Course: Cloud and Network Security
Name: Neville Ngothe Iregi
Student No.: CS-CNS10-25054
Date: Tuesday, 7th October 2025

Week 4 Assignment 2: Packet Tracer WLAN configuration

Introduction

A WLAN is a group of colocated computers or other devices that form a network based on radio transmissions instead of wired connections and aims to meet changing network demands. A WLAN transmits information over radio waves similarly to broadcast media. information is sent in packets which contain layers with labels and instructions that work hand in hand with MAC addresses that are assigned to endpoints to ensure the information is sent to the intended device. An example of a WLAN is a Wi-Fi network.

A WLAN can be configured in two ways: infrastructure mode(e.g. a home or office Wi-Fi network) and adhoc setup. A basic infrastructure setup is one in which all endpoints are connected and communicate with each other through a base station such as a wireless router, which may also provide internet access. In an adhoc setup, Wi-Fi Direct technology is commonly used for an ad hoc. The WLAN in an adhoc setup connects endpoints without the use of a base station and can provide basic peer-to-peer (P2P) communication.

Moreover, for security purposes, a WLAN uses encryption as the most common security method. Some of the encryption types include Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), with WPA2 as the standard authentication method.

A WLAN makes use of wireless access points and WLAN controllers. Wireless access points amplify the bandwidth coming from the router and stretches it to farther distances, thus allowing devices to get onto the network from those distances. A WLAN controller (WLC) is a network device that manages the wireless access points that allow wireless devices to connect to the network. It acts as a central hub for tasks like configuration, security policies, monitoring, and performance tracking. A WLC can be a dedicated device or software running on a server.

This assignment aims to help one apply WLAN skills and knowledge by configuring a home wireless router and an enterprise WLC. One also has to implement WPA2-PSK and WPA2-Enterprise security. Finally, the hosts are to be connected to each WLAN and connectivity is to be verified.

Objectives

- Configure a home router to provide Wi-Fi connectivity to a variety of devices.
- Configure WPA2-PSK security on a home router.
- Configure interfaces on a WLC.
- Configure WLANs on a WLC.
- Configure WPA2-PSK security on a WLAN and connect hosts to WLAN.
- Configure WPA2-Enteprise on a WLAN and connect hosts to the WLAN.
- Verify connectivity WLAN connectivity.

Addressing Table

Device	Interface	Ip Address
Home Wireless Router	Internet	DHCP
	LAN	192.168.6.1/27
RTR-1	G0/0/0.2	192.168.2.1/24
	G0/0/0.5	192.168.5.1/24
	G0/0/0.100	192.168.100.1/24
	G0/0/1	10.6.0.1/24
SW1	VLAN 200	192.168.100.100/24
LAP-1	G0	DHCP
WLC-1	Management	192.168.100.254/24
RADIUS Server	NIC	10.6.0.254/24
Home Admin	NIC	DHCP
Enterprise Admin	NIC	192.168.100.200/24
Web Server	NIC	203.0.113.78/24

DNS server	NIC	10.100.100.252
Laptop	NIC	DHCP
Tablet PC	Wireless0	DHCP
Smartphone	Wireless0	DHCP
Wireless Host 1	Wireless0	DHCP
Wireless Host 2	Wireless0	DHCP

WLAN Information

WLAN	SSID	Authentication	Username	Password
Home Network	HomeSSID	WPA2-Personal	N/A	Cisco123
WLAN VLAN 2	SSID-2	WPA-2 Personal	N/A	Cisco123
WLAN VLAN 5	SSID-5	WPA-2 Enterprise	userWLAN5	userW5pass

Instructions

Part 1: Configure a Home Wireless Router.

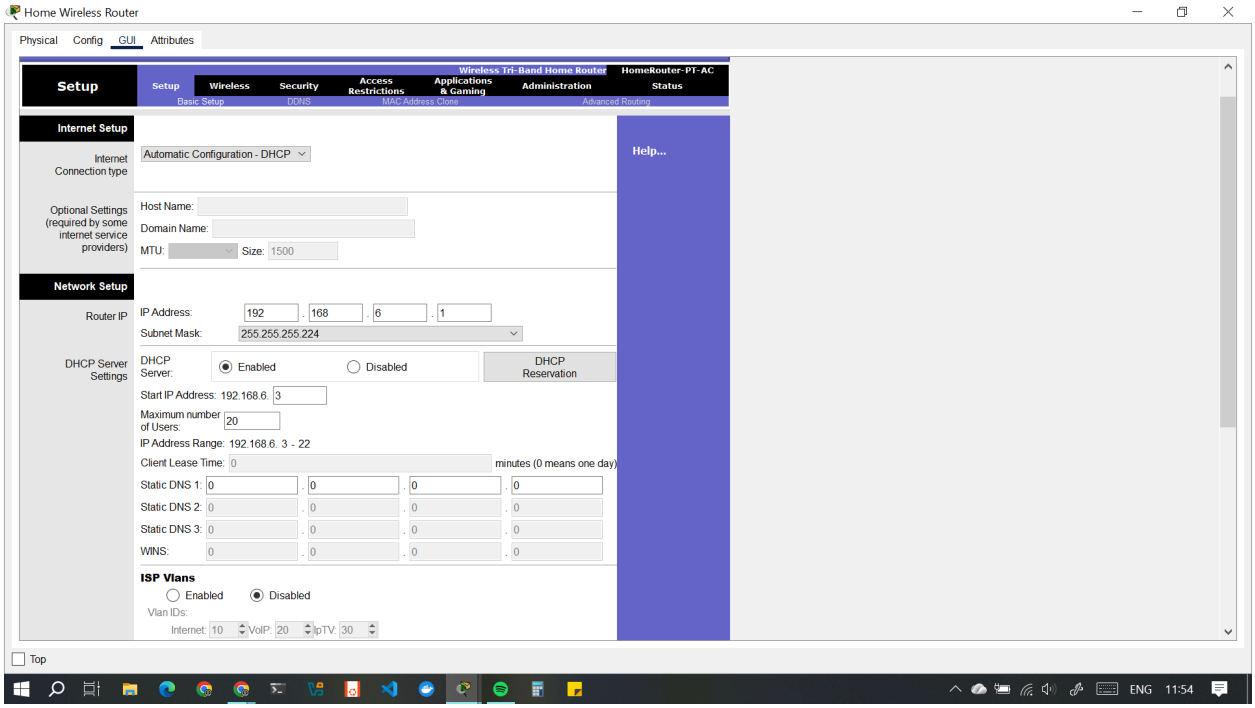
I was tasked with installing a new home wireless router at a friend's house. I needed to change settings on the router to enhance security and meet my friend's requirements.

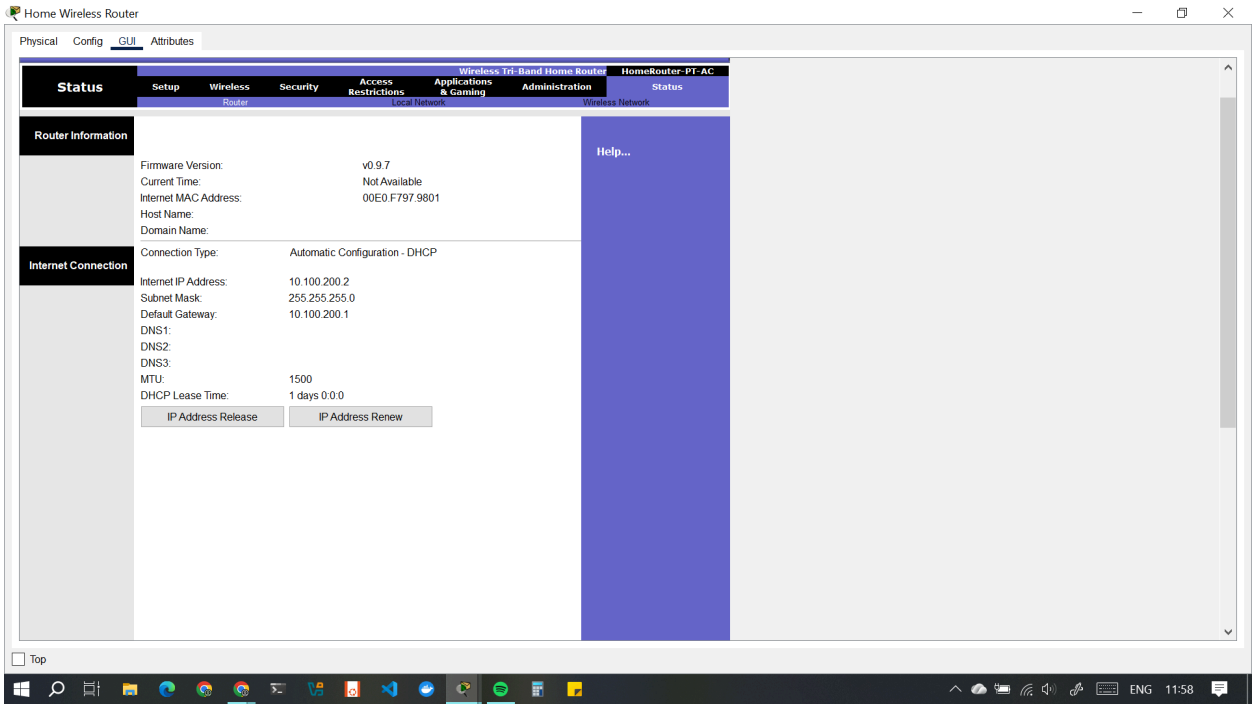
Step 1: Change DHCP settings.

a. Open the Home Wireless Router GUI and change the router IP and DHCP settings according to the information in the Addressing Table.
b. Permit a maximum of 20 addresses to be issued by the router.
c. Configure the DHCP server to start with IP address .3 of the LAN network.

