Cloud and Network Security-C1-2026

STUDENT NAME: FELIX WEBBO

STUDENT NO: CS-CNS11-26044

MONDAY, FEB 16, 2026

Week 4: Assignment 2

Class Exercise: **Packet Tracer WLAN configuration**

1 ABSTRACT

This report described the configuration of both a home wireless router and an enterprise Wireless LAN Controller (WLC) network in Packet Tracer. The activity implemented WLAN connectivity using WPA2-Personal and WPA2-Enterprise security models. A home router was configured to provide secure wireless access for multiple devices through DHCP and WPA2-PSK authentication. In the enterprise network, the WLC was configured with VLAN interfaces, internal DHCP scope, external RADIUS authentication, and two WLANs mapped to separate VLANs. Wireless hosts were successfully connected to the appropriate SSIDs, and end-to-end connectivity was verified through ping and web access tests.

Table of Contents

2 INTRODUCTION

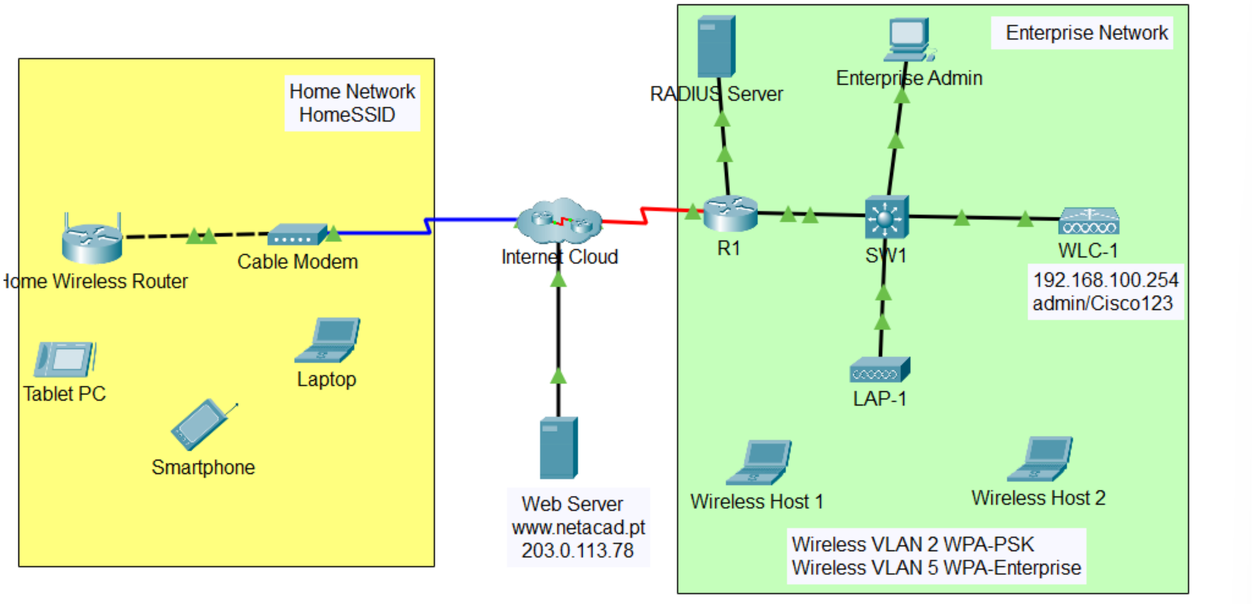
Wireless LANs were essential in modern networking due to their flexibility and support for mobile connectivity. However, wireless networks required strong security mechanisms such as WPA2 encryption and enterprise authentication through RADIUS servers. This activity focused on configuring a home WLAN using WPA2-Personal and an enterprise WLAN environment using a WLC with WPA2-Enterprise authentication.

3 OBJECTIVES

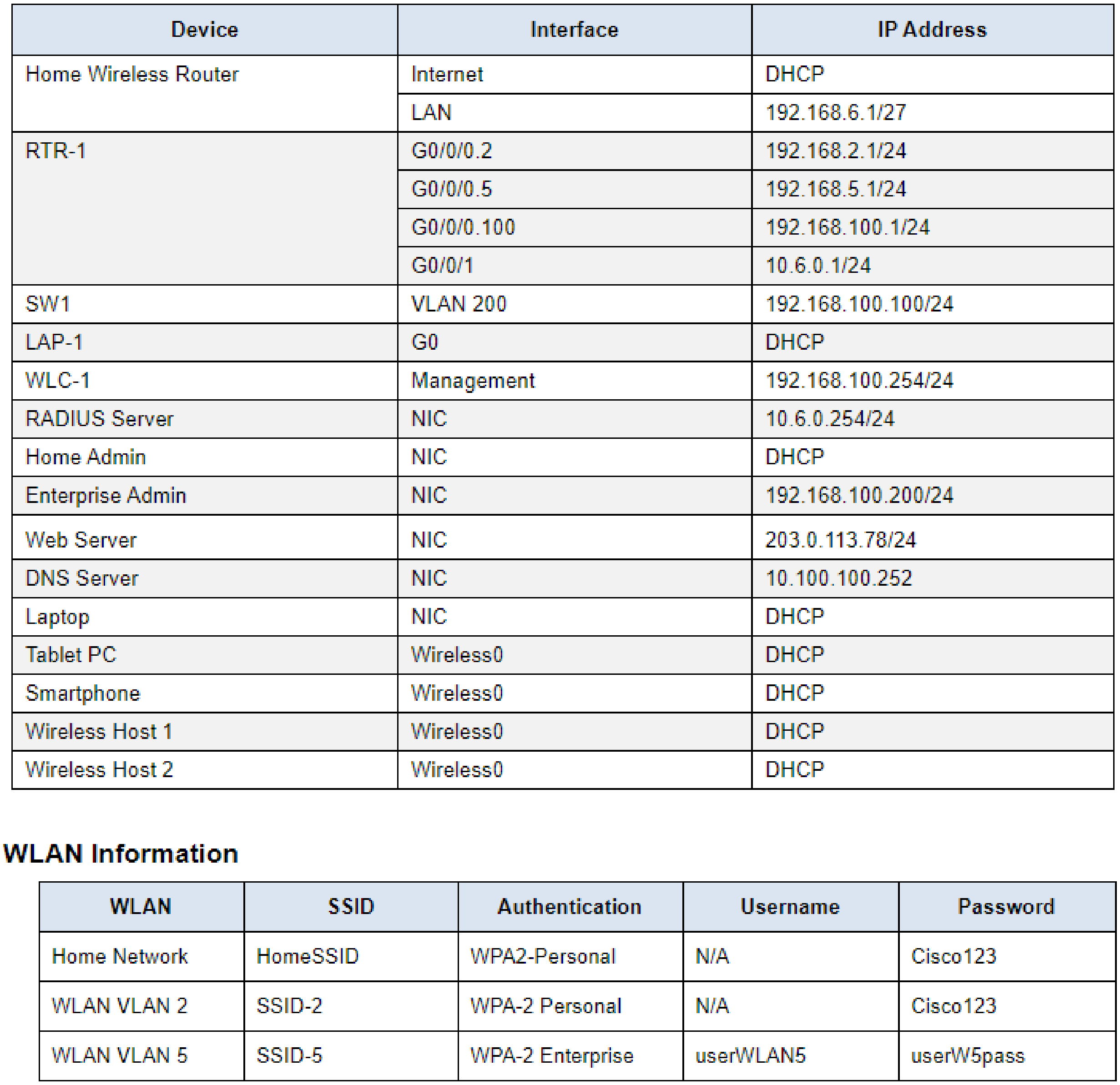
The objectives of this activity were:

- To configure a home wireless router to provide Wi-Fi connectivity to multiple devices.
- To implement WPA2-PSK security on a home WLAN.
- To configure VLAN interfaces on a Wireless LAN Controller.
- To create and configure WLANs on the WLC.
- To implement WPA2-PSK security on one enterprise WLAN and connect hosts to it.
- To implement WPA2-Enterprise authentication using a RADIUS server on a second WLAN.
- To verify end-to-end WLAN connectivity through ping and web access testing.

4 NETWORK TOPOLOGY



4.1 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

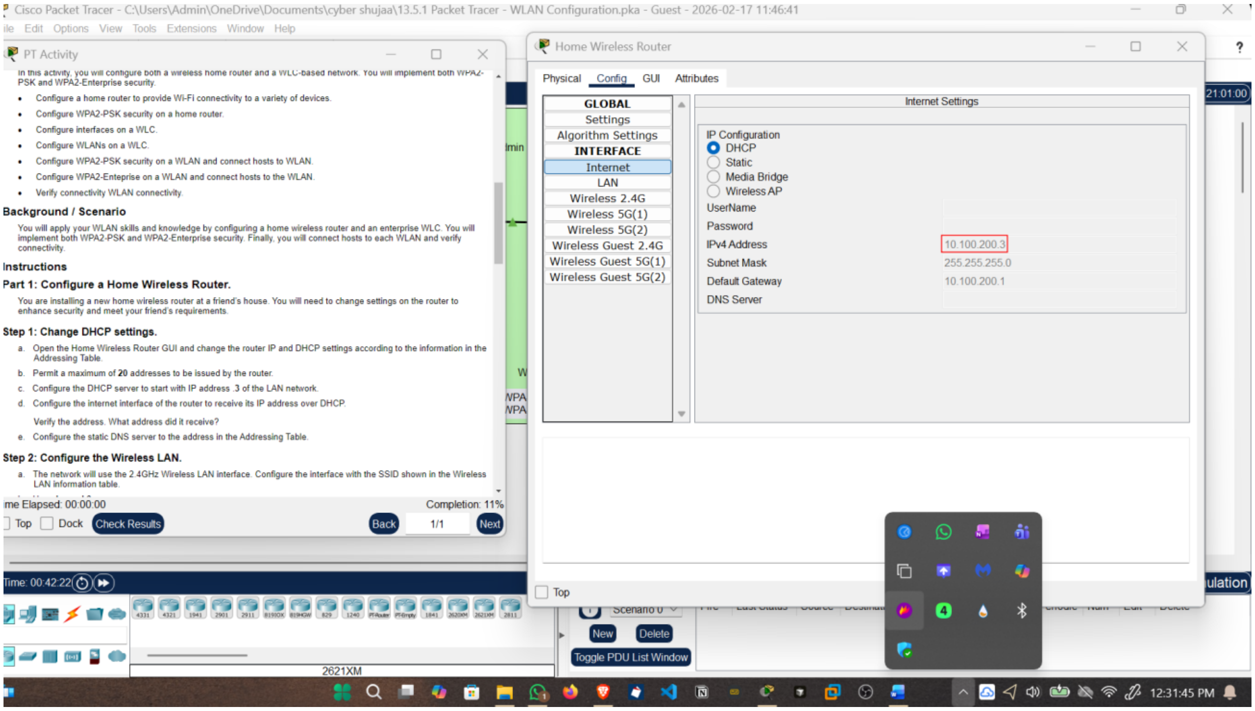
WLAN	SSID	Authentication	Username	Password
Home Network	HomeSSID	WPA2-Personal	N/A	Cisco123
WLAN VLAN 2	SSID-2	WPA-2 Personal	N/A	Cisco123
WLAN VLAN 5	SSID-5	WPA-2 Enterprise	userWLAN5	userW5pass

5 METHODOLOGY

5.1 Part 1: Configure a Home Wireless Router.

5.1.1 Step 1: Change DHCP settings.

1. Open the Home Wireless Router GUI and change the router IP and DHCP settings according to the information in the Addressing Table.
2. Permit a maximum of **20** addresses to be issued by the router.
3. Configure the DHCP server to start with IP address .**3** of the LAN network.
4. Configure the internet interface of the router to receive its IP address over DHCP.
5. Question:
6. Verify the address. What address did it receive?



In this activity, you will configure both a wireless home router and a WLC-based network. You 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.

Background / Scenario

You will apply your WLAN skills and knowledge by configuring a home wireless router and an enterprise WLC. You will implement both WPA2-PSK and WPA2-Enterprise security. Finally, you will connect hosts to each WLAN and verify connectivity.

Instructions

Part 1: Configure a Home Wireless Router.

You are installing a new home wireless router at a friend's house. You will need to change settings on the router to enhance security and meet your 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.

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.

