COURSE: CLOUD AND NETORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

WLAN CONFIGURATION

Table of Contents

INTRODUCTION

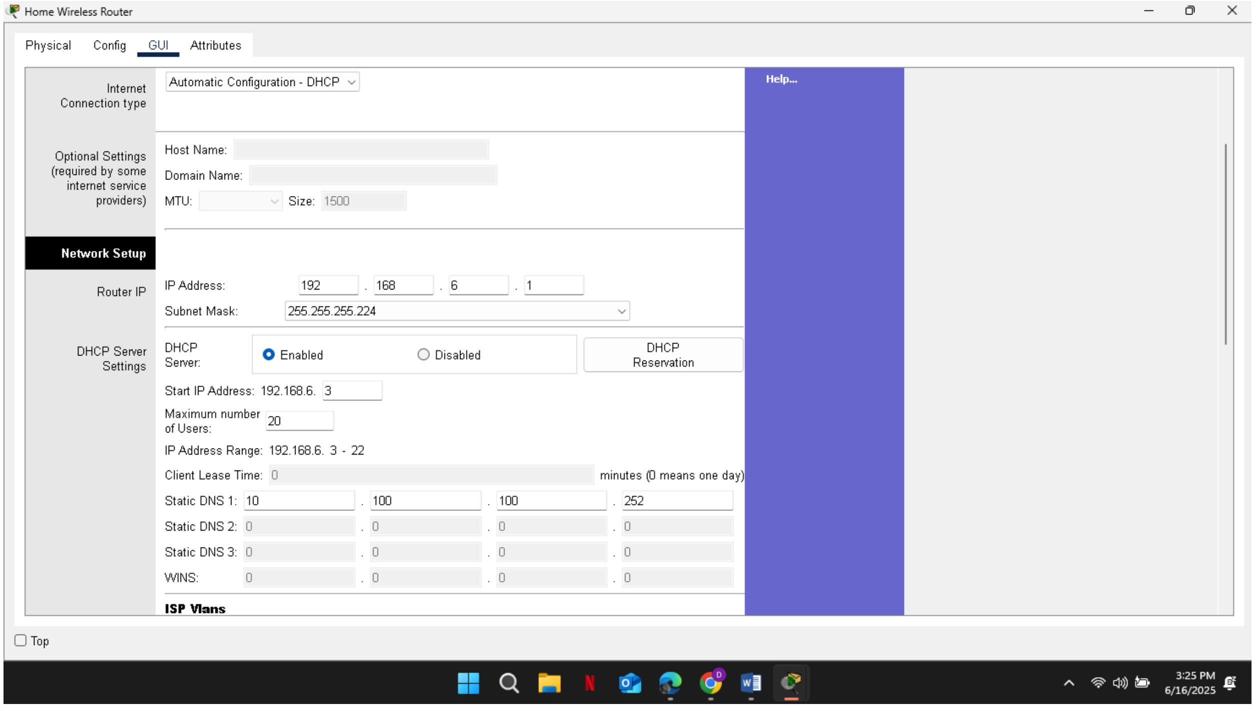
This lab exercise was designed to simulate and configure both a home wireless network and an enterprise wireless environment using a Wireless LAN Controller (WLC). It involved hands-on tasks that reflect real-world networking scenarios, including securing wireless access, assigning IP addresses, and enabling authentication protocols.

In Part 1, the focus was on configuring a home wireless router. This included assigning an IP address, setting up the 2.4GHz wireless interface with a specific SSID and channel, enabling WPA2 Personal security, changing the default password, and connecting wireless clients like a laptop, tablet, and smartphone. Connectivity was verified through successful pings and web server access.

In Part 2, the lab shifted to an enterprise-level setup with a WLC. The configuration included setting up two VLAN interfaces (WLAN 2 and WLAN 5), each with its own IP configuration. One WLAN was secured using WPA2-PSK, and the other used WPA2-Enterprise with RADIUS server authentication. Additional configurations included an internal DHCP scope for management and SNMP settings for network monitoring. WLANs were created and assigned SSIDs, interfaces, and authentication methods, followed by FlexConnect settings. Client devices were then connected and tested for network access and server communication.

PACKET TRACER WLAN CONFIGURATION

CONFIGURE A HOME WIRELESS ROUTER



Home Wireless Router

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

WINS: 0 . 0 . 0 . 0

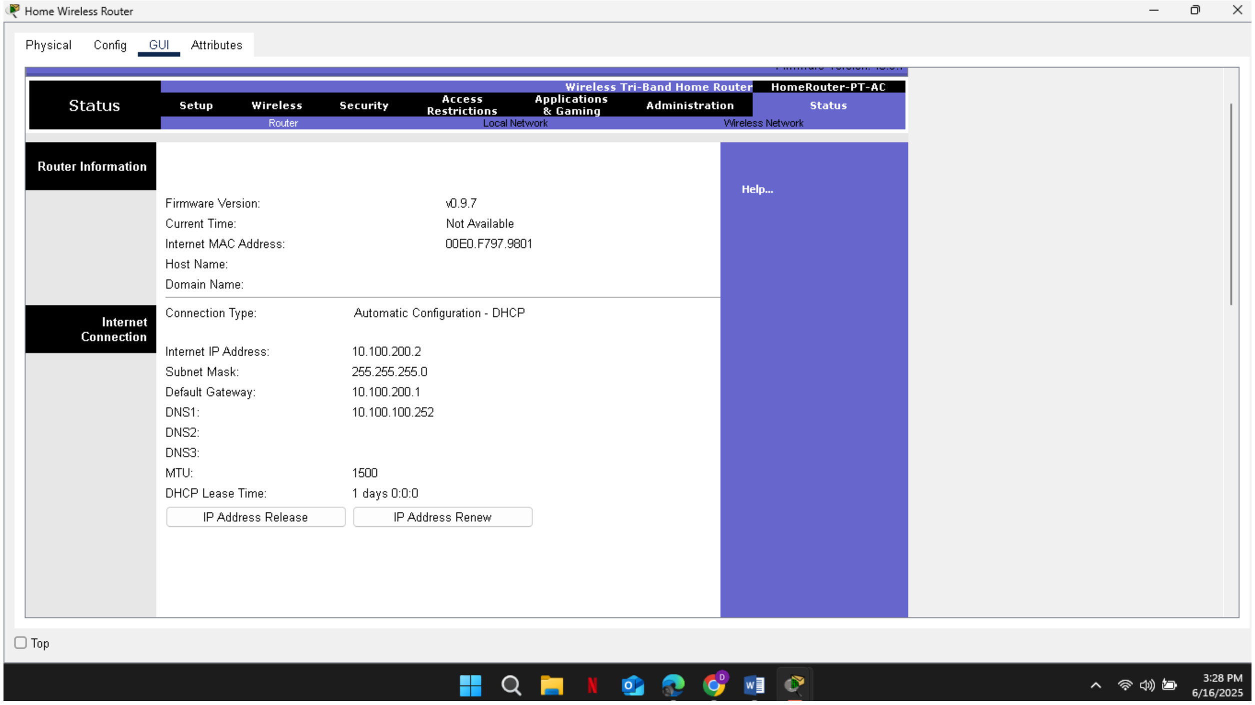
ISP Vlans

□ Top

3:25 PM
6/16/2025

Verify the address. What address did it receive?

10.100.200.2



Firmware Version: v0.9.7
Current Time: Not Available
Internet MAC Address: 00E0.F797.9801
Host Name:
Domain Name:

Connection Type: Automatic Configuration - DHCP

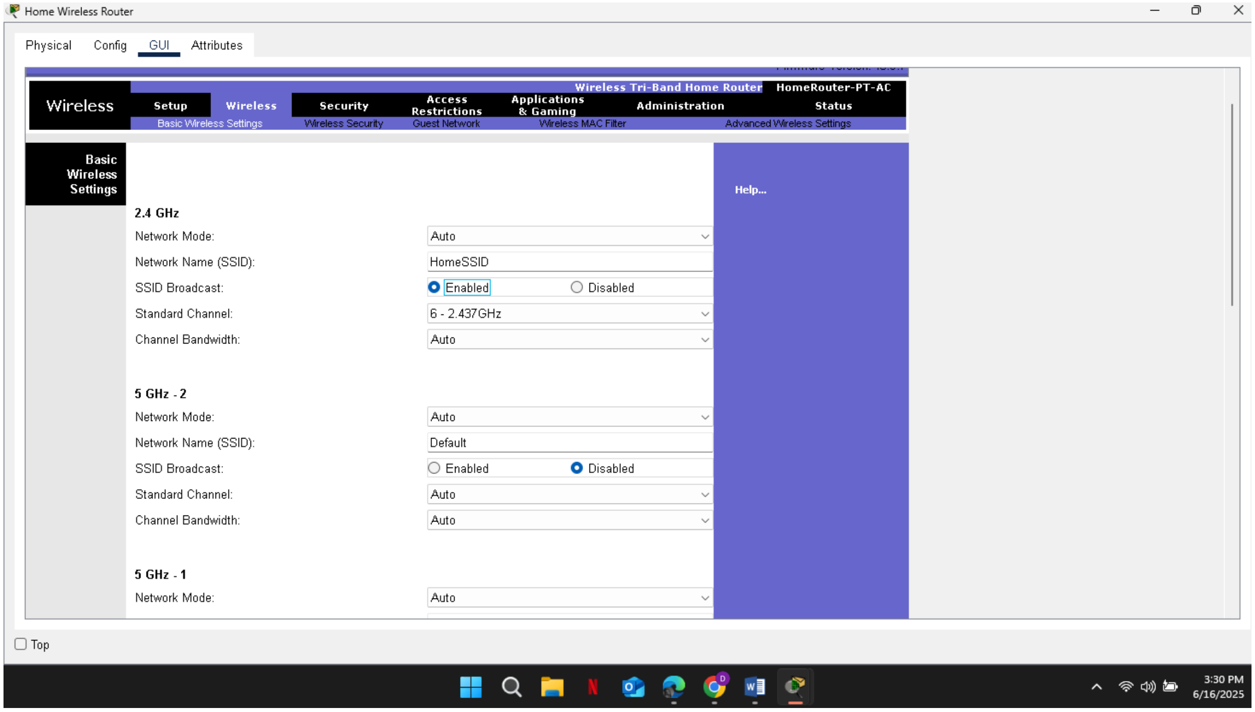
Internet IP Address: 10.100.200.2
Subnet Mask: 255.255.255.0
Default Gateway: 10.100.200.1
DNS1: 10.100.100.252
DNS2:
DNS3:
MTU: 1500
DHCP Lease Time: 1 days 0:0:0