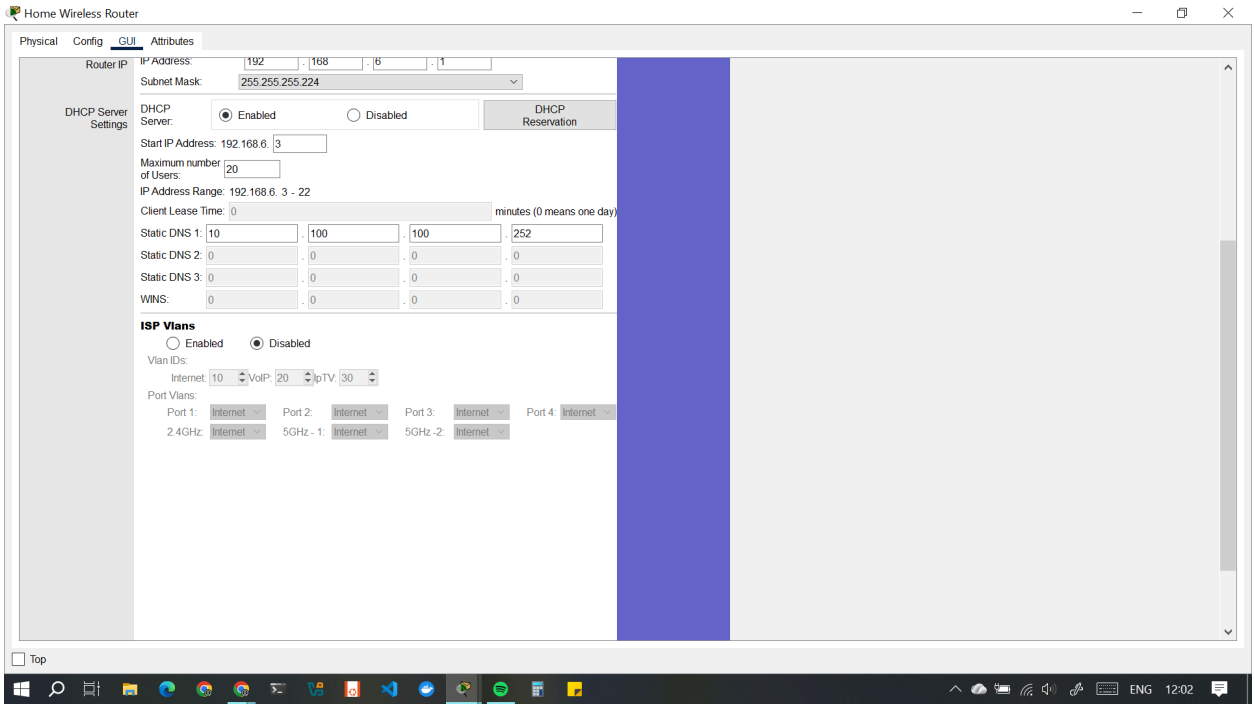
d. Configure the internet interface of the router to receive its IP address over DHCP.

   Question: Verify the address. What address did it receive? **10.100.200.2 with a subnet mask of /24**


Home Wireless Router
Physical Config GUI Attributes
Wireless Tri-Band Home Router
HomeRouter-PT-AC
Setup
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Basic Setup DDNS MAC Address Clone Advanced Routing
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: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0
ISP Vlans
Enabled Disabled
Vlan IDs:
Internet: 10 VoIP: 20 IpTV: 30
Help...
Top
ENG 11:54


Home Wireless Router
Physical Config GUI Attributes
Wireless Tri-Band Home Router
HomeRouter-PT-AC
Status
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Router Local Network Wireless Network
Router Information
Firmware Version: v0.9.7
Current Time: Not Available
Internet MAC Address: 00E0.F797.9801
Host Name:
Domain Name:
Internet Connection
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:
DNS2:
DNS3:
MTU: 1500
DHCP Lease Time: 1 days 0:0:0
IP Address Release
IP Address Renew
Help...
Top
ENG 11:58

e. Configure the static DNS server to the address in the Addressing Table.



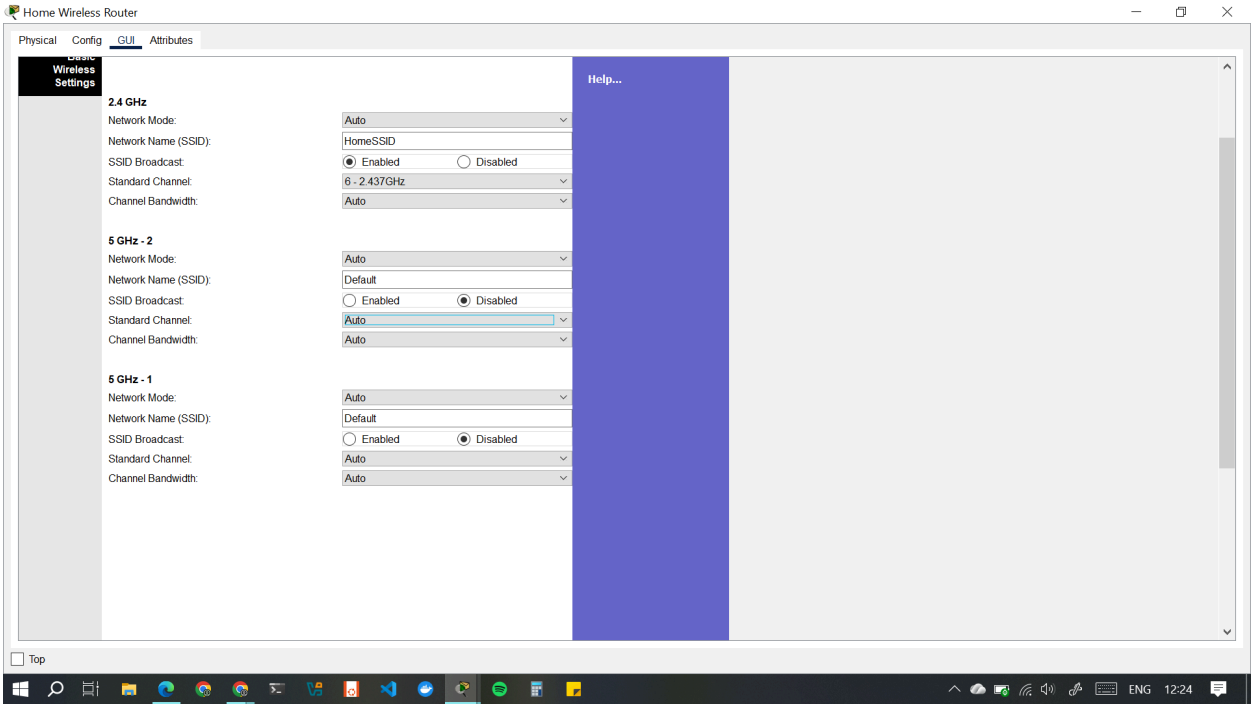
Step 2: Configure the Wireless LAN

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.

- The **2.4 GHz band** only has **11 channels**, and most of them **overlap** with each other. To minimize **interference**, only **channels 1, 6, and 11** are considered “non-overlapping.”
- Choosing **Channel 6** means using a **clean, middle frequency** with minimal overlap and interference. It’s a **standard best practice** for stable Wi-Fi in small networks.

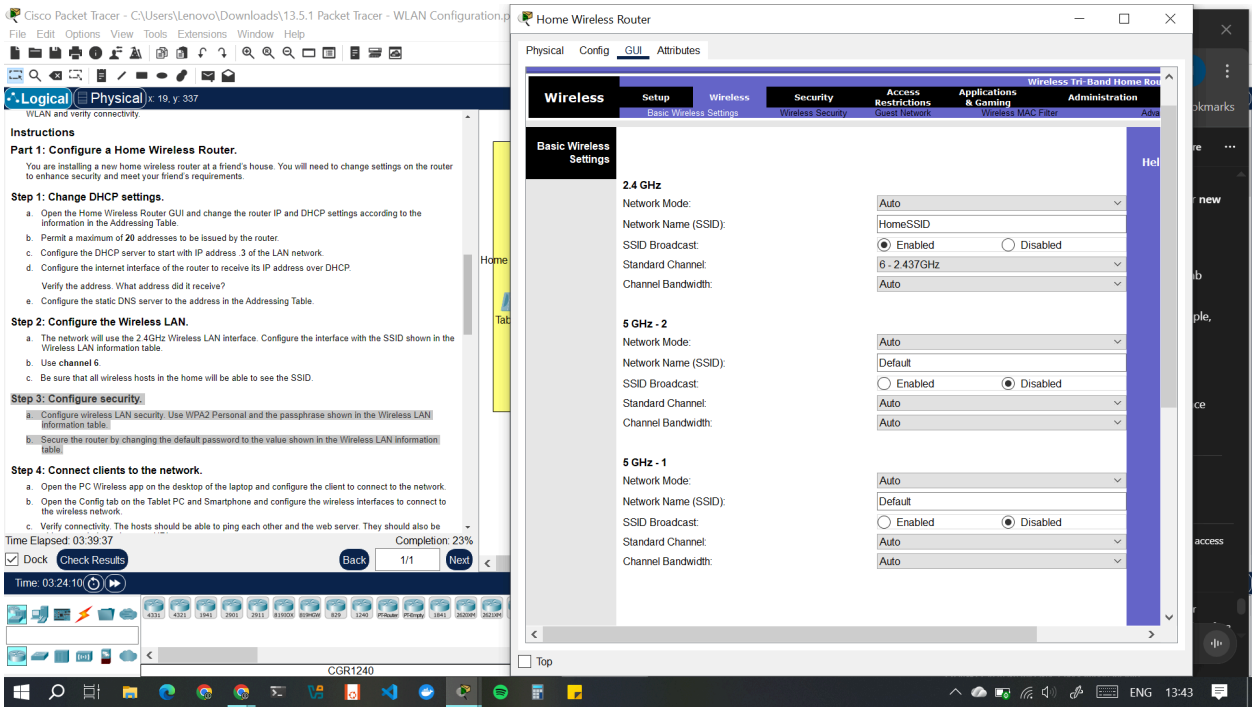
c. Be sure that all wireless hosts in the home will be able to see the SSID. - the SSID broadcast should be set to enabled