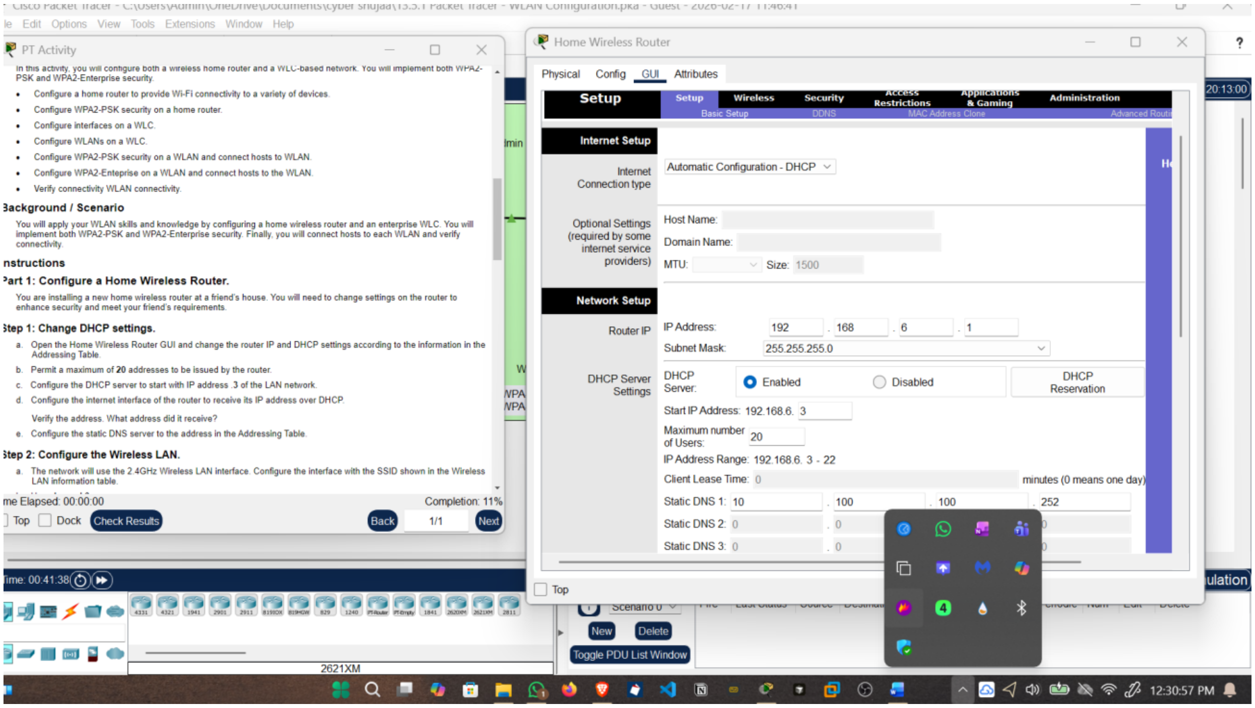
a. The network will use the 2.4GHz Wireless LAN interface. Configure the interface with the SSID shown in the Wireless LAN information table.

Internet Settings

IP Configuration
● DHCP
○ Static
○ Media Bridge
○ Wireless AP

UserName	
Password	
IPv4 Address	10.100.200.3
Subnet Mask	255.255.255.0
Default Gateway	10.100.200.1
DNS Server	

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



PT Activity

In this activity, you will configure both a wireless home router and a WLC-based network. You 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.

Background / Scenario

You will apply your WLAN skills and knowledge by configuring a home wireless router and an enterprise WLC. You will implement both WPA2-PSK and WPA2-Enterprise security. Finally, you will connect hosts to each WLAN and verify connectivity.

Instructions

Part 1: Configure a Home Wireless Router.

You are installing a new home wireless router at a friend's house. You will need to change settings on the router to enhance security and meet your 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.

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 the Wireless LAN information table.

Time Elapsed: 00:00:00 Completion: 11%

Home Wireless Router

Internet Setup
Internet Connection type: Automatic Configuration - DHCP

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

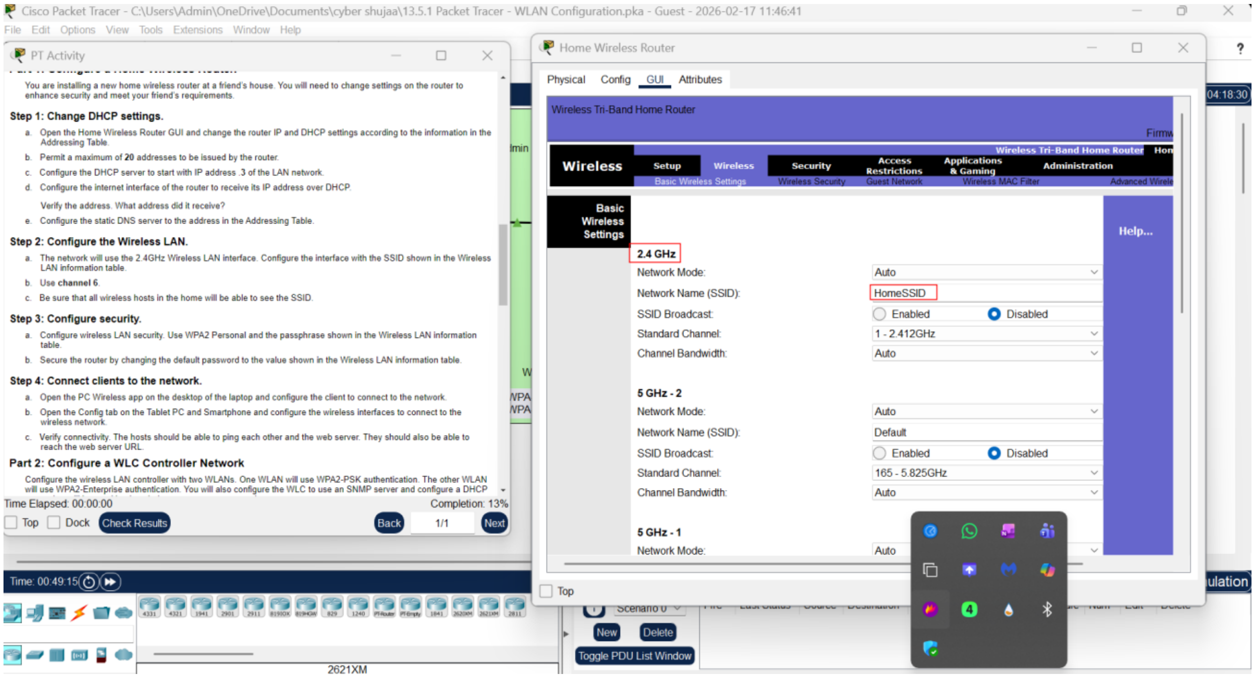
Network Setup
Router IP
IP Address: 192 . 168 . 6 . 1
Subnet Mask: 255.255.255.0

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

Cisco Packet Tracer - C:\Users\Admin\OneDrive\Documents\cyber shujaa\13.5.1 Packet Tracer - WLAN Configuration.pka - Guest - 2026-02-17 11:46:41
File Edit Options View Tools Extensions Window Help
Top Dock Check Results Back 1/1 Next
Time: 00:41:38
Physical Config GUI Attributes
Setup Wireless Security Access Restrictions Applications & Gaming Administration
Basic Setup DDNS MAC Address Clone Advanced Routing
DHCP Reservation
Top
Scenario 0 New Delete Toggle PDU List Window
2621XM
12:30:57 PM

5.1.2 Step 2: Configure the Wireless LAN.

1. The network will use the 2.4GHz Wireless LAN interface. Configure the interface with the SSID shown in the Wireless LAN information table.
2. Use **channel 6**.
3. Be sure that all wireless hosts in the home will be able to see the SSID.



