



WLAN CONFIGURATION REPORT

Packet tracer lab



BY
YUNIS MOHAMED

Table of Contents

Introduction	2
Step 1: Change DHCP settings.	2
Step 2: Configure the Wireless LAN.	2
Step 3: Configure security.	3
Step 4: Connect clients to the network.	4
Part 2: Configure a WLC Controller Network	7
Step 1: Configure VLAN interfaces.	7
Step 2: Configure a DHCP scope for the wireless management network.....	8
Step 3: Configure the WLC with external server addresses.	9
Step 4: Create the WLANs.....	10
Step 5: Configure the hosts to connect to the WLANs.....	12
Step 6: Test connectivity.	13
Conclusion.....	14

Introduction

This lab involves configuring a home router and a WLC- based network. I will be implementing various security parameters which include the WPA2-PSK and WPA2-Enterprise security. I will also implement the use of the radius AAA Servers which are used to authentication and validation. After configuration I will verify connectivity of the network and that the devices can communicate with each other.

Step 1: Change DHCP settings.

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

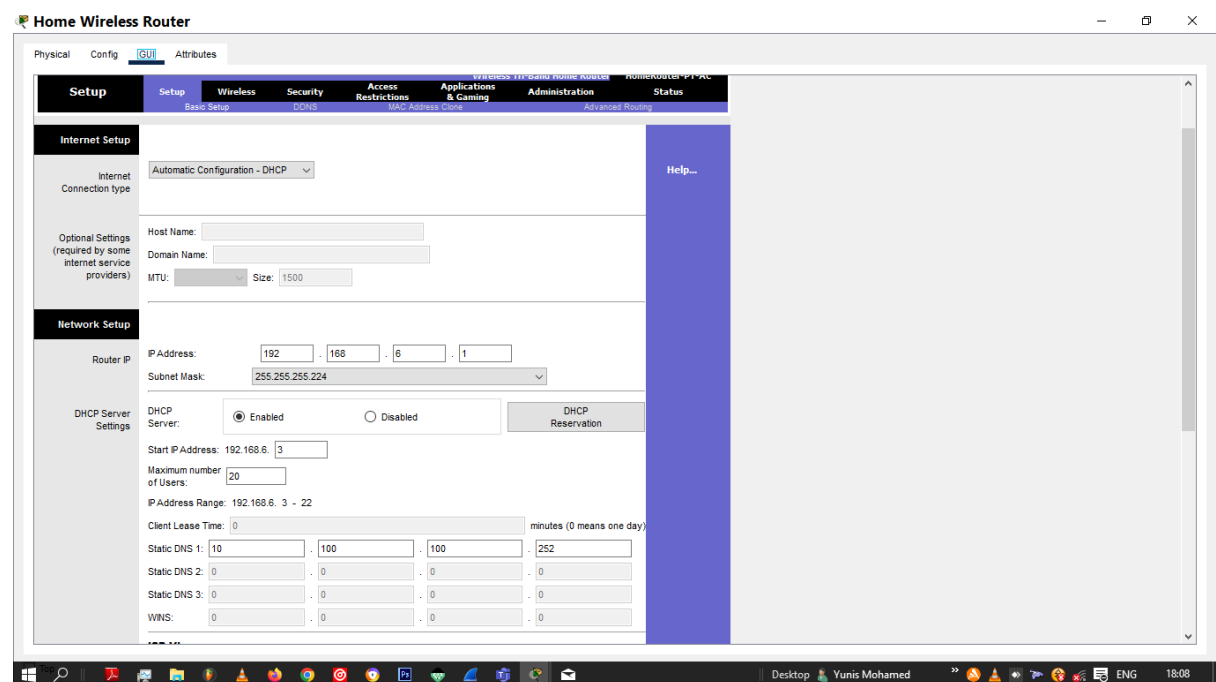


Figure 1 change dhcp setting

Step 2: Configure the Wireless LAN.

- The network will use the 2.4GHz Wireless LAN interface. Configure the interface with the SSID shown in the Wireless LAN information table.
- Use **channel 6**.

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

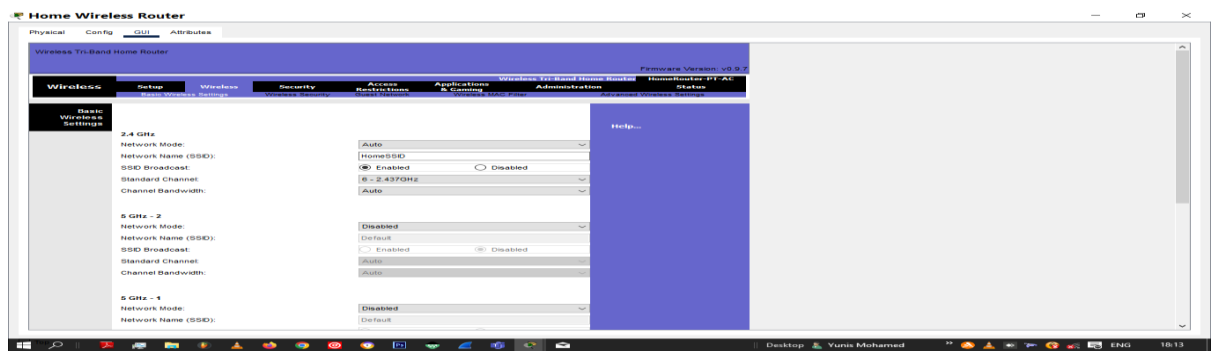
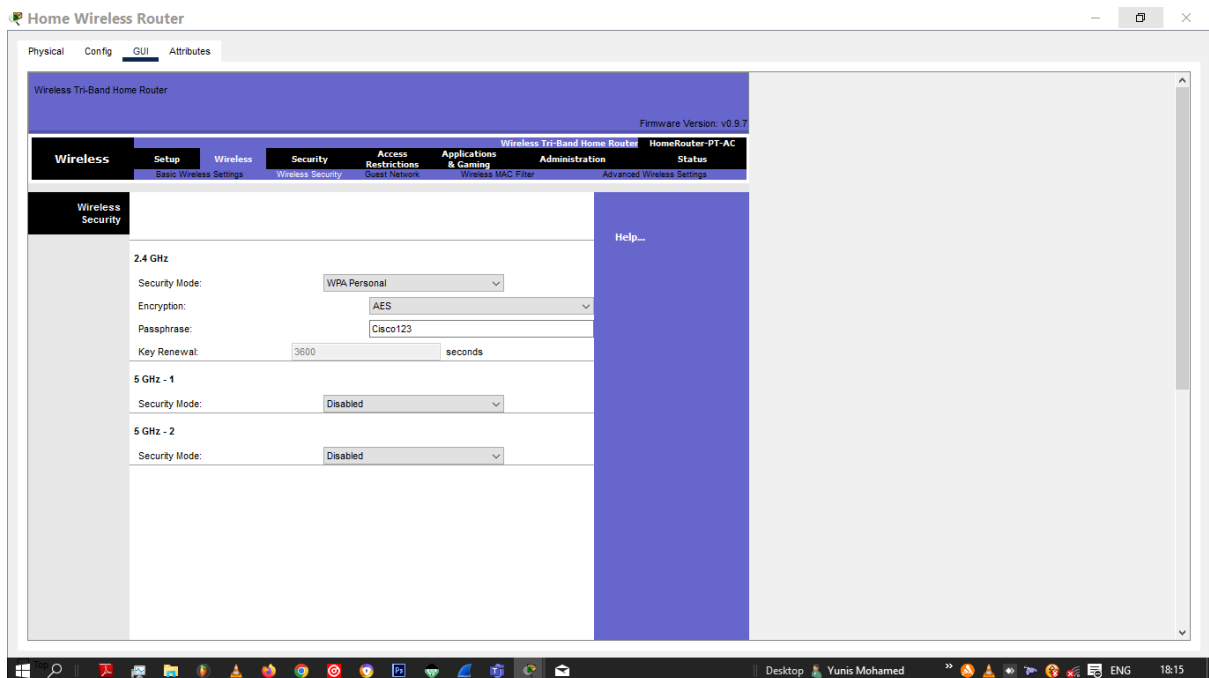