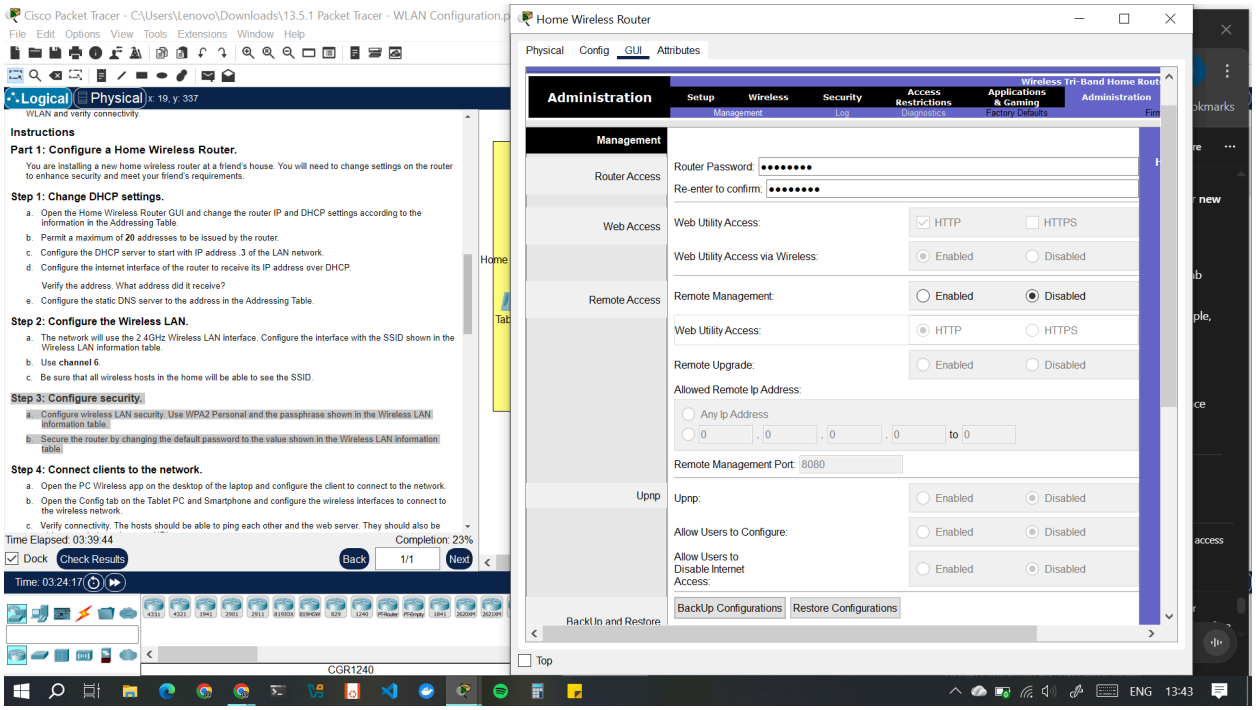


Step 3: Configure security

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

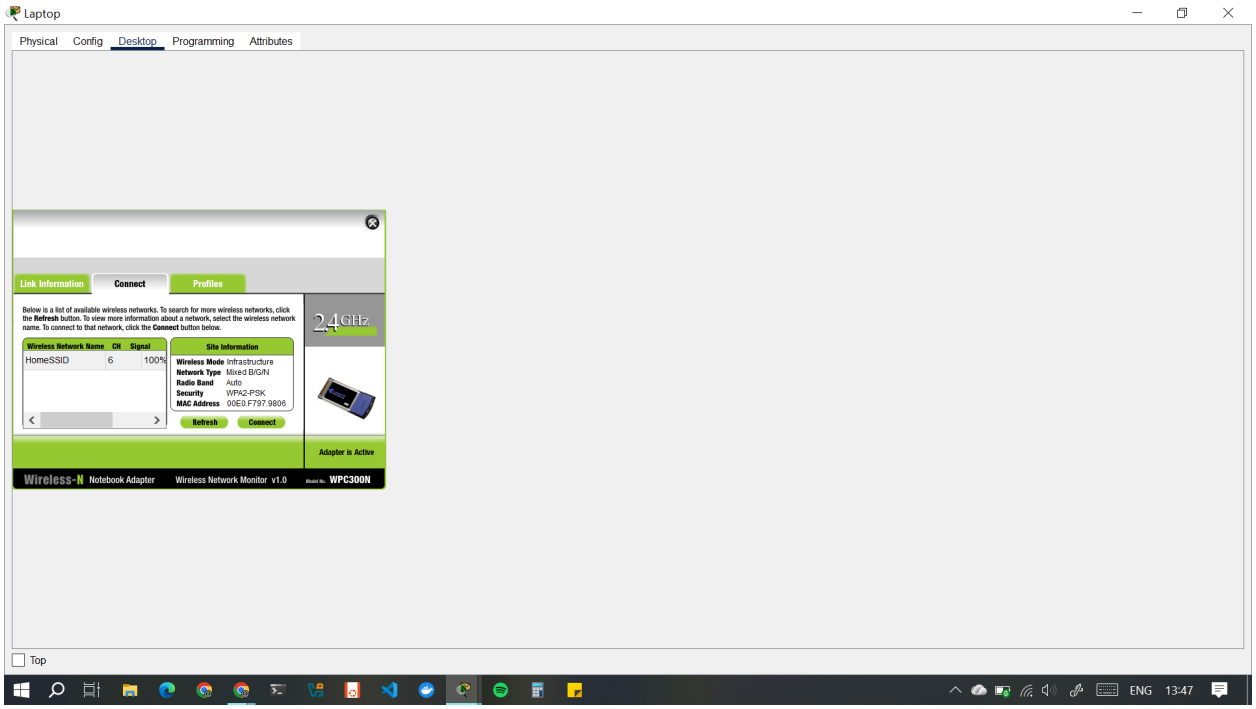
b. Secure the router by changing the default password to the value shown in the Wireless LAN information table.



