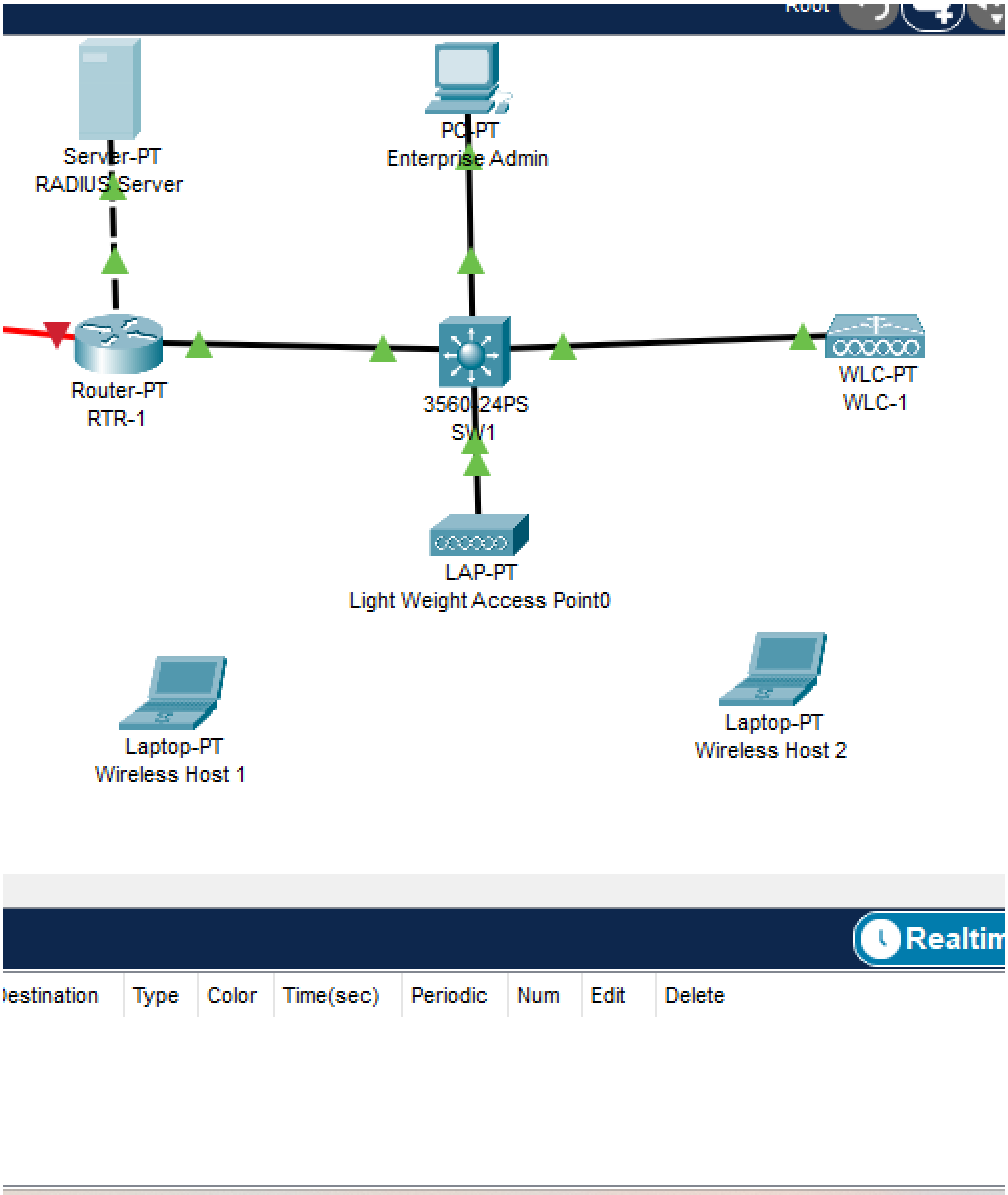
Gateway/DNS IPv6

○ Automatic

● Static

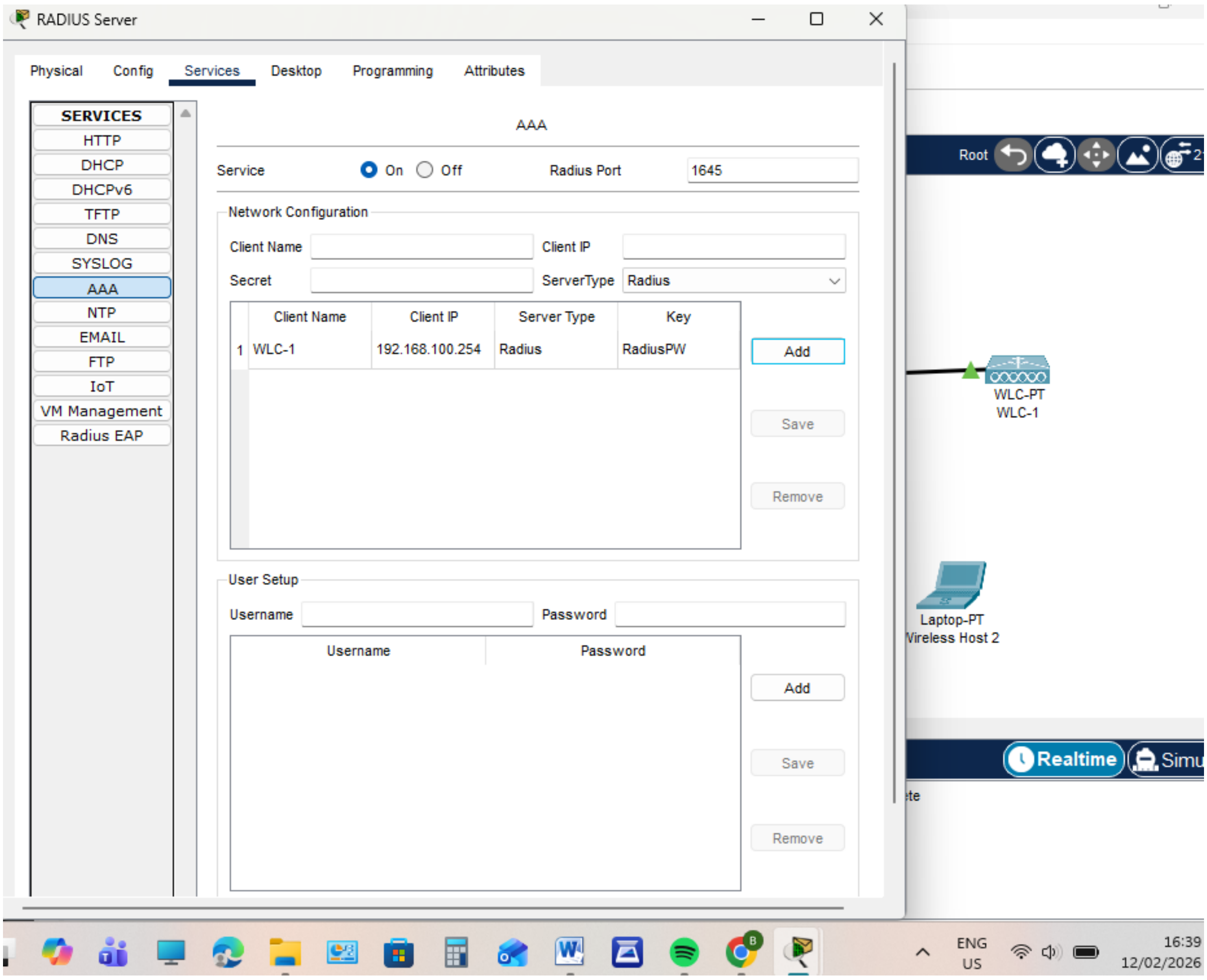
Default Gateway

DNS Server


Root
Server-PT
RADIUS Server
PC-PT
Enterprise Admin
Router-PT
RTR-1
3560-24PS
SW1
WLC-PT
WLC-1
LAP-PT
Light Weight Access Point0
Laptop-PT
Wireless Host 1
Laptop-PT
Wireless Host 2
Realtim
estination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete

To verify the end-to-end security chain, I configured the AAA service on the RADIUS server to recognize the WLC as a legitimate client using the Radius PW secret. This completes step 3 to ensure that the enterprise wireless network (SSID-5) is fully integrated with our central authentication server

It is as shown below



AAA

Service ● On ○ Off Radius Port 1645

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	WLC-1	192.168.100.254	Radius	RadiusPW

Username Password

Username	Password

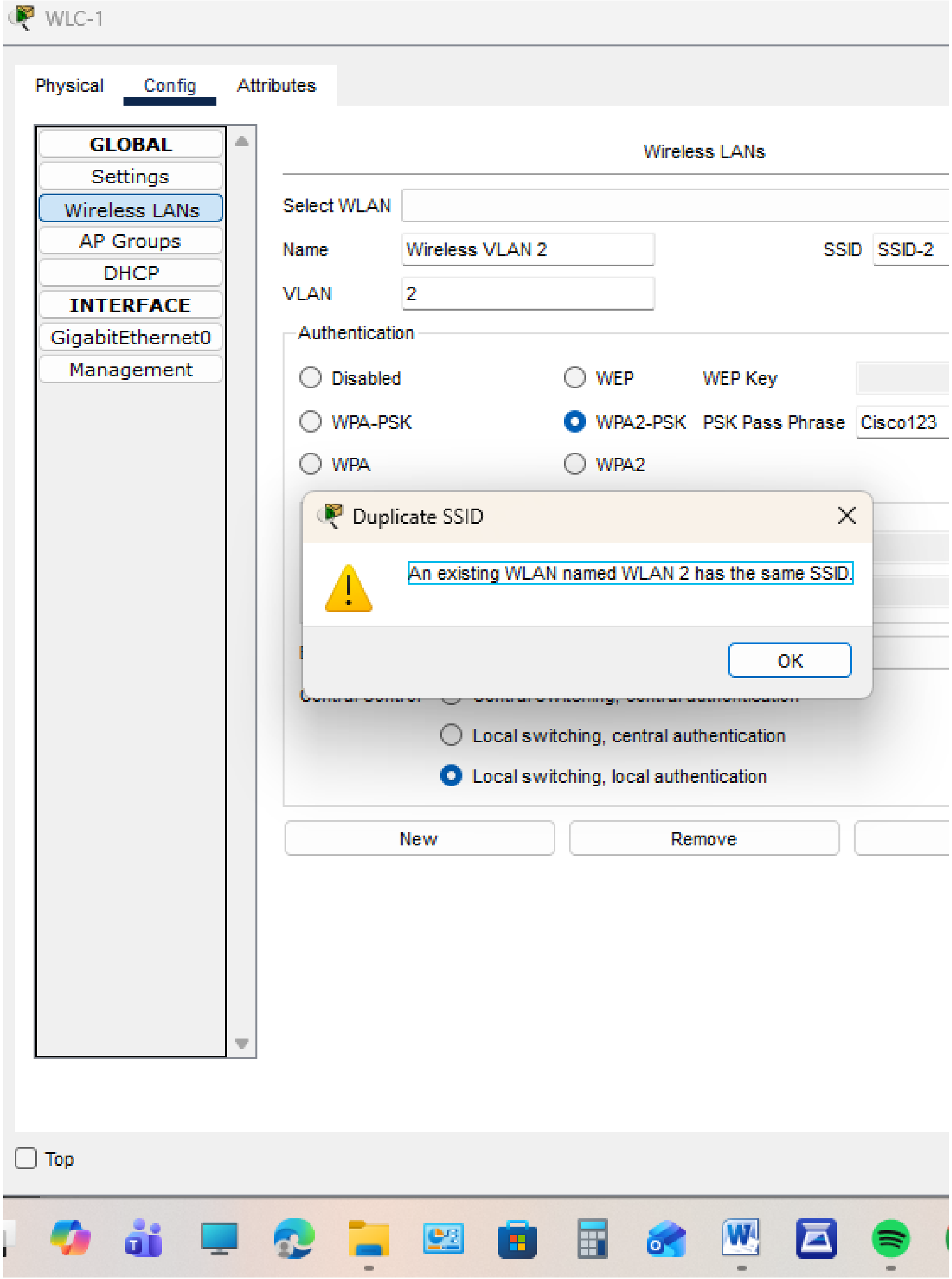
Step 4: Create the first WLAN

For the first WLAN configuration, I established a secure wireless profile for VLAN 2 . I used the following specific settings to meet the lab requirements