Figure 2 configure wireless LAN

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.

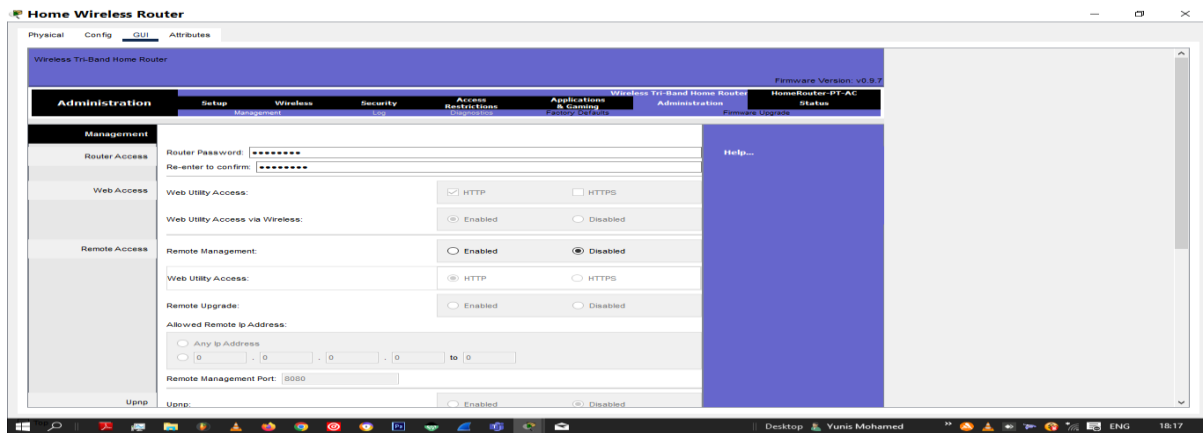
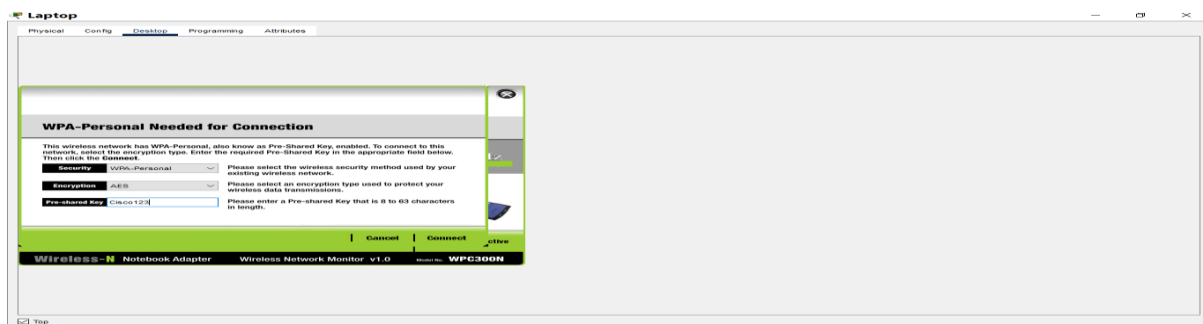


Figure 3 secure router

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.