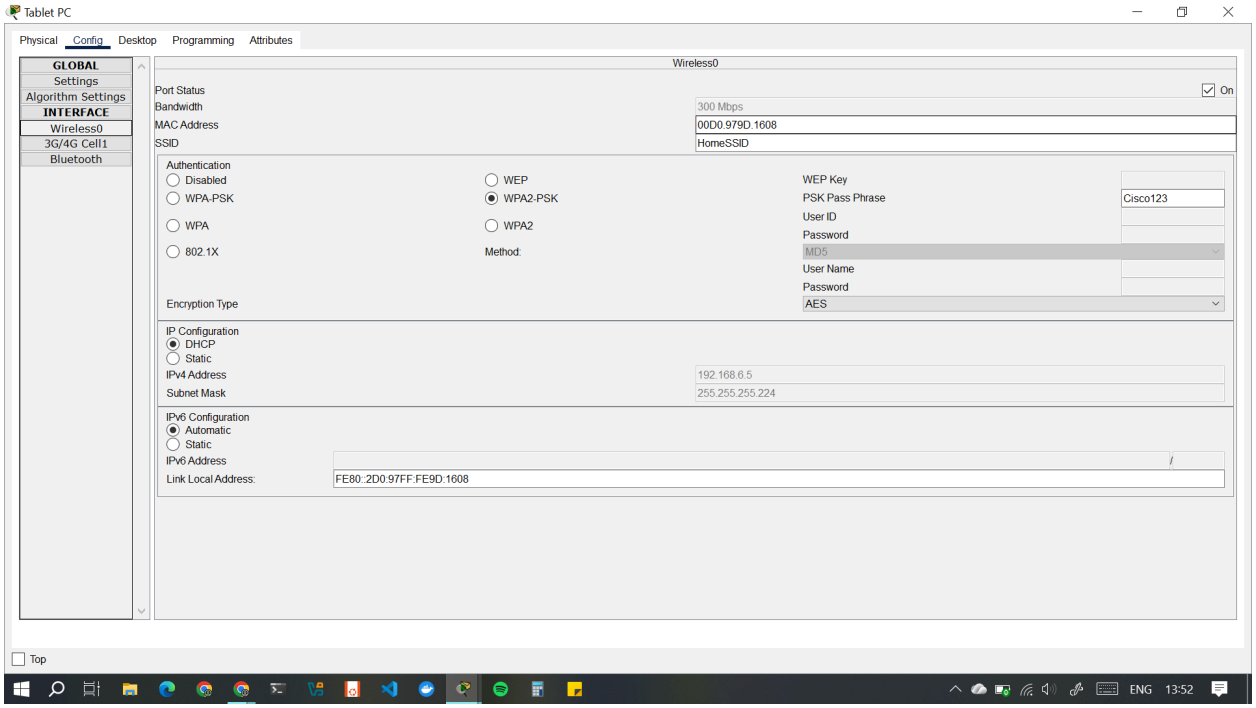


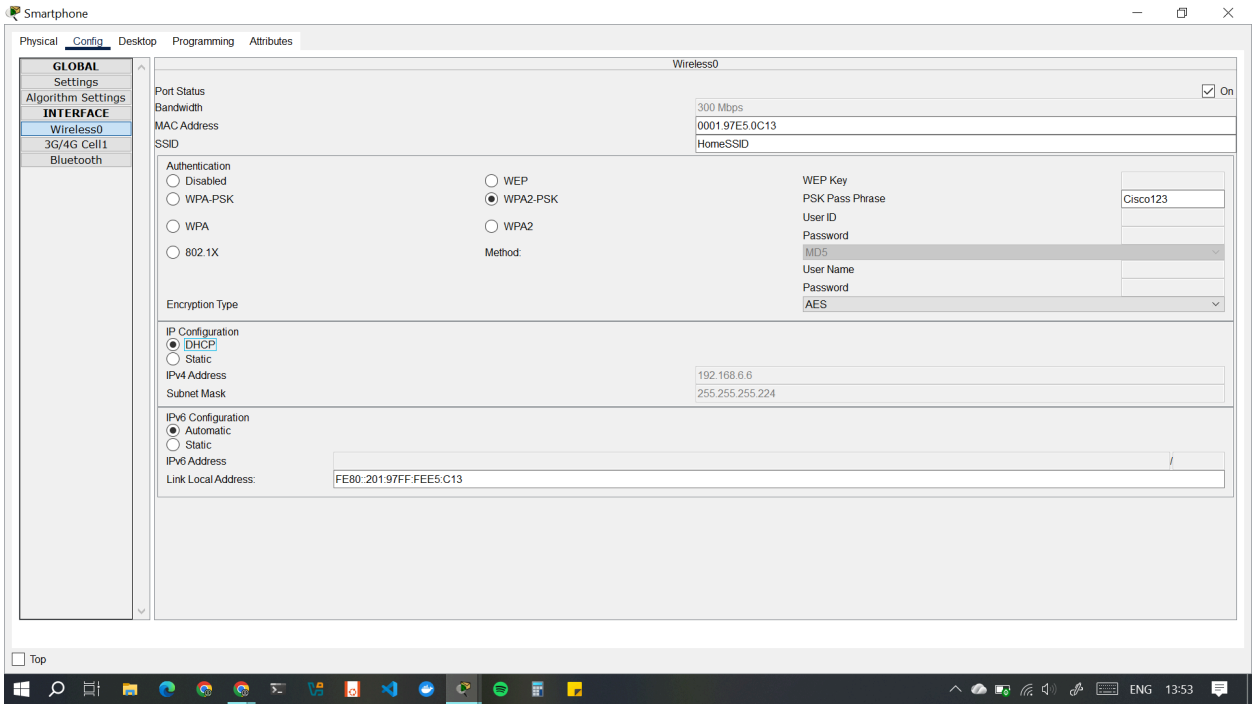
Step 4: Connect clients to the network.

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

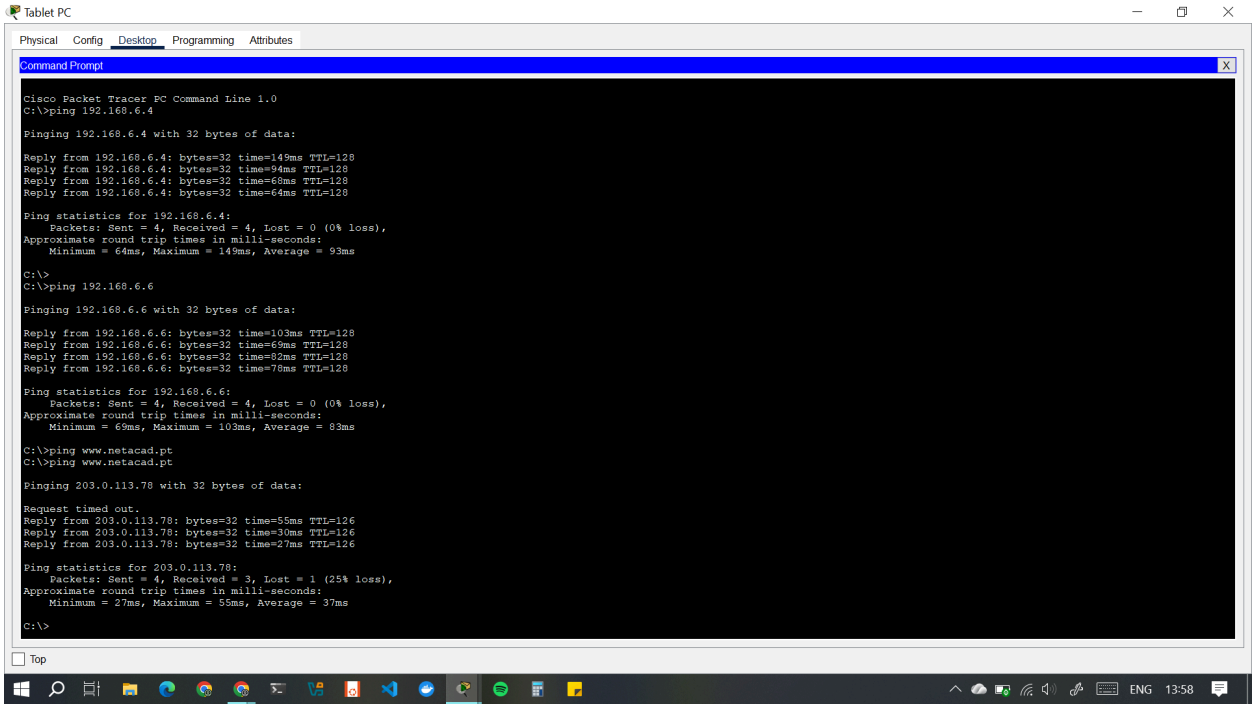


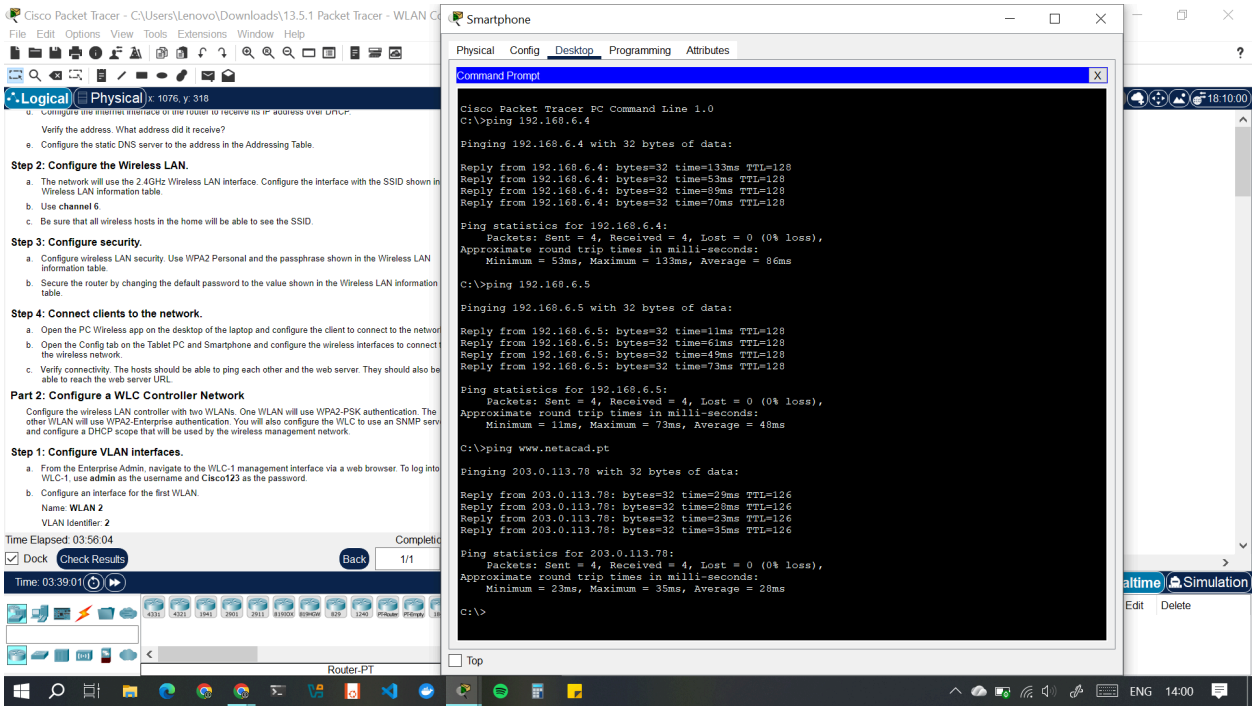
b. Open the Config tab on the Tablet PC and Smartphone and configure the wireless interfaces to connect to the wireless network.