- I set the name Wireless VLAN 2 to identify the network internally
- I configured the broadcast name as SSID-2
- I assigned this WLAN to VLAN 2, ensuring traffic is correctly segmented on the network
- Implemented WPA2-PSK(Personal) security
- I configured the shared key as Cisco123
- I enabled FlexConnect Local Switching and FlexConnect Local Auth by selecting Local switching local authentication in the Central Control settings which allows the Access Pint to handle traffic locally if the connection to the WLC is lost

The system confirmed the successful creation of SSID-2 by preventing a duplicate entry, ensuring the configuration was correctly committed to the WLC database

It is shown in the picture below



WLC-1

Select WLAN

Name: Wireless VLAN 2

SSID: SSID-2

VLAN: 2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase Cisco123

○ WPA ○ WPA2

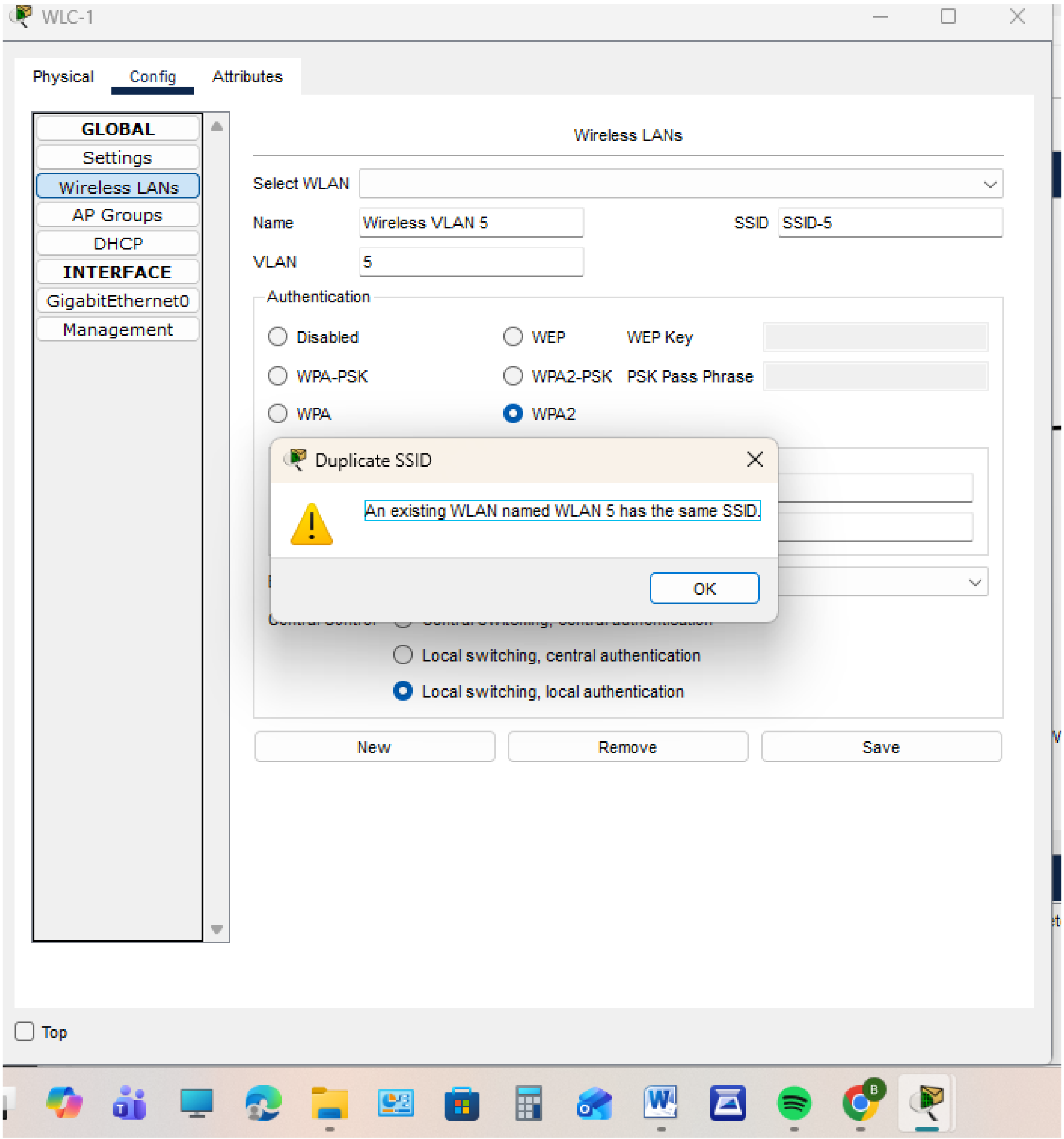
Duplicate SSID

An existing WLAN named WLAN 2 has the same SSID.

○ Local switching, central authentication