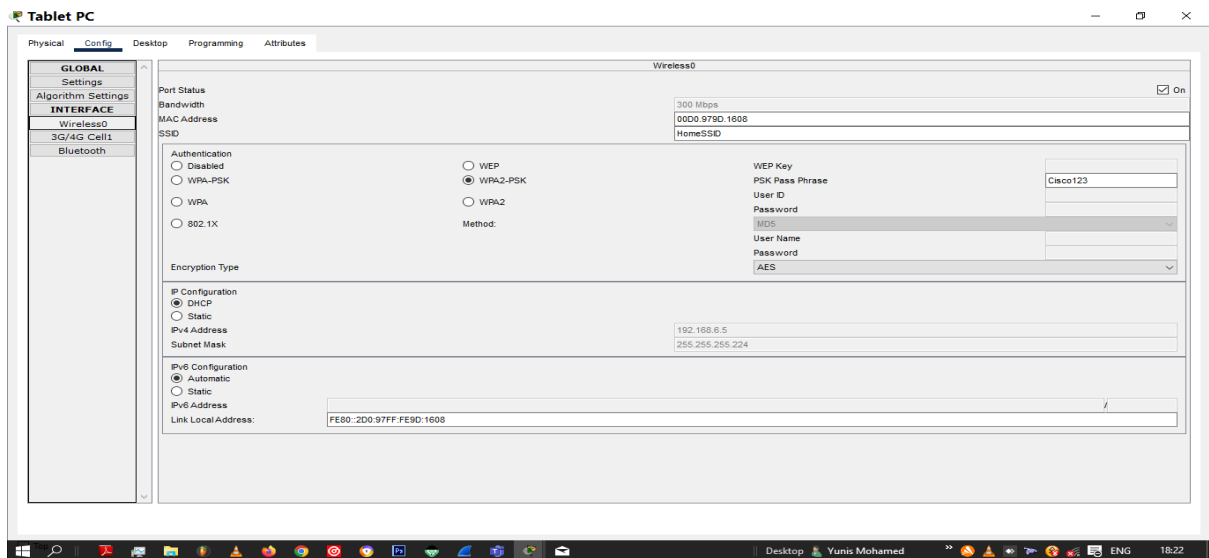


Figure 4 tablet Config

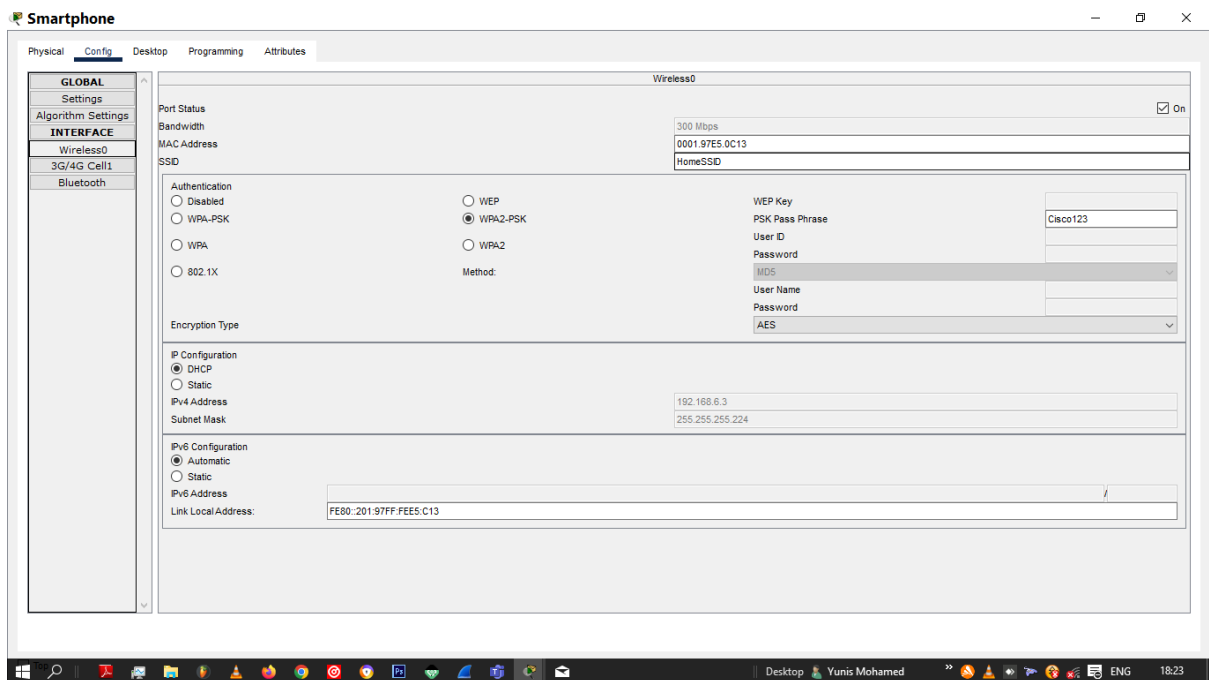


Figure 5 smartphone Config

- 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.

Smartphone ping from laptop

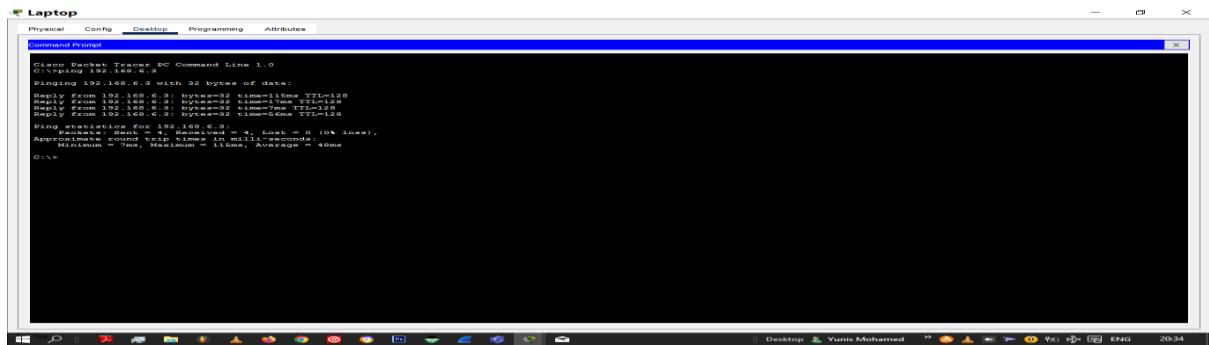


Figure 6 smartphone ping from laptop

Tablet ping from smartphone

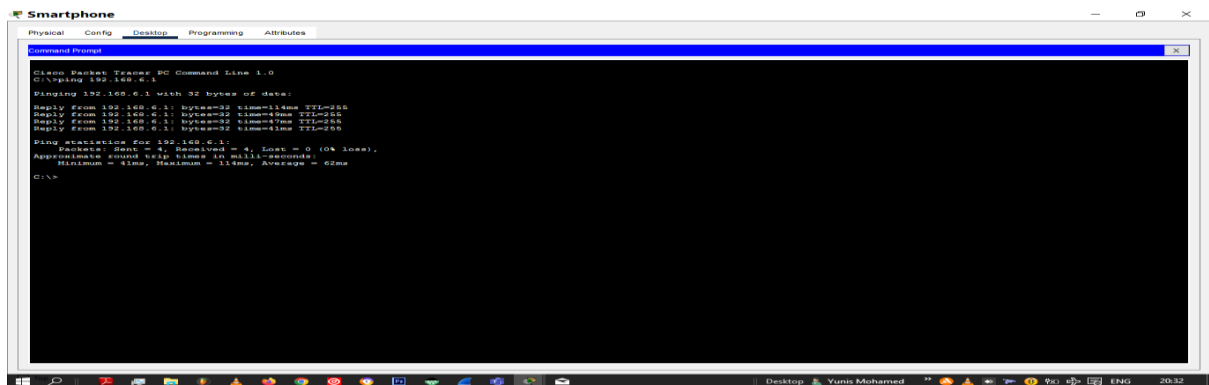


Figure 7 tablet ping from smartphone

Smartphone access to URL.