CONFIGURE WIRELESS LAN

a. The network will use the 2.4GHz Wireless LAN interface. Configure the interface with the SSID shown in the Wireless LAN information table.

b. Use **channel 6**.

c. Be sure that all wireless hosts in the home will be able to see the SSID.



2.4 GHz

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

5 GHz - 2

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

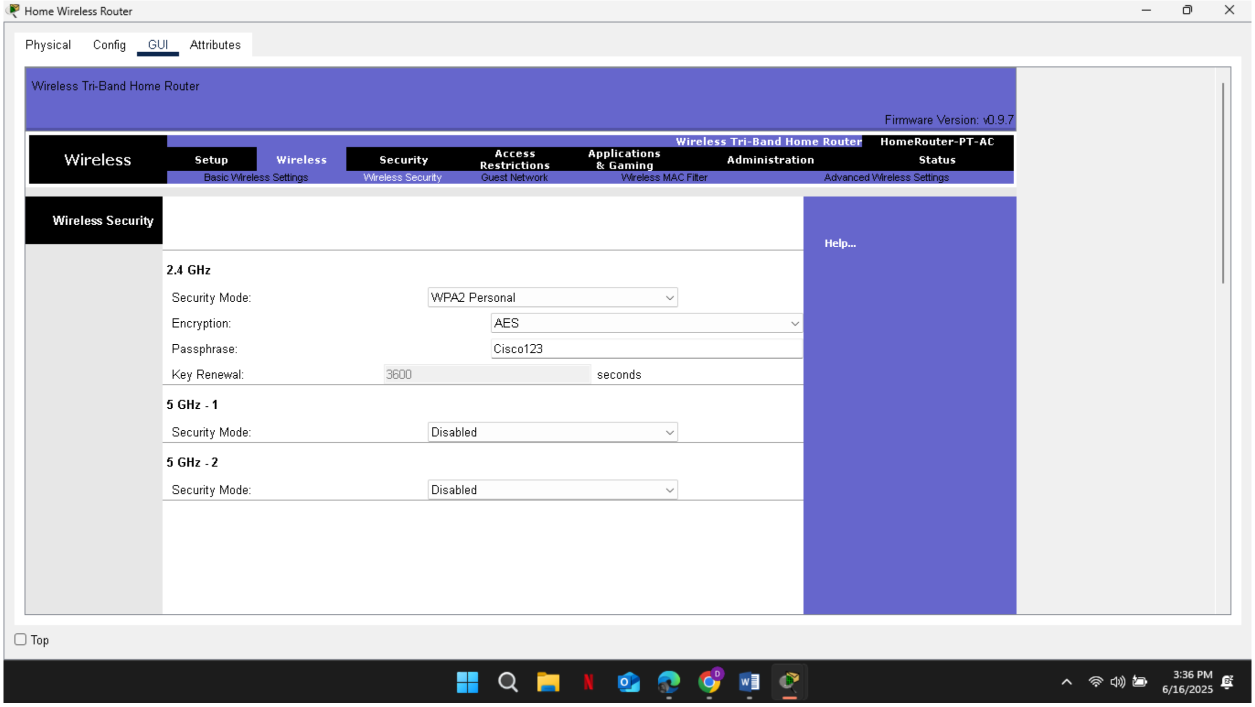
5 GHz - 1

Network Mode:	Auto

CONFIGURE SECURITY.

a. Configure wireless LAN security. Use WPA2 Personal and the passphrase shown in the Wireless LAN information table.

b. Secure the router by changing the default password to the value shown in the Wireless LAN information table.