PT Activity

You are installing a new home wireless router at a friend's house. You will need to change settings on the router to enhance security and meet your 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.

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 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.

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.

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 server and configure a DHCP

Time Elapsed: 00:00:00 Completion: 13%

Home Wireless Router

Wireless Tri-Band Home Router

Basic Wireless Settings

2.4 GHz
Network Mode: Auto
Network Name (SSID): HomeSSID
SSID Broadcast: ○ Enabled ● Disabled
Standard Channel: 1 - 2.412GHz
Channel Bandwidth: Auto

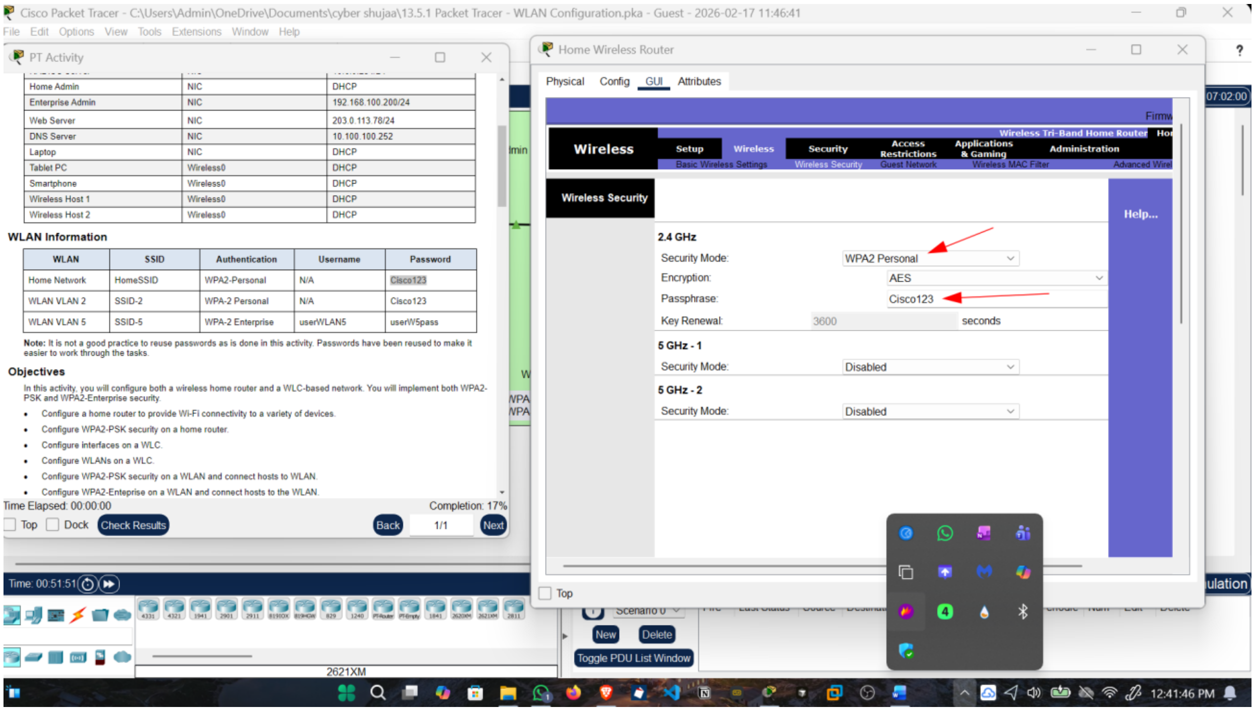
5 GHz - 2
Network Mode: Auto
Network Name (SSID): Default
SSID Broadcast: ○ Enabled ● Disabled
Standard Channel: 165 - 5.825GHz
Channel Bandwidth: Auto

5 GHz - 1
Network Mode: Auto

Cisco Packet Tracer - C:\Users\Admin\OneDrive\Documents\cyber shujaa\13.5.1 Packet Tracer - WLAN Configuration.pka - Guest - 2026-02-17 11:46:41
File Edit Options View Tools Extensions Window Help
Top Dock Check Results Back 1/1 Next
Time: 00:49:15
Physical Config GUI Attributes
Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration
Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter Advanced Wireless
Help...
Top
Scenario 0 New Delete Toggle PDU List Window
2621XM

5.1.3 Step 3: Configure security.

1. Configure wireless LAN security. Use WPA2 Personal and the passphrase shown in the Wireless LAN information table.
2. Secure the router by changing the default password to the value shown in the Wireless LAN information table.



Cisco Packet Tracer - C:\Users\Admin\OneDrive\Documents\cyber shujaa\13.5.1 Packet Tracer - WLAN Configuration.pka - Guest - 2026-02-17 11:46:41

PT Activity

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

Note: It is not a good practice to reuse passwords as is done in this activity. Passwords have been reused to make it easier to work through the tasks.

Objectives

In this activity, you will configure both a wireless home router and a WLC-based network. You 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.

