Assignment 2: Packet Tracer WLAN configuration

Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction

The growing reliance on wireless technology in contemporary networks has made the configuration and optimization of WLAN (Wireless Local Area Network) infrastructure a critical skill for IT professionals.

In this report, I delve into the configuration of a WLAN using Cisco's Packet Tracer, a robust network simulation tool widely utilized in both educational and professional settings. This assignment aims to demonstrate the practical application of theoretical networking concepts, highlighting the processes and considerations involved in setting up a secure and efficient wireless network.

Through this exercise, I will explore the fundamental aspects of WLAN configuration, including SSID settings, security protocols, and connectivity testing, thereby underscoring the importance of meticulous planning and execution in network management.

Objectives

In this activity, I will configure both a wireless home router and a WLC-based network. I will implement both WPA2-PSK and WPA2-Enterprise security.

- 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.

Part 1: Configure a Home Wireless Router

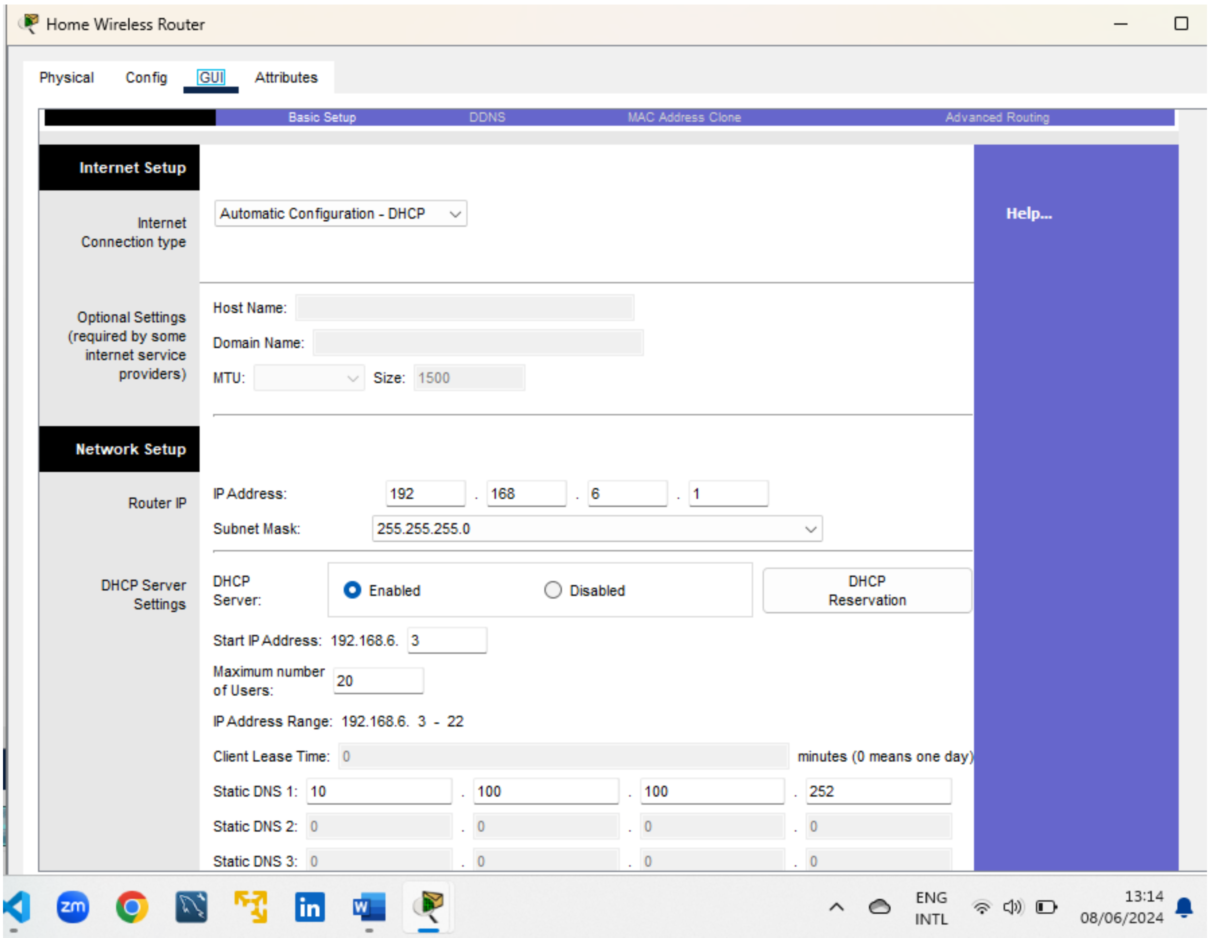
In this section, we configured a home wireless router to enhance security and meet specific requirements. The following steps outline the process:

Step 1: Change DHCP Settings:

- Accessed the router’s GUI and adjusted the router IP and DHCP settings as per the Addressing Table.
- Set the DHCP pool to issue a maximum of 20 addresses.
- Configured the DHCP server to start at IP address .3 of the LAN network.

- ○ Set the internet interface to receive its IP address dynamically over DHCP.
- ○ Verified the IP address received by the internet interface: [Insert received IP address here].
- ○ Configured the static DNS server address as specified in the Addressing Table.

These steps ensured that the home wireless router was set up with a secure and efficient DHCP configuration, meeting the specified requirements and enhancing network security.



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: 255.255.255.0

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)

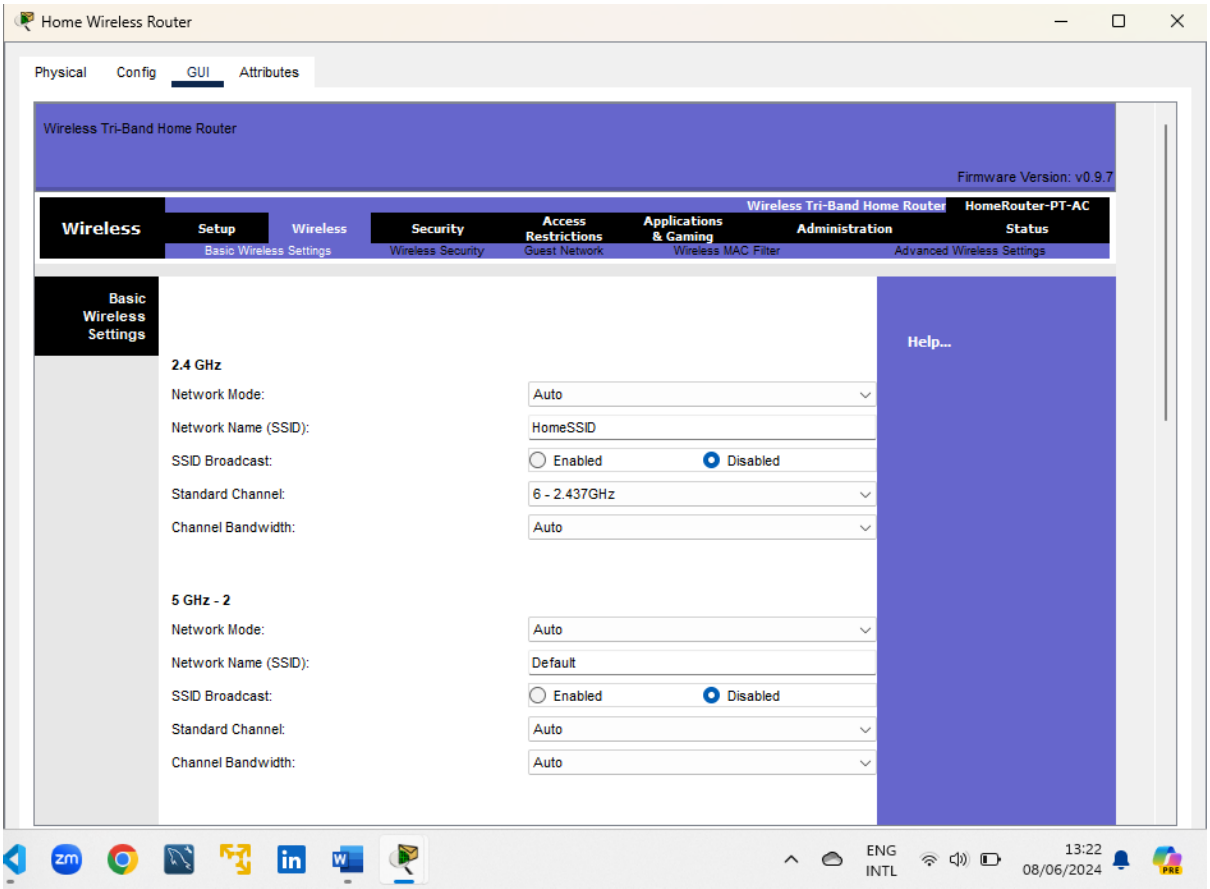
Static DNS 1: 10 . 100 . 100 . 252

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

Step 2: Configure the Wireless LAN

1. **2.4GHz Wireless LAN Interface Configuration**:
   - ○ Accessed the router’s GUI and configured the SSID as per the Wireless LAN information table.
   - ○ Set the wireless channel to 6.