2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Cisco123

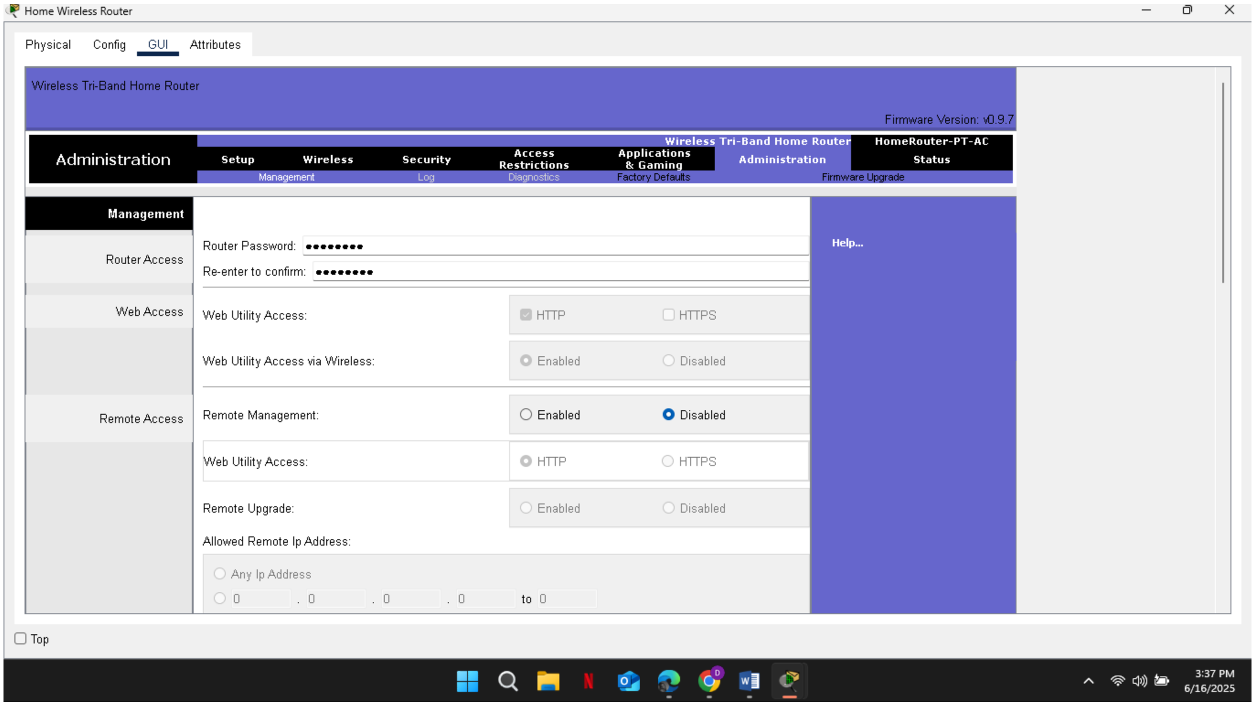
Key Renewal: 3600 seconds

5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled



Router Password: ••••••••

Re-enter to confirm: ••••••••

Web Utility Access: ☑ HTTP □ HTTPS

Web Utility Access via Wireless: ● Enabled ○ Disabled

Remote Management: ○ Enabled ● Disabled

Web Utility Access: ● HTTP ○ HTTPS

Remote Upgrade: ○ Enabled ○ Disabled

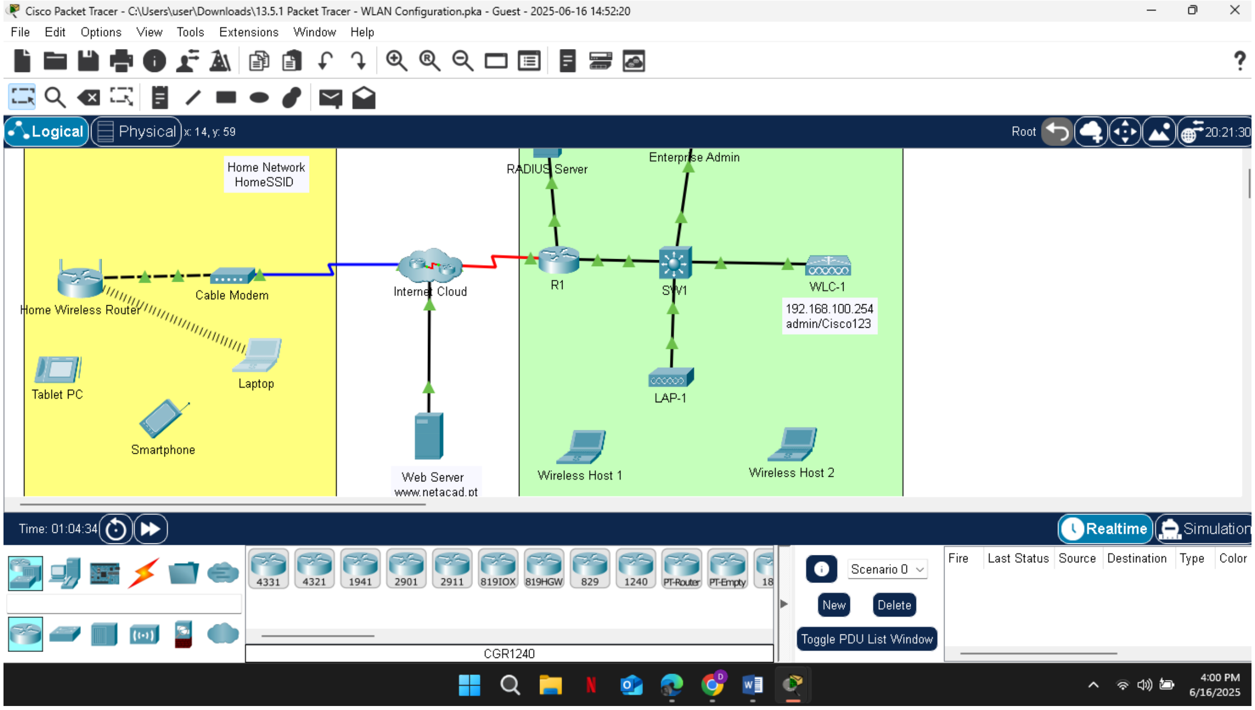
Allowed Remote Ip Address:

○ Any Ip Address

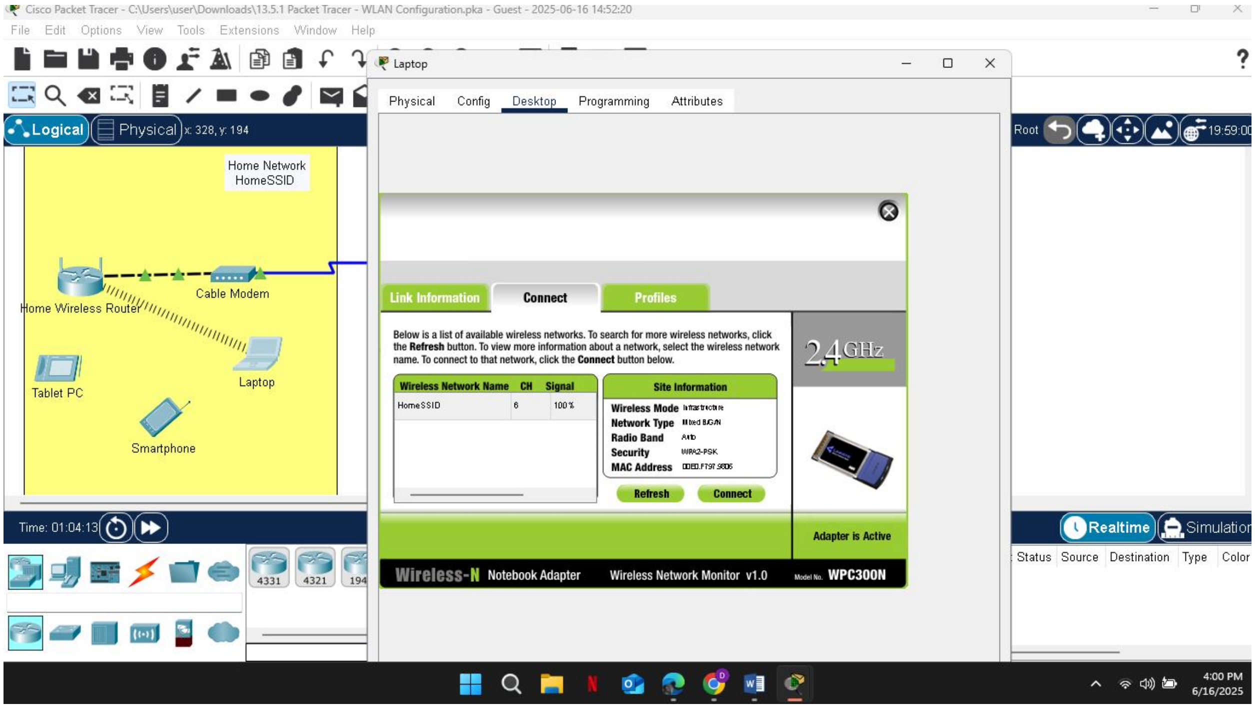
○ 0 . 0 . 0 . 0 to 0

Connect clients to the network.

a. Open the PC Wireless app on the desktop of the laptop and configure the client to connect to the network.


Cisco Packet Tracer - C:\Users\user\Downloads\13.5.1 Packet Tracer - WLAN Configuration.pka - Guest - 2025-06-16 14:52:20

This shows an active connection between the router and the laptop


Cisco Packet Tracer - C:\Users\user\Downloads\13.5.1 Packet Tracer - WLAN Configuration.pka - Guest - 2025-06-16 14:52:20

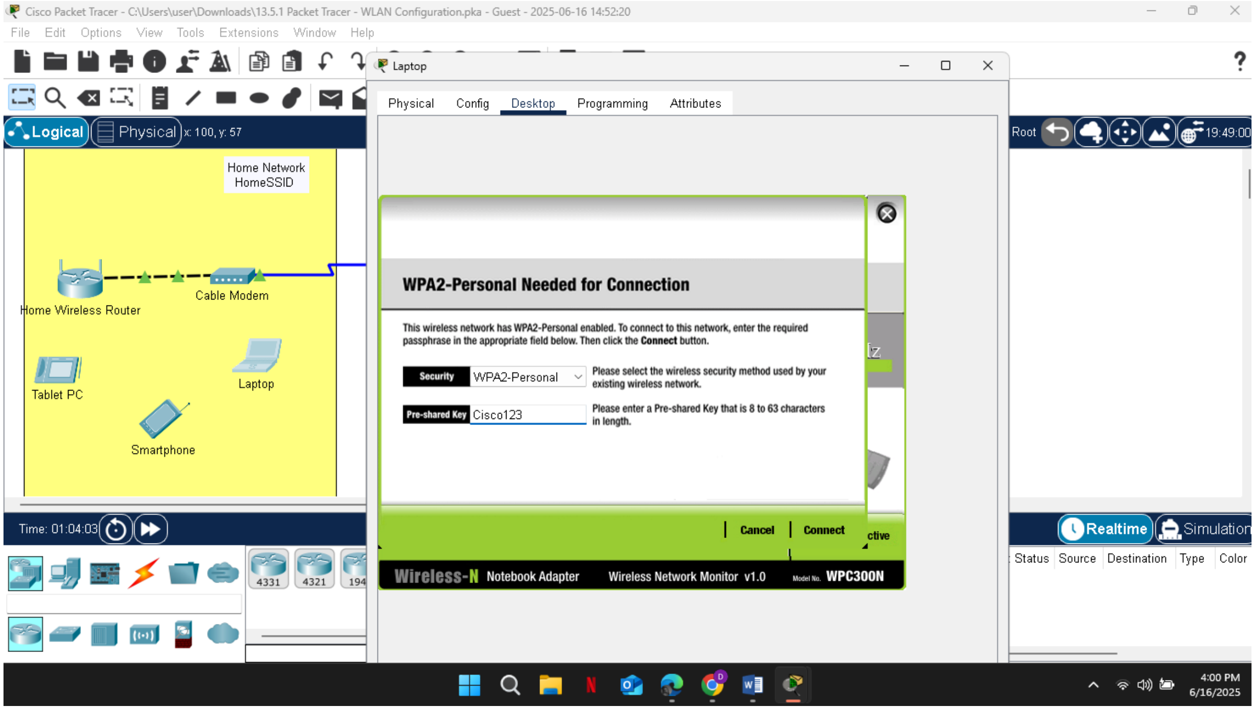
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
HomeSSID	6	100%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA2-PSK
MAC Address	00E0.F797.9806

Connection to the home SSID



WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security: WPA2-Personal — Please select the wireless security method used by your existing wireless network.