Time Elapsed: 00:00:00 Completion: 17%

Home Wireless Router

Wireless Security

2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Cisco123

Key Renewal: 3600 seconds

5 GHz - 1

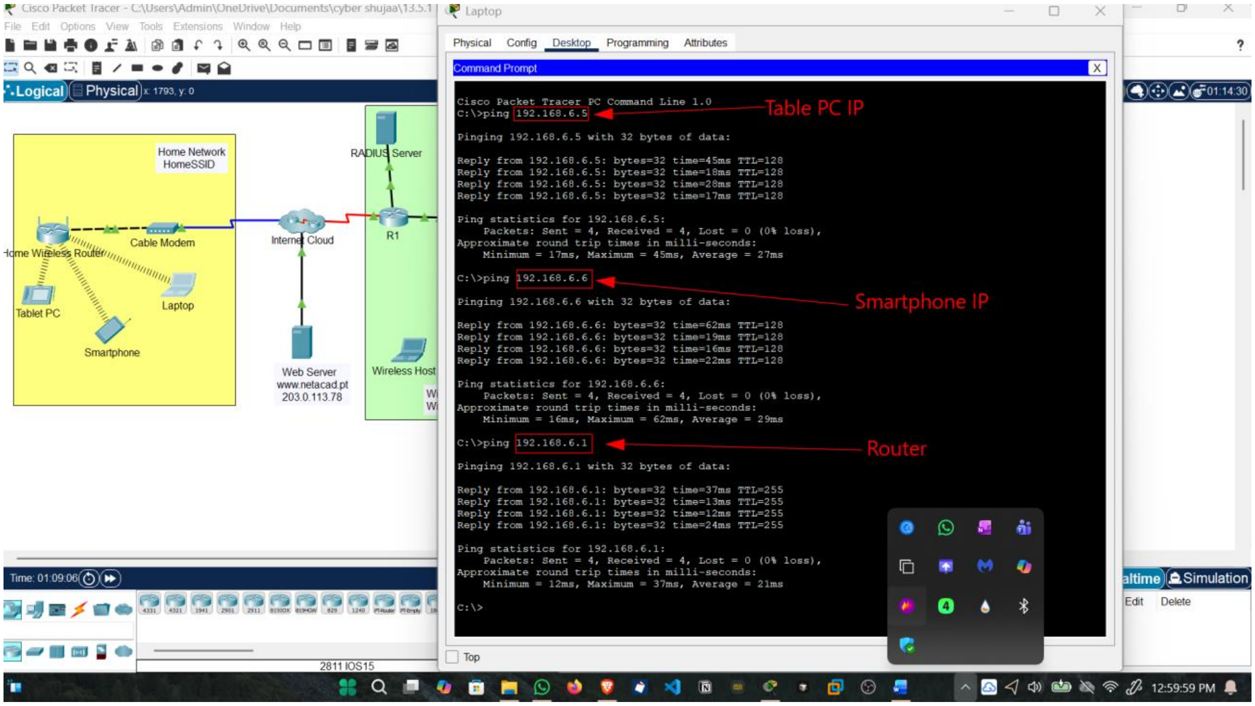
Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

5.1.4 Step 4: Connect clients to the network.

1. Open the PC Wireless app on the desktop of the laptop and configure the client to connect to the network.
2. Open the Config tab on the Tablet PC and Smartphone and configure the wireless interfaces to connect to the wireless network.
3. 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 192.168.6.5

Pinging 192.168.6.5 with 32 bytes of data:

Reply from 192.168.6.5: bytes=32 time=45ms TTL=128
Reply from 192.168.6.5: bytes=32 time=18ms TTL=128
Reply from 192.168.6.5: bytes=32 time=28ms TTL=128
Reply from 192.168.6.5: bytes=32 time=17ms 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 = 17ms, Maximum = 45ms, Average = 27ms

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=62ms TTL=128
Reply from 192.168.6.6: bytes=32 time=19ms TTL=128
Reply from 192.168.6.6: bytes=32 time=16ms TTL=128
Reply from 192.168.6.6: bytes=32 time=22ms 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 = 16ms, Maximum = 62ms, Average = 29ms

C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:

Reply from 192.168.6.1: bytes=32 time=37ms TTL=255
Reply from 192.168.6.1: bytes=32 time=13ms TTL=255
Reply from 192.168.6.1: bytes=32 time=12ms TTL=255
Reply from 192.168.6.1: bytes=32 time=24ms TTL=255

