

**NST21022 - Practical
for Network Switching
and Routing**

Department of Information
and Communication
Technology
Faculty of Technology



Lab sheet :18E1&E2
Reg. Number: SEU/IS/20/ICT/084
Academic Year :2020/2021
Practical No :18

Title: Configure a Wireless LAN

Aim:

- Getting familiar with Wireless Network
- Getting familiar with WPA2 Enterprise WLAN on the WLC

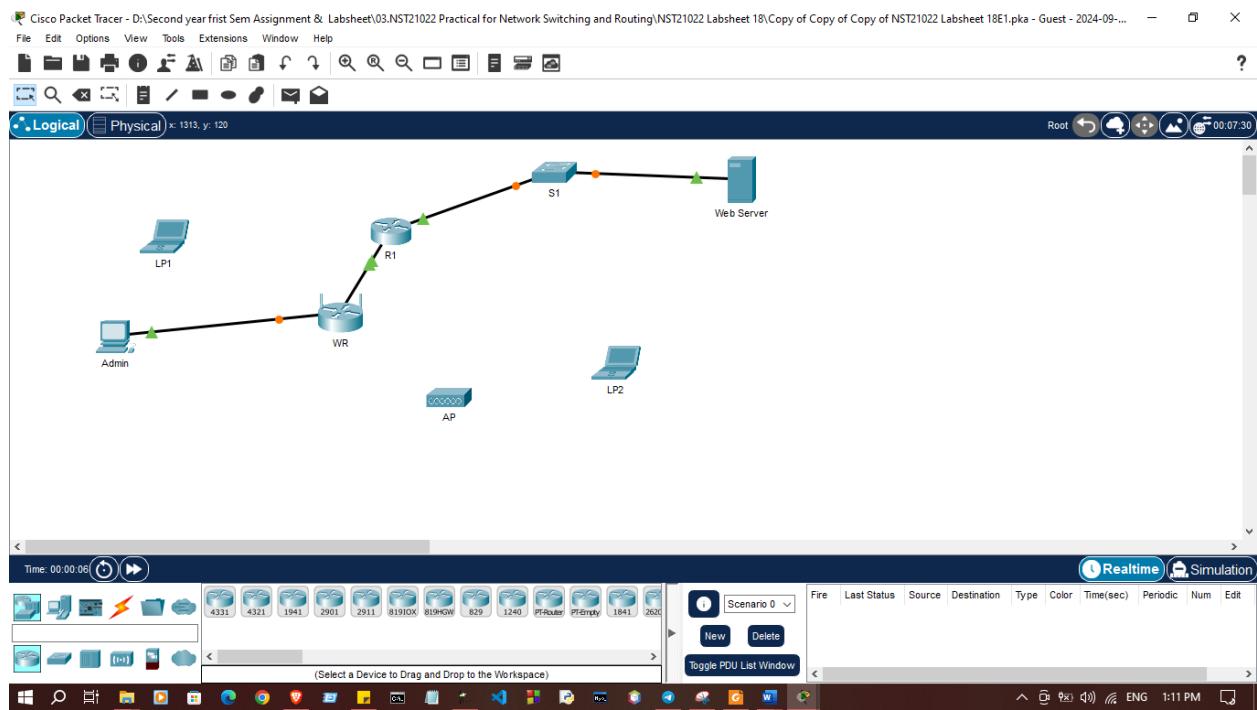
Task:

- Configure wireless router
- Connect wireless devices to the wireless router
- Add an access point to extend wireless coverage
- Configure a new VLAN interface on a WLC.
- Configure a new WLAN on a WLC.
- Configure a new scope on the WLC internal DHCP server.
- Configure the WLC with SNMP settings.
- Configure the WLC to user a RADIUS server to authenticate WLAN users.
- Secure a WLAN with WPA2-Enterprise.
- Connect hosts to the new WLC.