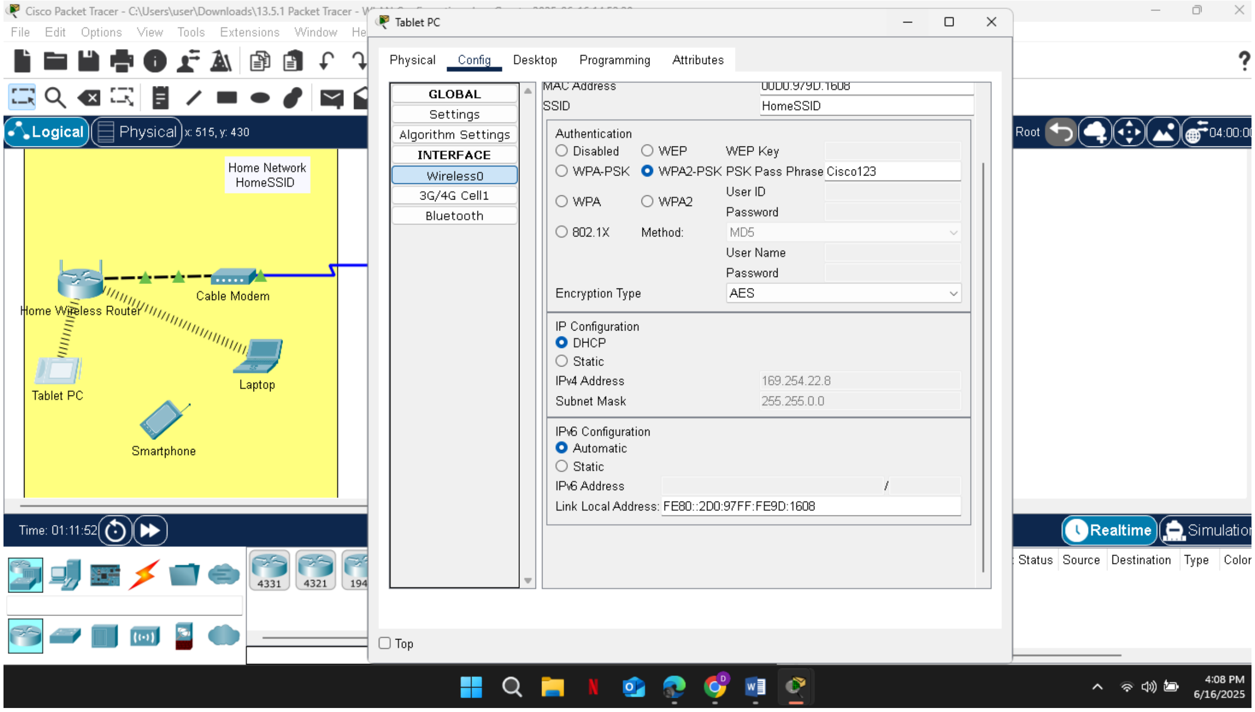
Pre-shared Key: Cisco123 — Please enter a Pre-shared Key that is 8 to 63 characters in length.

Cancel | Connect

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

Inputting the password

b. Open the Config tab on the Tablet PC and Smartphone and configure the wireless interfaces to connect to the wireless network.



MAC Address: 00D0.979D.1608

SSID: HomeSSID

Authentication

○ Disabled ○ WEP WEP Key

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

○ WPA ○ WPA2 User ID / Password

○ 802.1X Method: MD5 User Name / Password

Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 169.254.22.8

Subnet Mask: 255.255.0.0

IPv6 Configuration

● Automatic

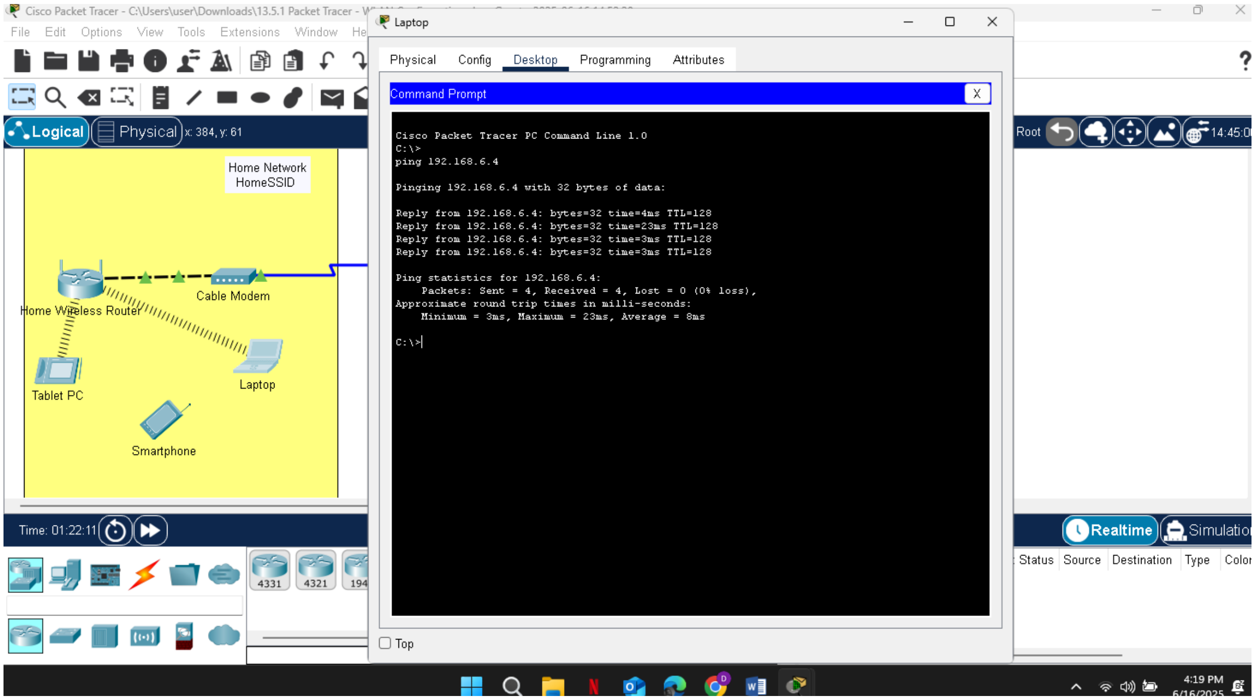
○ Static

IPv6 Address: /

Link Local Address: FE80::2D0:97FF:FE9D:1608

Shows the connection between the tablet and the router

c. Verify connectivity. The hosts should be able to ping each other and the web server. They should also be able to reach the web server URL



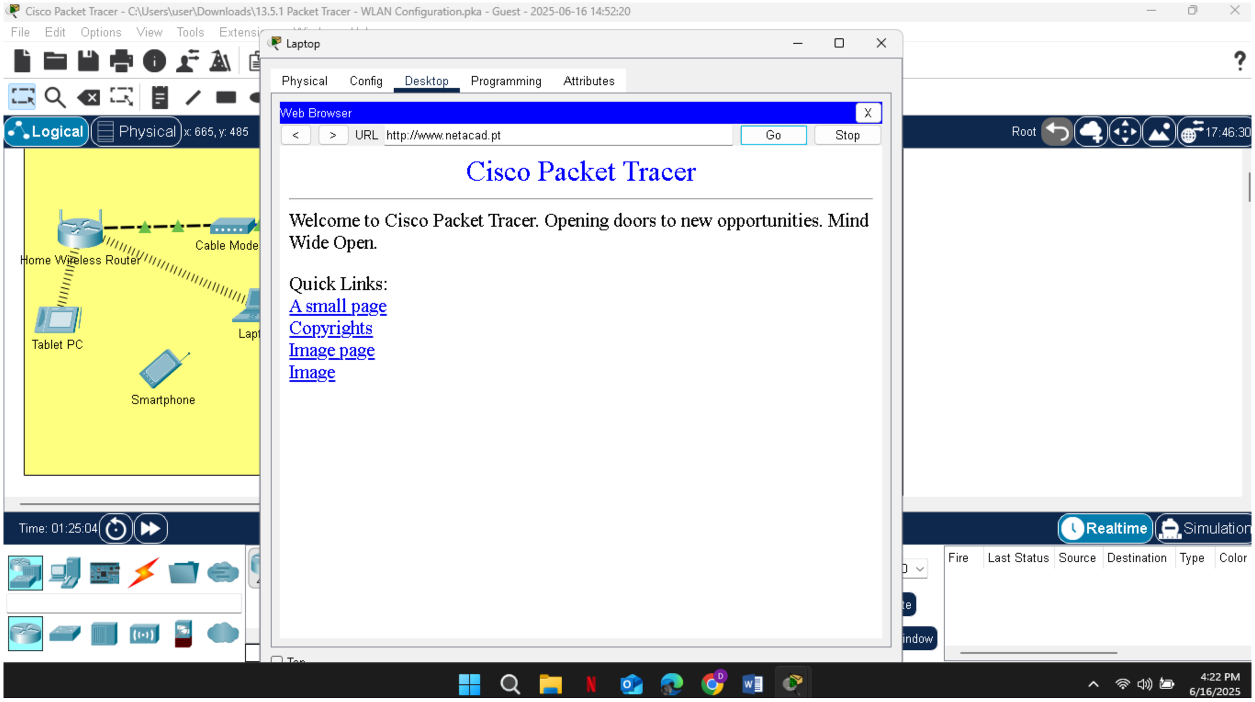
```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 192.168.6.4

Pinging 192.168.6.4 with 32 bytes of data:

Reply from 192.168.6.4: bytes=32 time=4ms TTL=128
Reply from 192.168.6.4: bytes=32 time=23ms TTL=128
Reply from 192.168.6.4: bytes=32 time=3ms TTL=128
Reply from 192.168.6.4: bytes=32 time=3ms 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 = 3ms, Maximum = 23ms, Average = 8ms

C:\>
```