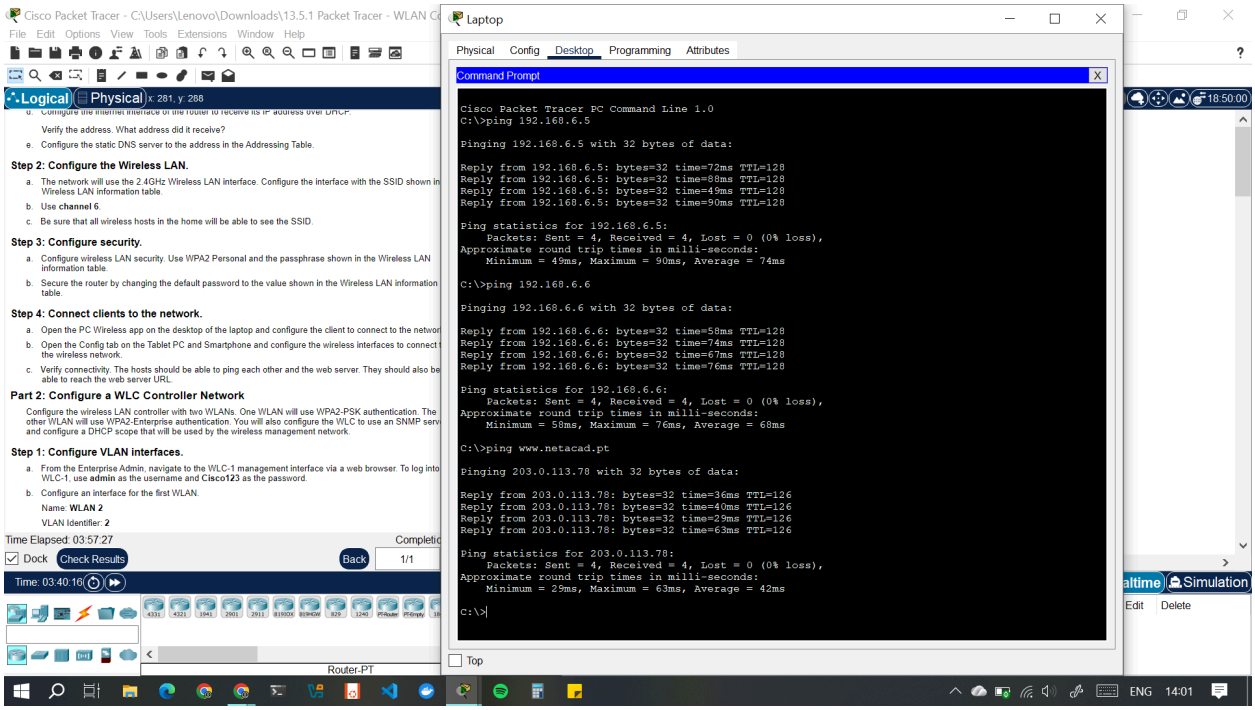




c. Verify connectivity. The hosts should be able to ping each other and the web server. They should also be able to reach the web server URL.


Tablet PC
Physical Config Desktop Programming Attributes
Command Prompt
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=149ms TTL=128
Reply from 192.168.6.4: bytes=32 time=94ms TTL=128
Reply from 192.168.6.4: bytes=32 time=68ms TTL=128
Reply from 192.168.6.4: bytes=32 time=64ms 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 = 64ms, Maximum = 149ms, Average = 93ms
C:\>
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=103ms TTL=128
Reply from 192.168.6.6: bytes=32 time=69ms TTL=128
Reply from 192.168.6.6: bytes=32 time=82ms TTL=128
Reply from 192.168.6.6: bytes=32 time=70ms 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 = 69ms, Maximum = 103ms, Average = 83ms
C:\>ping www.netacad.pt
C:\>ping www.netacad.pt
Pinging 203.0.113.78 with 32 bytes of data:
Request timed out.
Reply from 203.0.113.78: bytes=32 time=55ms TTL=126
Reply from 203.0.113.78: bytes=32 time=30ms TTL=126
Reply from 203.0.113.78: bytes=32 time=27ms 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 = 27ms, Maximum = 55ms, Average = 37ms
C:\>
Top
ENG 13:58


Cisco Packet Tracer - C:\Users\Lenovo\Downloads\13.5.1 Packet Tracer - WLAN C
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1076, y: 318
Verify the address. What address did it receive?
e. Configure the static DNS server to the address in the Addressing Table.
Step 2: Configure the Wireless LAN.
a. The network will use the 2.4GHz Wireless LAN interface. Configure the interface with the SSID shown in 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.
Step 3: 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.
Step 4: 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 networ
b. Open the Config tab on the Tablet PC and Smartphone and configure the wireless interfaces to connect t the wireless network.
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.
Part 2: 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 serv and configure a DHCP scope that will be used by the wireless management network.
Step 1: Configure VLAN interfaces.
a. From the Enterprise Admin, navigate to the WLC-1 management interface via a web browser. To log into WLC-1, use admin as the username and Cisco123 as the password.
b. Configure an interface for the first WLAN.
Name: WLAN 2
VLAN Identifier: 2
Time Elapsed: 03:56:04
Dock Check Results
Back 1/1
Time: 03:39:01
Router-PT
Smartphone
Physical Config Desktop Programming Attributes
Command Prompt
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=133ms TTL=128
Reply from 192.168.6.4: bytes=32 time=53ms TTL=128
Reply from 192.168.6.4: bytes=32 time=89ms TTL=128
Reply from 192.168.6.4: bytes=32 time=70ms 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 = 53ms, Maximum = 133ms, Average = 86ms
C:\>ping 192.168.6.5
Pinging 192.168.6.5 with 32 bytes of data:
Reply from 192.168.6.5: bytes=32 time=11ms TTL=128
Reply from 192.168.6.5: bytes=32 time=61ms TTL=128
Reply from 192.168.6.5: bytes=32 time=49ms TTL=128
Reply from 192.168.6.5: bytes=32 time=73ms TTL=128
Ping statistics for 192.168.6.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 73ms, Average = 48ms
C:\>ping www.netacad.pt
Pinging 203.0.113.78 with 32 bytes of data:
Reply from 203.0.113.78: bytes=32 time=29ms TTL=126
Reply from 203.0.113.78: bytes=32 time=28ms TTL=126
Reply from 203.0.113.78: bytes=32 time=23ms TTL=126
Reply from 203.0.113.78: bytes=32 time=35ms 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 = 23ms, Maximum = 35ms, Average = 28ms
C:\>
Top
18:10:00
Simulation
Edit Delete
ENG 14:00



Part 2: Configure a WLC Controller Network

I was tasked with configuring 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.

Step 1: Configure VLAN interfaces.

a. From the Enterprise Admin, navigate to the WLC-1 management interface via a web browser. To log into WLC-1, use admin as the username and Cisco123 as the password.

b. Configure an interface for the first WLAN.

   Name: WLAN 2

   VLAN Identifier: 2

Port Number: 1

Interface IP Address: 192.168.2.254

Netmask: 255.255.255.0

Gateway: RTR-1 G0/0/0.2 address

Primary DHCP Server: Gateway address

c. Configure an interface for the second WLAN.

Name: WLAN 5

VLAN Identifier: 5

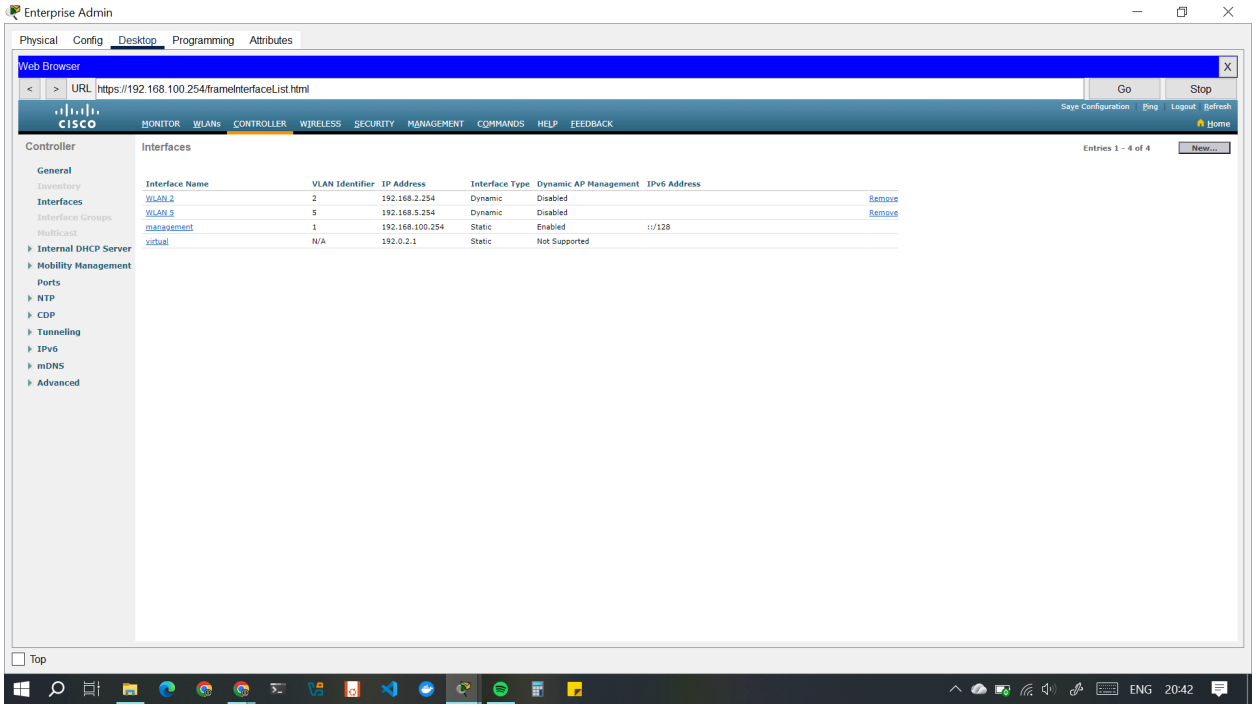
Port Number: 1

Interface IP Address: 192.168.5.254

Netmask: 255.255.255.0

Gateway: RTR-1 interface G0/0/0.5 address

Primary DHCP Server: Gateway address



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

a. Configure and enable an internal DHCP scope as follows:

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

Default Routers: 192.168.100.1

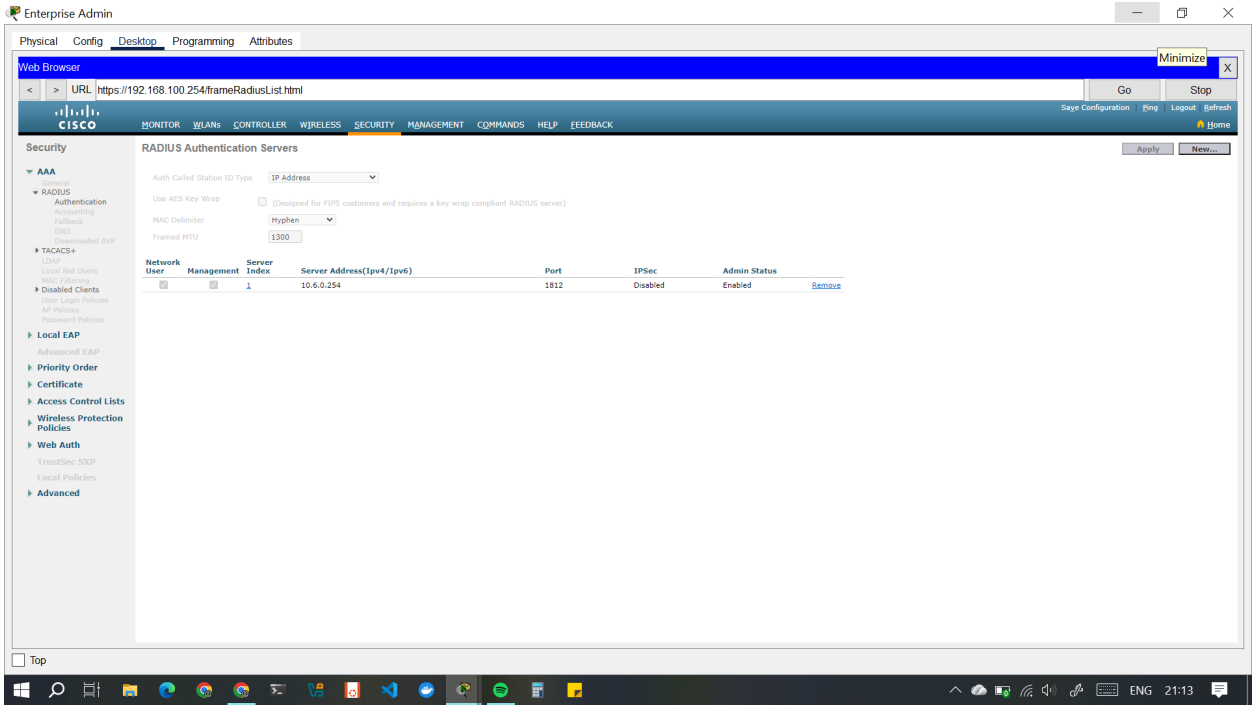
Step 3: Configure the WLC with external server addresses.

a. Configure the RADIUS server information as follows:

Sever Index: 1

Server Address: 10.6.0.254

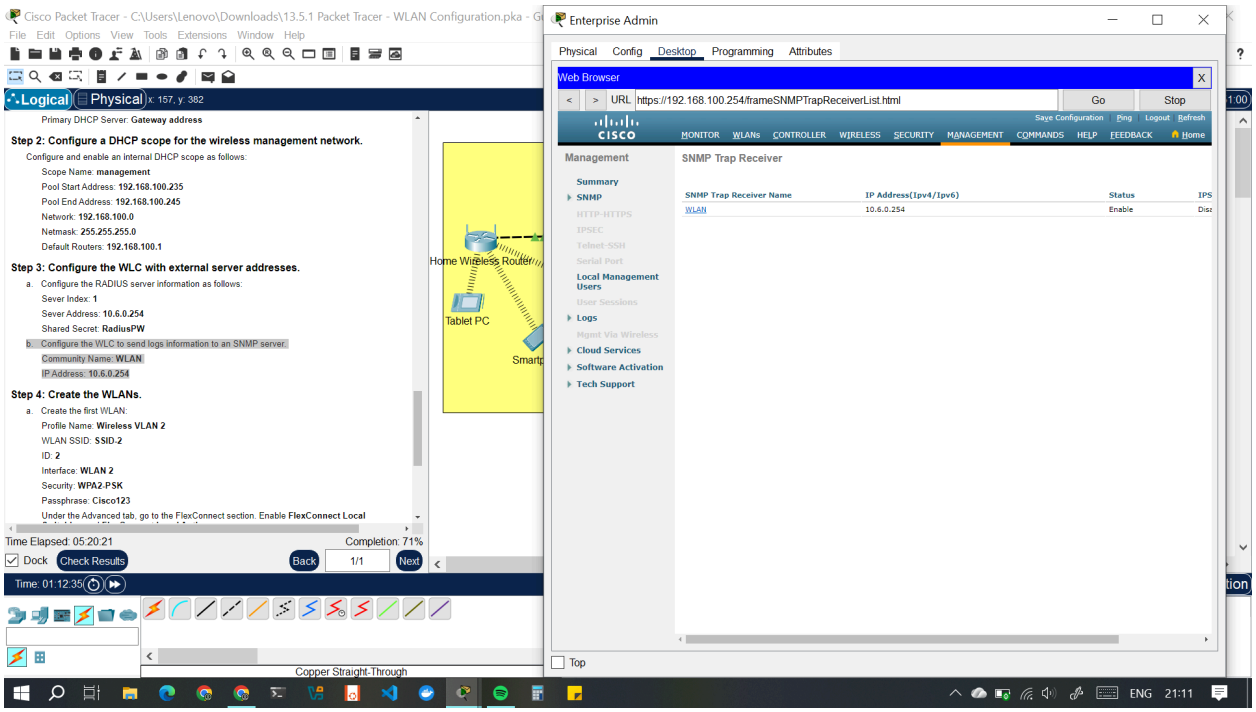
Shared Secret: RadiusPW



b. Configure the WLC to send logs information to an SNMP server.

Community Name: WLAN

IP Address: 10.6.0.254



Step 4: Create the WLANs.

a. 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.

b. Create the second WLAN:

Profile Name: Wireless VLAN 5

WLAN SSID: SSID-5

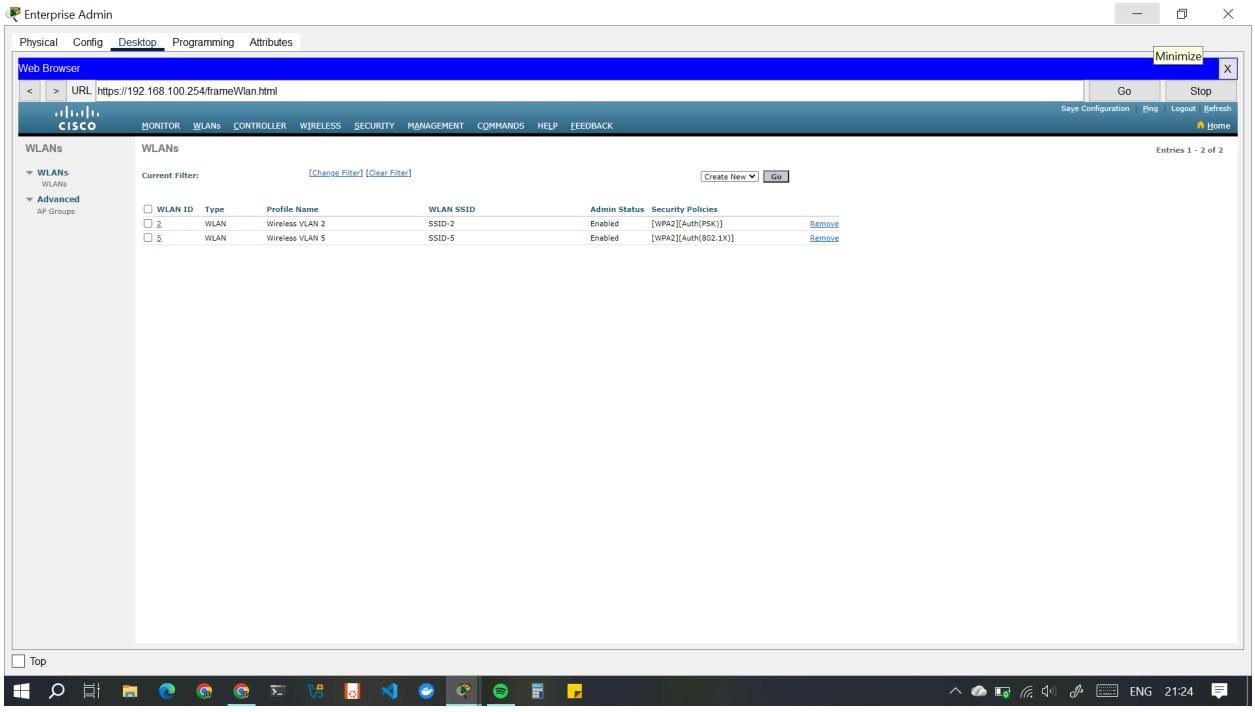
Interface: WLAN 5

ID: 5

Security: 802.1x - WPA2-Enterprise

Configure the WLAN to use the RADIUS server for authentication.