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

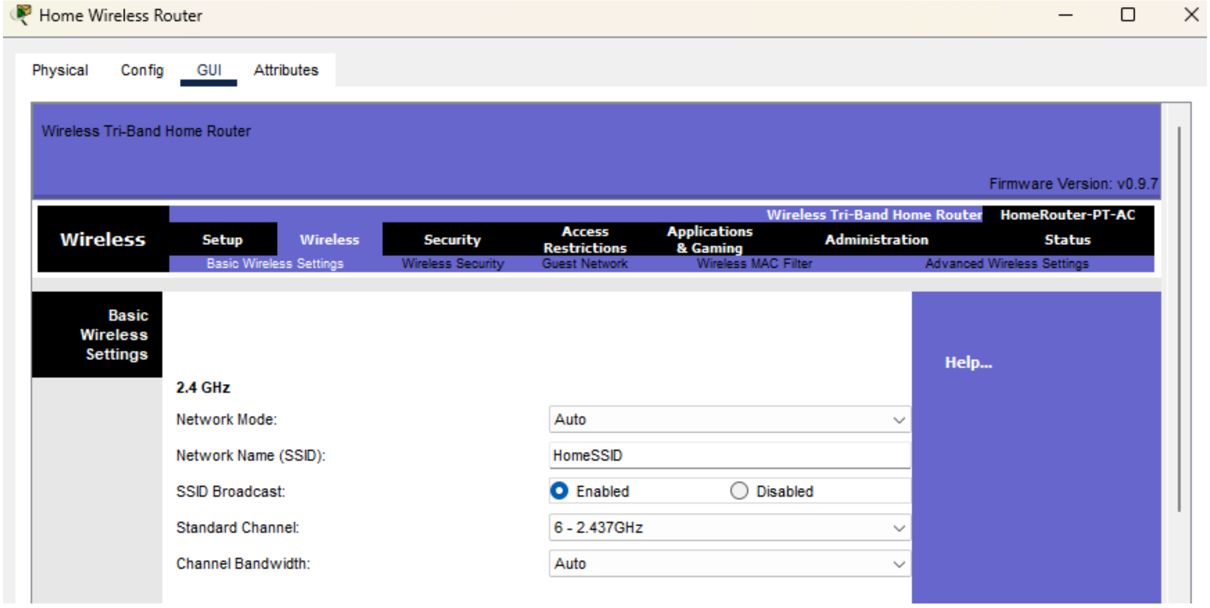
Network Name (SSID): Default

SSID Broadcast: ○ Enabled ● Disabled

Standard Channel: Auto

Channel Bandwidth: Auto

- Enabled SSID broadcast to ensure visibility for all wireless hosts.



2.4 GHz

Network Mode: Auto

Network Name (SSID): HomeSSID

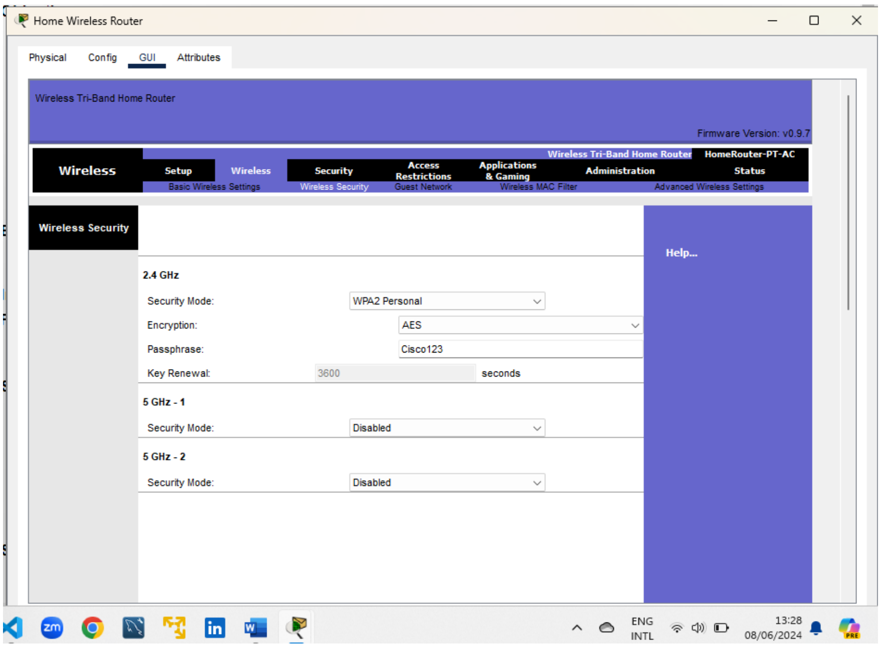
SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: 6 - 2.437GHz

Channel Bandwidth: Auto

Step 3: Configure Security

1. **Wireless LAN Security**:
   - Configured WPA2 Personal security with the specified passphrase.



2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Cisco123

Key Renewal: 3600 seconds

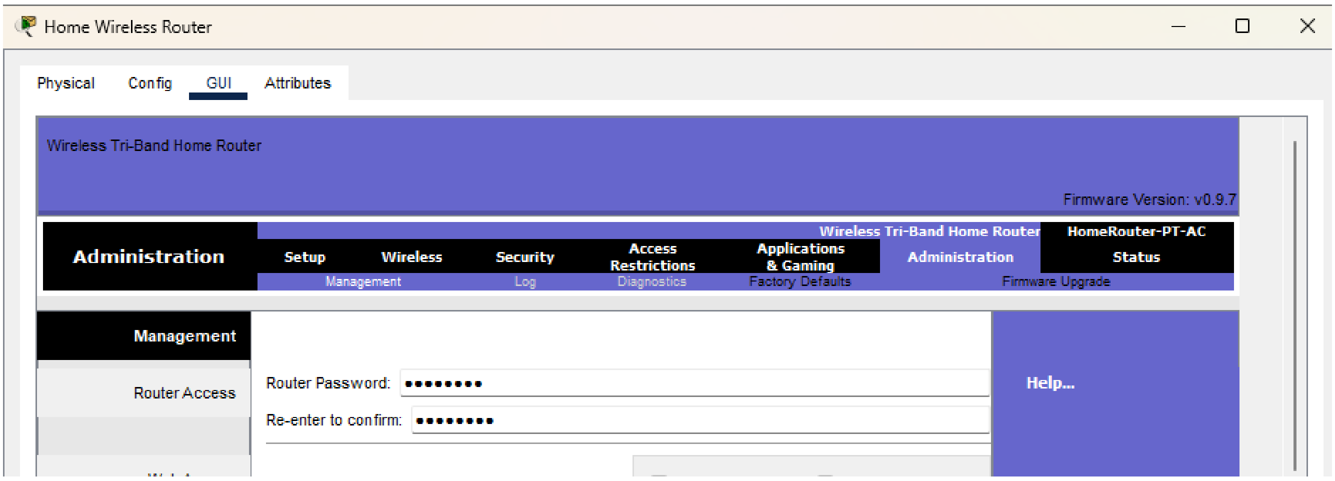
5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

   - Changed the default router password to enhance security.

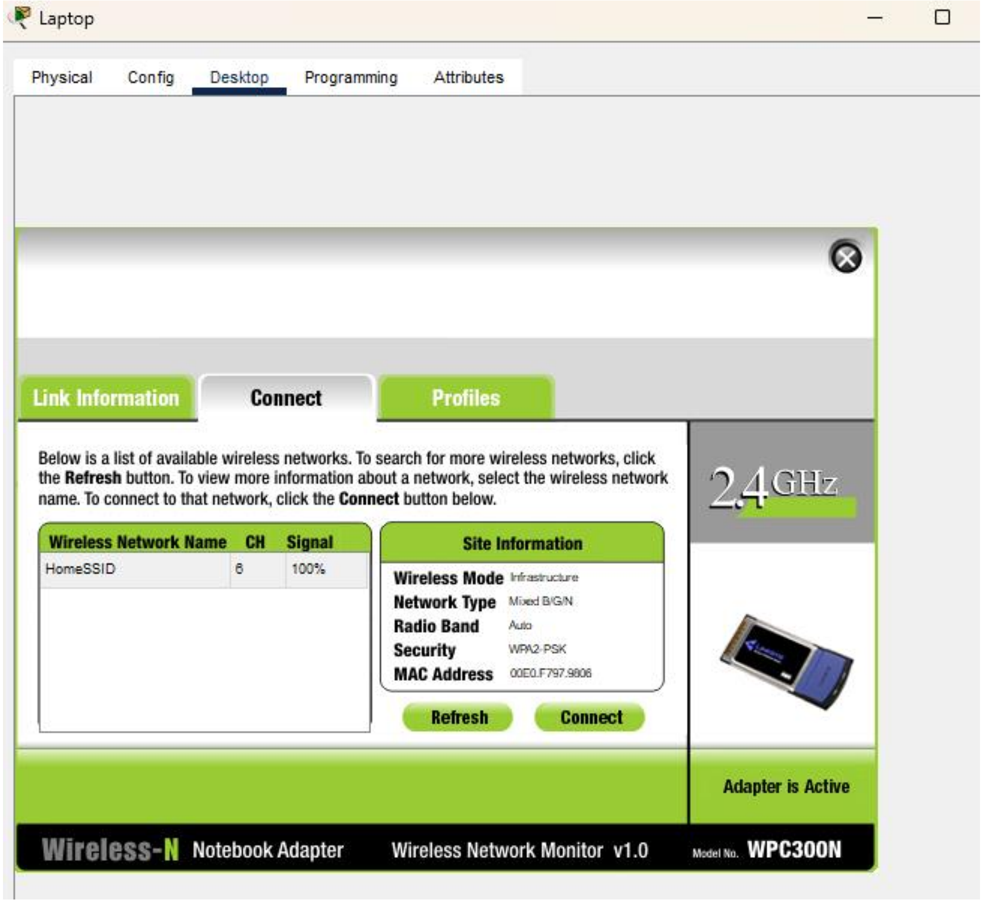


Router Password: ••••••••

Re-enter to confirm: ••••••••

Step 4: Connect Clients to the Network

1. **Laptop Client Configuration**:
   - Used the PC Wireless app to connect to the network using the SSID and passphrase.