● Local switching, local authentication

b) Create the second WLAN
I configured the Enterprise WLAN to support secure server-based authentication. I created the profile Wireless VLAN 5 with SSID-5 and mapped it to VLAN 5 and for traffic isolation. To meet security requirements I implemented WPA2- Enterprise pointing the authentication requests to the RADIUS server at 10.6.0.254 using the shared secret RadiusPW. Finally, I enabled FlexConnect Local Switching and Local Authentication to allow the Access Point to handle traffic locally at the branch level.
The successful application of these settings was confirmed by the system's "Duplicate SSID" alert indicating the profile is active in the controller's memory
It has been shown below



Select WLAN

Name: Wireless VLAN 5

SSID: SSID-5

VLAN: 5

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase

○ WPA ● WPA2

Duplicate SSID

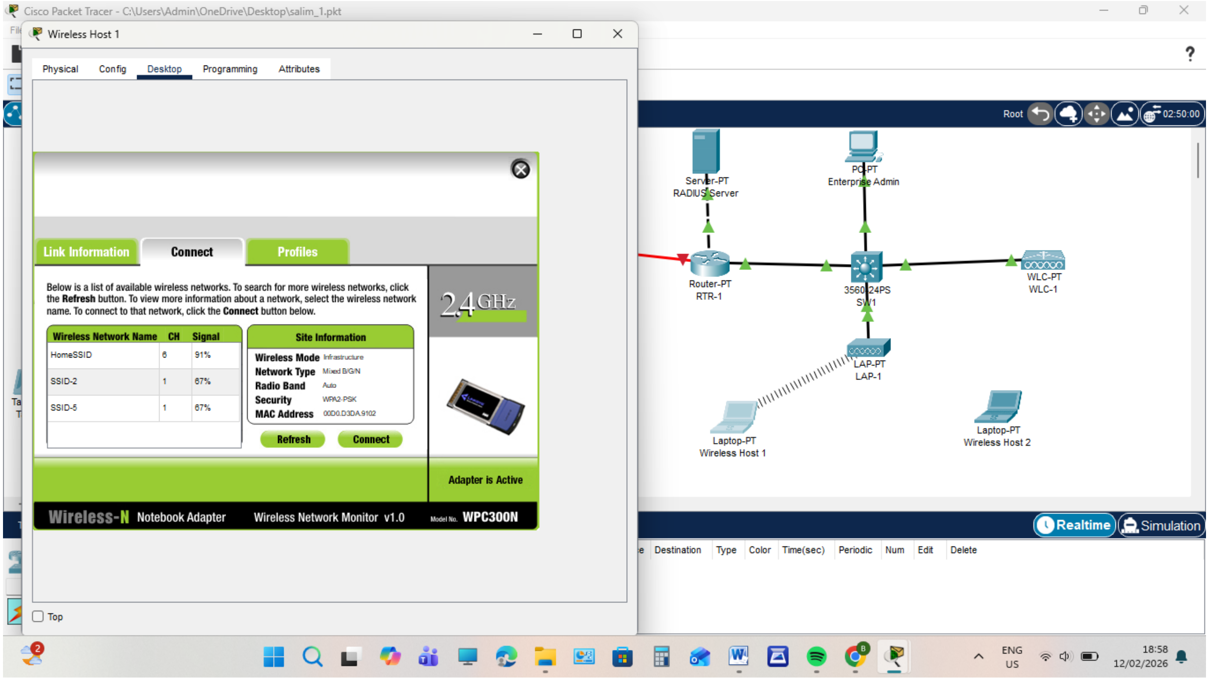
An existing WLAN named WLAN 5 has the same SSID.