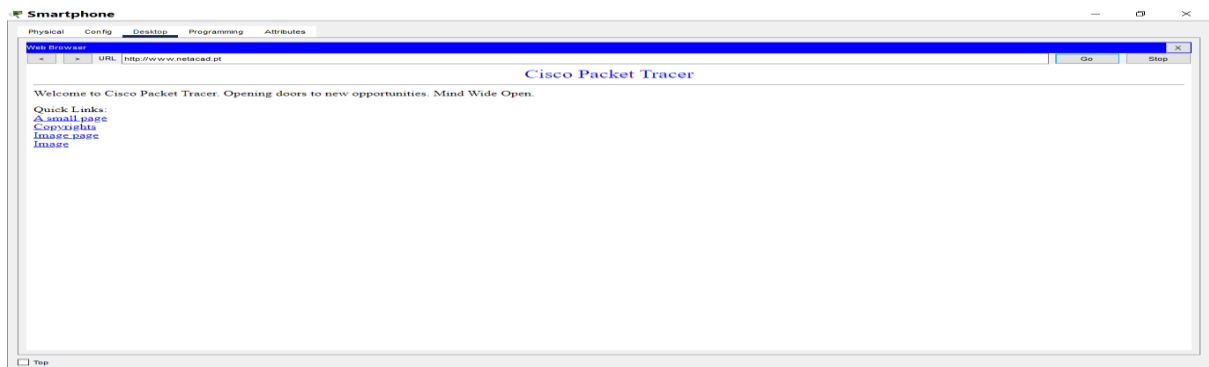


Figure 8 smartphone access to URL

Laptop access to URL

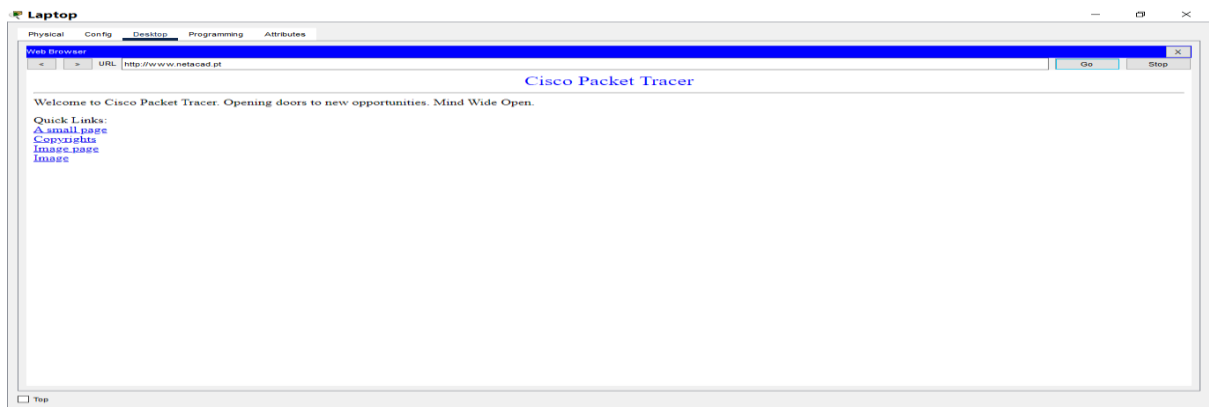


Figure 9 laptop access to URL

Part 2: Configure a WLC Controller Network

Step 1: Configure VLAN interfaces.

- 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.
- 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**