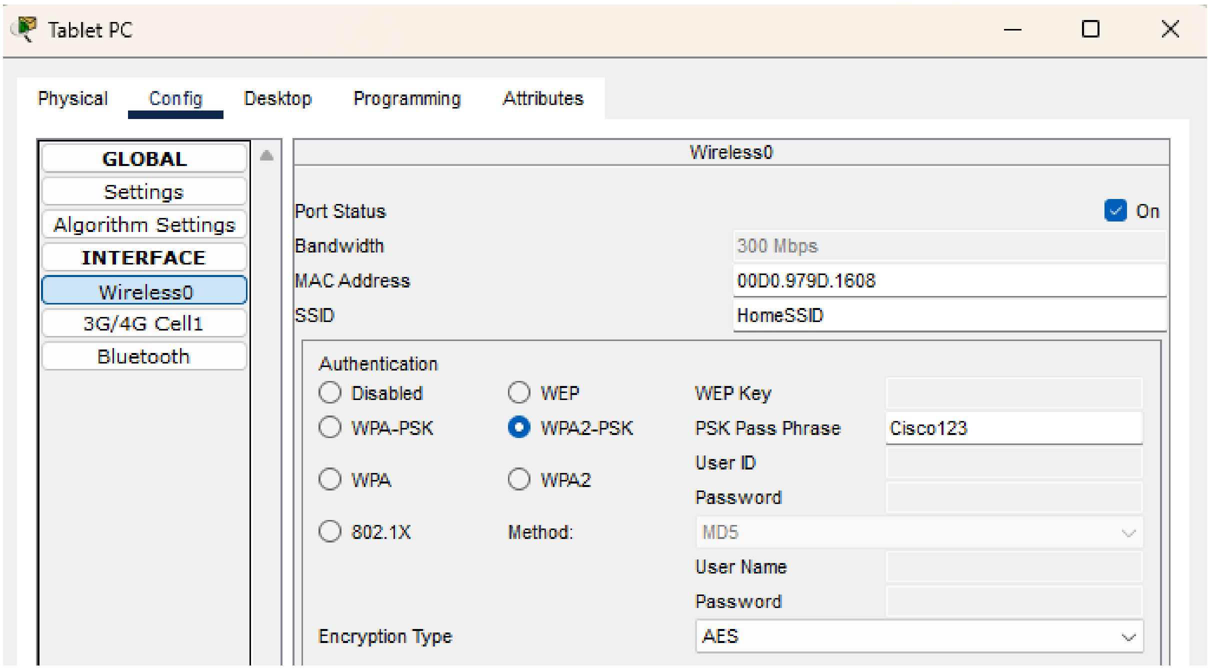
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

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

2. **Tablet PC and Smartphone Configuration**:
   - Configured the wireless interfaces on both devices to connect to the network using the SSID and passphrase.



Wireless0

Port Status	☑ On
Bandwidth	300 Mbps
MAC Address	00D0.979D.1608
SSID	HomeSSID

Authentication

○ Disabled ○ WEP WEP Key

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

User ID

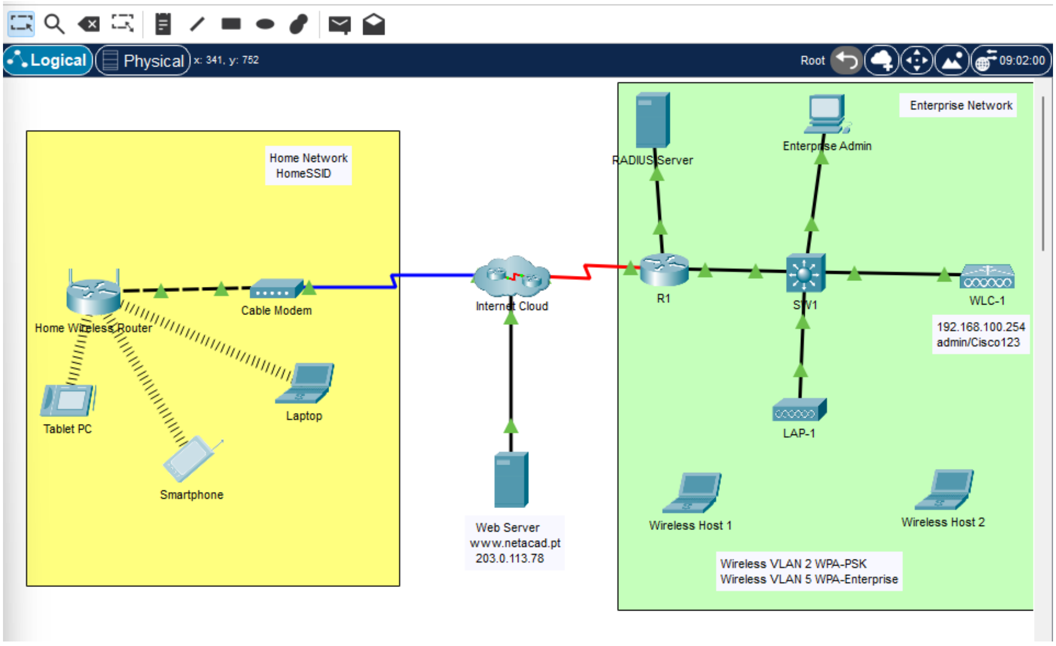
○ WPA ○ WPA2 Password

○ 802.1X Method: MD5

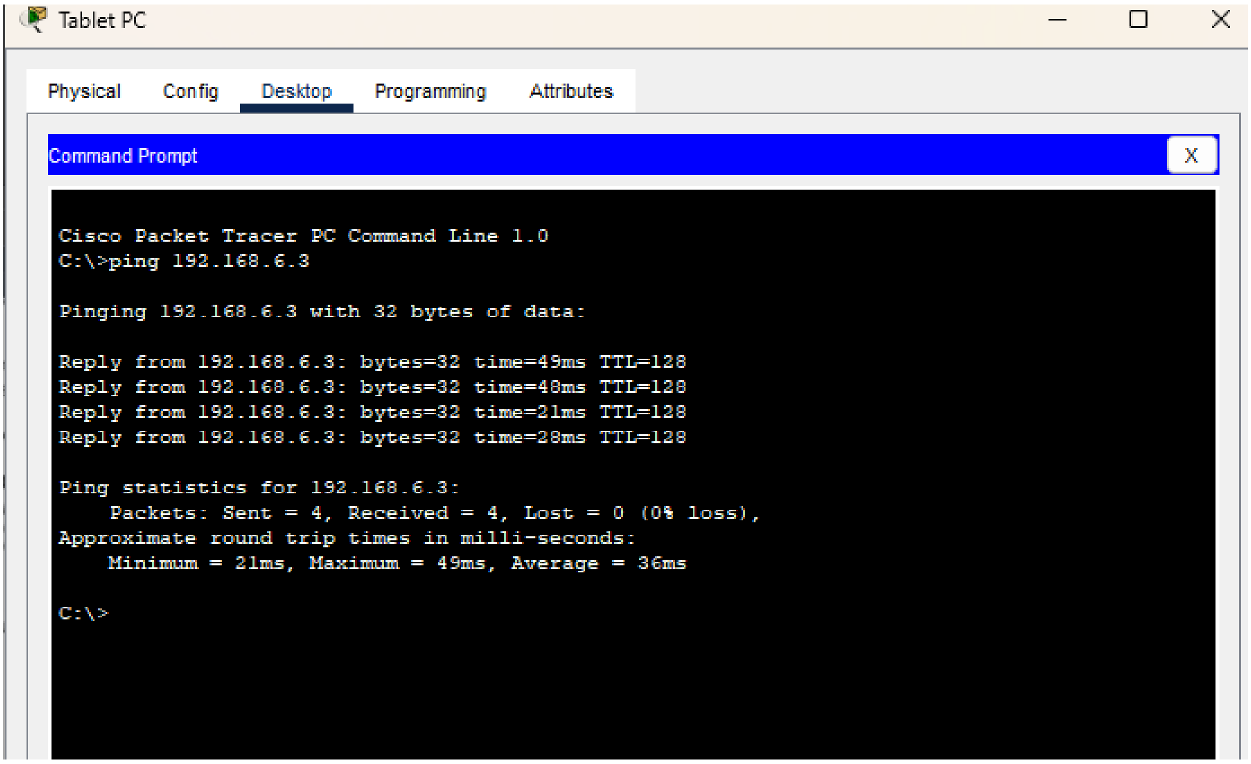
User Name

Password

Encryption Type AES



3. **Verification of Connectivity**:
   - Verified that all connected devices could ping each other and the web server.
   - Confirmed that the devices could access the web server URL successfully.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.3

Pinging 192.168.6.3 with 32 bytes of data:

Reply from 192.168.6.3: bytes=32 time=49ms TTL=128
Reply from 192.168.6.3: bytes=32 time=48ms TTL=128
Reply from 192.168.6.3: bytes=32 time=21ms TTL=128
Reply from 192.168.6.3: bytes=32 time=28ms TTL=128

Ping statistics for 192.168.6.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 49ms, Average = 36ms