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 37ms, Average = 21ms

C:\>
```

5.2 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 server and configure a DHCP scope that will be used by the wireless management network.

5.2.1 Step 1: Configure VLAN interfaces.

1. 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.
2. Configure an interface for the first WLAN.

    Name: WLAN 2

    VLAN Identifier: 2

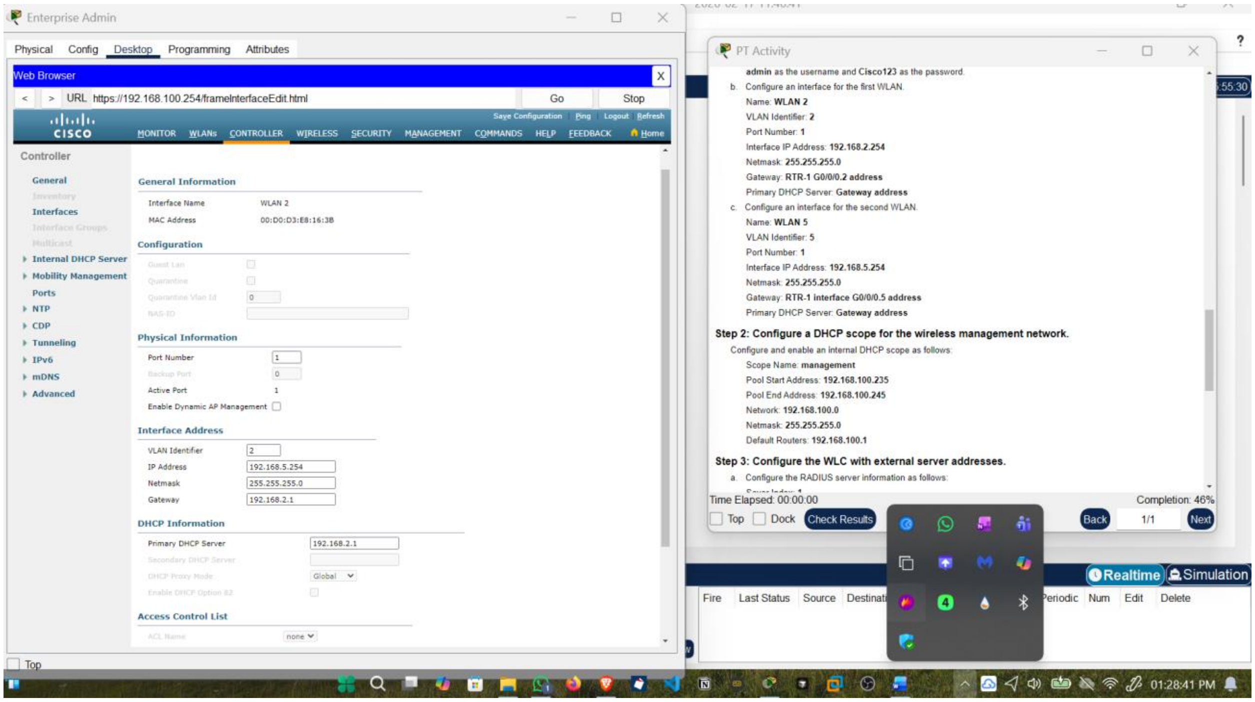
    Port Number: 1

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



General Information

Interface Name WLAN 2

MAC Address 00:D0:D3:E8:16:38

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 192.168.5.254

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

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.

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:

Time Elapsed: 00:00:00 Completion: 46%

□ Top □ Dock Check Results Back 1/1 Next

3. Configure an interface for the second WLAN

   Name: WLAN 5

   VLAN Identifier: 5

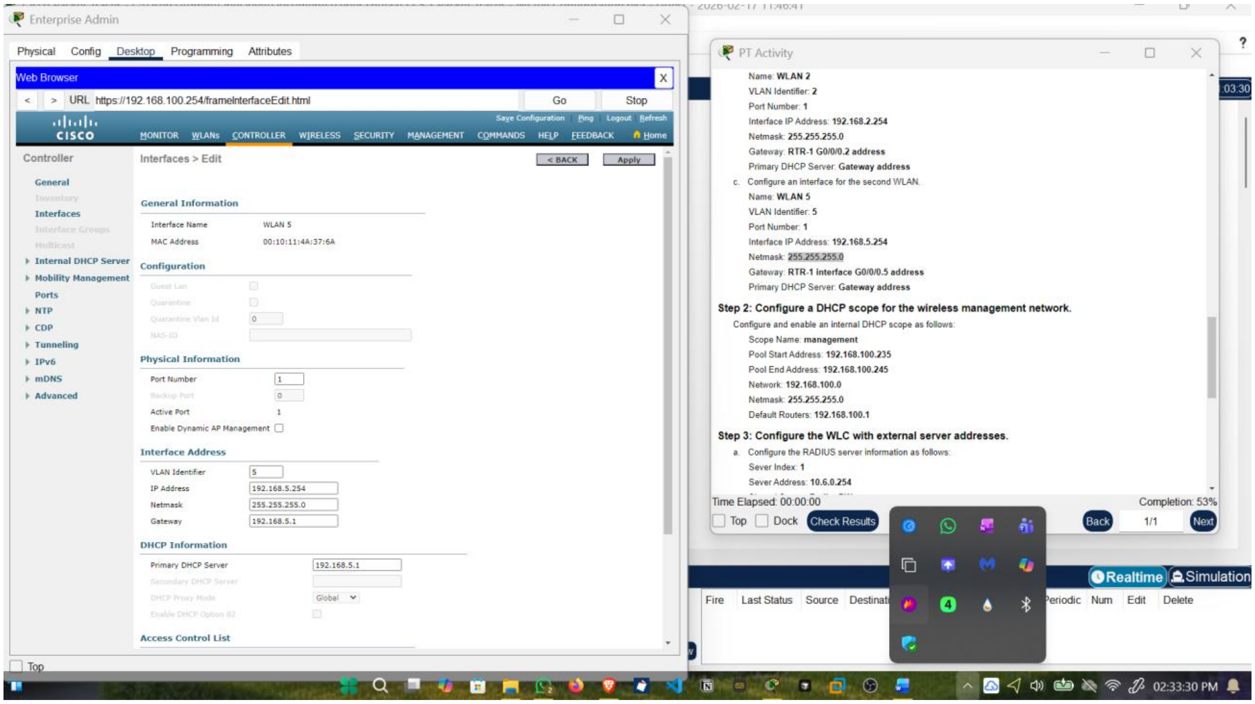
   Port Number: 1

   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



URL https://192.168.100.254/frameInterfaceEdit.html

Interfaces > Edit

General Information

Interface Name WLAN 5

MAC Address 00:10:11:4A:37:6A

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 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 □

Access Control List

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.

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**
Sever Address: **10.6.0.254**

Time Elapsed: 00:00:00

Completion: 53%

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

Configure and enable an internal DHCP scope as follows:

Scope Name: **management**

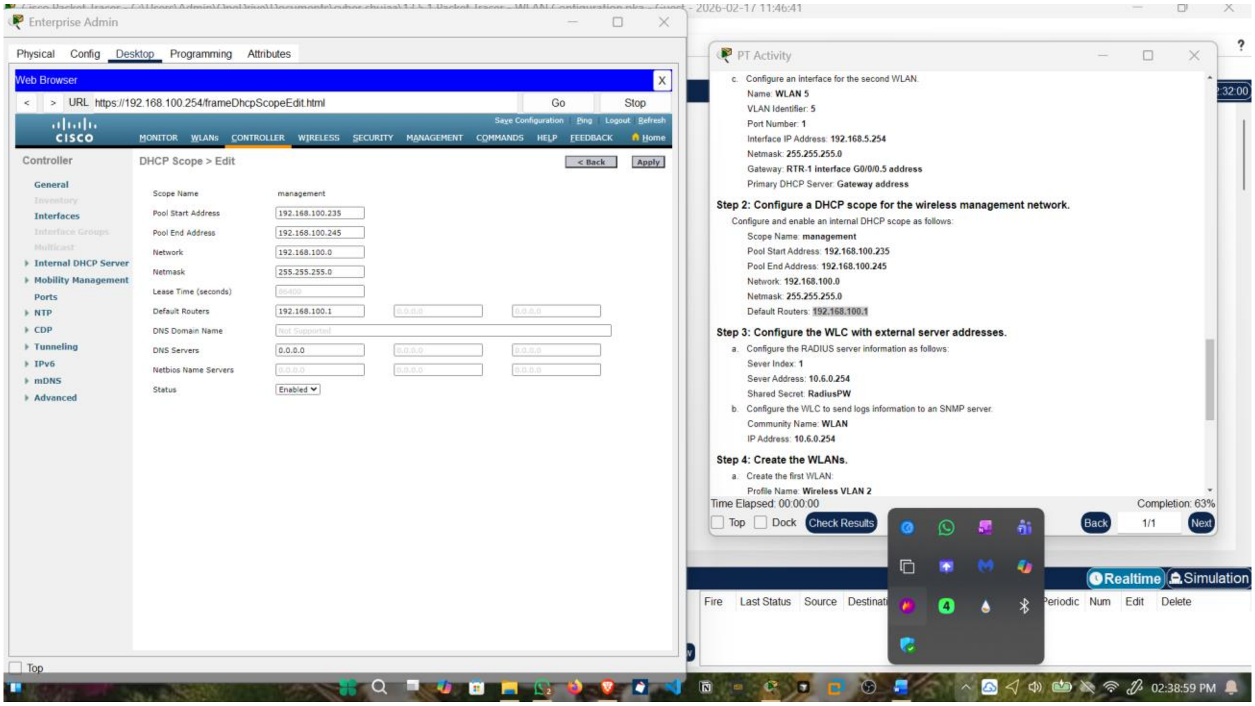
Pool Start Address: **192.168.100.235**

Pool End Address: **192.168.100.245**

Network: **192.168.100.0**

Netmask: **255.255.255.0**

Default Routers: **192.168.100.1**



DHCP Scope > Edit

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		

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.

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**
Sever 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**