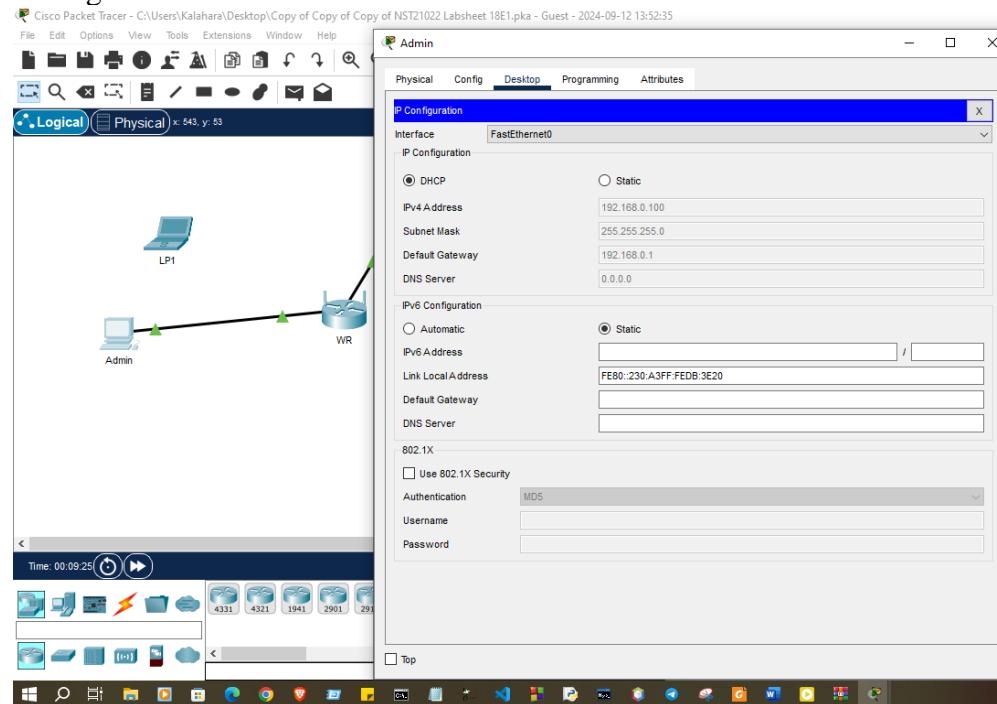
Activities

Exercise 01: Configure Personal Wireless LAN

Use “NST21022 Lab sheet 18E1.pka” file

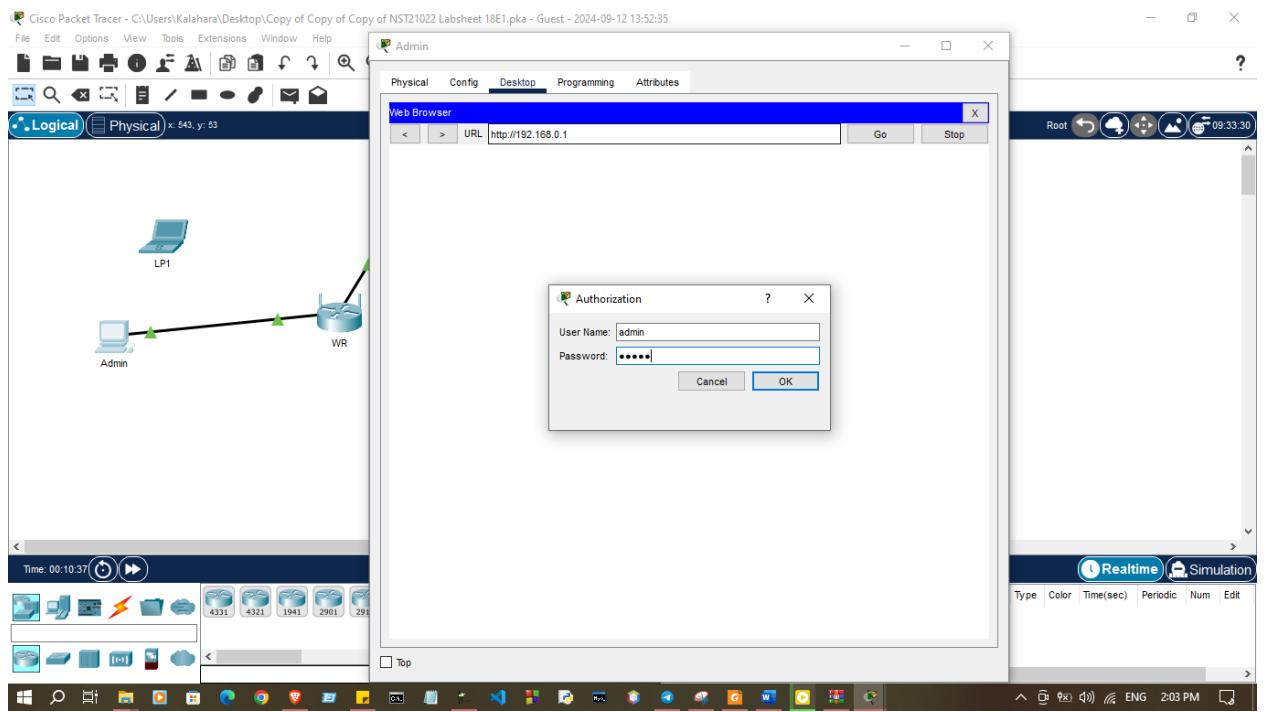


1. Configure Admin to use DHCP

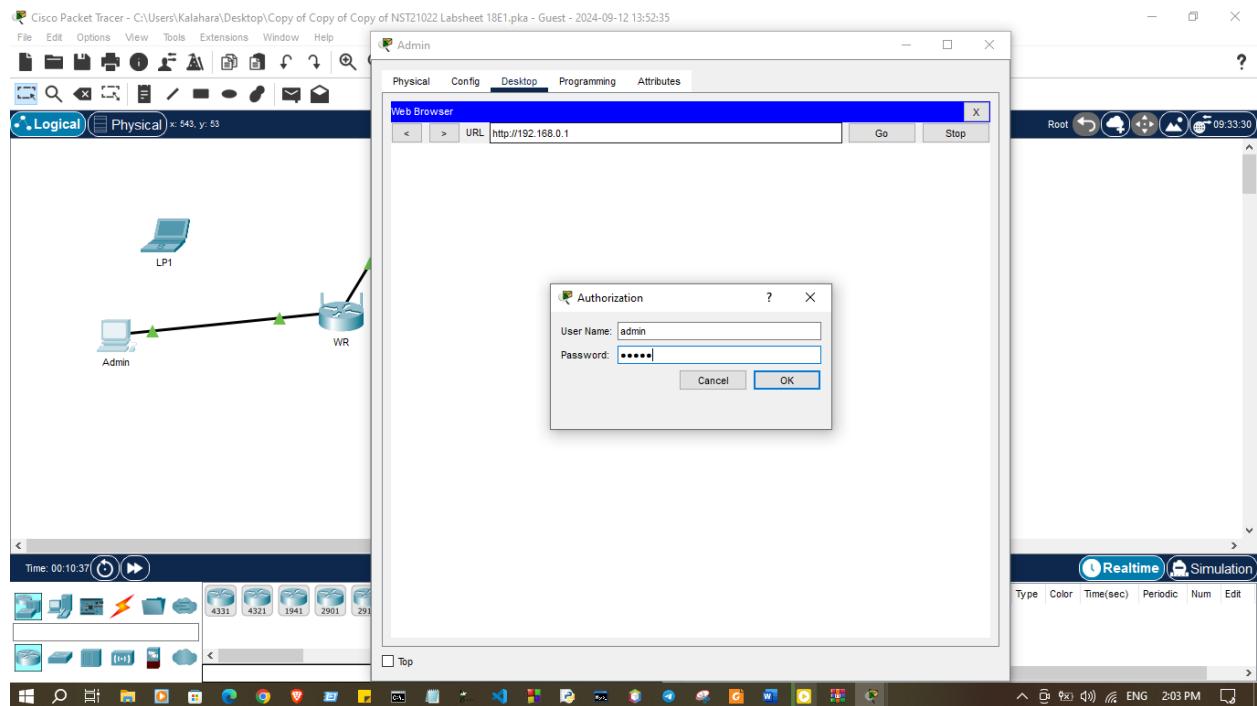


2. Connect to the WR Web Interface (192.168.0.1)

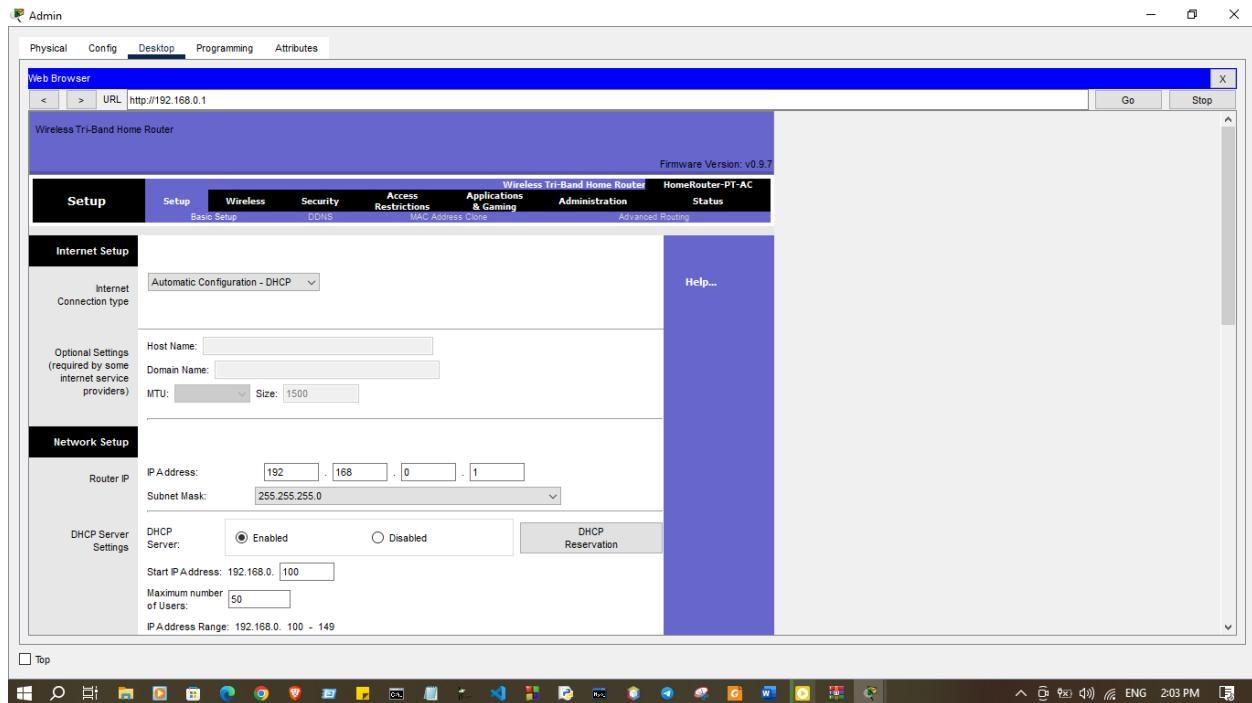
- In Web Browser



b. Use **admin** for both username and password



c. Under the Network Setup heading on the **Basic Setup** page, notice the IP address range for the DHCP server.



3. Configure the Internet Port of WR

a. Under the **Internet Setup** at the top of the **Basic Setup** page, change the Internet IP address method to **Static IP**



b. Following IP address have to be assigned to the **Internet interface**:

Internet IP address : 10.1.2.10

Subnet Mask : 255.255.255.0

Default Gateway : 10.1.2.1

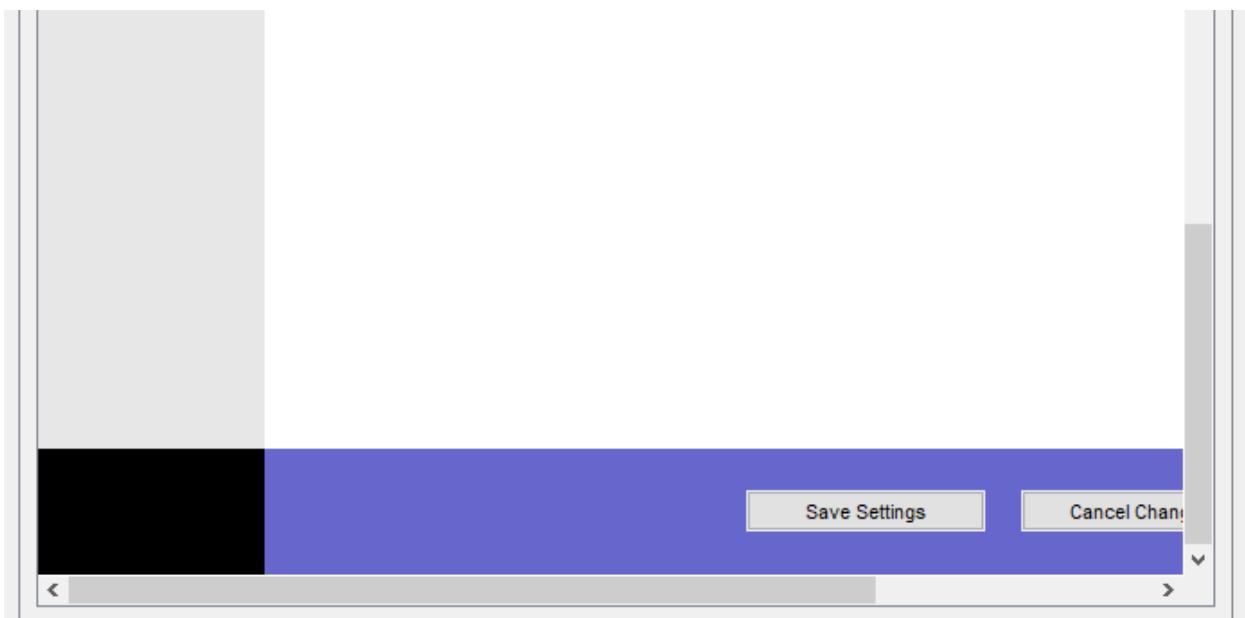
DNS Server : 10.1.1.10

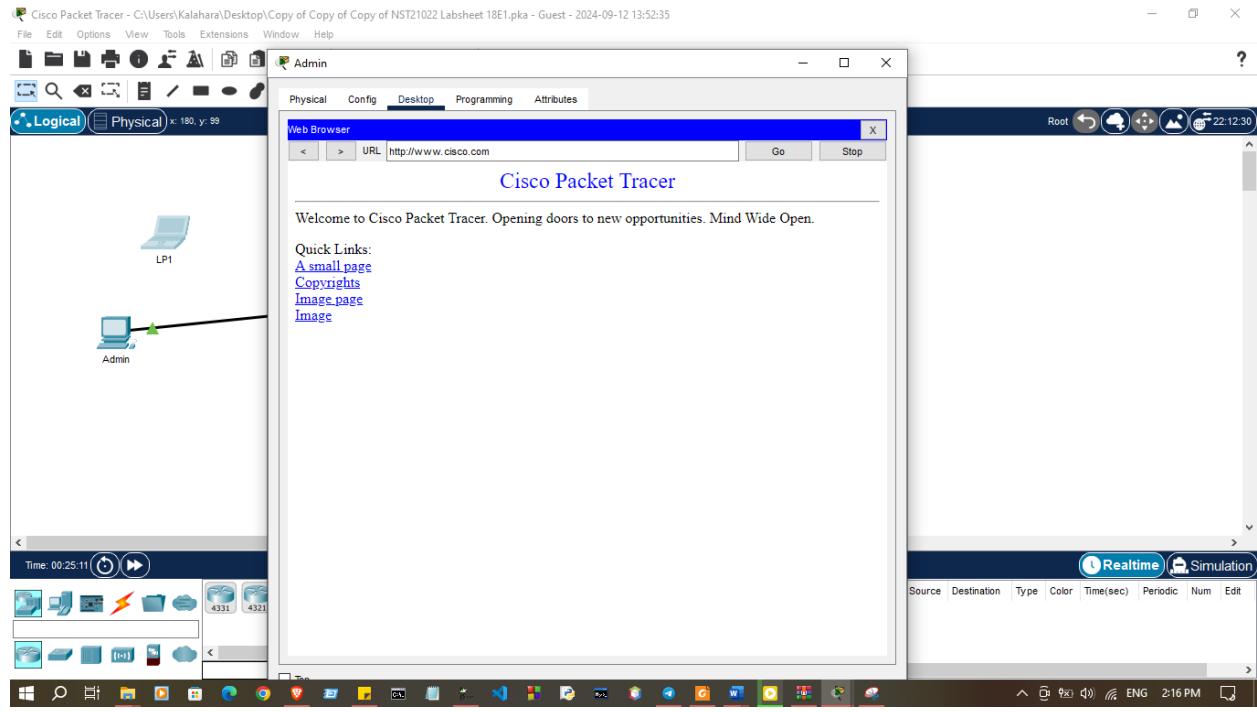
The screenshot shows the 'Internet Setup' configuration page. Under 'Internet Connection type', 'Static IP' is selected. The configuration fields are as follows:

- Internet IP Address: 10.1.2.10
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.1.2.1
- DNS 1: 10.1.1.10
- DNS 2 (Optional): 0.0.0.0
- DNS 3 (Optional): 0.0.0.0

Below these fields, there are optional settings for Host Name and Domain Name.

c. Save Settings and verify connectivity through access www.cisco.com



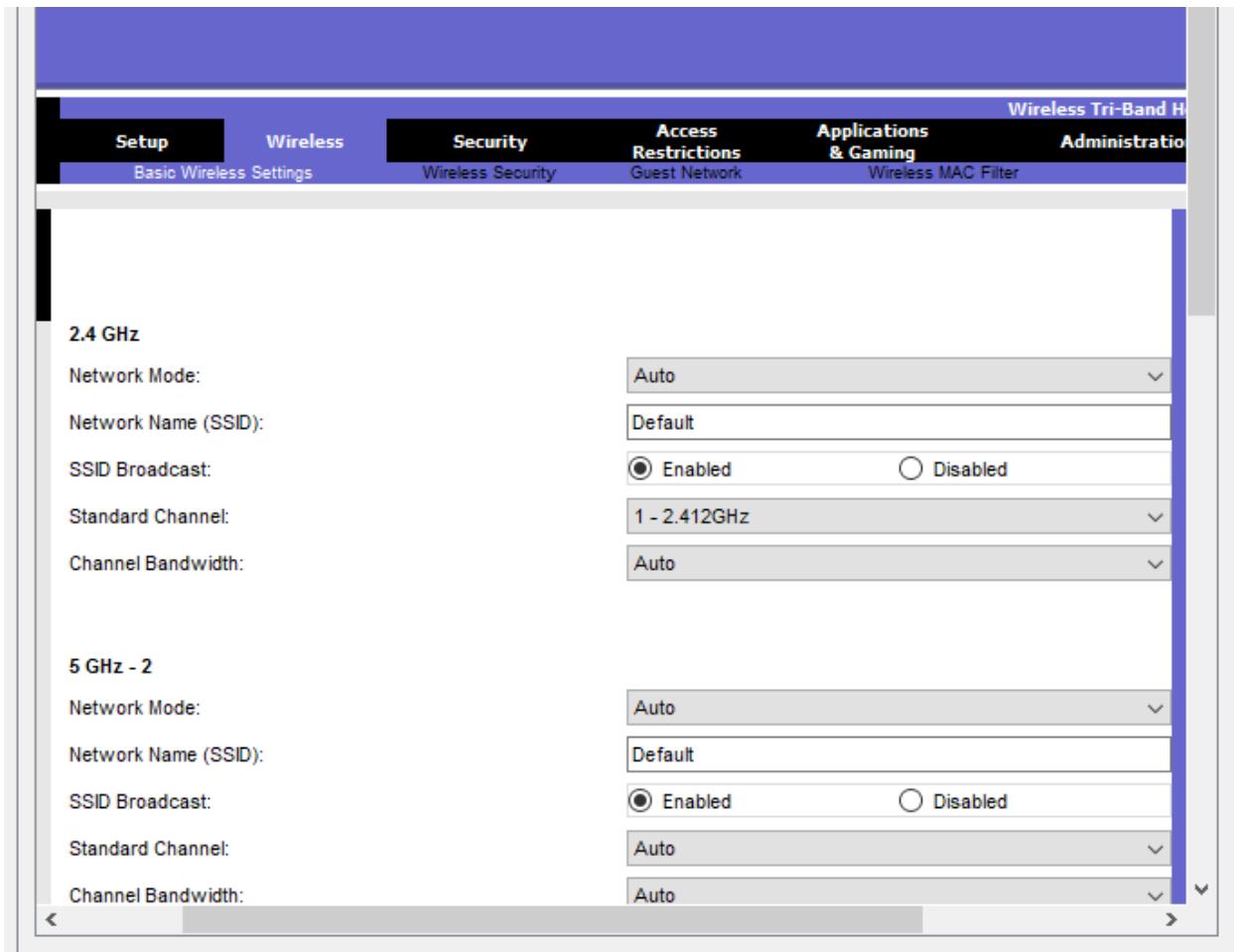


4. Configure Wireless Settings

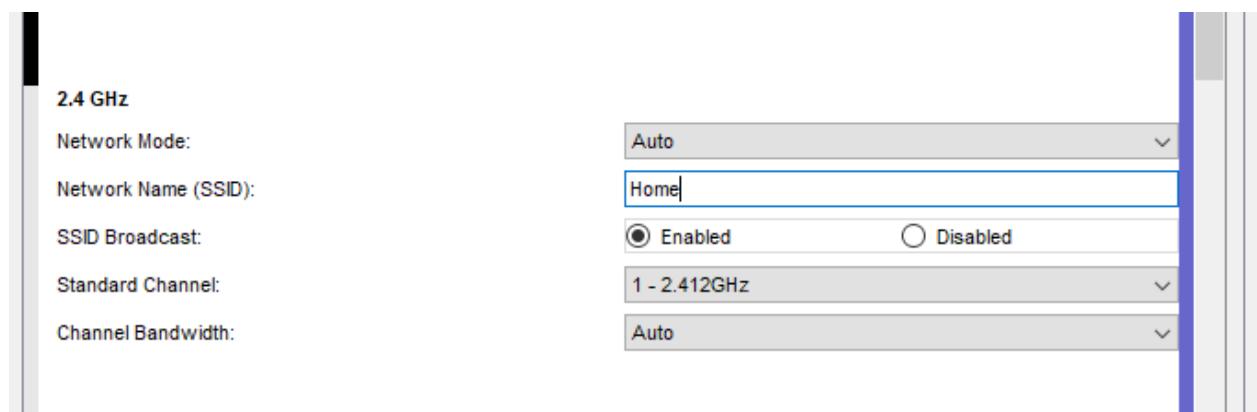
a. Connect to the WR web interface

2.4 GHz		5 GHz - 2	
Network Mode:	Auto	Network Mode:	Auto
Network Name (SSID):	Default	Network Name (SSID):	Default
SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Standard Channel:	1 - 2.412GHz	Standard Channel:	Auto
Channel Bandwidth:	Auto	Channel Bandwidth:	Auto

b. Navigate to **Wireless** → **Basic Wireless Settings**



c. Change **Network Name (SSID)** to **Home** for only 2.4GHz. Note that SSIDs are case sensitive



d. Change the Standard Channel to **6 – 2.437GHz**

2.4 GHz

Network Mode: Auto

Network Name (SSID): Home

SSID Broadcast: Enabled Disabled

Standard Channel: 6 - 2.437GHz

Channel Bandwidth: Auto

5 GHz - 2

e. Disable 5GHz frequencies.