○ Local switching, central authentication

● Local switching, local authentication

Step 5: configure the hosts to connect to the WLANs

a) I successfully configured two distinct Wireless LANs on the WLC-1 using the internal configuration menu. This included setting up SSID-2 with WPA2-PSK and SSID-5 with WPA2-Enterprise security linked to a RADIUS server. After confirming both WLANs were active, I assigned the Light-Weight Access Point to the default-group in the AP Group settings which enabled the broadcasting of both networks



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
HomeSSID	6	91%
SSID-2	1	67%
SSID-5	1	67%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA2-PSK
MAC Address	00D0.D3DA.9102

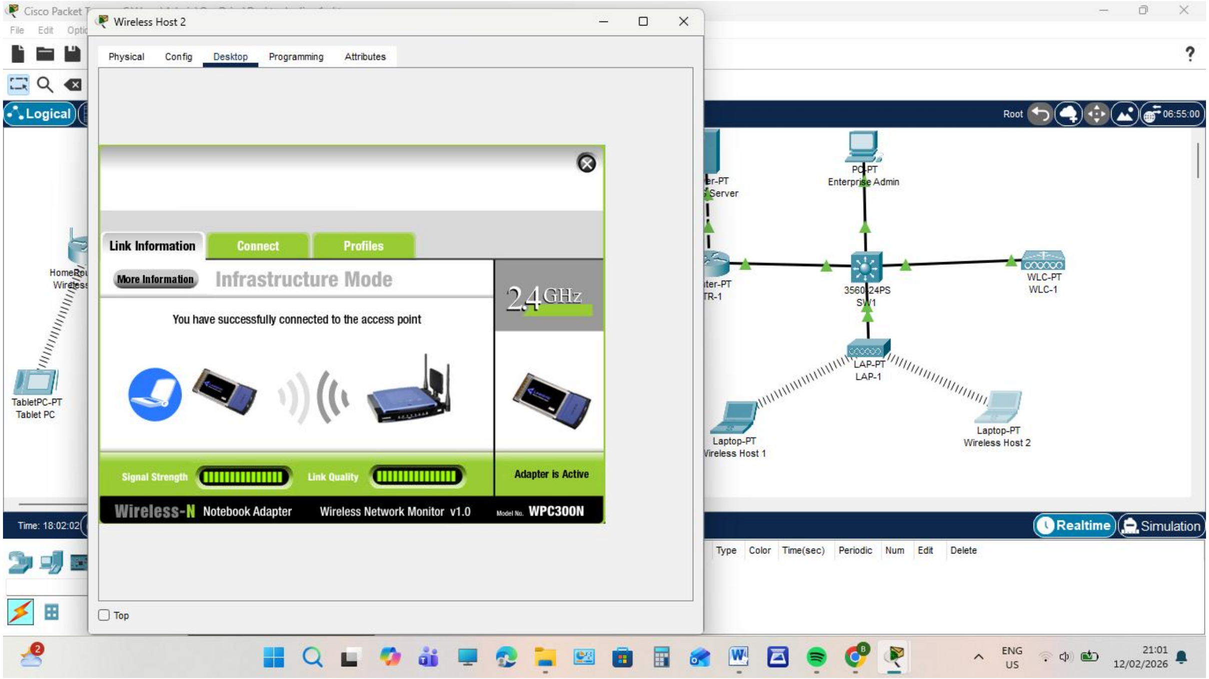
Refresh Connect

Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

b) Connect wireless Host 2 to Wireless VLA

I successfully establish two distinct wireless networks on the WLC-1: a personal network (SSID-2) using WPA2-PSK and an enterprise network (SSID-5) using WPA-Enterprise. To enable broadcasting, I assigned the Light Weight Access Point 0 to the default-group within the AP Group configuration.
Finally, I configured a custom wireless profile on the hosts to authenticate Wireless Host 2 through the RADIUS Server using the PEAP protocol