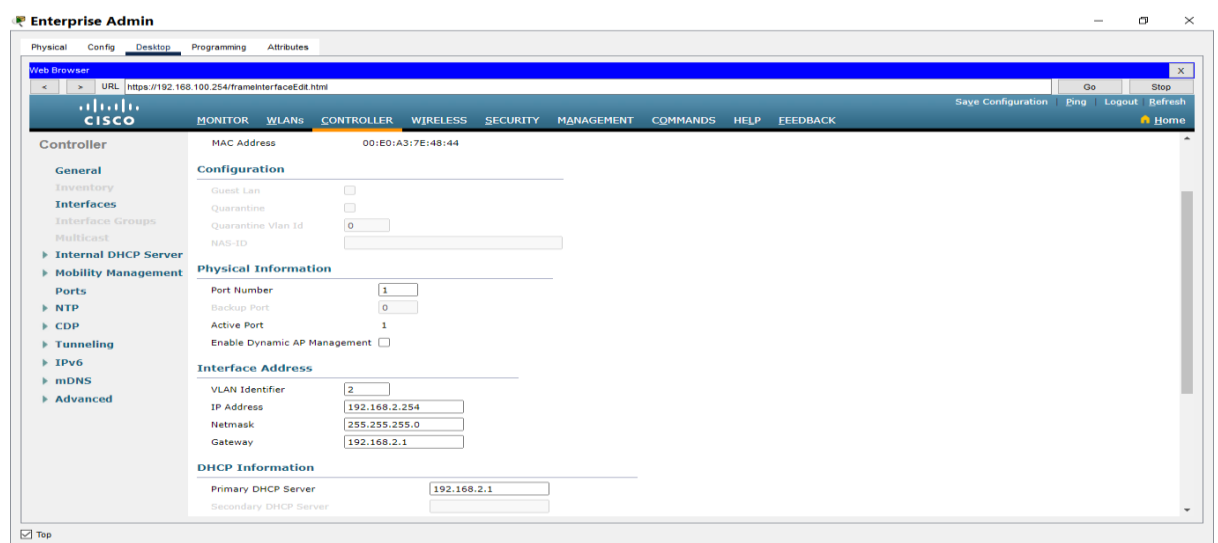


Figure 10 wlan 2

- 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**

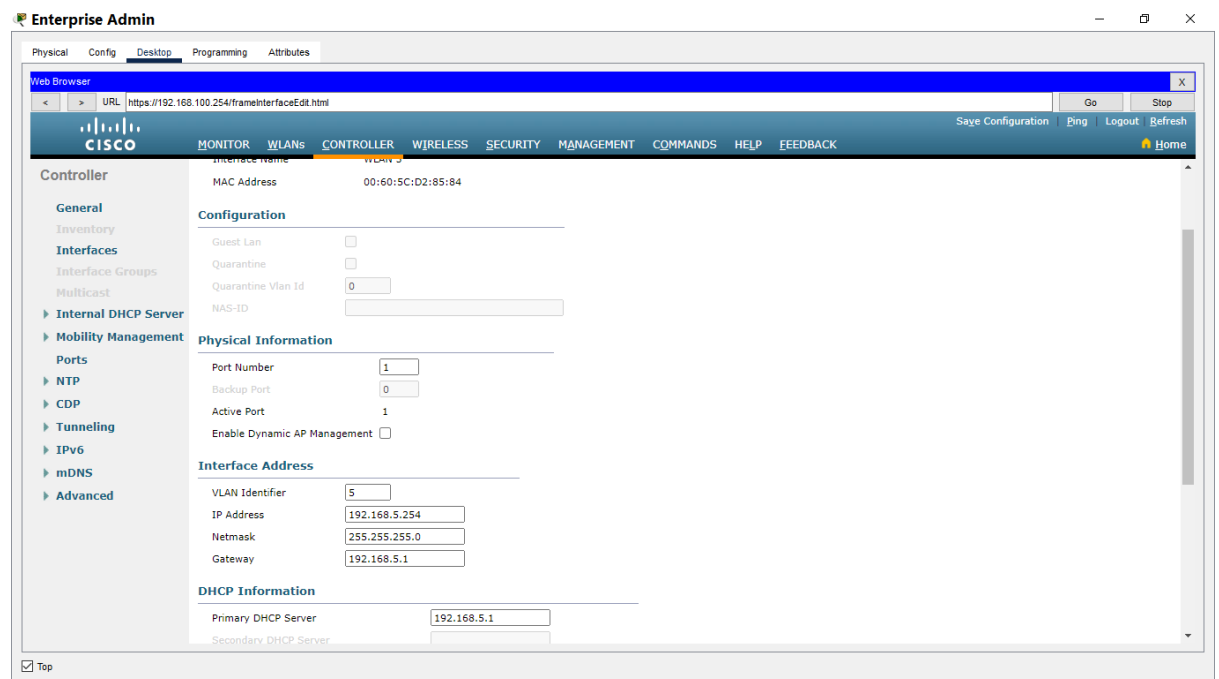


Figure 11 wlan 5

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**

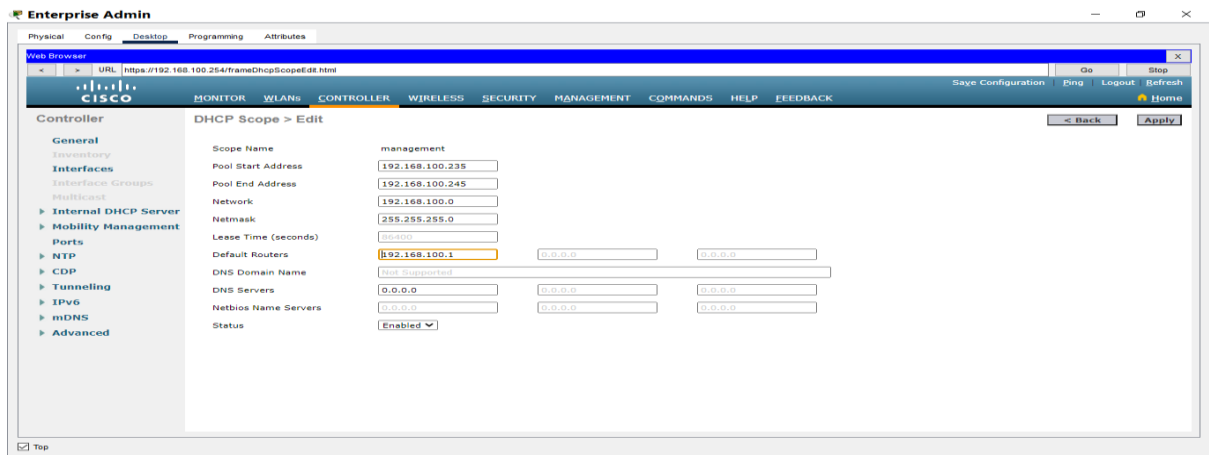


Figure 12 dhcp scope

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: **Radius PW**

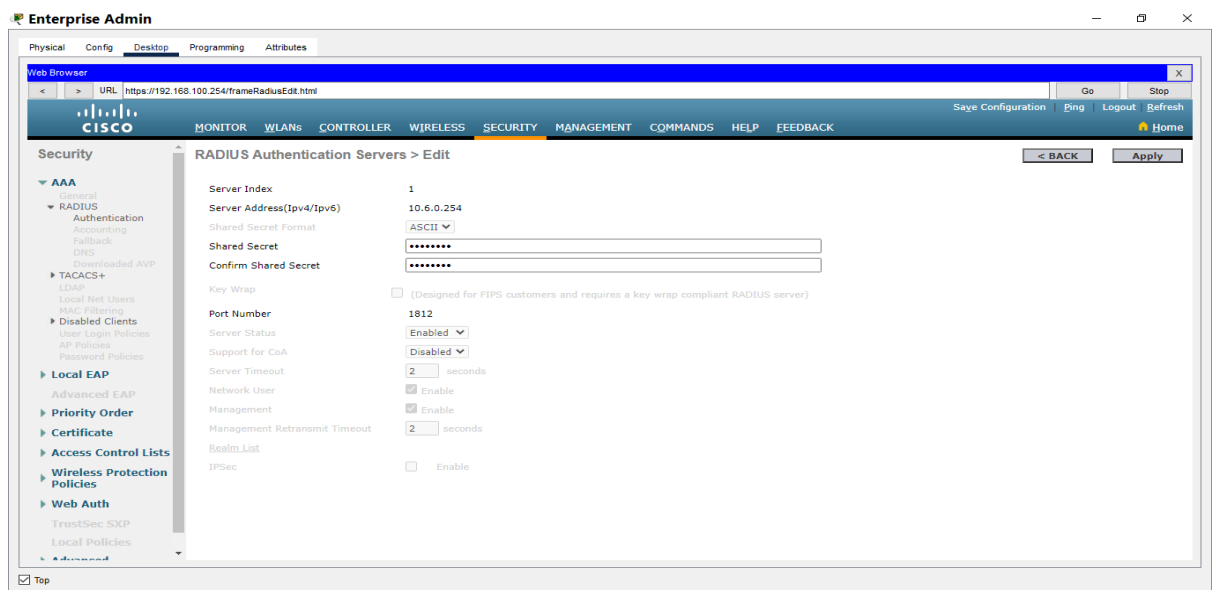


Figure 13 radius server

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

Community Name: **WLAN**

IP Address: **10.6.0.254**

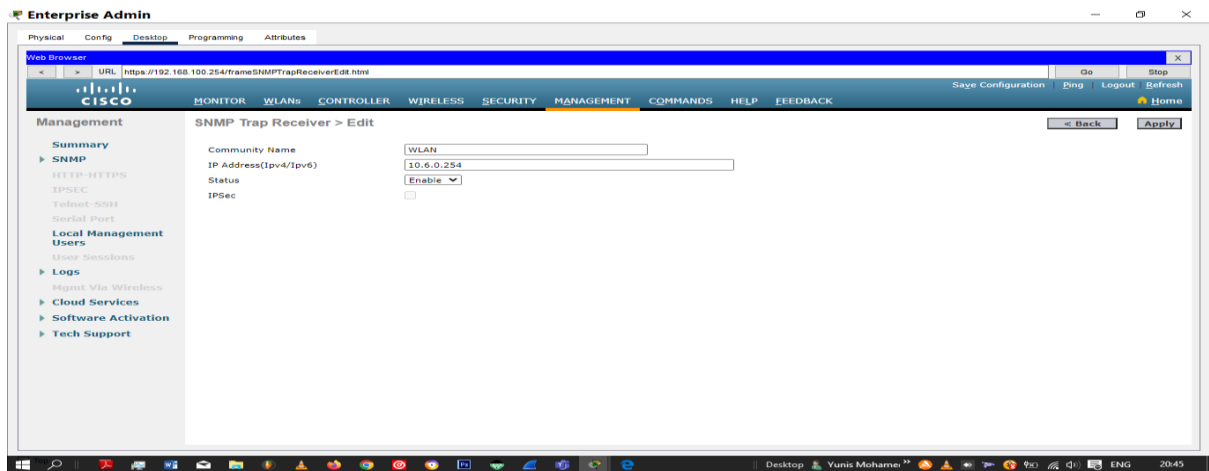


Figure 14 wlc

Step 4: Create the WLANs.