C:\>
```

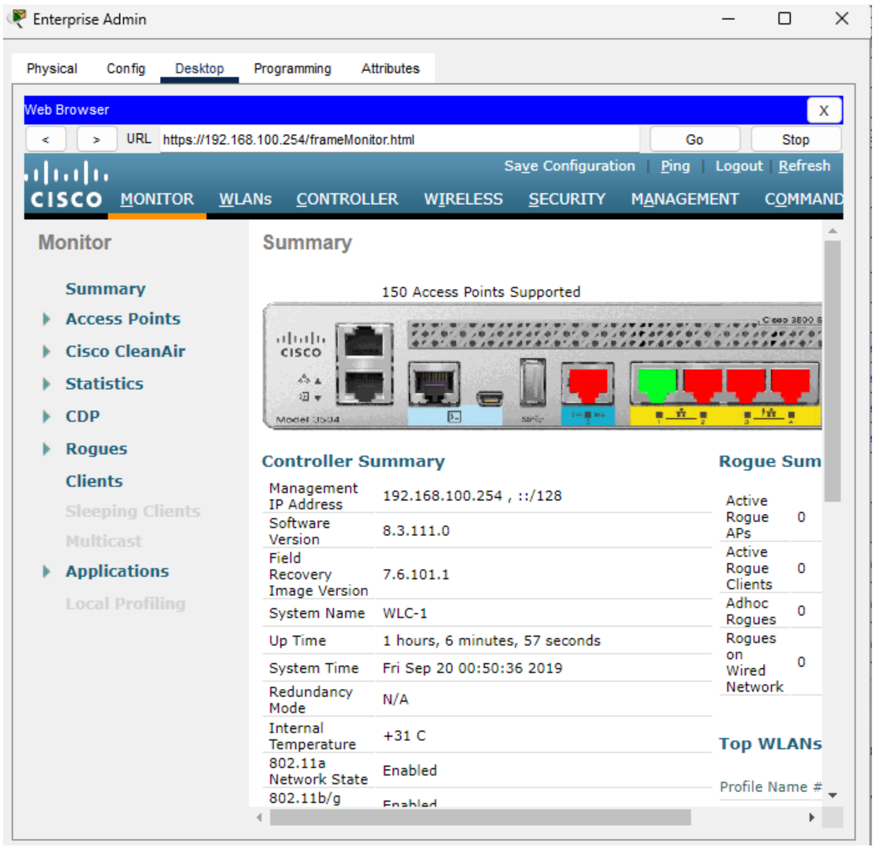
These steps ensured that the home wireless network was securely configured, with all devices successfully connected and verified for proper connectivity.

Part 2: Configure a WLC Controller Network

In this section, we will configure the wireless LAN controller (WLC) with two WLANs using different authentication methods, set up an SNMP server, and configure a DHCP scope for the wireless management network.

Step 1: Configure VLAN Interfaces

1. **Access the WLC-1 Management Interface**:
   - Logged into WLC-1 using admin credentials.



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	1 hours, 6 minutes, 57 seconds
System Time	Fri Sep 20 00:50:36 2019
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g	Enabled

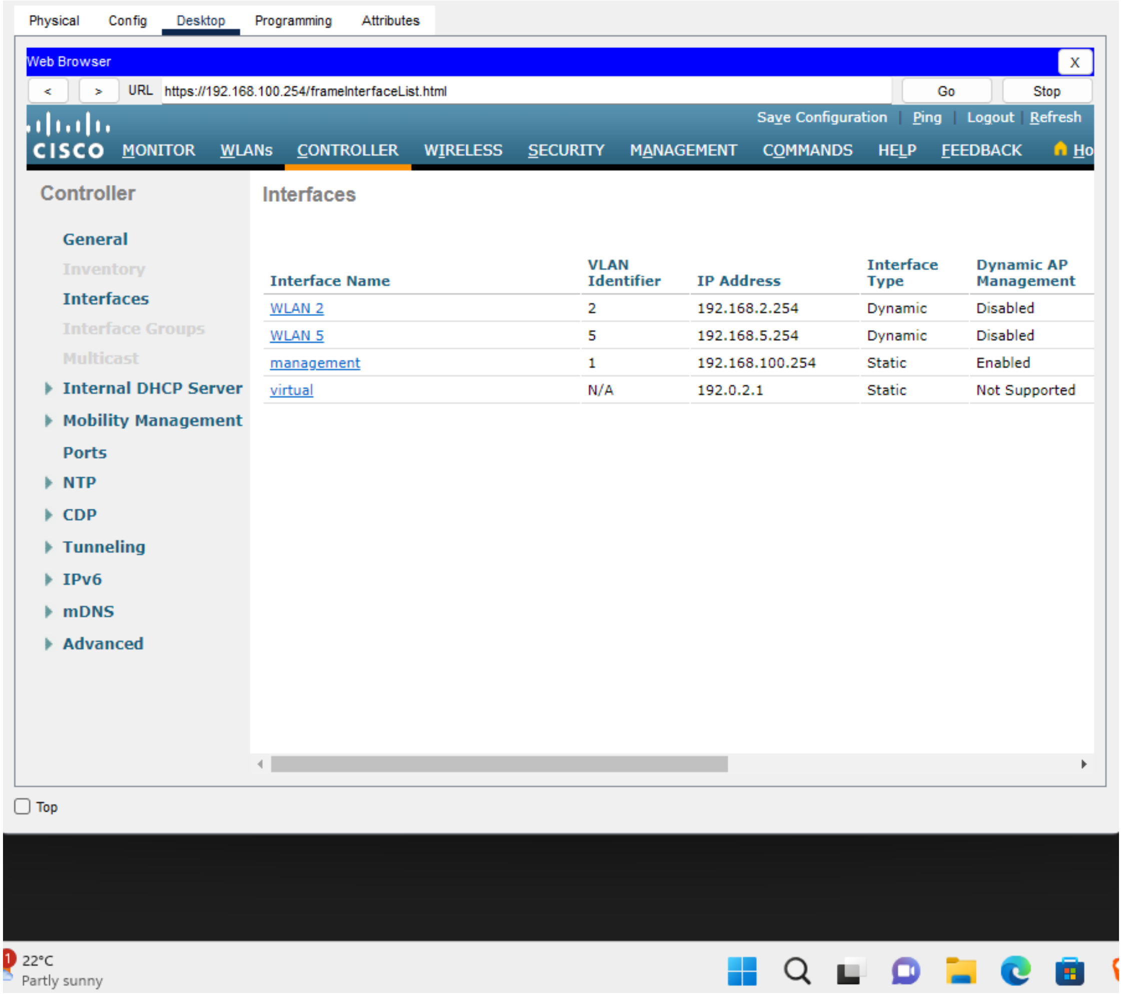
Rogue Sum

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

Top WLANs

Profile Name #

2. **Configured Interface for WLAN 2**:
   - Set up the interface with the specified VLAN ID, IP address, netmask, gateway, and DHCP server.
3. **Configured Interface for WLAN 5**:
   - Set up the interface with the specified VLAN ID, IP address, netmask, gateway, and DHCP server.

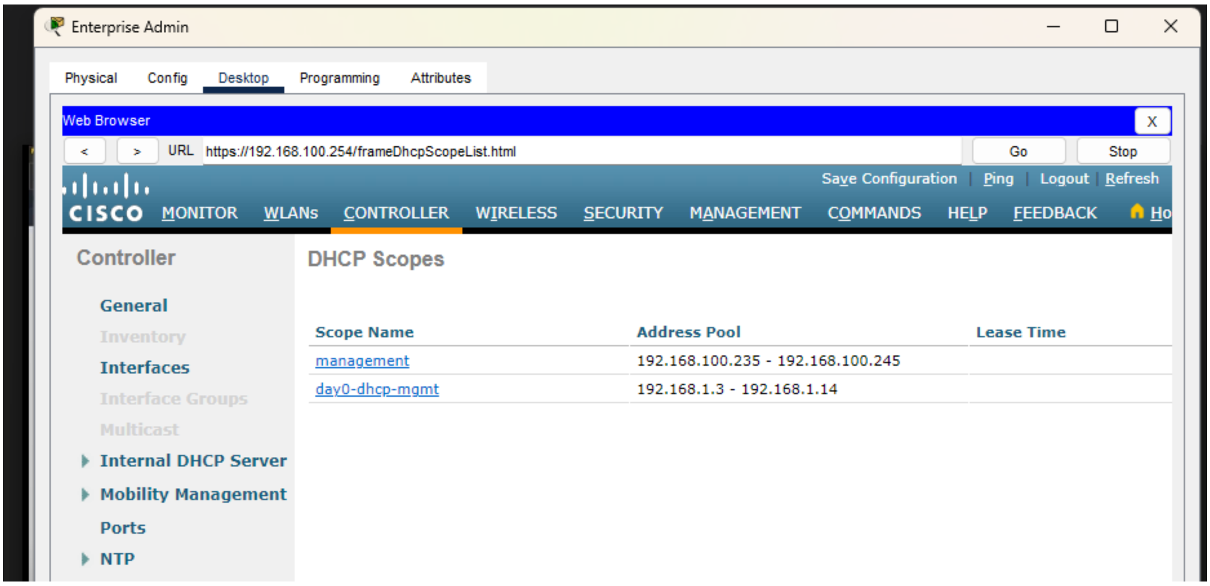


Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
WLAN 2	2	192.168.2.254	Dynamic	Disabled
WLAN 5	5	192.168.5.254	Dynamic	Disabled
management	1	192.168.100.254	Static	Enabled
virtual	N/A	192.0.2.1	Static	Not Supported

Step 2: Configure a DHCP Scope for the Wireless Management Network

1. Configured an internal DHCP scope with the specified pool range, network, netmask, and default router.

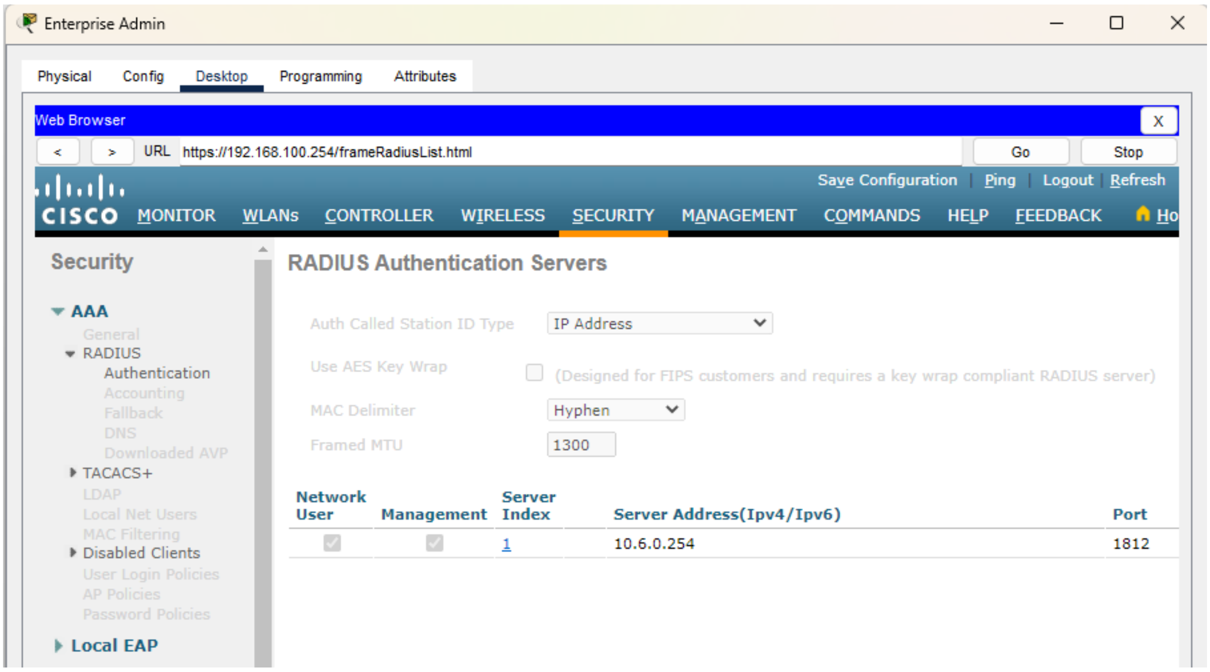


DHCP Scopes

Scope Name	Address Pool	Lease Time
management	192.168.100.235 - 192.168.100.245	
day0-dhcp-mgmt	192.168.1.3 - 192.168.1.14	

Step 3: Configure the WLC with External Server Addresses

1. **RADIUS Server Configuration**:
   - Entered the server index, address, and shared secret.



URL https://192.168.100.254/frameRadiusList.html

RADIUS Authentication Servers

Auth Called Station ID Type: IP Address

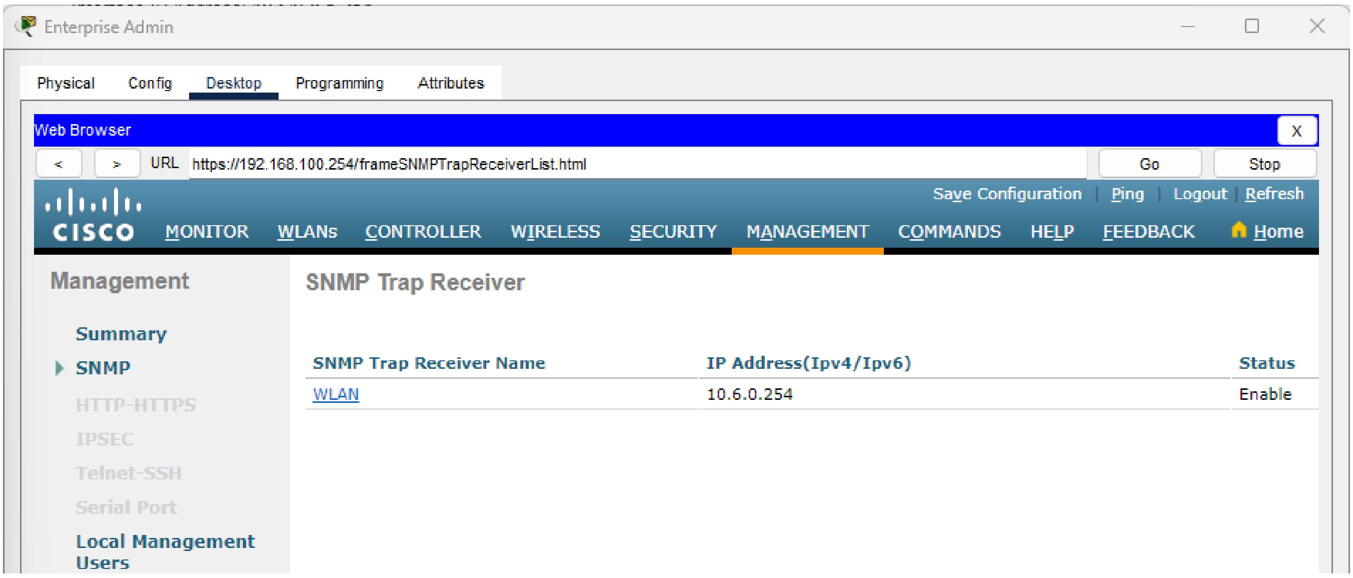
Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Framed MTU: 1300

Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port
☑	☑	1	10.6.0.254	1812

2. **SNMP Server Configuration**:
   - Entered the community name and IP address



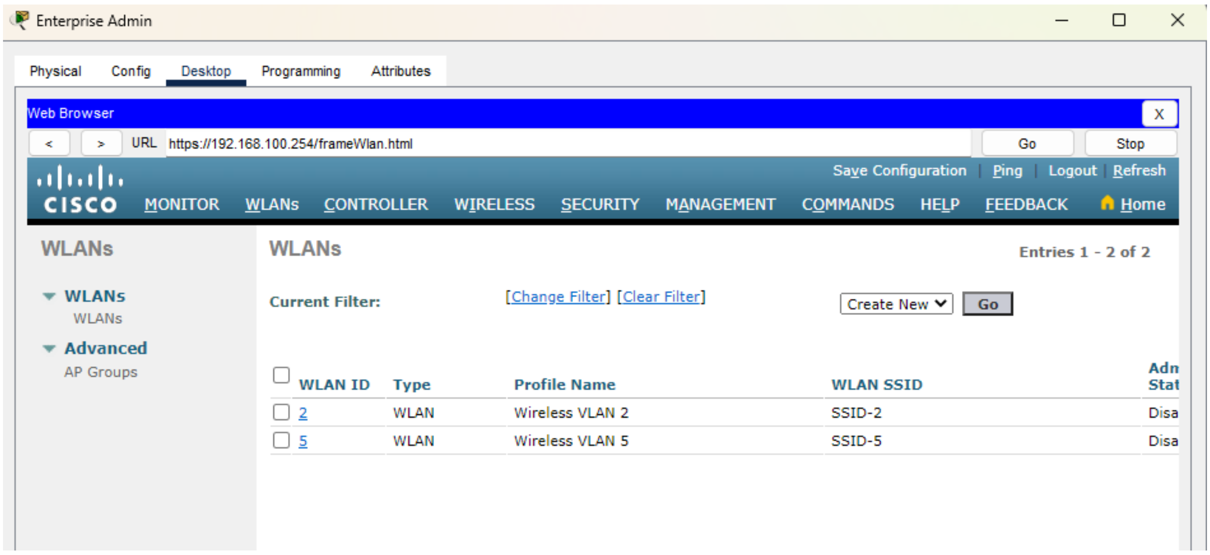
URL https://192.168.100.254/frameSNMPTrapReceiverList.html

SNMP Trap Receiver