5 GHz - 2

Network Mode: Disabled

Network Name (SSID): Default

SSID Broadcast: Enabled Disabled

Standard Channel: 149 - 5.745GHz

Channel Bandwidth: Auto

5 GHz - 1

Network Mode: N-Only

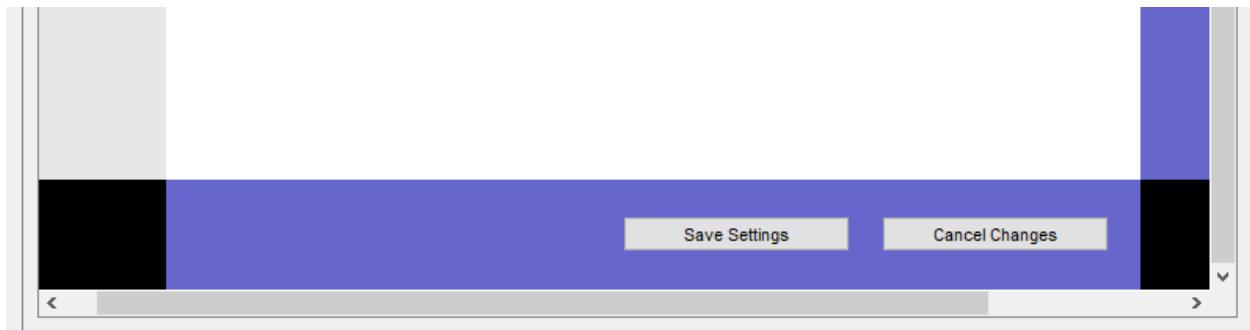
Network Name (SSID): Default

SSID Broadcast: Enabled Disabled

Standard Channel: Auto

Channel Bandwidth: Auto

f. Save Settings



5. Configure wireless security settings

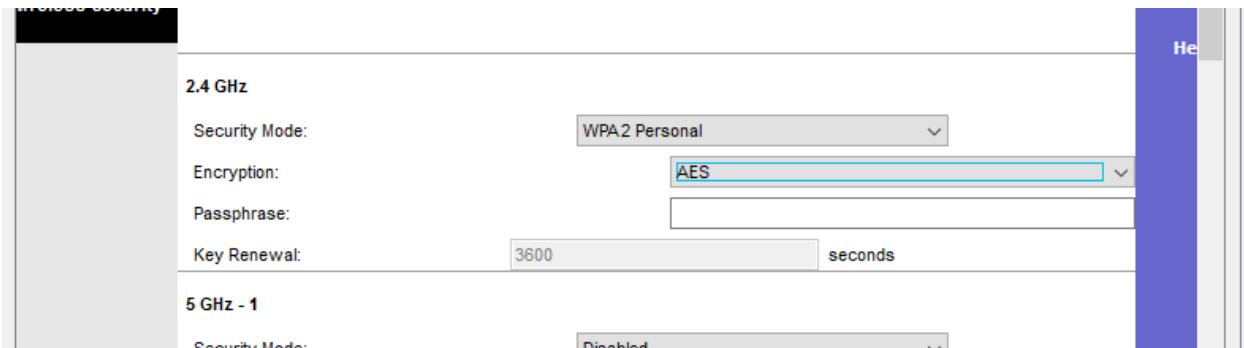
a. Navigate to **Wireless → Wireless Security**

A screenshot of a web-based configuration interface for a wireless router. The top navigation bar includes tabs for Wireless, Setup, Wireless, Security, Access Restrictions, Applications & Gaming, and Administration. The Security tab is active. On the left, a sidebar shows "Wireless Security". The main content area has sections for "2.4 GHz", "5 GHz - 1", and "5 GHz - 2", each with a "Security Mode" dropdown set to "Disabled". A vertical help menu is visible on the right.

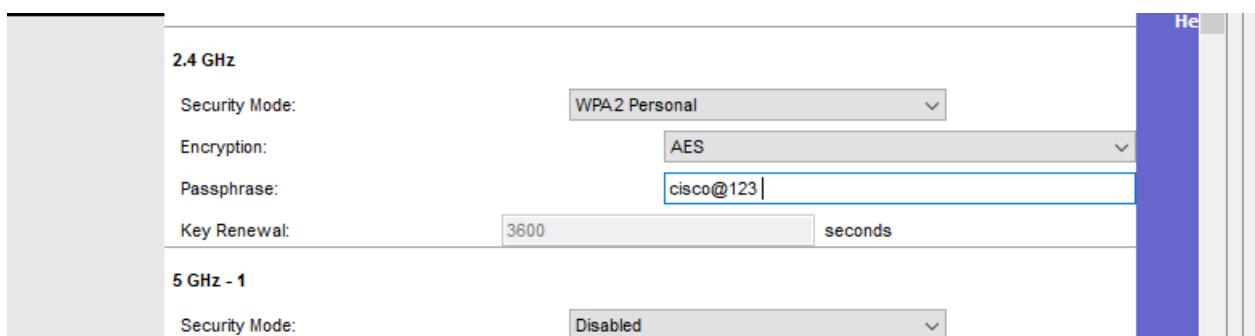
b. Under the **2.4 GHz** heading, select **WPA2 Personal** for the security mode.

A screenshot of the "2.4 GHz" configuration section. It includes fields for "Security Mode" (set to "WPA2 Personal"), "Encryption" (set to "AES"), "Passphrase" (an empty input field), "Key Renewal" (set to "3600 seconds"), and "5 GHz - 1" (with its "Security Mode" set to "Disabled"). The "WPA2 Personal" selection is highlighted with a blue border.

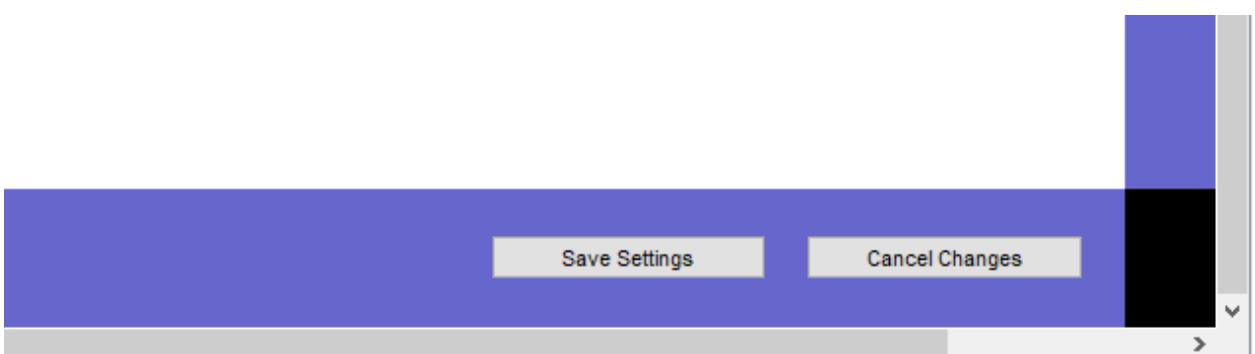
c. Keep the default **AES** encryption settings