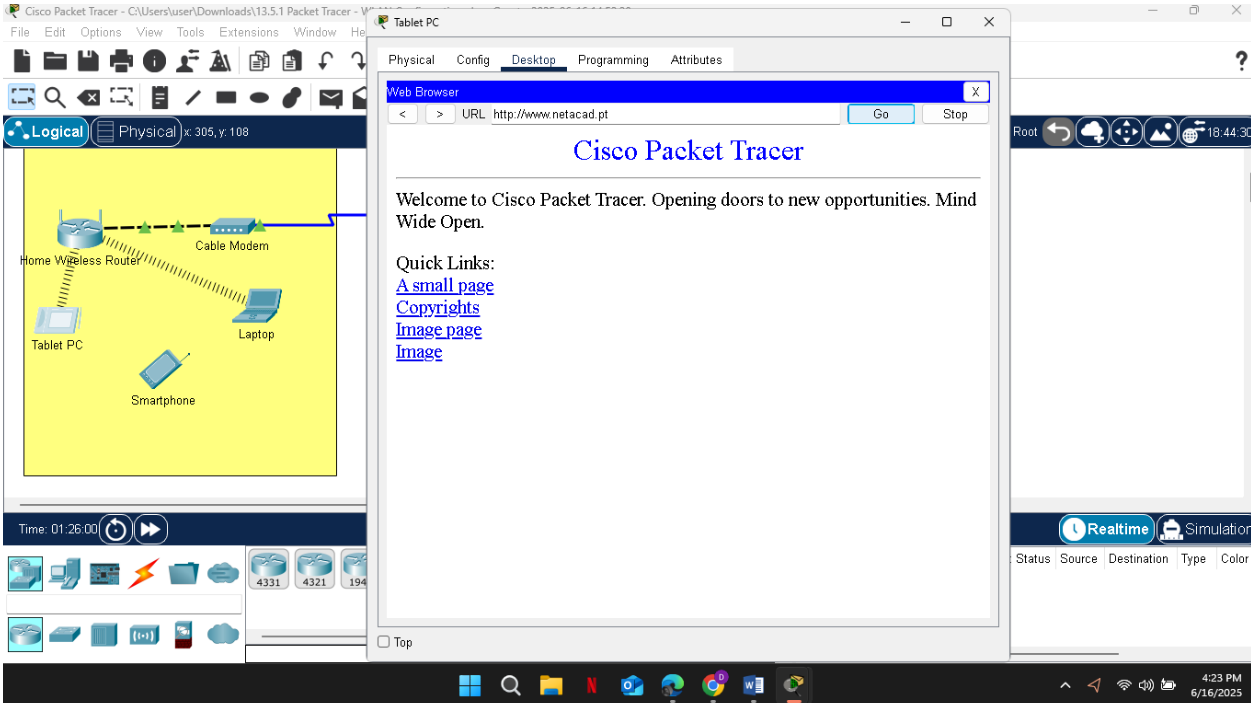
URL http://www.netacad.pt

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

Laptop is able to access the web server



URL http://www.netacad.pt

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

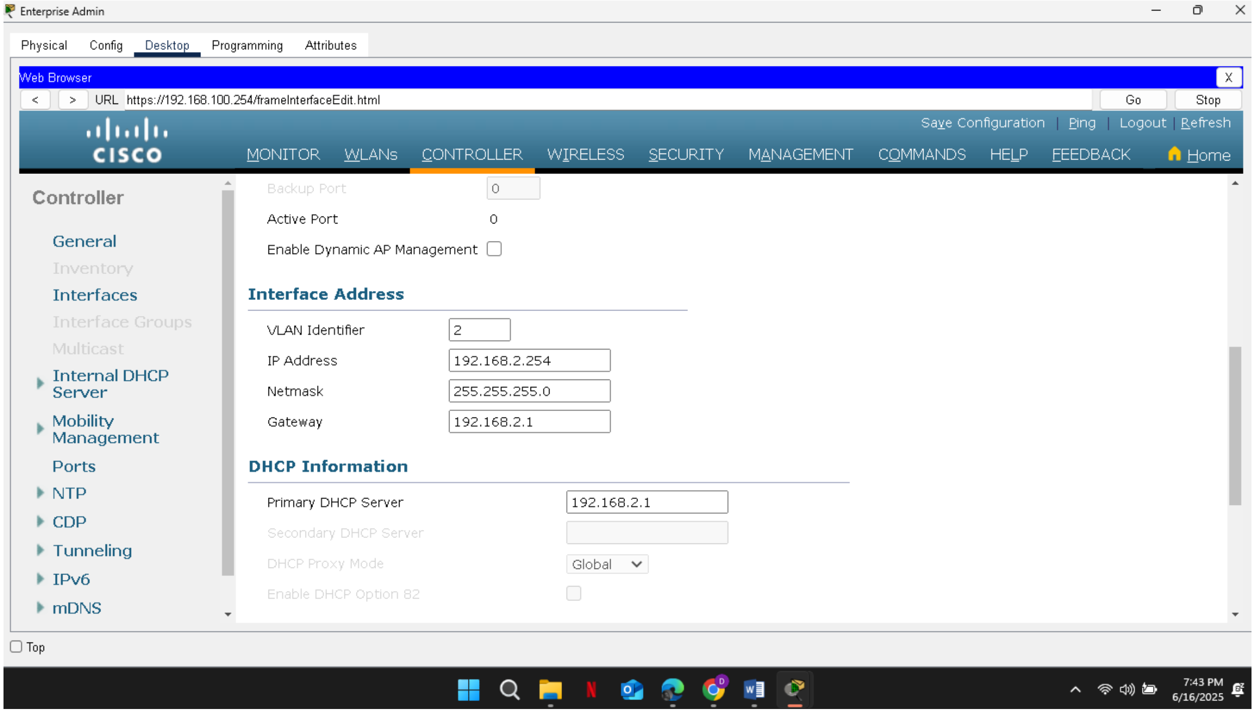
Tablet is also able to access web server

CONFIGURE A WLC CONTROLLER NETWORK

Configure the wireless LAN controller with two WLANs. One WLAN will use WPA2-PSK authentication. The other WLAN will use WPA2-Enterprise authentication. You will also configure the

WLC to use an SNMP server and configure a DHCP scope that will be used by the wireless management network.

CONFIGURE VLAN INTERFACES.



URL https://192.168.100.254/frameInterfaceEdit.html

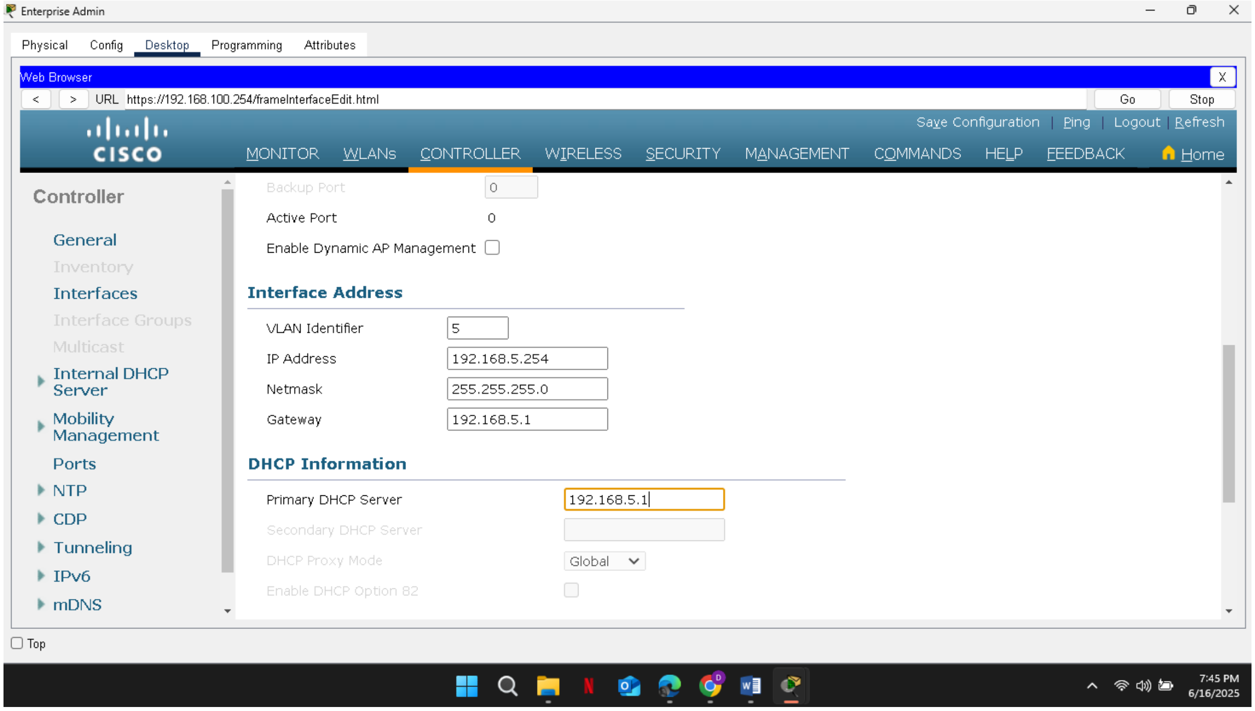
Backup Port	0
Active Port	0
Enable Dynamic AP Management	□