- a. Create the first WLAN:

Profile Name: **Wireless VLAN 2**

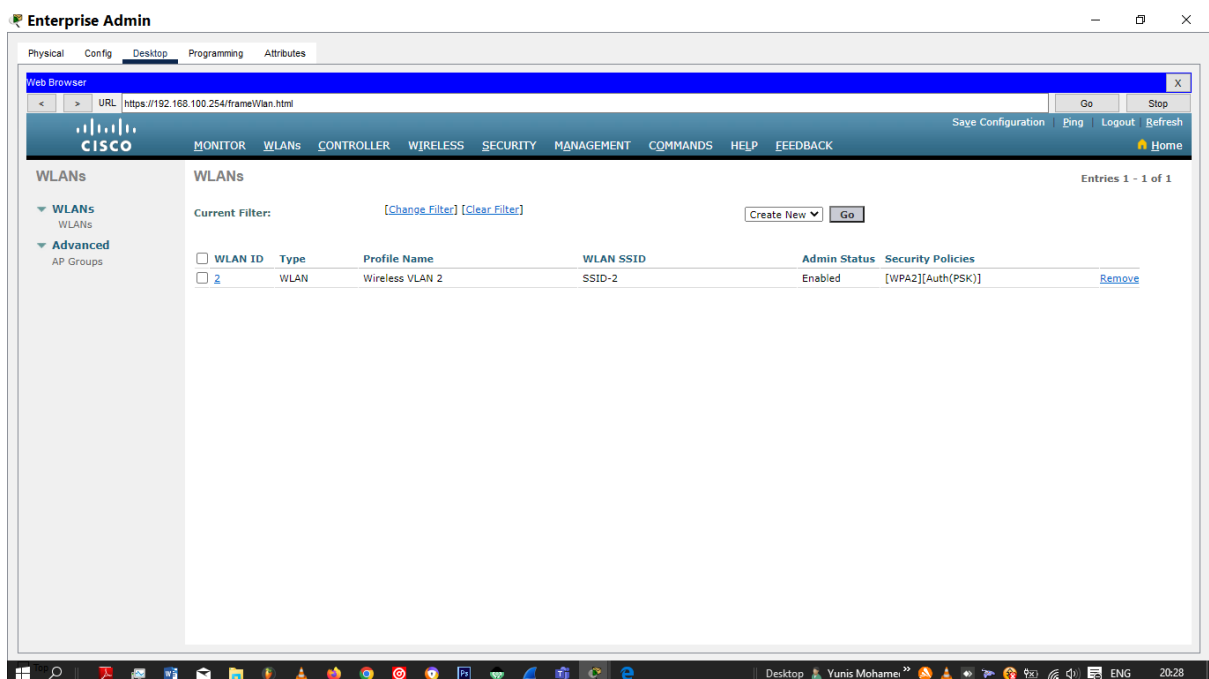
WLAN SSID: **SSID-2**

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**.

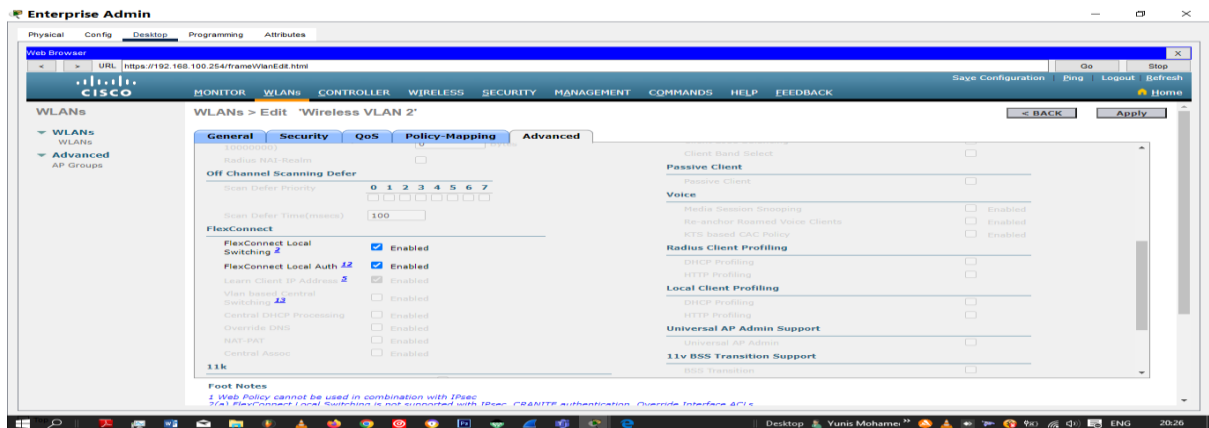


Figure 15 enable flex

- b. Create the second WLAN:
 Profile Name: **Wireless VLAN 5**
 WLAN SSID: **SSID-5**
 Interface: **WLAN 5**
 ID: **5**

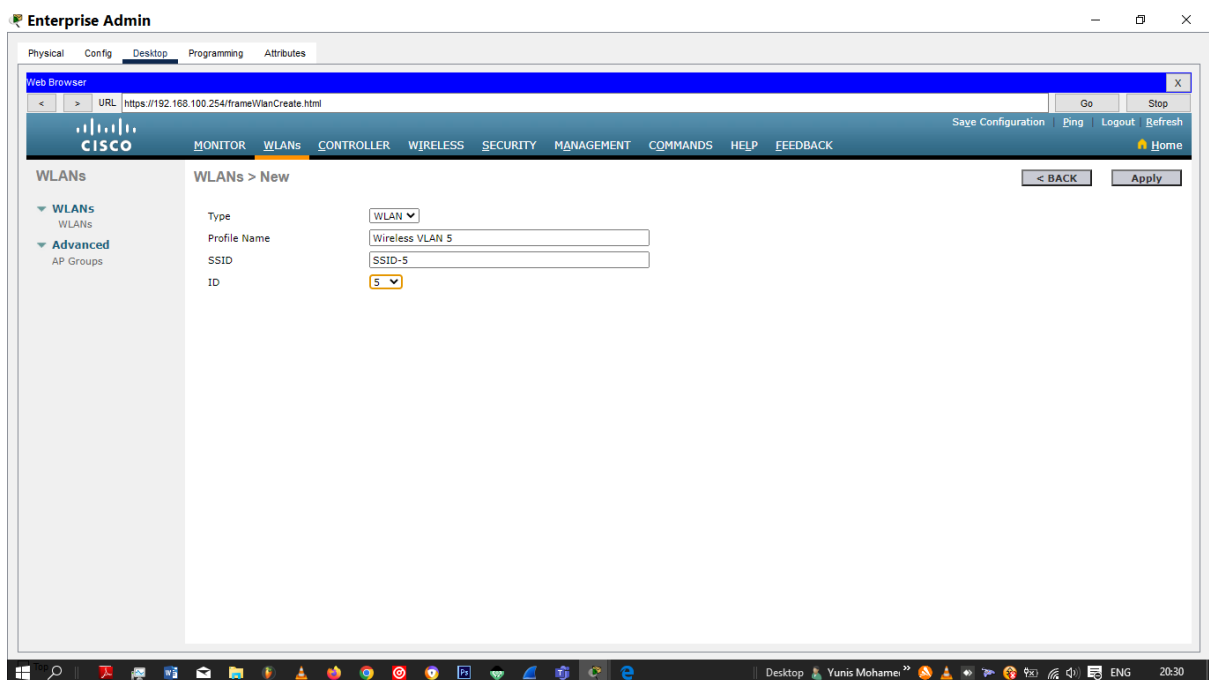


Figure 16 wlan 5

Security: 802.1x - WPA2-Enterprise

Configure the WLAN to use the RADIUS server for authentication.