d. Enter **cisco@123** as the passphrase



e. Save Settings



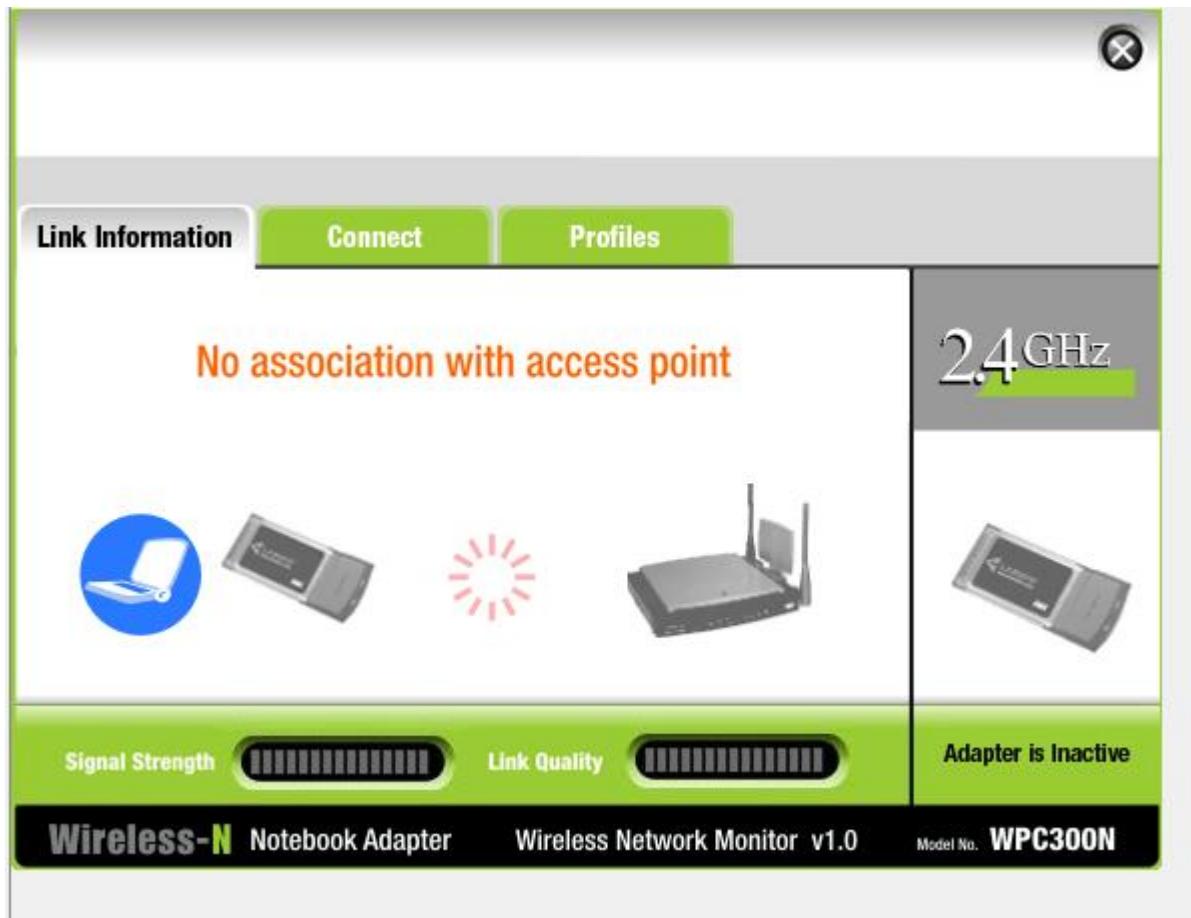
6. Connect the Wireless Clients

- Turn on wireless interface in **LP1**

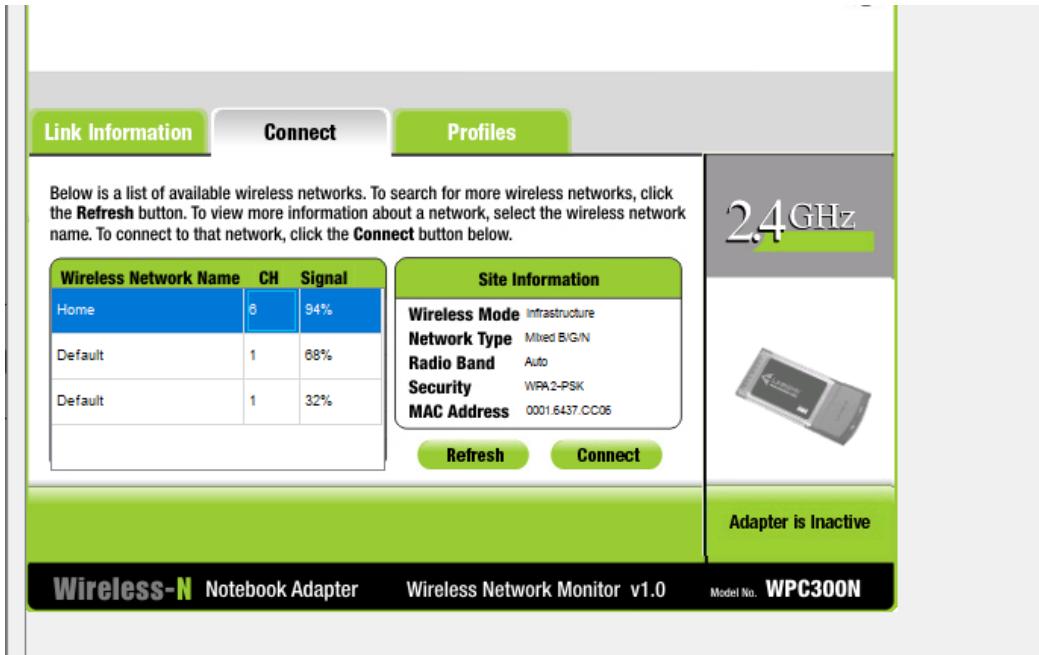
The screenshot shows the configuration interface for the LP1 device. On the left, there is a sidebar with a tree view: GLOBAL, Settings, Algorithm Settings, INTERFACE, **Wireless0**, and Bluetooth. The 'Wireless0' node is selected. The main panel is titled 'Wireless0' and contains the following settings:

Port Status	<input checked="" type="checkbox"/> On	
Bandwidth	300 Mbps	
MAC Address	00E0.F782.5AA1	
SSID	Default	
Authentication		
<input checked="" type="radio"/> Disabled	<input type="radio"/> WEP	WEP Key
<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK	PSK Pass Phrase

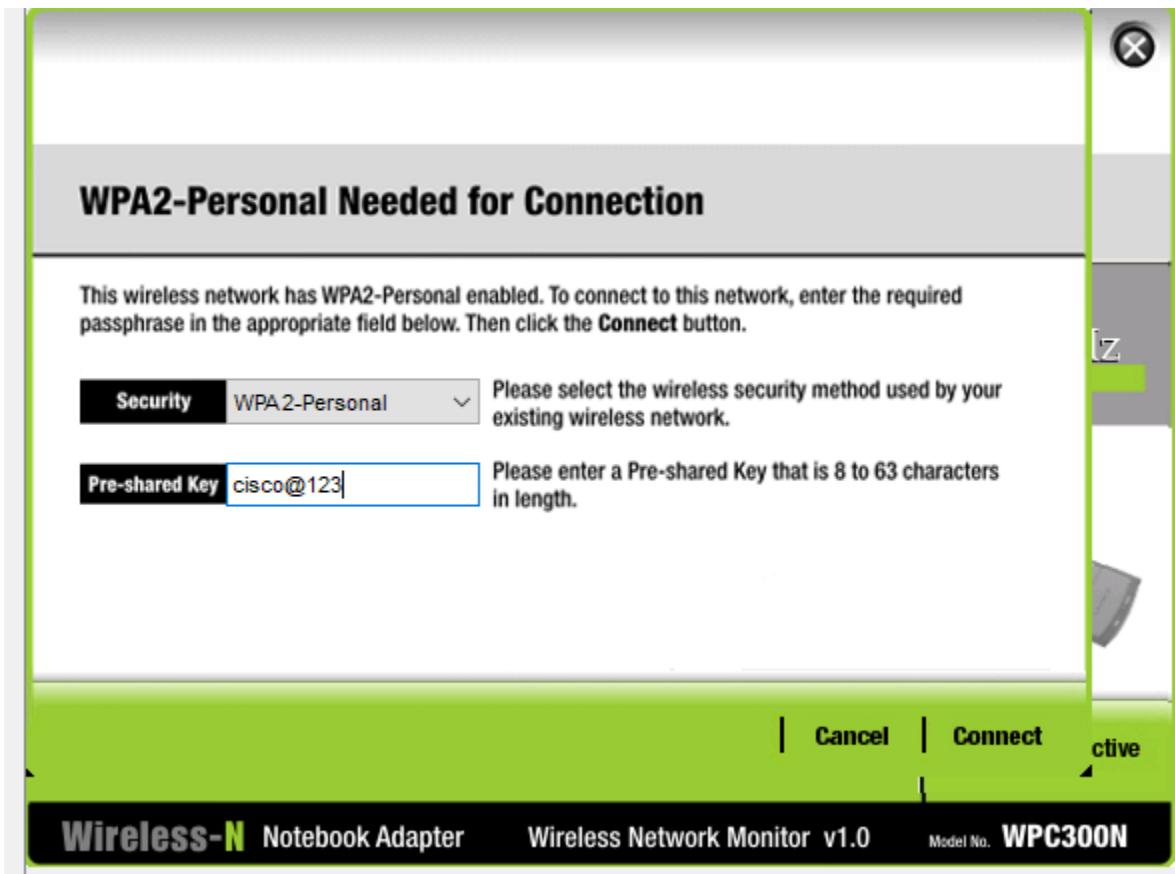
- Navigate to **PC Wireless** on LP1



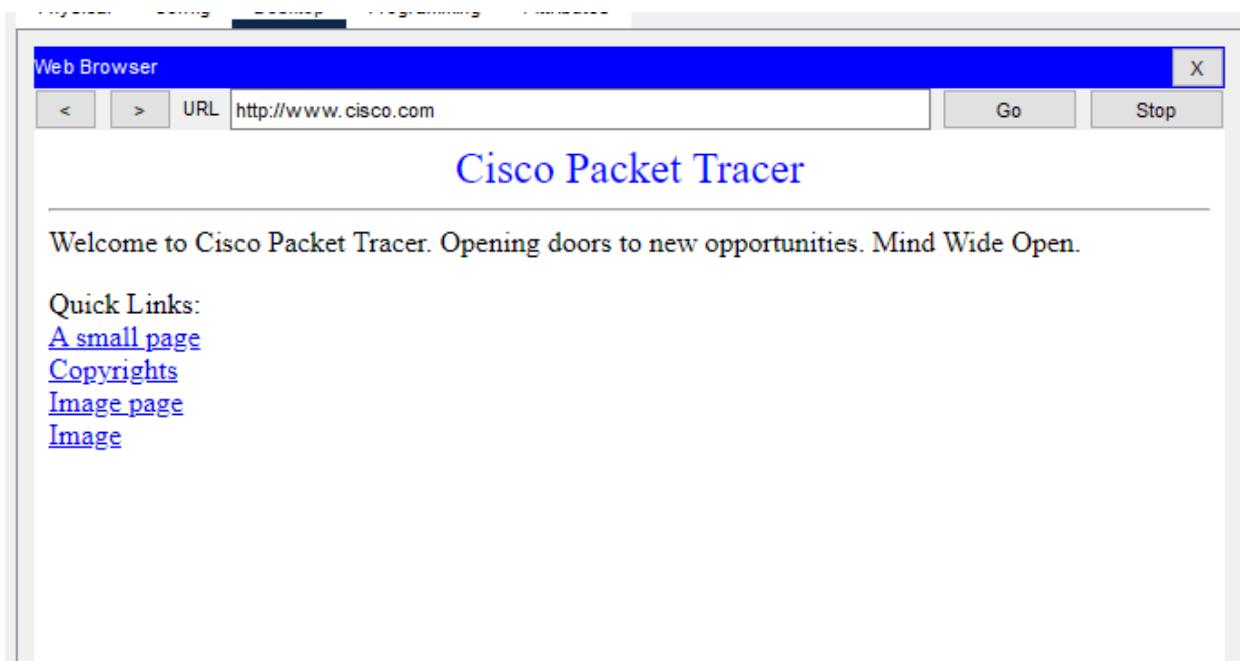
c. Select **Connect** tab and refresh as necessary, select the wireless network name **Home**



d. Enter passphrase and click connect.