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

Step 4: Create the WLANs

1. **Created First WLAN**:
   - Set up the WLAN with WPA2-PSK security and enabled FlexConnect settings.
2. **Created Second WLAN**:
   - Set up the WLAN with WPA2-Enterprise security and RADIUS server authentication. Enabled FlexConnect settings.



WLANs

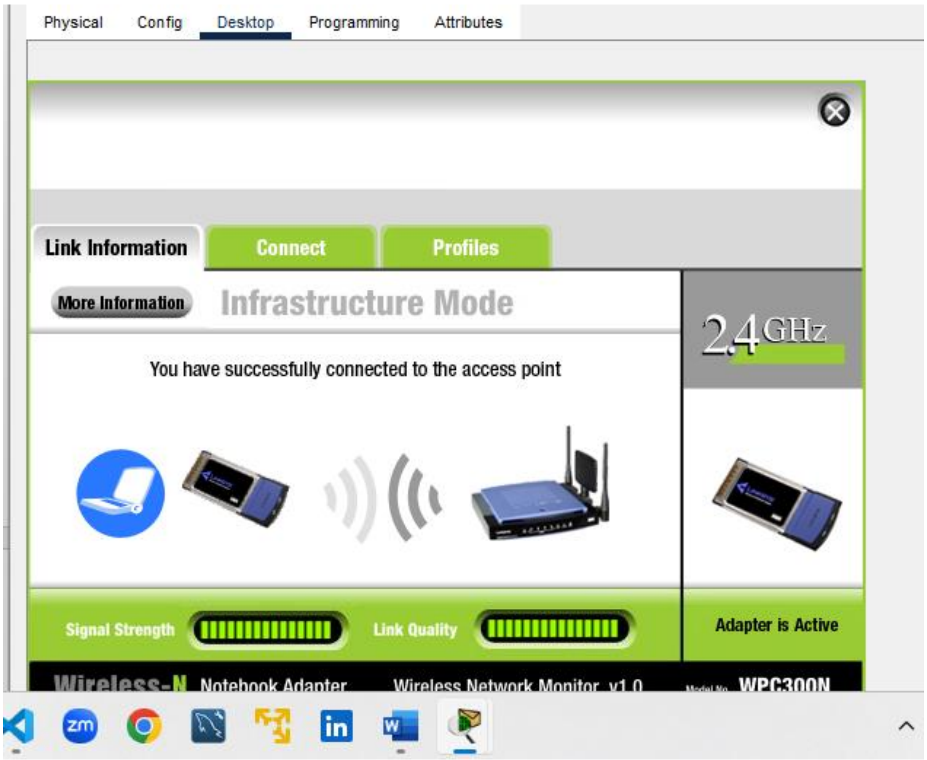
Entries 1 - 2 of 2

Current Filter: [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Adn Stat
□ 2	WLAN	Wireless VLAN 2	SSID-2	Disa
□ 5	WLAN	Wireless VLAN 5	SSID-5	Disa

Step 5: Configure the Hosts to Connect to the WLANs

1. Configured Wireless Host 1 to connect to Wireless VLAN 2.

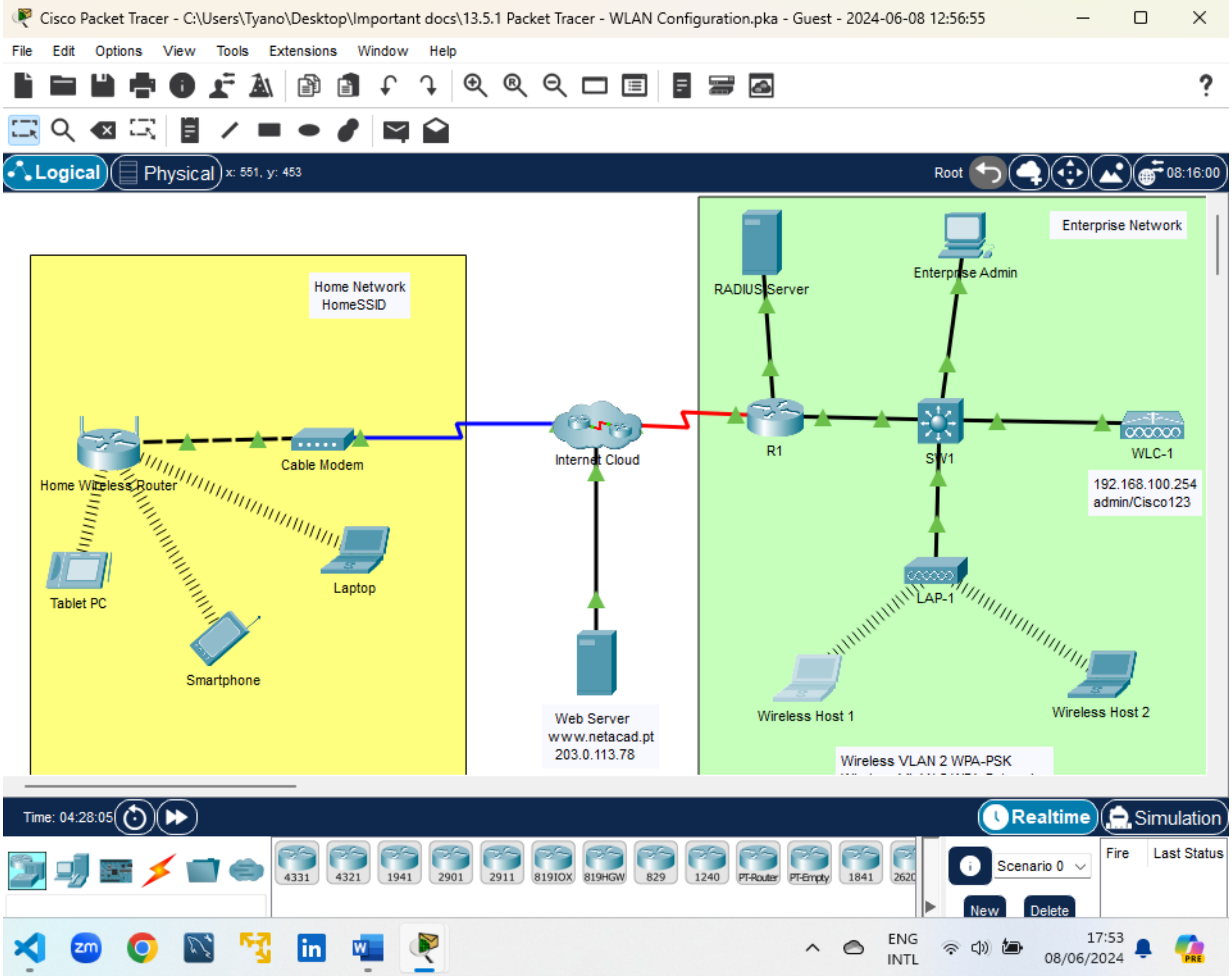


Infrastructure Mode

You have successfully connected to the access point

Adapter is Active

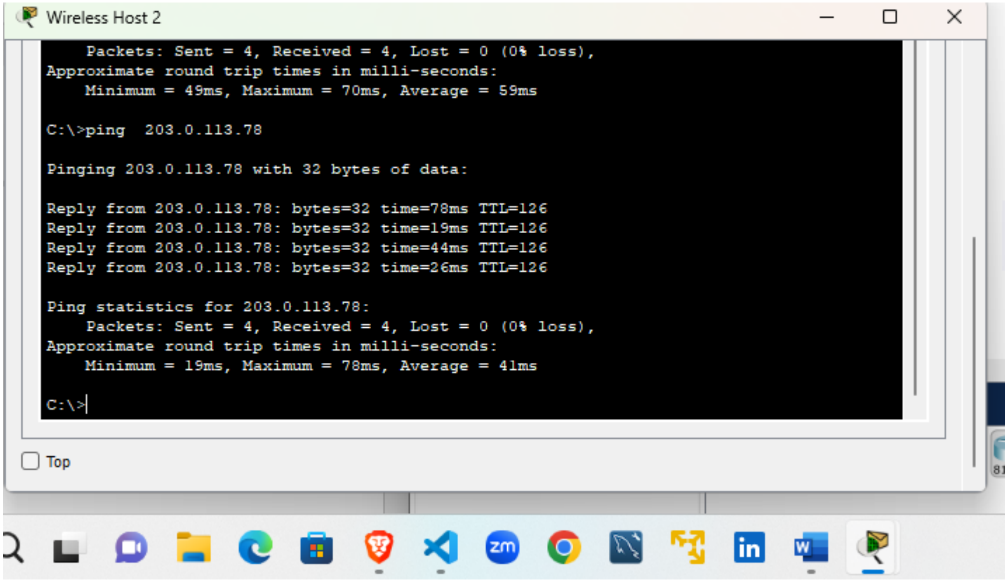
2. Configured Wireless Host 2 to connect to Wireless VLAN 5 using RADIUS server credentials.



step 6: Test connectivity.

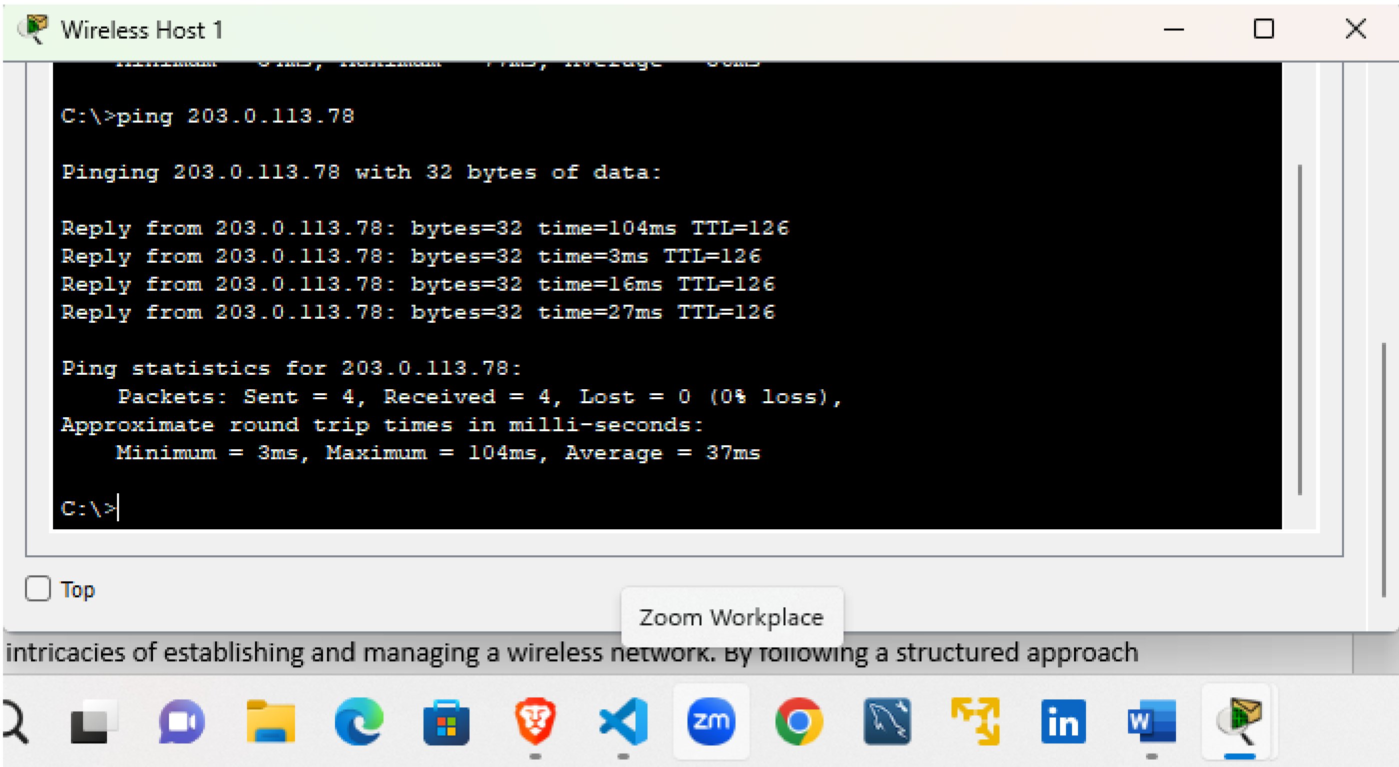
Testing connectivity between the wireless hosts and the Web Server by ping and URL.

Pinged web server from Wireless Host 2 successfully.



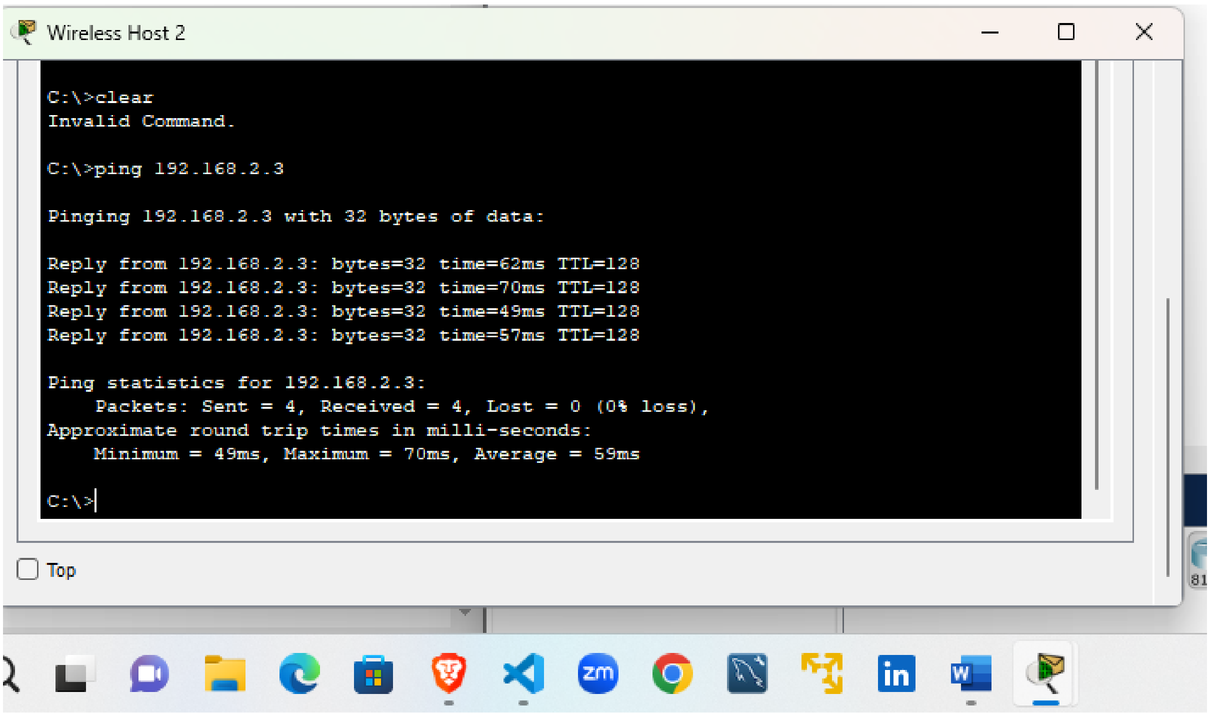
```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 49ms, Maximum = 70ms, Average = 59ms