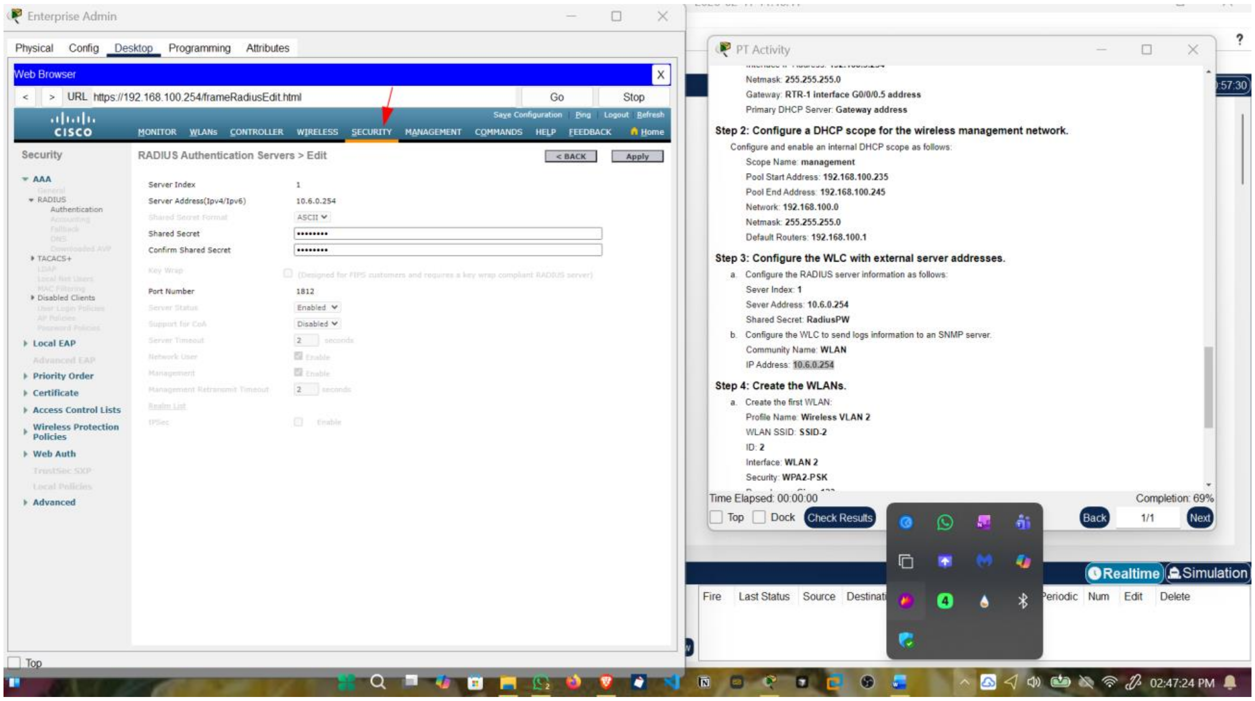
Step 4: Create the WLANs.

a. Create the first WLAN:

Profile Name: **Wireless VLAN 2**

5.2.3 Step 3: Configure the WLC with external server addresses.

1. Configure the RADIUS server information as follows:
   - a. Sever Index: **1**
   - b. Sever Address: **10.6.0.254**
   - c. Shared Secret: **RadiusPW**



URL https://192.168.100.254/frameRadiusEdit.html

RADIUS Authentication Servers > Edit

Server Index 1
Server 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
Management Retransmit Timeout 2 seconds
Realm List
IPSec □ Enable

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.

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**
Sever Address: **10.6.0.254**
Shared Secret: **RadiusPW**

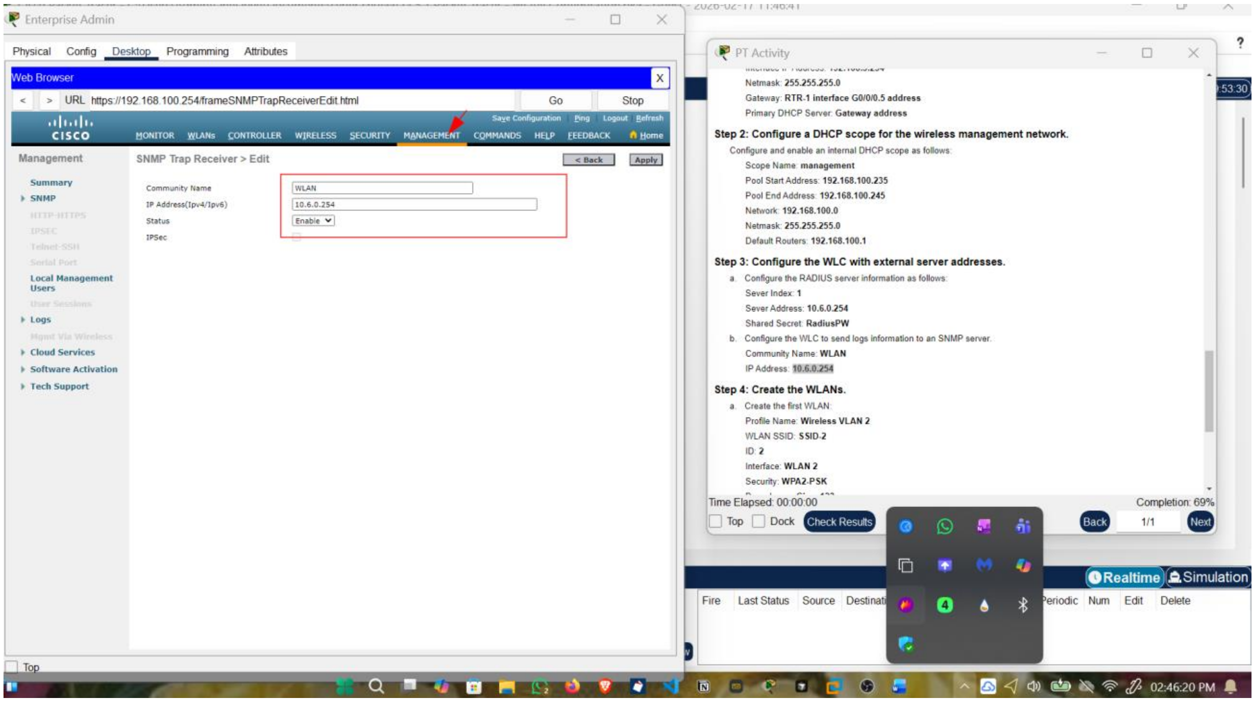
b. Configure the WLC to send logs information to an SNMP server.
Community Name: **WLAN**
IP Address: **10.6.0.254**

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**

Time Elapsed: 00:00:00 Completion: 69%
1/1

2. Configure the WLC to send logs information to an SNMP server.
   a. Community Name: **WLAN**
   b. IP Address: **10.6.0.254**



URL https://192.168.100.254/frameSNMPTrapReceiverEdit.html

SNMP Trap Receiver > Edit

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

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.

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**
Sever 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**

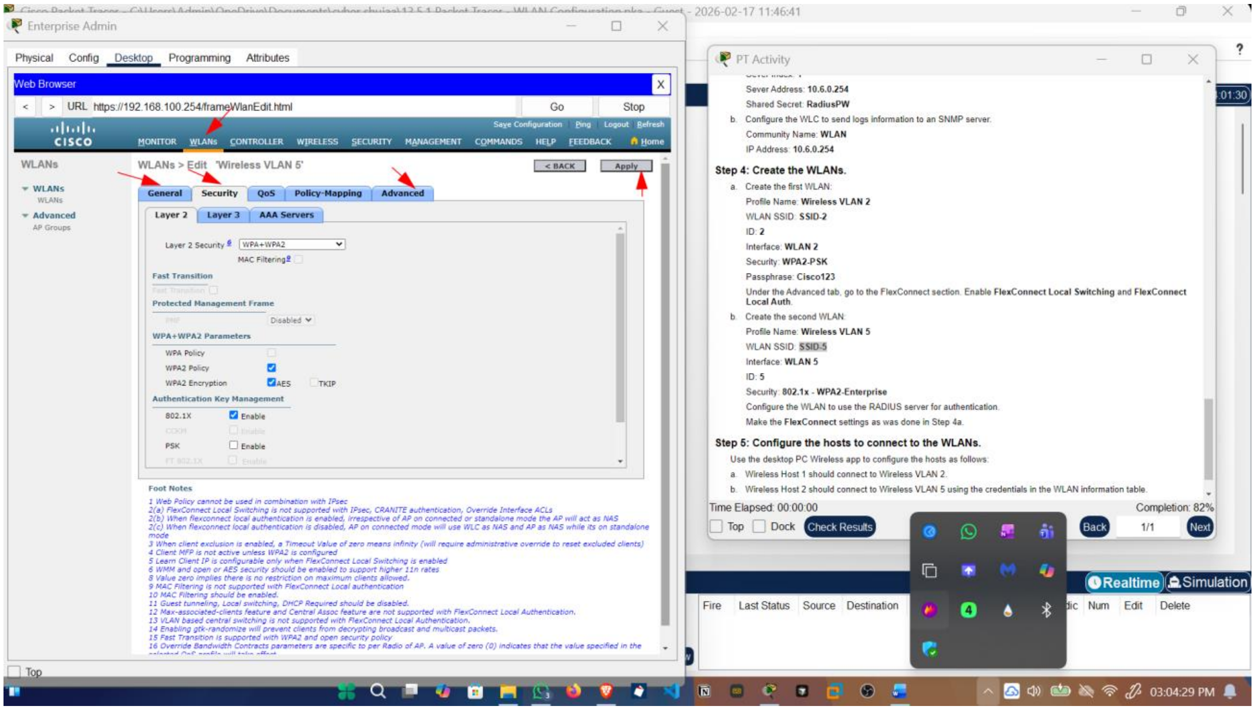
Step 4: Create the WLANs.

a. Create the first WLAN:
Profile Name: **Wireless VLAN 2**
WLAN SSID: **SSID-2**
ID: **2**
Interface: **WLAN 2**
Security: **WPA2-PSK**

Time Elapsed: 00:00:00 Completion: 69%
1/1

5.2.4 Step 4: Create the WLANs.

1. Create the first WLAN:
   a. Profile Name: **Wireless VLAN 2**
   b. WLAN SSID: **SSID-2**
   c. ID: **2**
   d. Interface: **WLAN 2**
   e. Security: **WPA2-PSK**
   f. Passphrase: **Cisco123**
   g. Under the Advanced tab, go to the FlexConnect section. Enable **FlexConnect Local Switching** and **FlexConnect Local Auth**.
2. Create the second WLAN:
   a. Profile Name: **Wireless VLAN 5**
   b. WLAN SSID: **SSID-5**
   c. Interface: **WLAN 5**
   d. ID: **5**