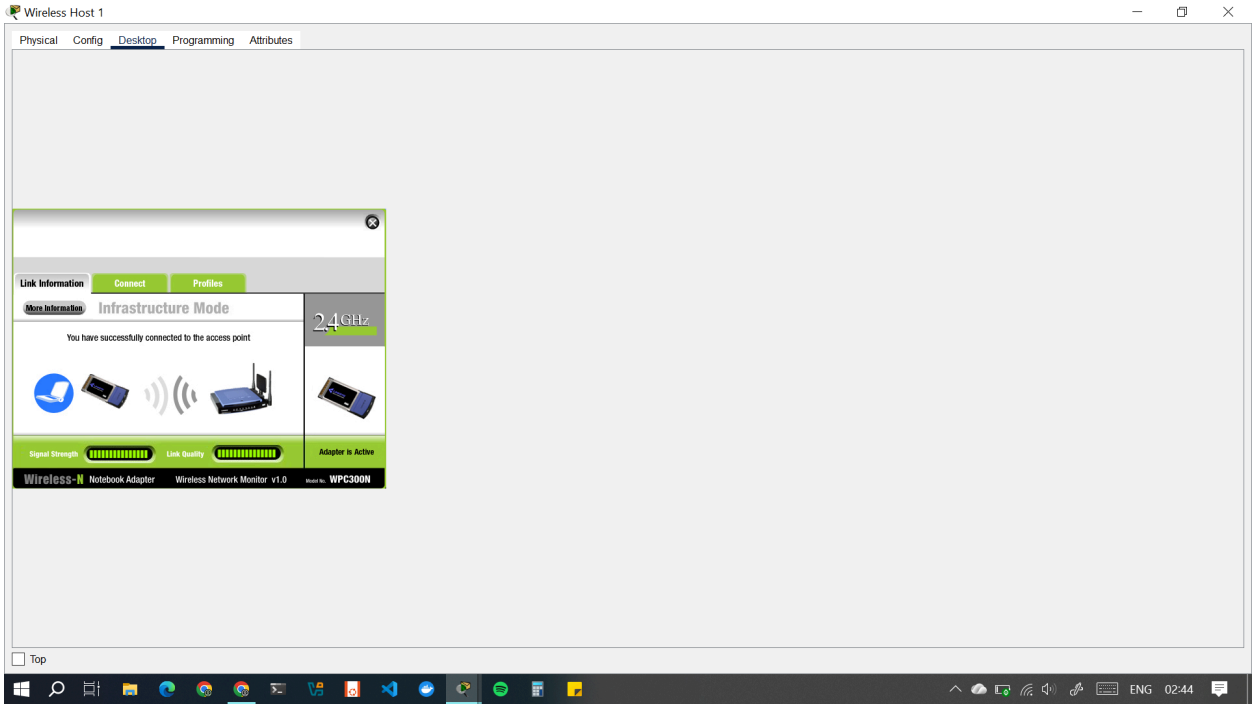
Make the FlexConnect settings as was done in Step 4a.



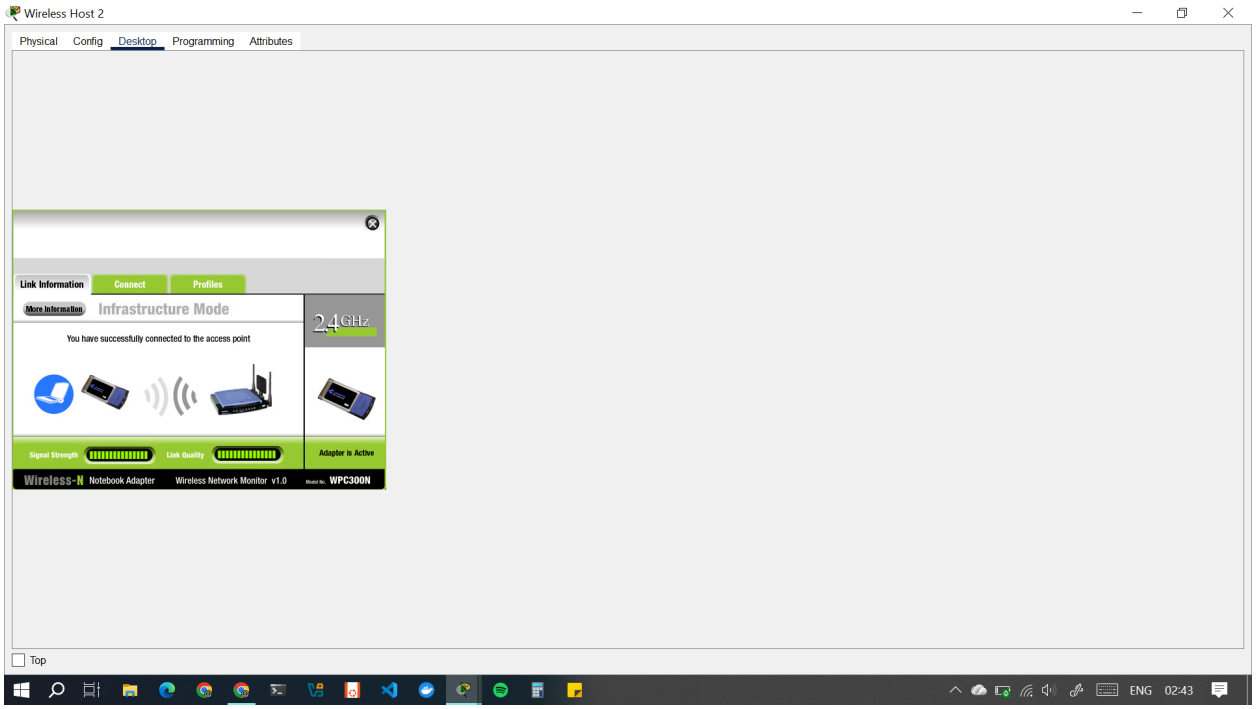
Step 5: Configure the hosts to connect to the WLANs.

Use the desktop PC Wireless app to configure the hosts as follows:

a. Wireless Host 1 should connect to Wireless VLAN 2.