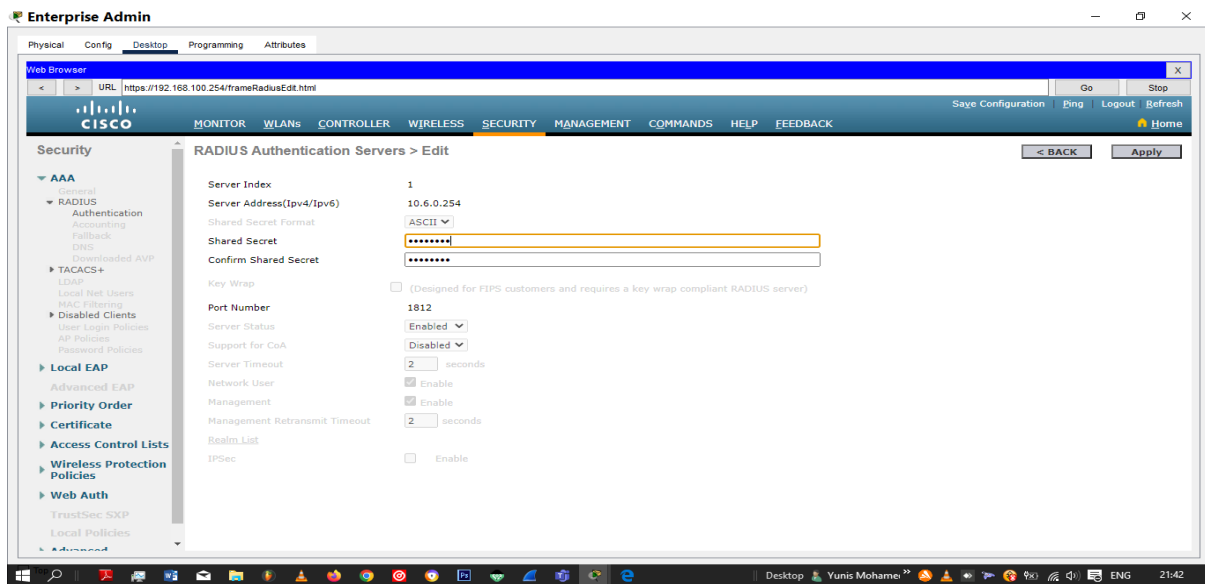


Figure 17 radius server

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

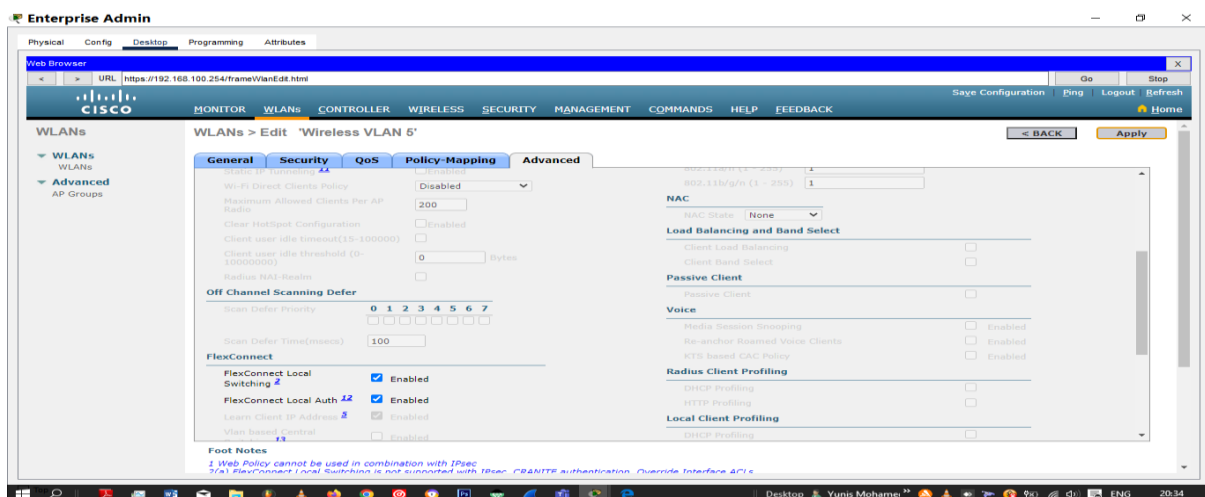


Figure 18 flex connect wlan 5

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.