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=78ms TTL=126
Reply from 203.0.113.78: bytes=32 time=19ms TTL=126
Reply from 203.0.113.78: bytes=32 time=44ms TTL=126
Reply from 203.0.113.78: bytes=32 time=26ms 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 = 19ms, Maximum = 78ms, Average = 41ms

C:\>
```

Pinging Web Server from Wireless Host 1 Successfully


Wireless Host 1
□ Top
Zoom Workplace
intricacies of establishing and managing a wireless network. By following a structured approach

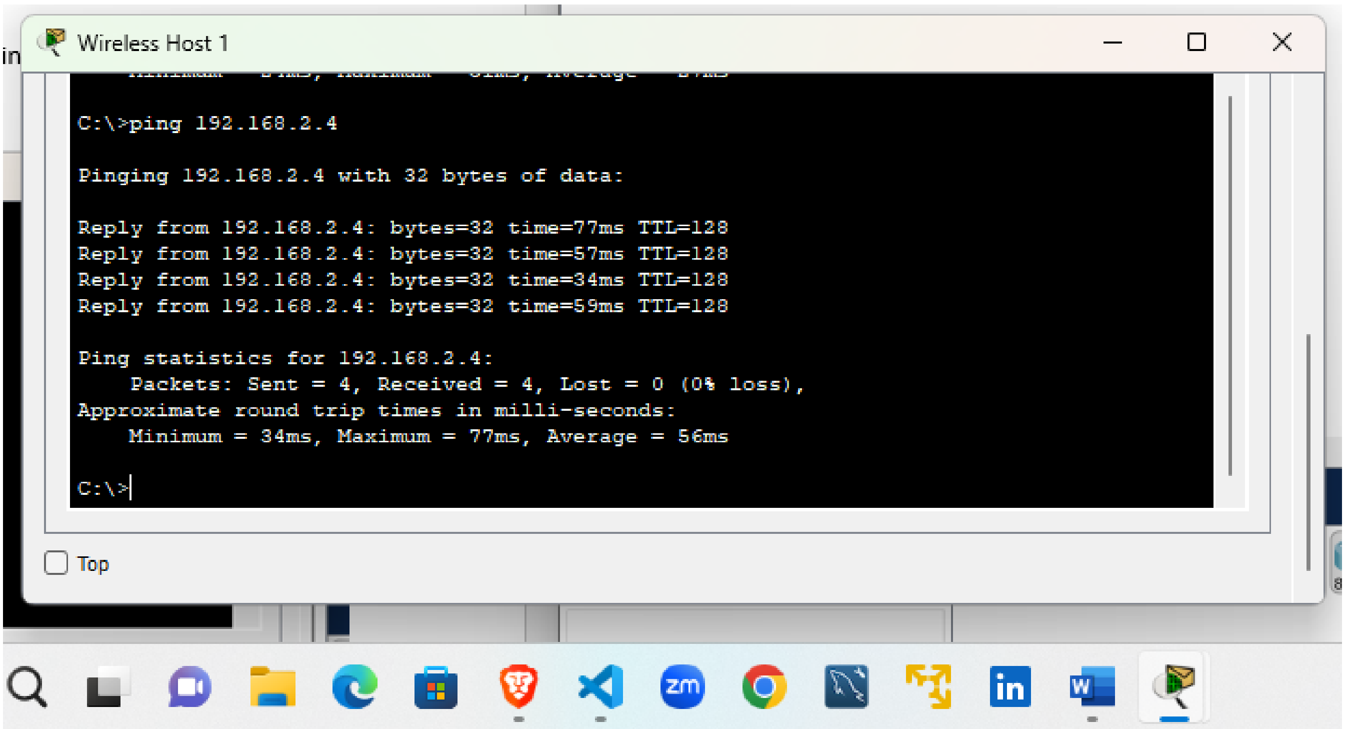
```
C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=104ms TTL=126
Reply from 203.0.113.78: bytes=32 time=3ms TTL=126
Reply from 203.0.113.78: bytes=32 time=16ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 104ms, Average = 37ms