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	□



URL https://192.168.100.254/frameInterfaceEdit.html

Backup Port	0
Active Port	0
Enable Dynamic AP Management	□

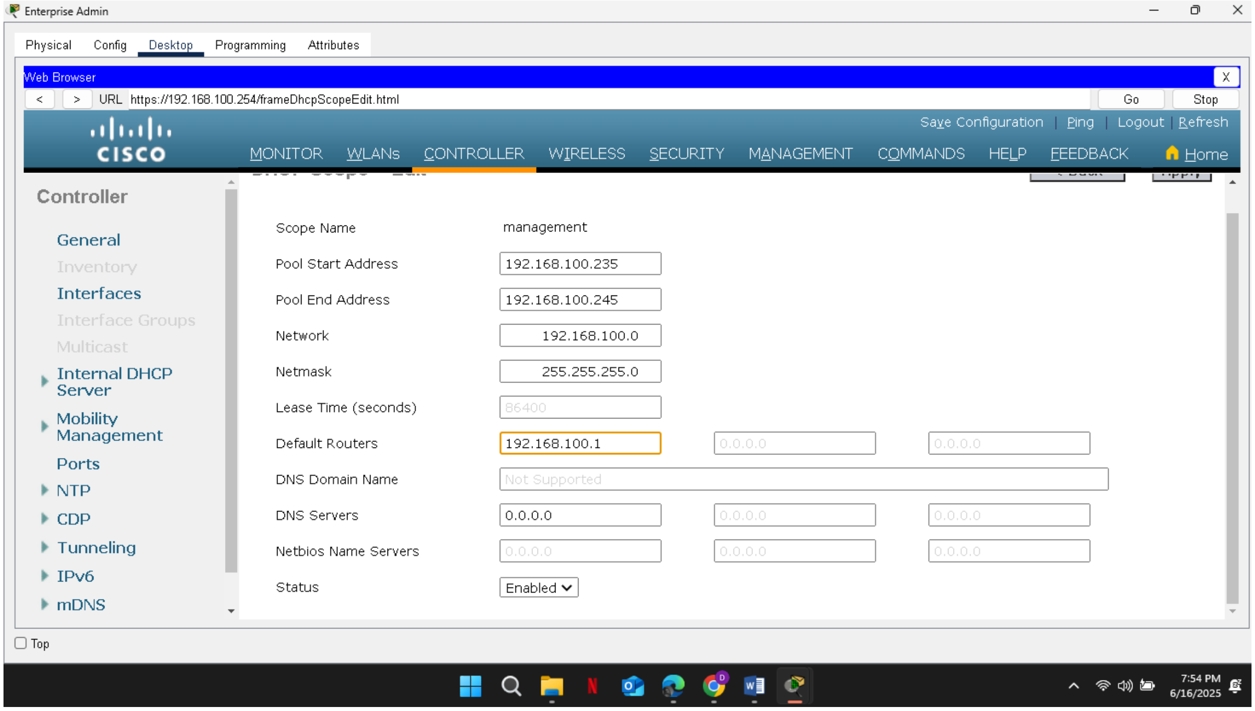
Interface Address

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	□

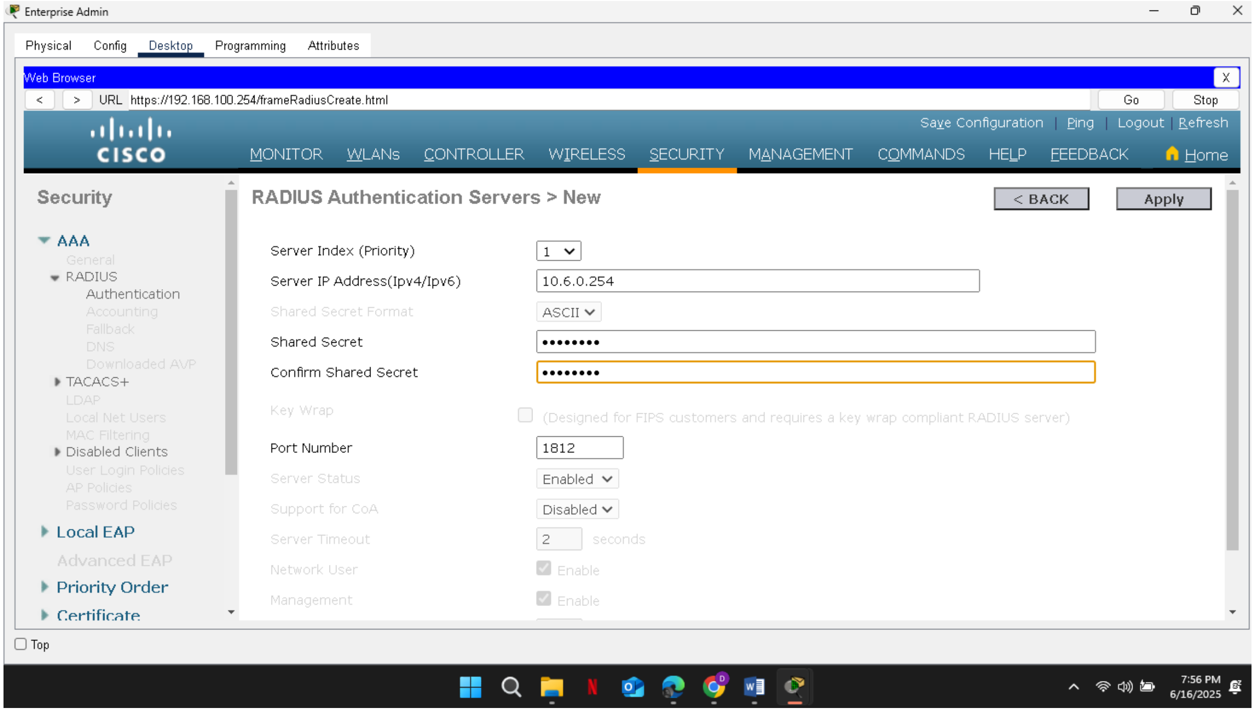
CONFIGURE INTERNAL DHCP SCOPE



URL https://192.168.100.254/frameDhcpScopeEdit.html

Scope Name	management		
Pool Start Address	192.168.100.235		
Pool End Address	192.168.100.245		
Network	192.168.100.0		
Netmask	255.255.255.0		
Lease Time (seconds)	86400		
Default Routers	192.168.100.1	0.0.0.0	0.0.0.0
DNS Domain Name	Not Supported		
DNS Servers	0.0.0.0	0.0.0.0	0.0.0.0
Netbios Name Servers	0.0.0.0	0.0.0.0	0.0.0.0
Status	Enabled		