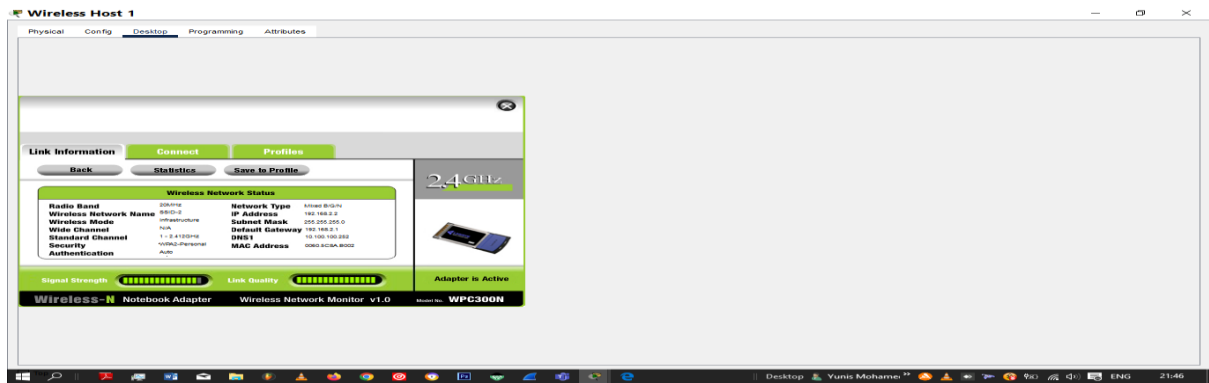


Figure 19 wireless host vlan 2

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

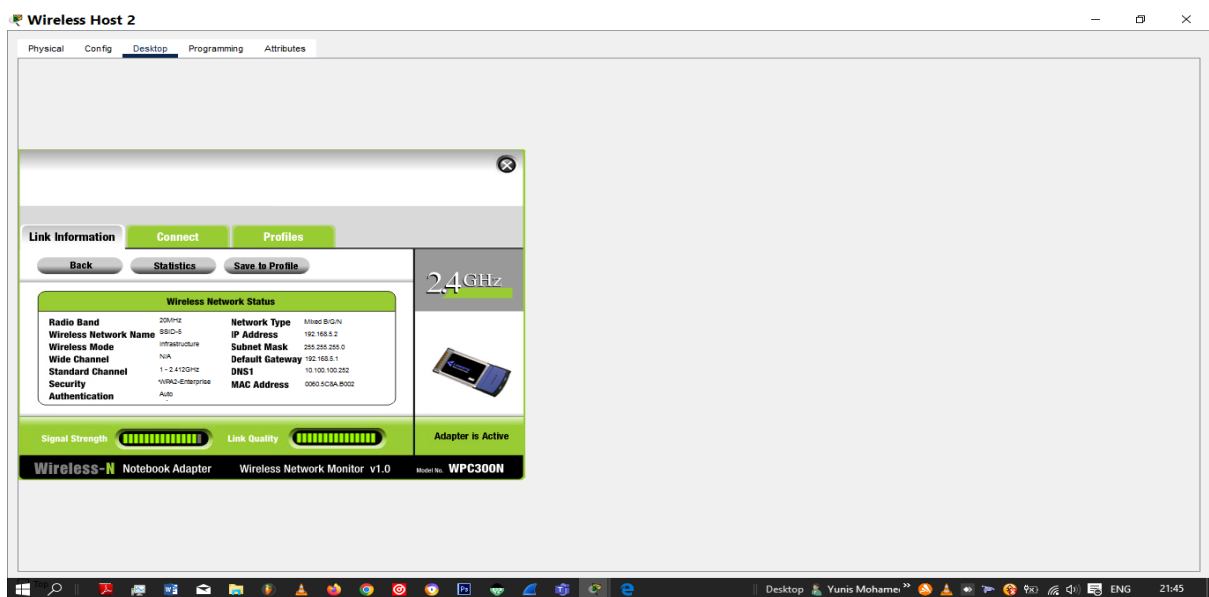


Figure 20 wireless connectivity

Step 6: Test connectivity.

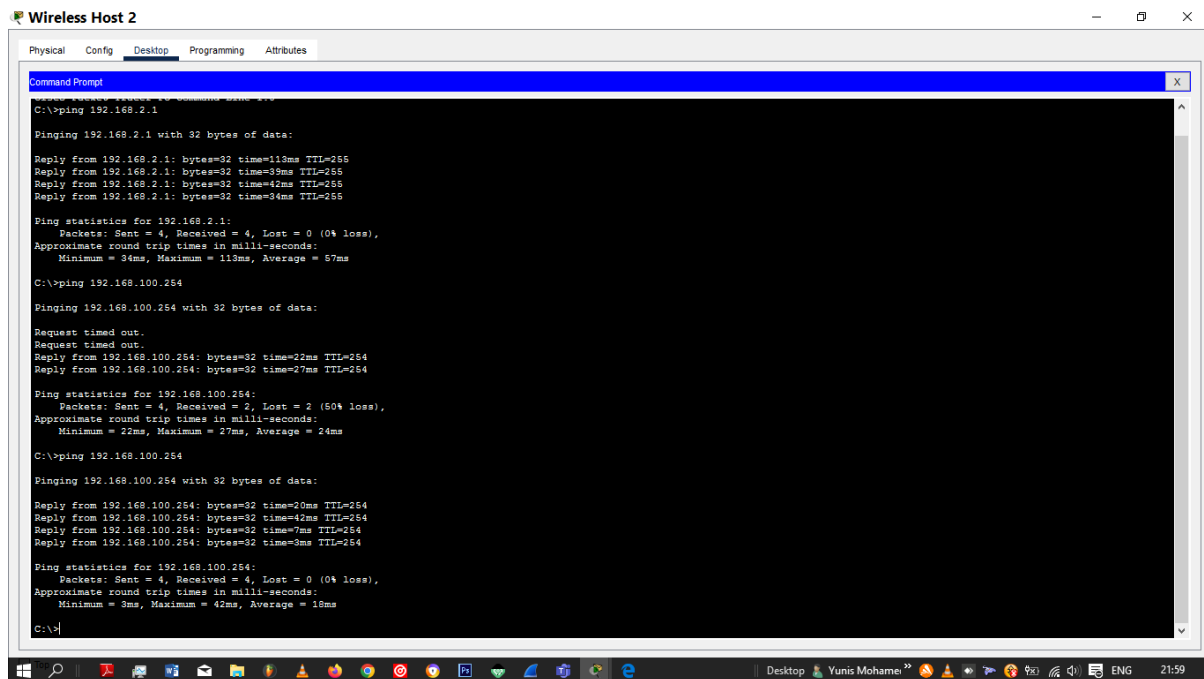
Test connectivity between the wireless hosts and the Web Server by ping and URL

Wireless host 1 ping to web server and wireless host 2 successful.



Figure 21 wireless host ping

Wireless host 2 ping to web server and wireless host 1 successful.



```
Wireless Host 2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=113ms TTL=255
Reply from 192.168.2.1: bytes=32 time=33ms TTL=255
Reply from 192.168.2.1: bytes=32 time=42ms TTL=255
Reply from 192.168.2.1: bytes=32 time=34ms TTL=255
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 113ms, Average = 57ms
C:\>ping 192.168.100.254
Pinging 192.168.100.254 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.100.254: bytes=32 time=22ms TTL=254
Reply from 192.168.100.254: bytes=32 time=27ms TTL=254
Ping statistics for 192.168.100.254:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 27ms, Average = 24ms
C:\>ping 192.168.100.254
Pinging 192.168.100.254 with 32 bytes of data:
Reply from 192.168.100.254: bytes=32 time=20ms TTL=254
Reply from 192.168.100.254: bytes=32 time=42ms TTL=254
Reply from 192.168.100.254: bytes=32 time=7ms TTL=254
Reply from 192.168.100.254: bytes=32 time=3ms TTL=254
Ping statistics for 192.168.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 42ms, Average = 18ms
C:\>
```

Figure 22 wireless host 2 ping

Conclusion

This practical lab helps in acquiring WLAN configuration skills by configuring a home router and an enterprise WLC (wireless LAN controller). I was able to converse with the user interface of both devices and configure various parameters such as DHCP scope which will provide IP address dynamically. I also configured the WLC with external server addresses by use of the Radius server. Configuring wireless LAN security by use of the WPA2 personal or WPA2 enterprise help in securing network from unauthorized personnel. The lab has assisted me in getting the various wireless security measures required to help secure wireless networks.