C:\>
```

Pinging Wireless Host 1 from Wireless Host 2 Successfully.



```
C:\>clear
Invalid Command.

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=62ms TTL=128
Reply from 192.168.2.3: bytes=32 time=70ms TTL=128
Reply from 192.168.2.3: bytes=32 time=49ms TTL=128
Reply from 192.168.2.3: bytes=32 time=57ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 49ms, Maximum = 70ms, Average = 59ms

C:\>
```

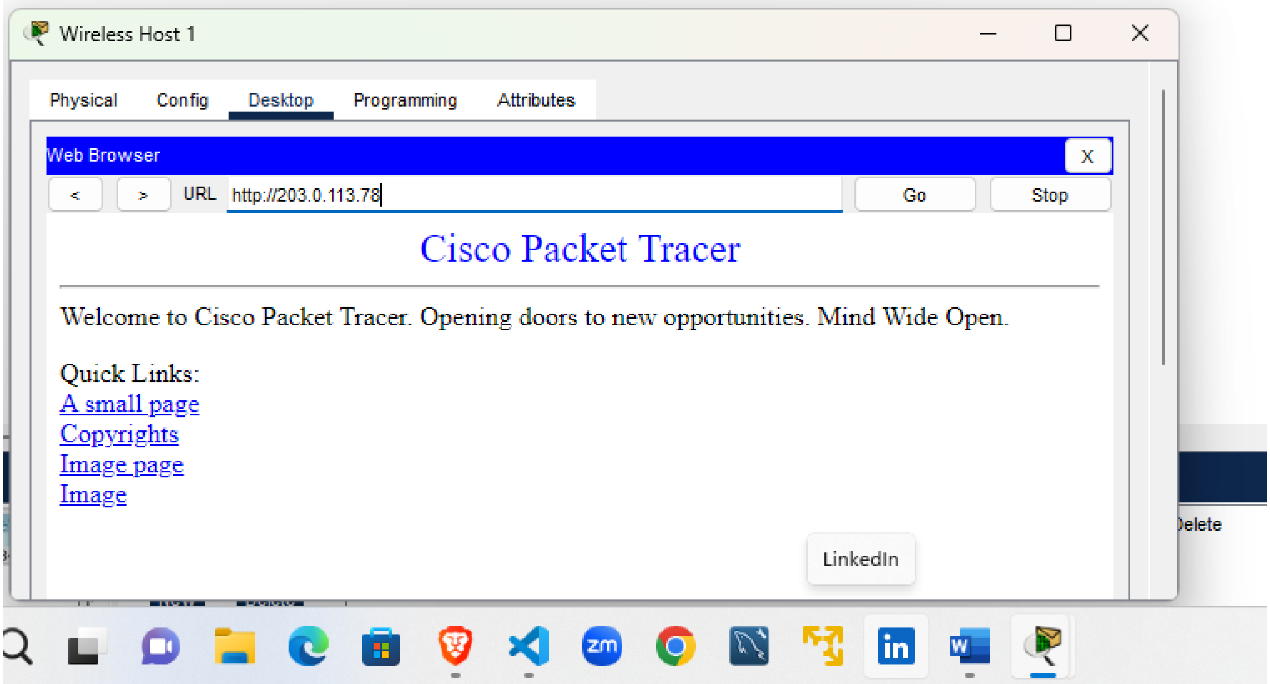
Pinging Wireless Host 2 from Wireless Host 1 Successfully.



```
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=77ms TTL=128
Reply from 192.168.2.4: bytes=32 time=57ms TTL=128
Reply from 192.168.2.4: bytes=32 time=34ms TTL=128
Reply from 192.168.2.4: bytes=32 time=59ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 77ms, Average = 56ms

C:\>
```

Testing connectivity to the Web Server using URL from both Wireless Host 1 and Wireless Host 2

a) Wireless Host 1



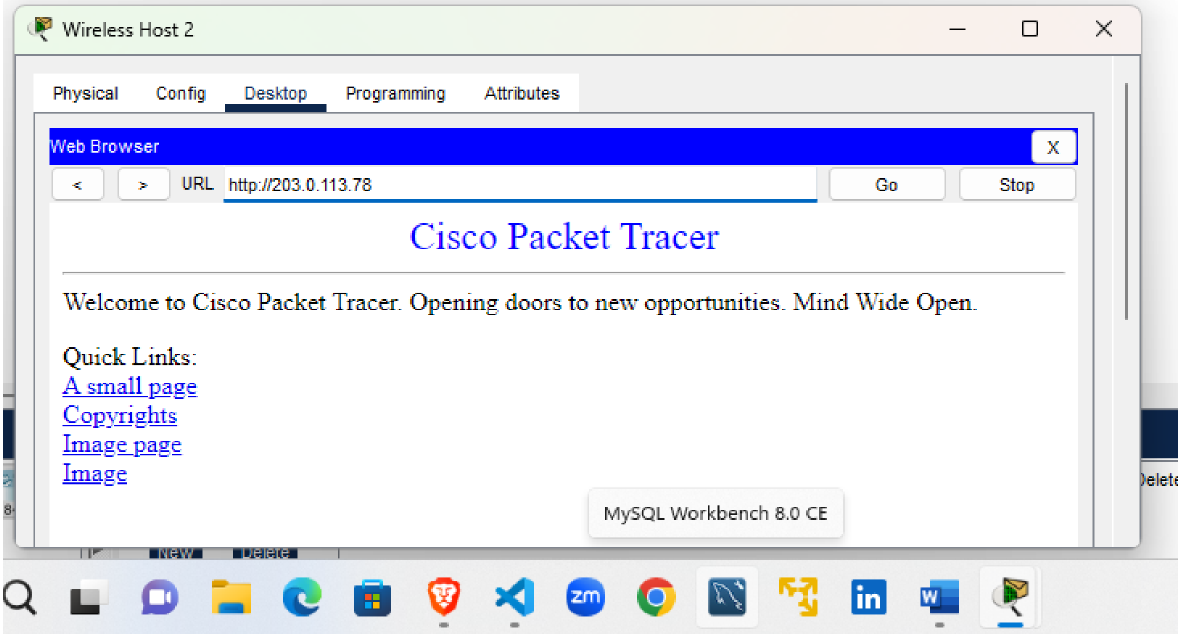
URL http://203.0.113.78

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

b) Wireless Host 2



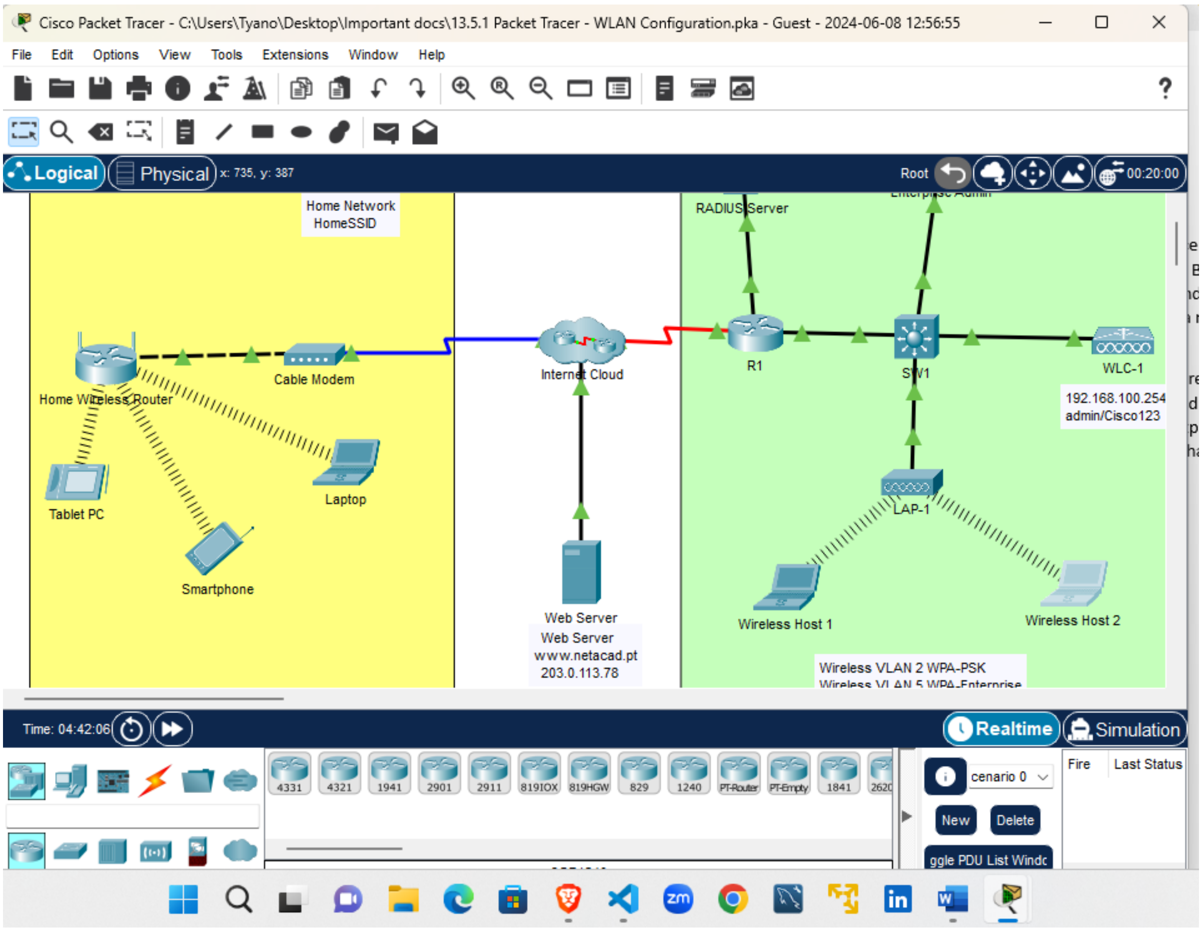
http://203.0.113.78

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

Overall view of the configuration with all the connections.



Conclusion

n conclusion, the WLAN configuration exercise using Packet Tracer has provided valuable insights into the intricacies of establishing and managing a wireless network. By following a structured approach to configuring SSIDs, implementing robust security measures, and conducting thorough connectivity tests, we have illustrated the essential steps required to create a reliable and secure WLAN environment.

This assignment has not only reinforced my understanding of wireless networking principles but also emphasized the practical skills necessary for effective network administration. As wireless technology continues to evolve and expand its reach, the knowledge and experience gained through this exercise will be indispensable in addressing future networking challenges and ensuring seamless connectivity in various contexts.