   e. Security: **802.1x - WPA2-Enterprise**
   f. Configure the WLAN to use the RADIUS server for authentication.
   g. Make the **FlexConnect** settings as was done in Step 4.1.



WLANs > Edit 'Wireless VLAN 5'

Layer 2 Security: WPA+WPA2

MAC Filtering ☐

Fast Transition

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

- WPA Policy ☐
- WPA2 Policy ☑
- WPA2 Encryption ☑ AES ☐ TKIP

Authentication Key Management

- 802.1X ☑ Enable
- CCKM ☐ Enable
- PSK ☐ Enable
- FT 802.1X ☐ Enable

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.
13 VLAN based central switching is not supported with FlexConnect Local Authentication.
14 Enabling gtk-randomize will prevent clients from decrypting broadcast and multicast packets.
15 Fast Transition is supported with WPA2 and open security policy
16 Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the

Sever 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.

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

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

1. Wireless Host 1 should connect to Wireless VLAN 2.
2. Wireless Host 2 should connect to Wireless VLAN 5 using the credentials in the WLAN information table.

5.2.6 Step 6: Test connectivity.

Connectivity testing confirmed successful WLAN deployment. Both wireless hosts were able to obtain IP addresses via DHCP, communicate across the network, and access the external web server through ping and URL testing. The results verified that both WPA2-Personal and WPA2-Enterprise WLANs operated correctly with secure authentication and proper VLAN segmentation.

6 CONCLUSION

The WLAN configuration activity highlighted the deployment of secure wireless networking in both home and enterprise environments. The home router provided wireless connectivity using WPA2-Personal security and controlled DHCP addressing. In the enterprise scenario, the WLC supported multiple VLAN-based WLANs with WPA2-PSK and WPA2-Enterprise authentication through a RADIUS server. Overall, the exercise emphasized the importance of WLAN security, VLAN integration, and centralized wireless management in ensuring reliable and protected wireless communication.

7 REFERENCES

1. Cyber Shujaa lab Manual