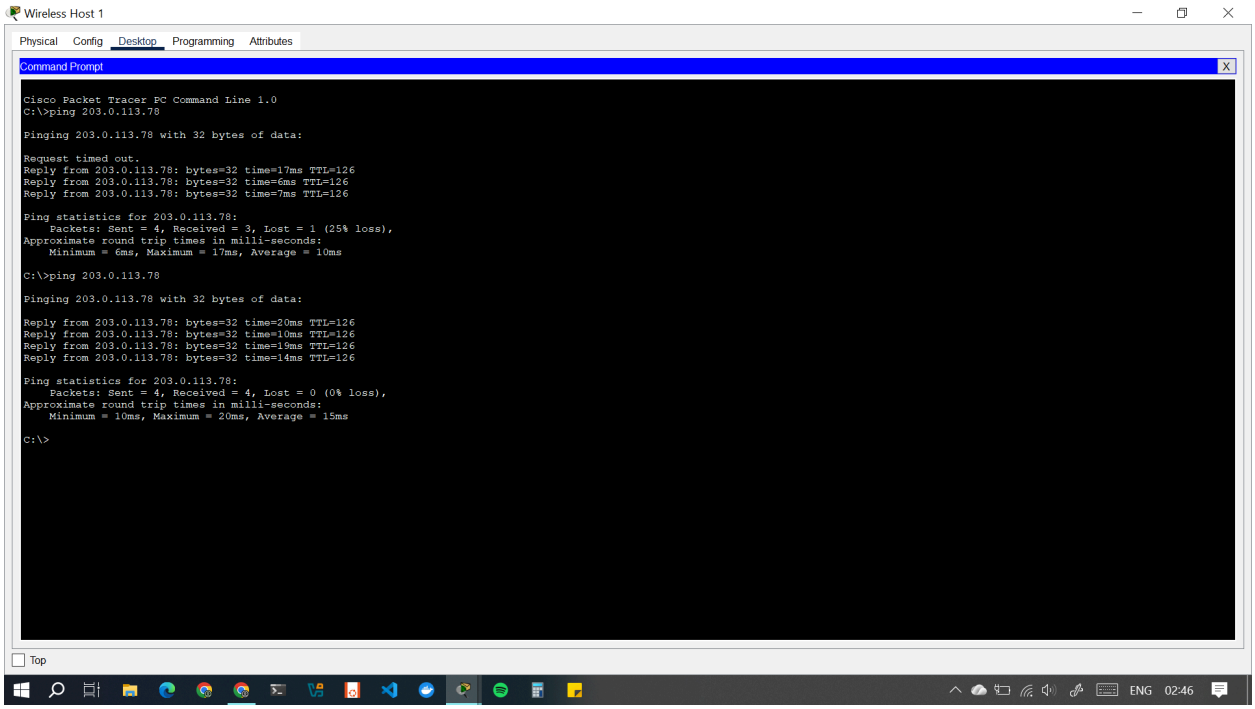


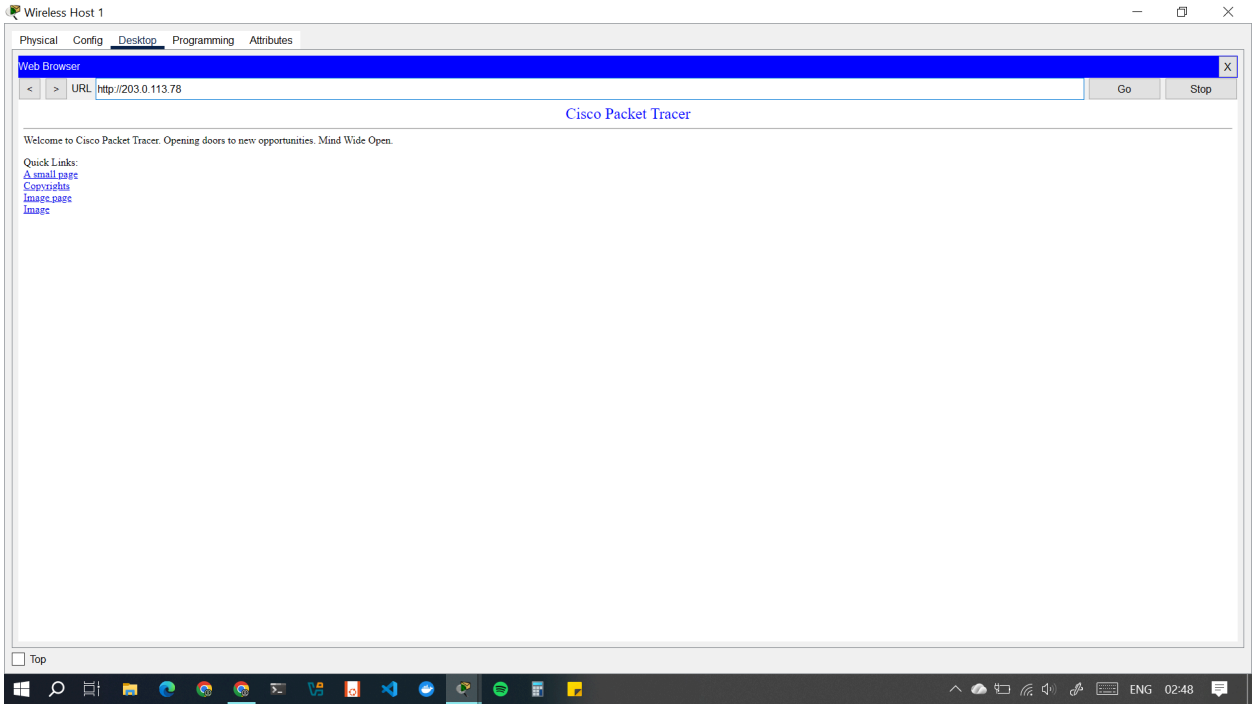
b. Wireless Host 2 should connect to Wireless VLAN 5 using the credentials in the WLAN information table.

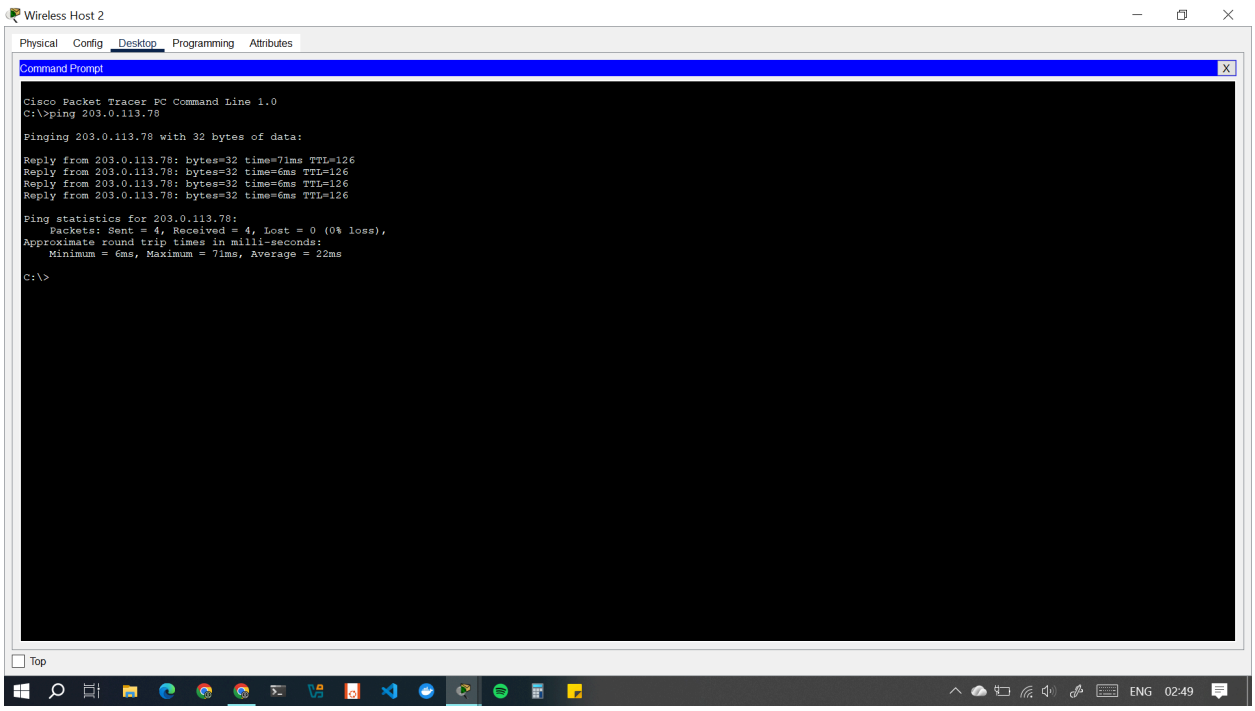


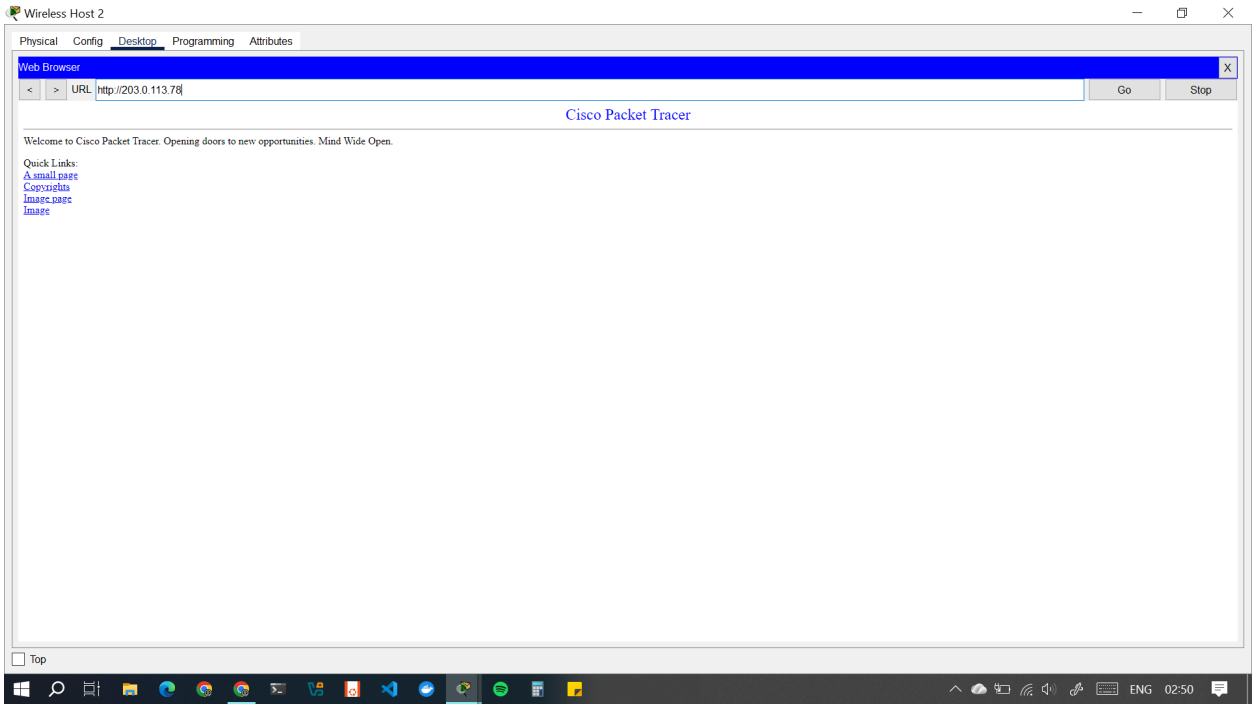
Step 6: Test connectivity.

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




Wireless Host 1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://203.0.113.78
Go
Stop
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
Top
ENG
02:48


Wireless Host 2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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=71ms TTL=126
Reply from 203.0.113.78: bytes=32 time=6ms TTL=126
Reply from 203.0.113.78: bytes=32 time=6ms TTL=126
Reply from 203.0.113.78: bytes=32 time=6ms 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 = 6ms, Maximum = 71ms, Average = 22ms
C:\>
Top
ENG
02:49



Conclusion

During this activity, the configuration for both a home wireless router and an enterprise-level Wireless LAN Controller (WLC) were successfully implemented to support secure wireless connectivity in various environments. The home router was configured using an IP addressing scheme that is private, a static DHCP range, and security mechanisms that include WPA2-Personal (PSK), thus enabling many household devices to easily connect and communicate with each other and with outside networks.

At the enterprise end, VLAN division and WLC interfaces were set up to accommodate two WLANs, one with WPA2-PSK and the other with WPA2-Enterprise security with integration to a RADIUS server. The WLC was further connected to SNMP and DHCP server to carry out network administration and IP addressing.

By this practice, fundamental networking principles including WLAN configuration, wireless security (WPA2-PSK and WPA2-Enterprise), RADIUS authentication, and DHCP administration were cemented. The final verification step also ensured all the wireless clients were able to connect to the corresponding networks, authenticate properly, and

interact with the Web Server, showing an effective and secured WLAN implementation both for homes and business environments.