EXTERNAL SERVER CONFIGS

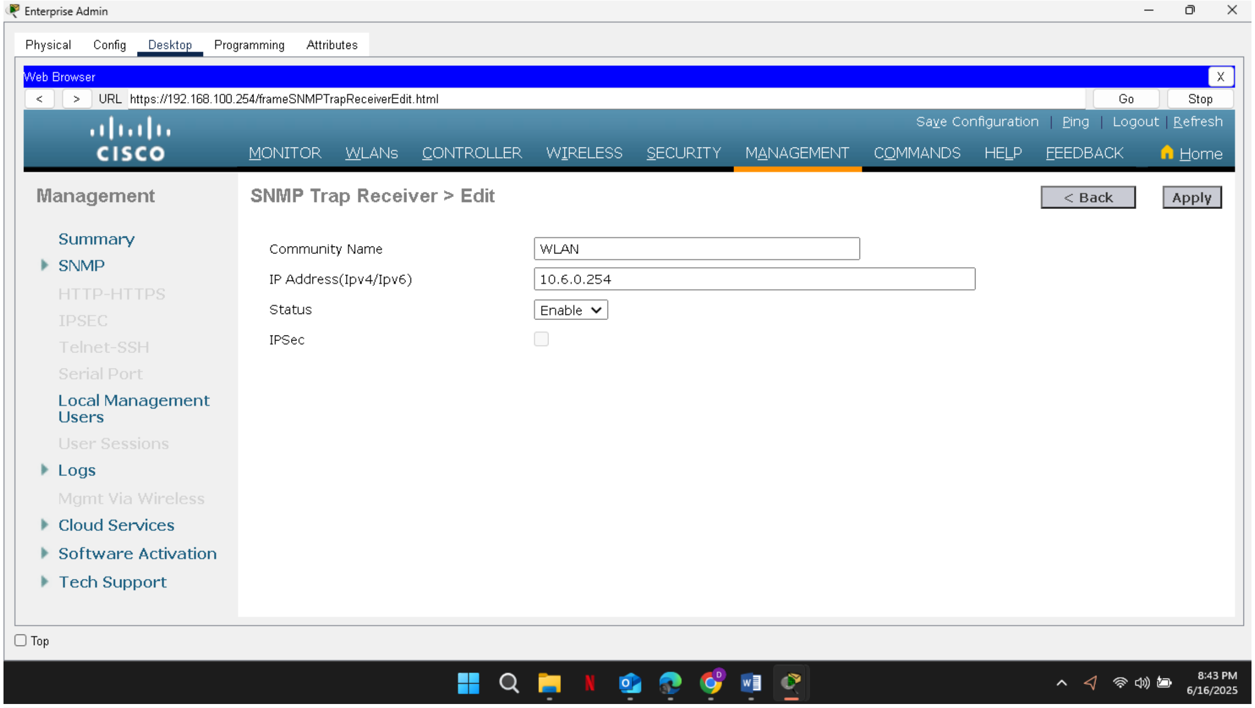


URL https://192.168.100.254/frameRadiusCreate.html

RADIUS Authentication Servers > New

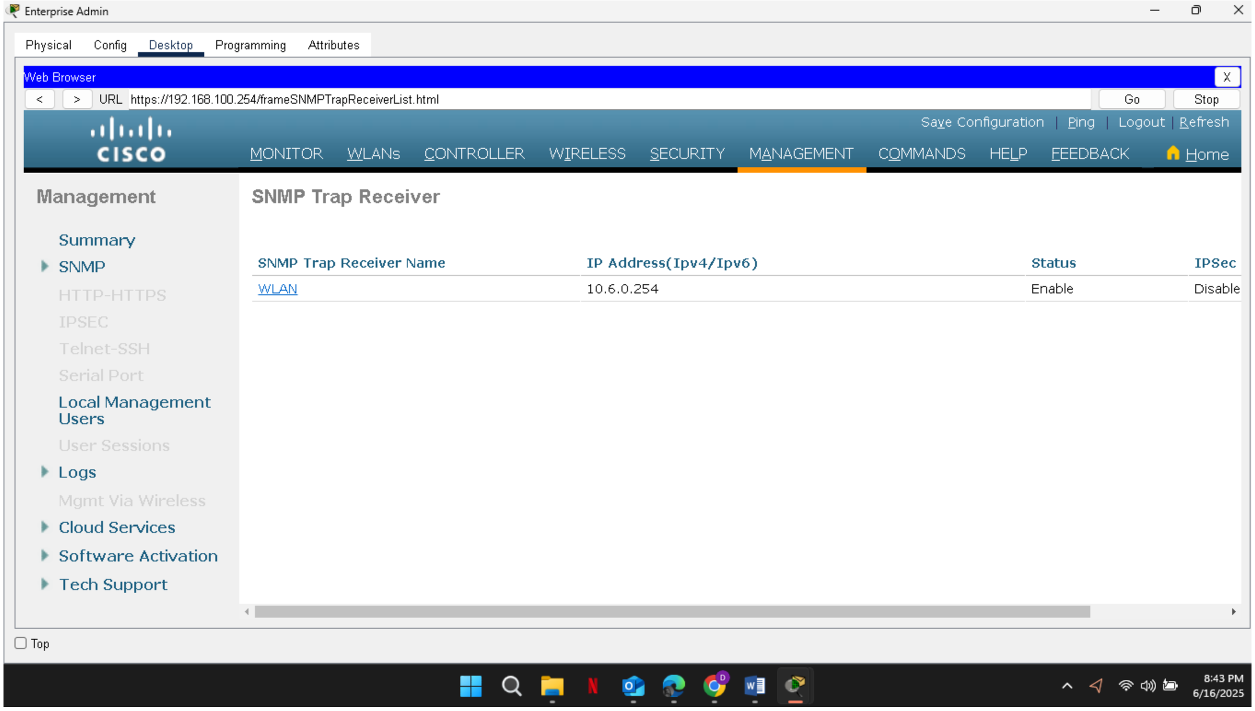
Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	10.6.0.254
Shared Secret Format	ASCII
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable

CREATE THE WLANS.



SNMP Trap Receiver > Edit

Community Name	WLAN
IP Address(Ipv4/Ipv6)	10.6.0.254
Status	Enable
IPSec	□

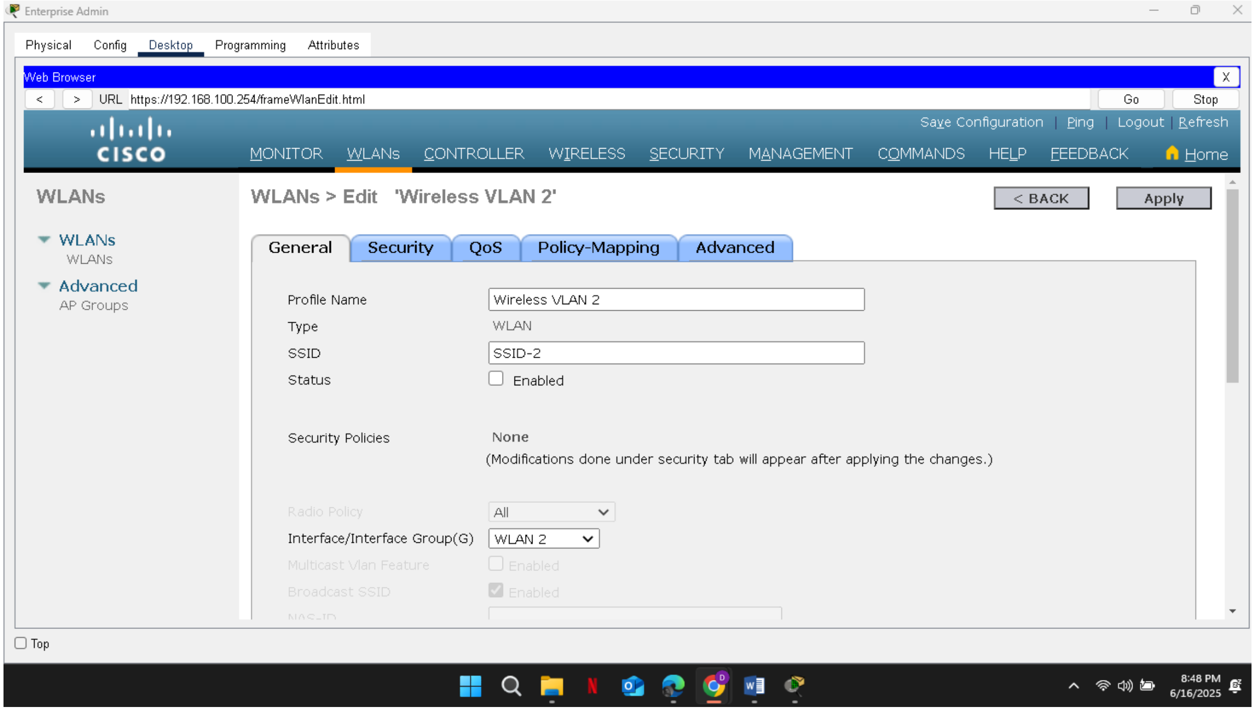


SNMP Trap Receiver

SNMP Trap Receiver Name	IP Address(Ipv4/Ipv6)	Status	IPSec
WLAN	10.6.0.254	Enable	Disable

Create the first WLAN: Profile Name: **Wireless VLAN 2**, WLAN SSID: **SSID-2**, ID: **2**, Interface: **WLAN 2**, Security: **WPA2-PSK**, Passphrase: **Cisco123**

Under the Advanced tab, go to the FlexConnect section. Enable **FlexConnect Local Switching** and **FlexConnect Local Auth**.



WLANs > Edit 'Wireless VLAN 2'

Profile Name: Wireless VLAN 2

Type: WLAN

SSID: SSID-2

Status: □ Enabled

Security Policies: None

(Modifications done under security tab will appear after applying the changes.)

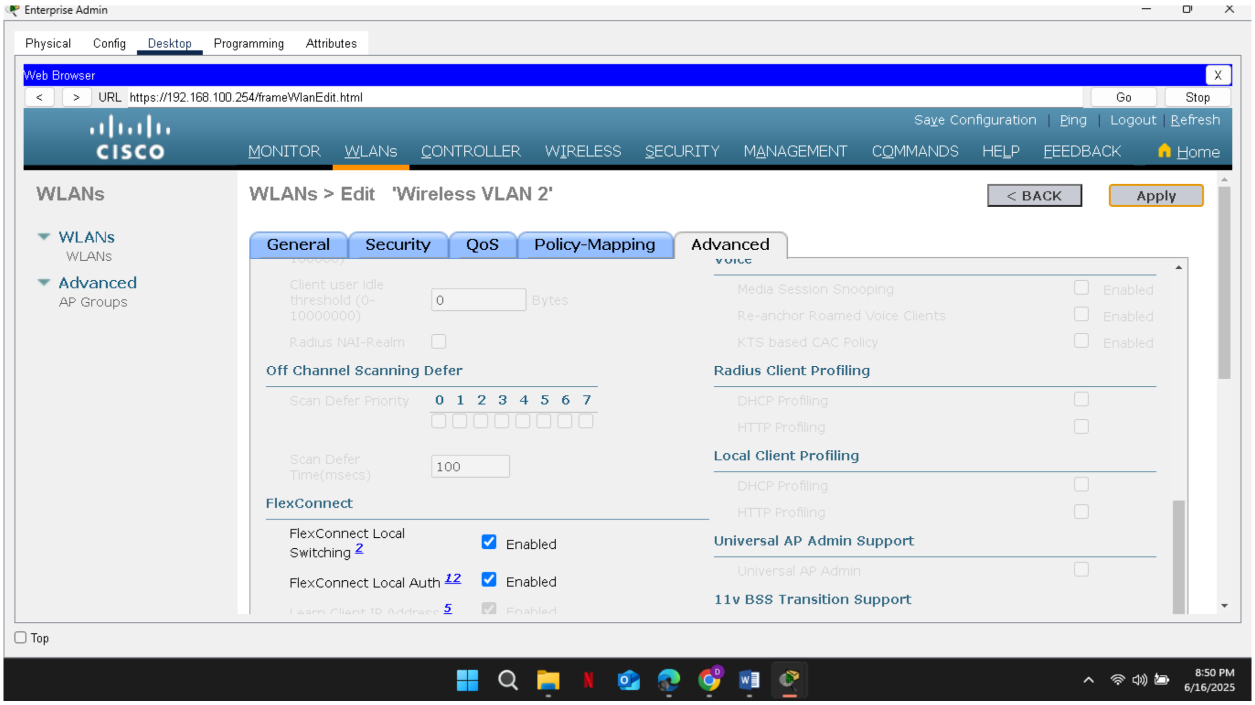
Radio Policy: All

Interface/Interface Group(G): WLAN 2

Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID



WLANs > Edit 'Wireless VLAN 2'