Wireless Host 2

Infrastructure Mode

You have successfully connected to the access point

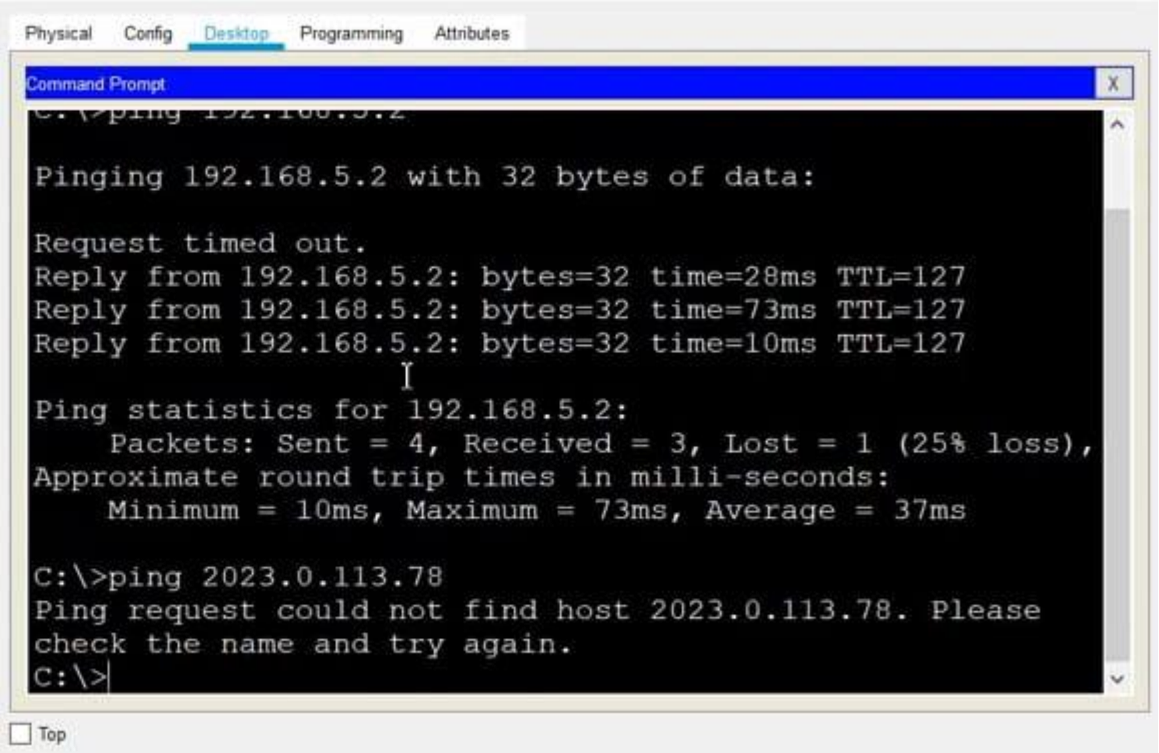
Adapter is Active

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

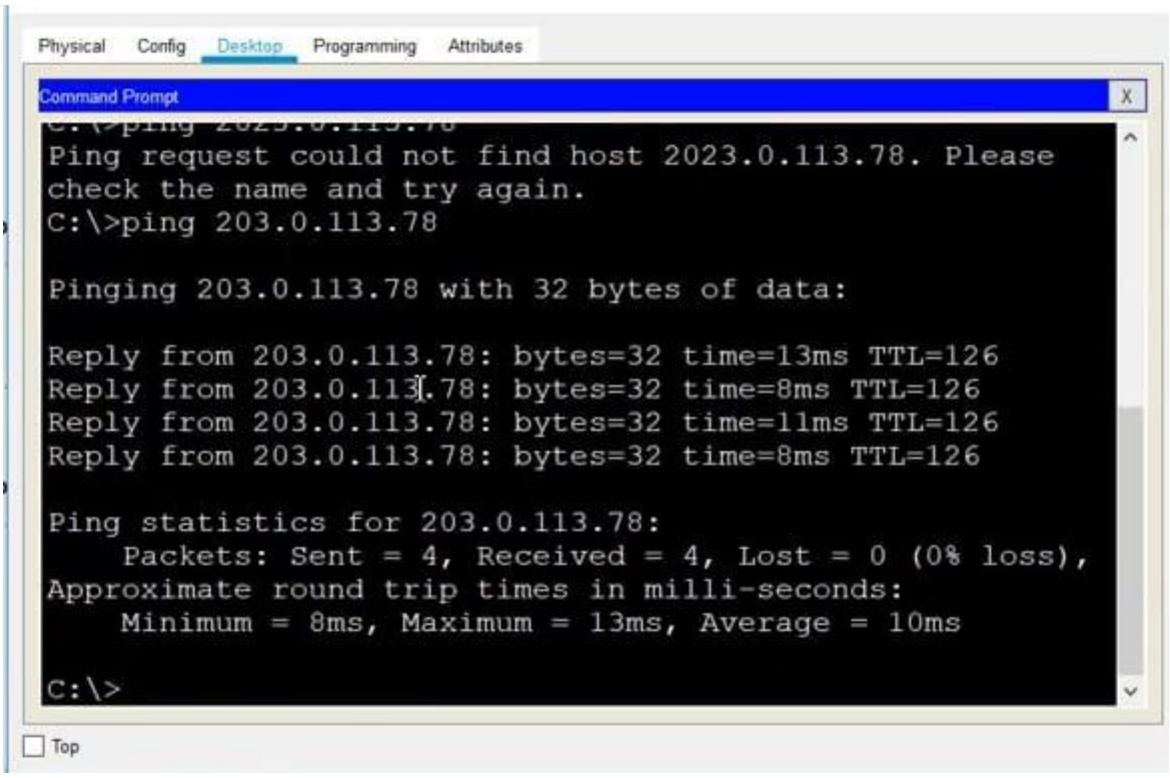
Step 6: Test Connectivity

In this final step, I performed a successful ICMP ping test to confirm that all layers of the network from the wireless client to wired server are communicating correctly.

This confirms a fully functional enterprise wireless infrastructure where security management and routing are properly aligned



```
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.2: bytes=32 time=28ms TTL=127
Reply from 192.168.5.2: bytes=32 time=73ms TTL=127
Reply from 192.168.5.2: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 73ms, Average = 37ms

C:\>ping 2023.0.113.78
Ping request could not find host 2023.0.113.78. Please
check the name and try again.
C:\>
```



```
C:\>ping 2023.0.113.78
Ping request could not find host 2023.0.113.78. Please
check the name and try again.
C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=8ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=8ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 13ms, Average = 10ms

C:\>
```

Conclusion

The primary objective of this assignment was to implement a secure scalable enterprise wireless infrastructure using a wireless LAN Controller (WLC) and RADIUS authentication. While the initial configuration of SSIDs and security protocols was successful, the final verification phase required extensive troubleshooting of the routing and addressing layers. By aligning the IP subnets of the WLC management, the default gateway and the target web server I successfully established end-to-end connectivity. This lab demonstrates that in enterprise networking successful authentication is only half the battel; proper IP routing and interface mapping are essential for data to flow across the network.

One notable challenge that I encounter was a persistent ‘Connection Reset’ error at the Application Layer. Even after ICMP pings were successful confirming that the Network Layer was functional the Web Server initially refused HTTP requests. This required a manual reset of the server’s HTTP services and ‘Fast Forward’ of the simulation time to clear the ARP cache and allow the TCP three way handshake to complete over the new routing path.