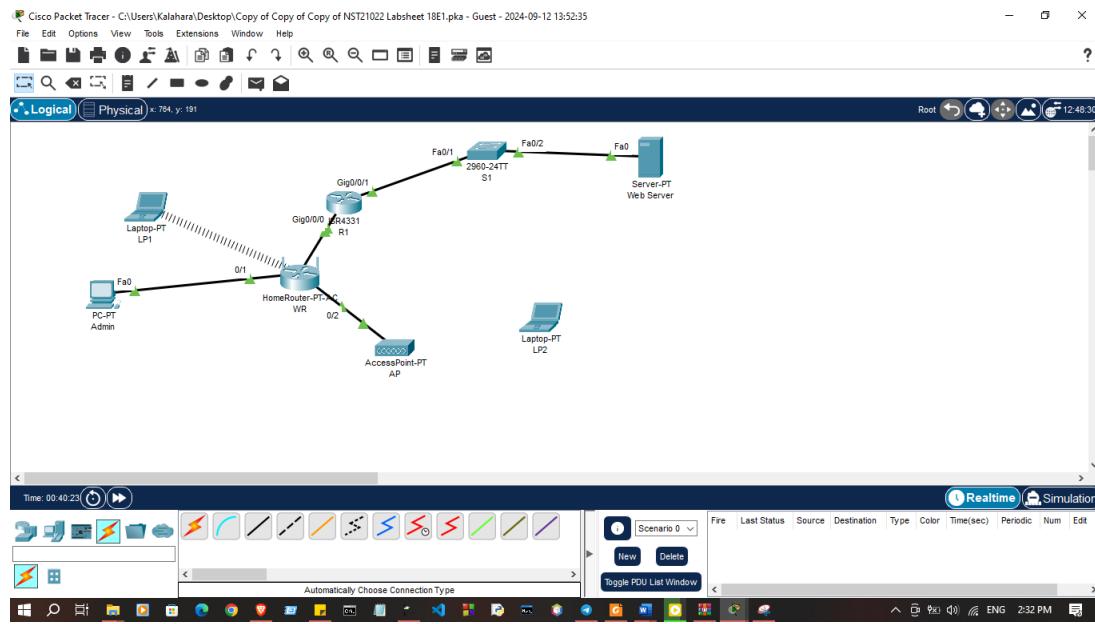


e. Open browser and try to access www.cisco.com

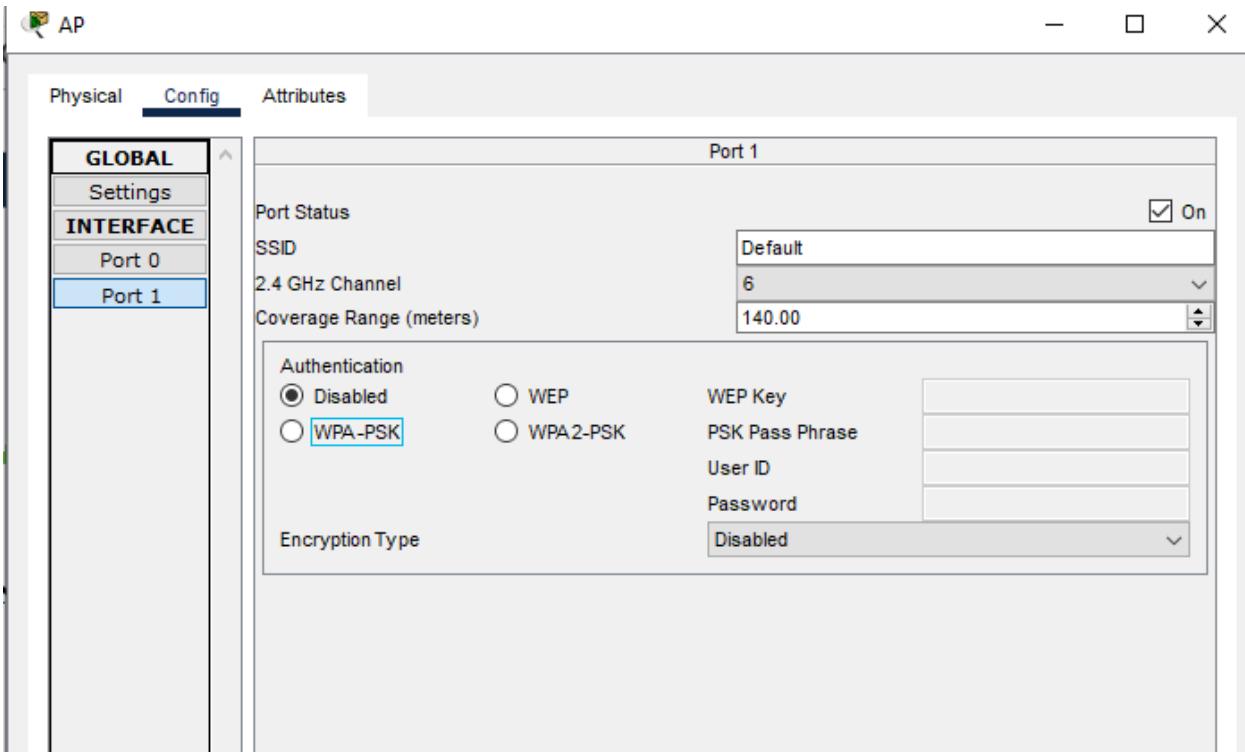


7. Connect wireless clients to an Access Point

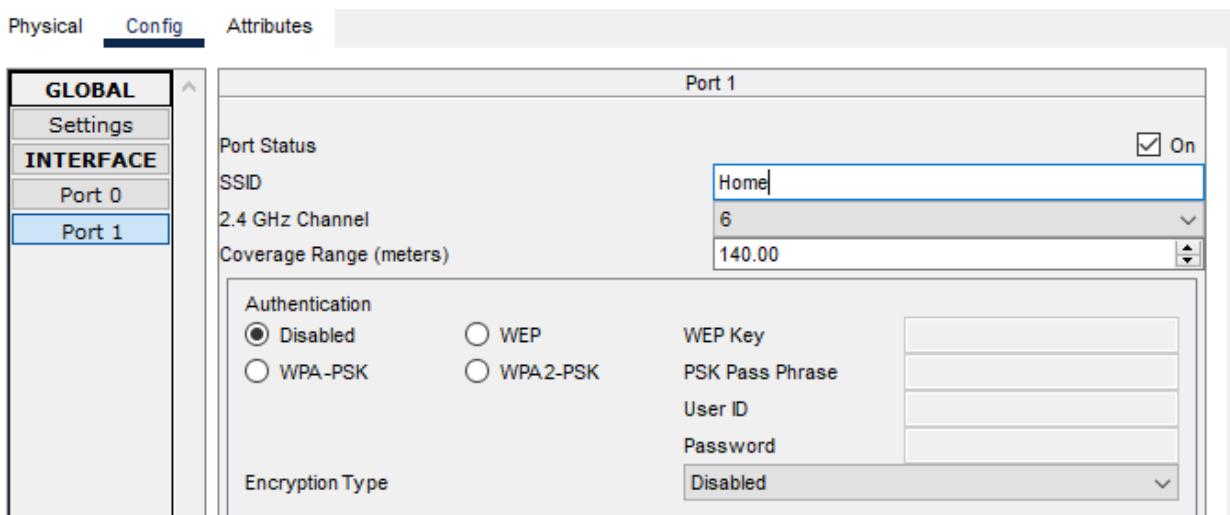
a. Connect Port 0 of AP with WR



b. In the **config** tab select **Port 1**



c. Enter SSID as **Home**



d. Keep **channel 1** if it is not change to **channel 1**

The screenshot shows the configuration interface for Port 1. The left sidebar lists 'GLOBAL', 'Settings', 'INTERFACE', 'Port 0', and 'Port 1'. The main panel is titled 'Port 1' and contains the following fields:

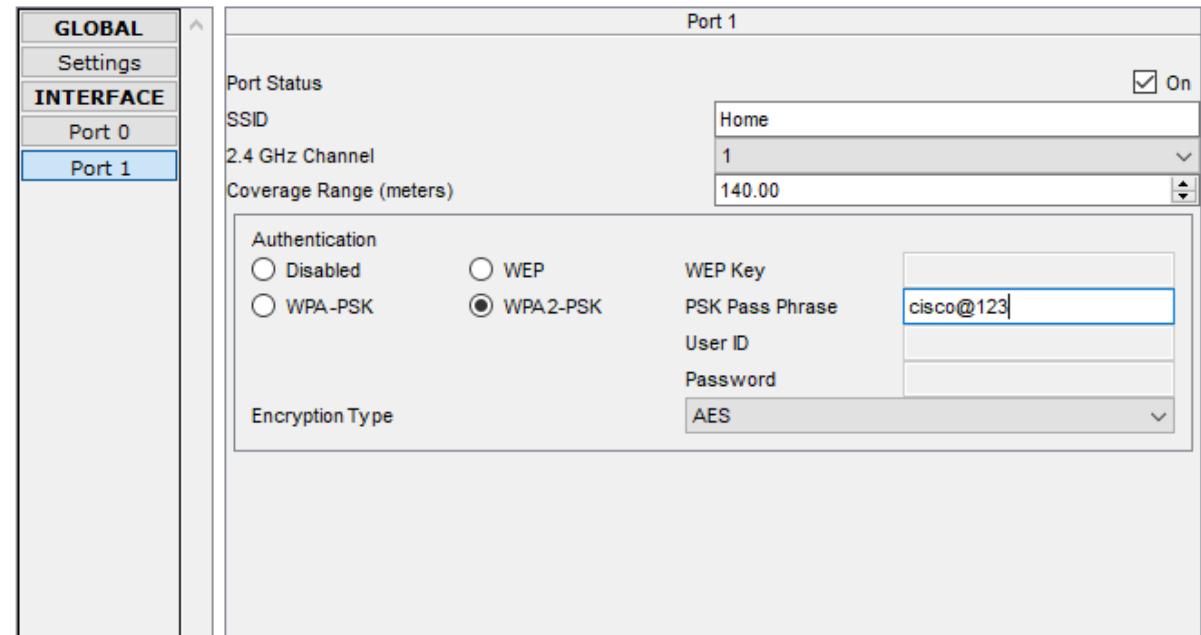
- Port Status:** On (checkbox checked)
- SSID:** Home
- 2.4 GHz Channel:** 1
- Coverage Range (meters):** 140.00
- Authentication:** Disabled, WEP, WPA-PSK
- Encryption Type:** Disabled
- WEP Key:** (empty field)
- PSK Pass Phrase:** (empty field)
- User ID:** (empty field)
- Password:** (empty field)

e. Select **WPA2-PSK** and enter the passphrase **cisco@123**

The screenshot shows the configuration interface for Port 1. The left sidebar lists 'GLOBAL', 'Settings', 'INTERFACE', 'Port 0', and 'Port 1'. The main panel is titled 'Port 1' and contains the following fields:

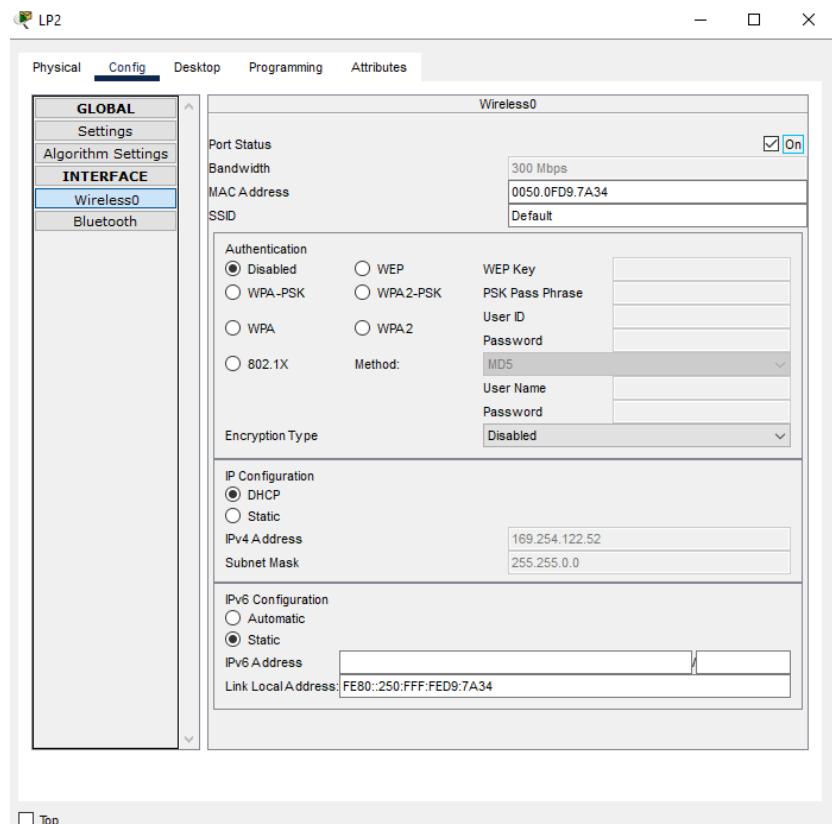
- Port Status:** On (checkbox checked)
- SSID:** Home
- 2.4 GHz Channel:** 1
- Coverage Range (meters):** 140.00
- Authentication:** Disabled, WEP, WPA2-PSK
- Encryption Type:** AES
- WEP Key:** (empty field)
- PSK Pass Phrase:** cisco@123
- User ID:** (empty field)
- Password:** (empty field)

f. Keep **AES** as the default encryption type.

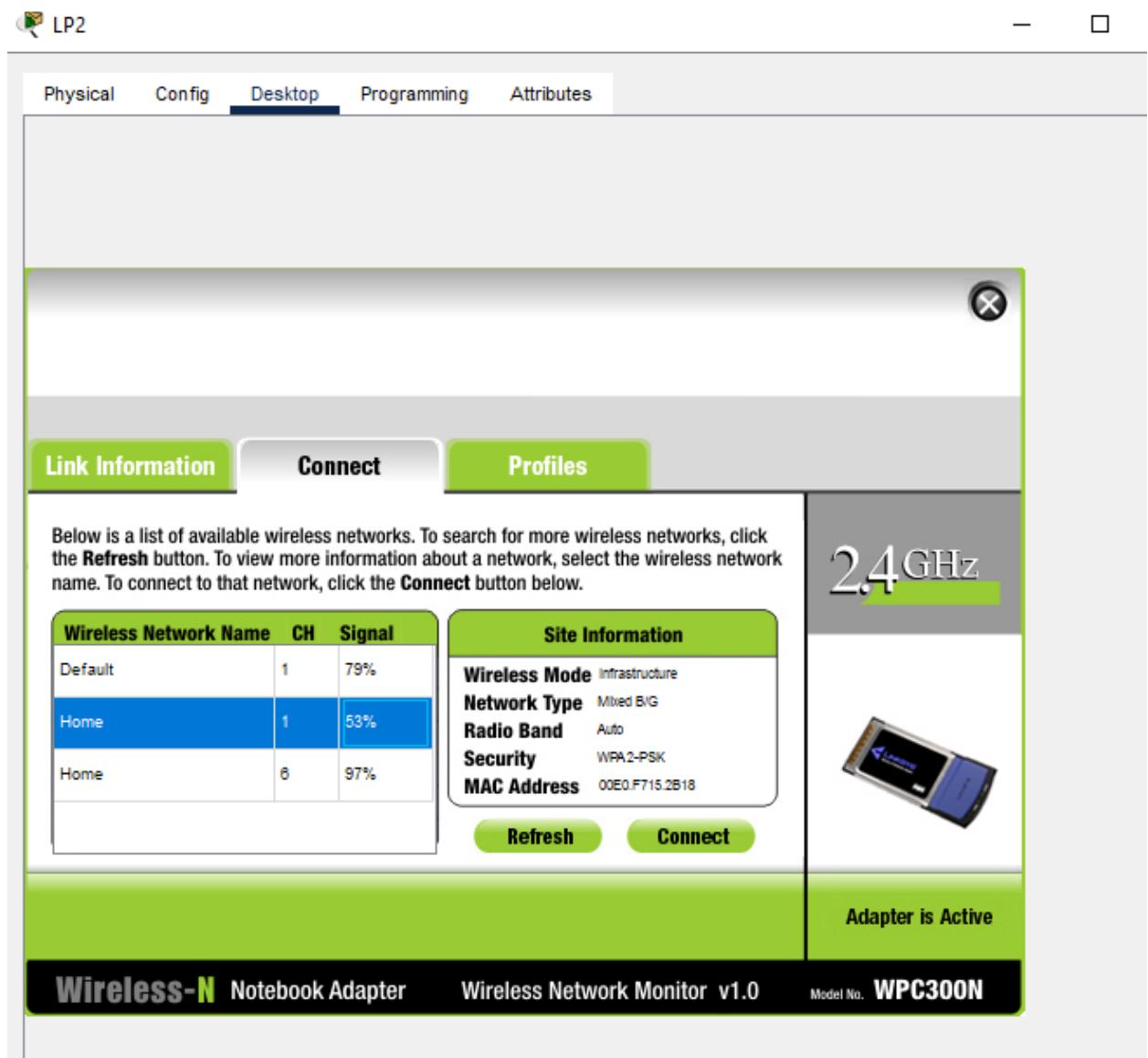


8. Connect the wireless clients

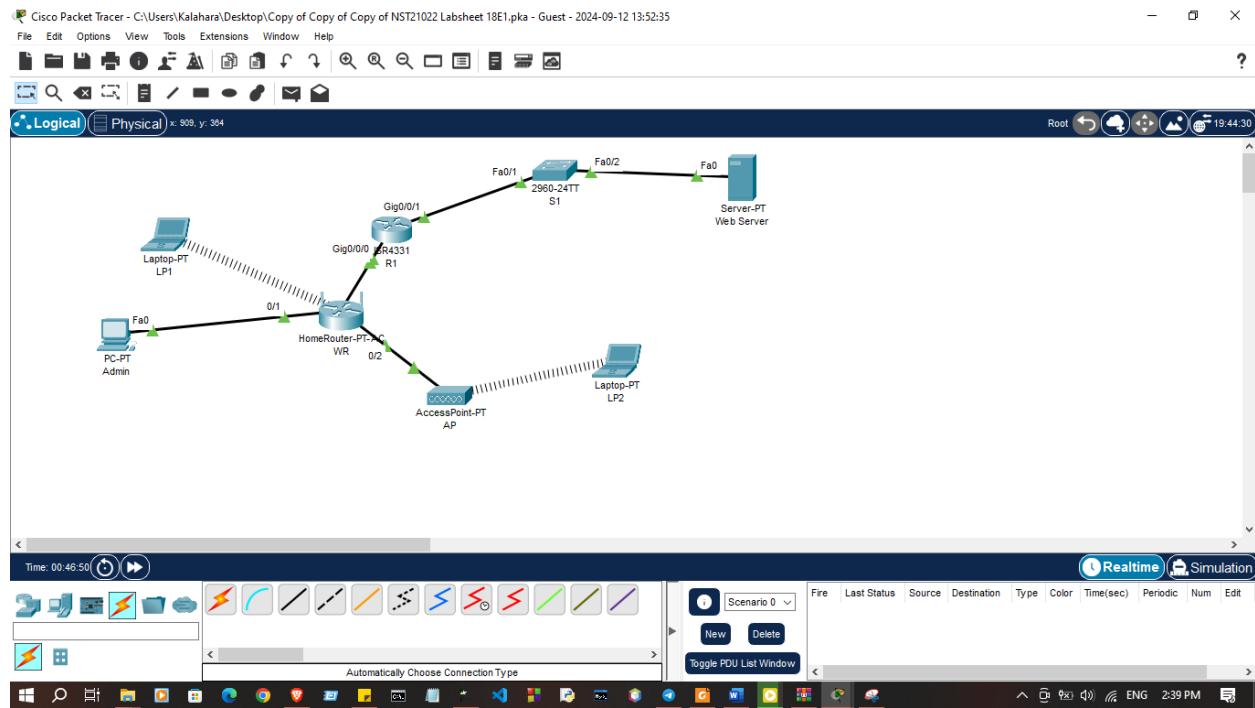
a. On **LP2** turn on wireless interface and go to **PC Wireless**