Client user idle threshold (0-10000000): 0 Bytes

Radius NAI-Realm: □

Off Channel Scanning Defer

Scan Defer Priority: 0 1 2 3 4 5 6 7 □ □ □ □ □ □ □ □

Scan Defer Time(msecs): 100

FlexConnect

FlexConnect Local Switching [2]: ☑ Enabled

FlexConnect Local Auth [12]: ☑ Enabled

Learn Client IP Address [5]: ☑ Enabled

Voice

Media Session Snooping: □ Enabled

Re-anchor Roamed Voice Clients: □ Enabled

KTS based CAC Policy: □ Enabled

Radius Client Profiling

DHCP Profiling: □

HTTP Profiling: □

Local Client Profiling

DHCP Profiling: □

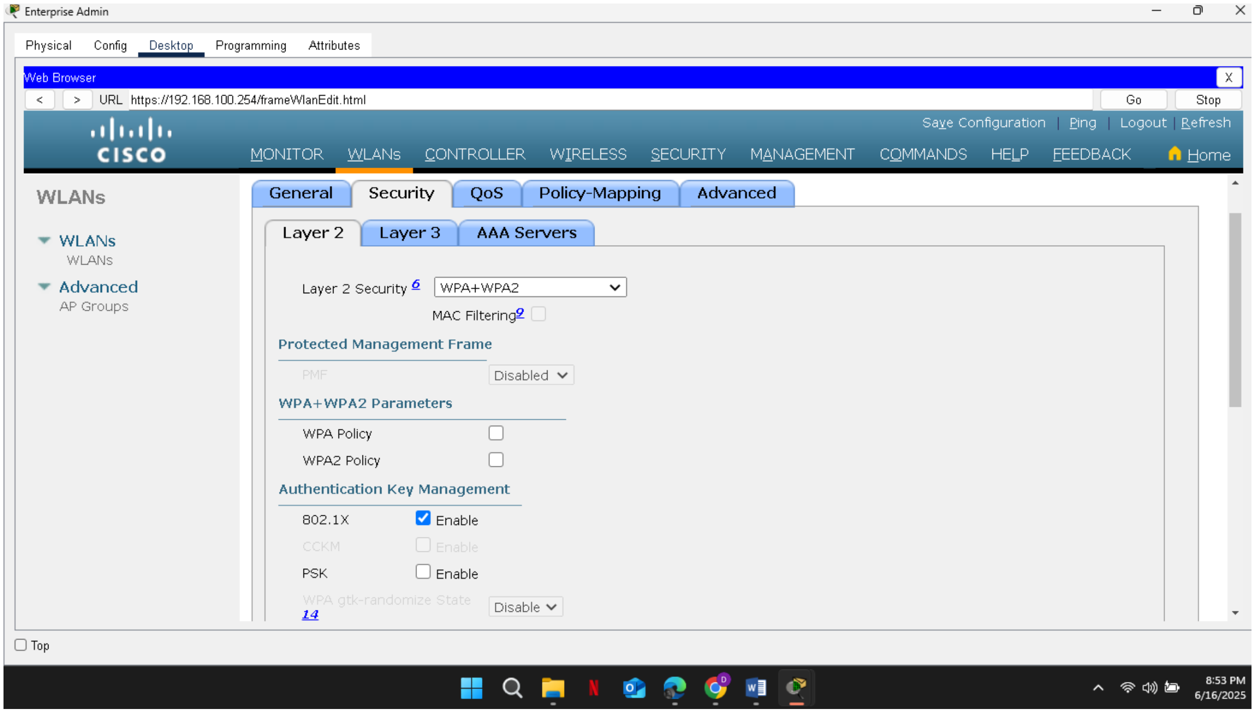
HTTP Profiling: □

Universal AP Admin Support

Universal AP Admin: □

11v BSS Transition Support

Create the second WLAN: Profile Name: **Wireless VLAN 5**, WLAN SSID: **SSID-5**, Interface: **WLAN 5**, ID: **5**, Security: **802.1x - WPA2-Enterprise**, Configure the WLAN to use the RADIUS server for authentication.



URL https://192.168.100.254/frameWlanEdit.html

Layer 2 Security 6: WPA+WPA2

MAC Filtering9 ☐

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☐

Authentication Key Management

802.1X ☑ Enable

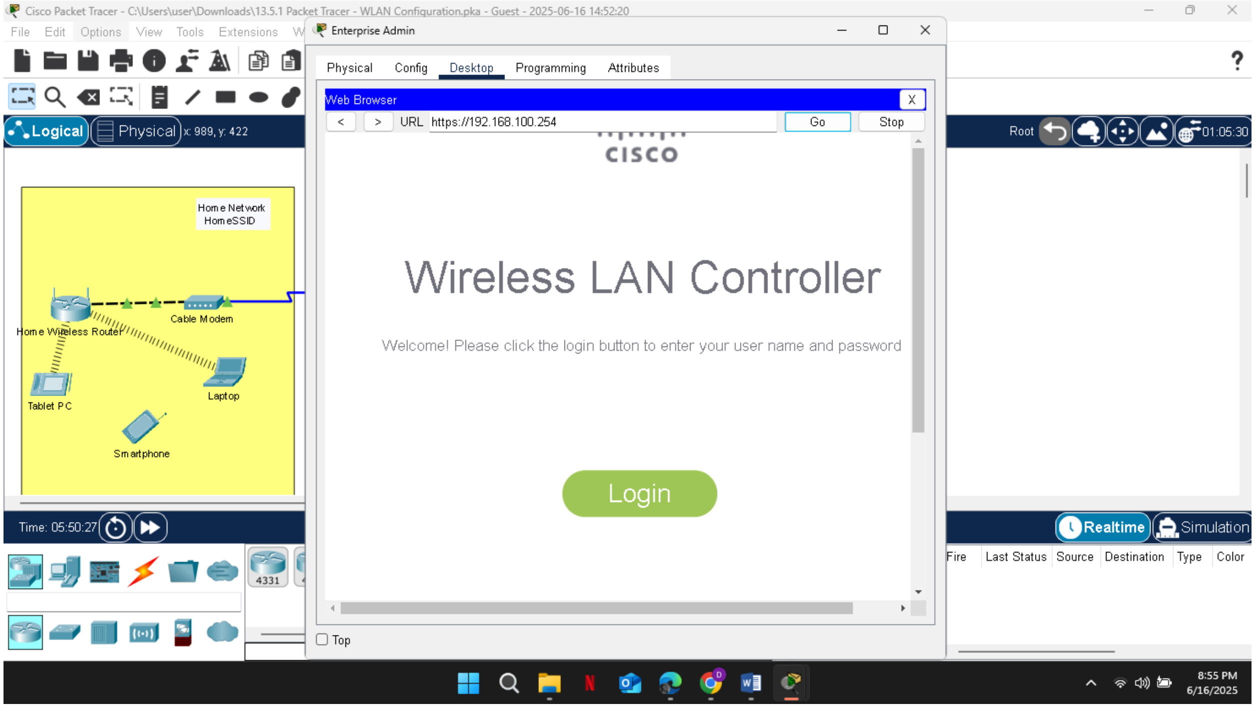
CCKM ☐ Enable

PSK ☐ Enable

WPA gtk-randomize State 14: Disable

TEST CONNECTIVITY.

Test connectivity between the wireless hosts and the Web Server by ping and URL.



Cisco Packet Tracer - C:\Users\user\Downloads\13.5.1 Packet Tracer - WLAN Configuration.pka - Guest - 2025-06-16 14:52:20

Enterprise Admin

Web Browser

URL https://192.168.100.254

Wireless LAN Controller

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

CONCLUSION

This lab provided a structured approach to setting up wireless networks in both home and enterprise contexts. The home network configuration demonstrated how to establish a secure, functional wireless environment with client connectivity and internet access.

The enterprise WLC setup allowed for a deeper understanding of network segmentation, security through both PSK and 802.1x methods, and integration with external services like DHCP and SNMP. Creating separate WLANs for different VLANs and authenticating users through a RADIUS server mirrored the kind of wireless infrastructure used in professional environments.

By the end of the lab, all client devices were able to successfully connect to their respective WLANs and communicate with the web server, confirming that the configuration was correct and functional. This exercise reinforced the importance of planning, securing, and testing wireless networks, especially when dealing with multi-layered environments like those found in modern organizations.