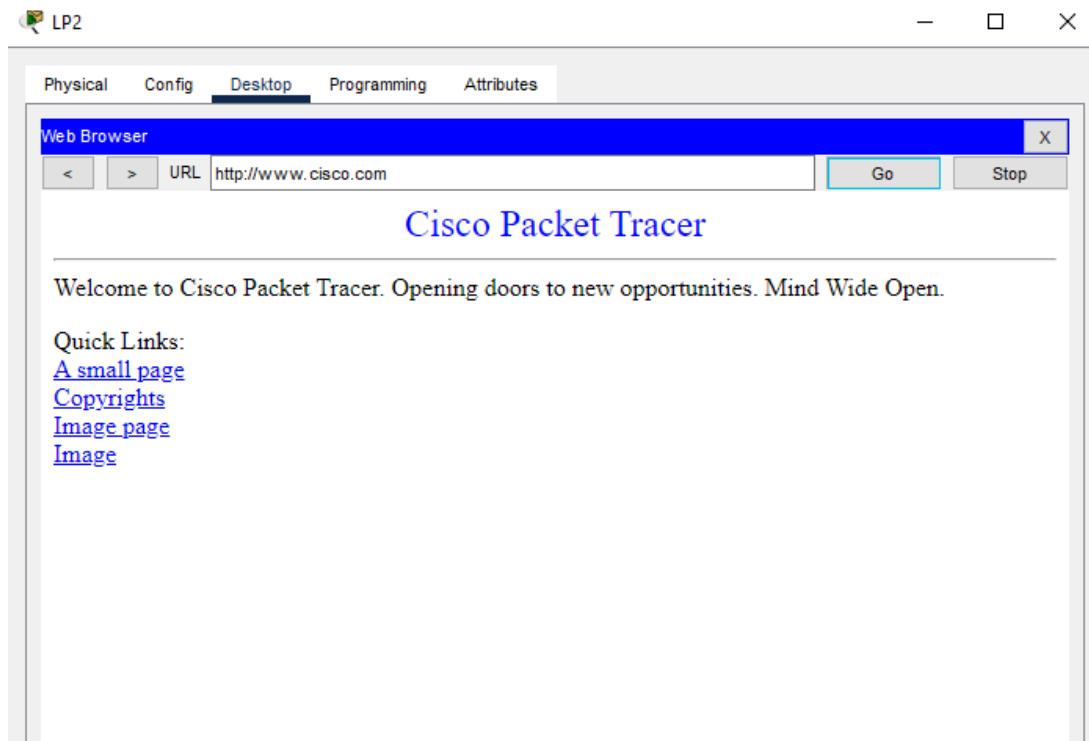
- b. Select **Connect** and refresh



c. Select **Home** with the strong single and connect

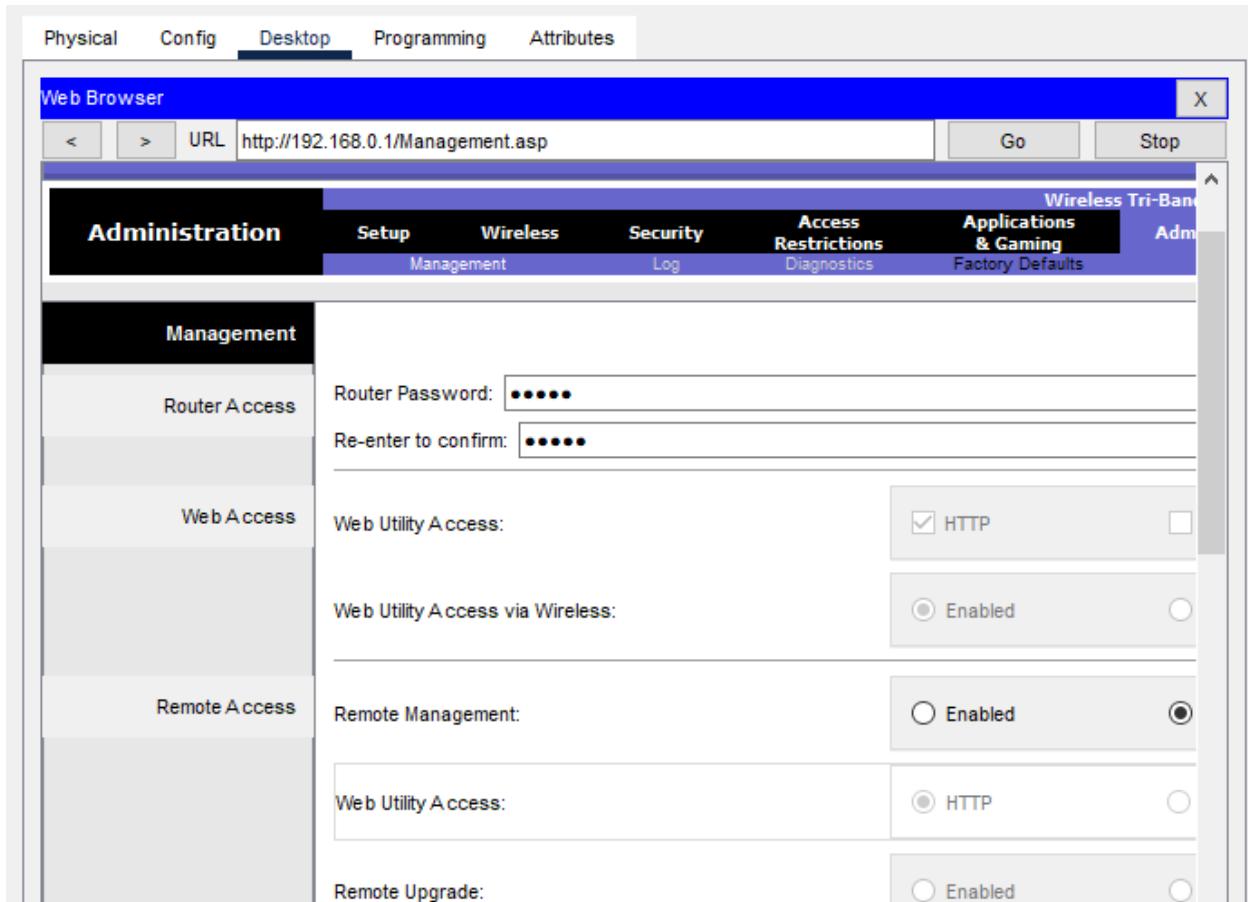


d. Open web browser and try to access www.cisco.com

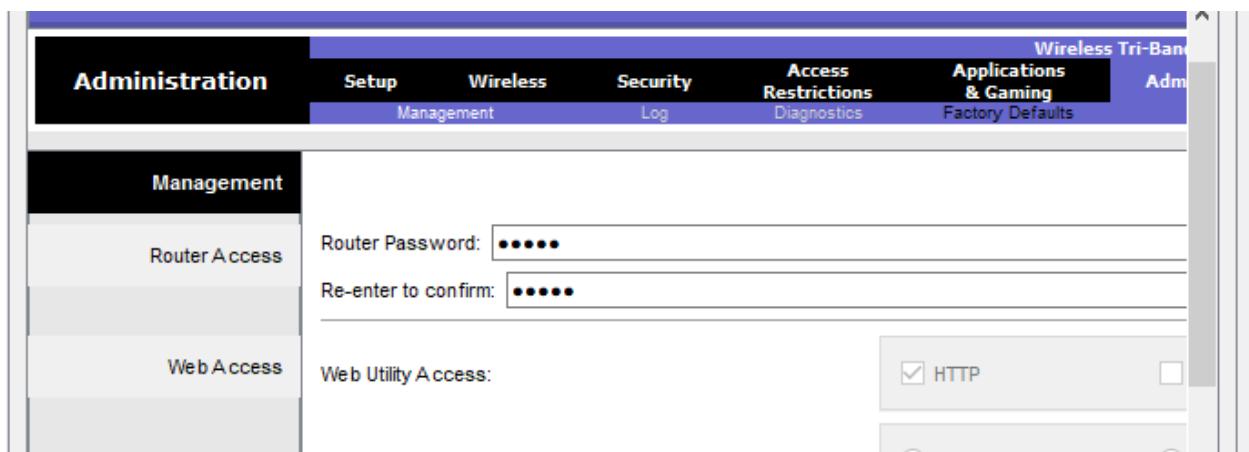


9. Change the WR access password

- Connect to the **WR** web interface



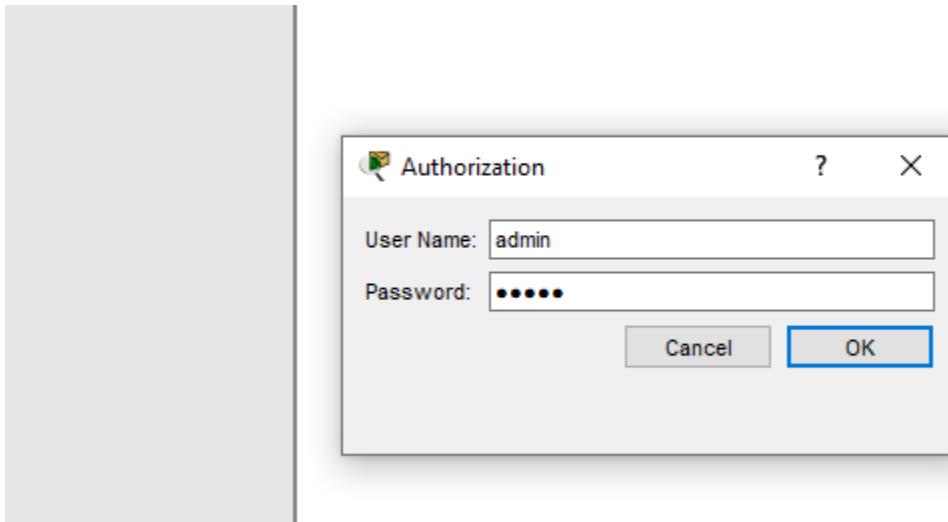
- Navigate to **Administration** → **Management** and change the current router password to **cisco**



c. Save Settings



- c. Use **admin** as the username and new password when prompted to log in to the wireless router.



10. Change the DHCP address range in WR

- a. Navigate to **Setup ➔ Basic Setup**



b. Scroll down the page to **Network Setup**

The screenshot shows the 'Network Setup' configuration page. On the left, there's a sidebar with 'Router IP' and 'DHCP Server Settings'. Under 'Router IP', the IP Address is set to 192.168.0.1 and the Subnet Mask is 255.255.255.0. Under 'DHCP Server Settings', the DHCP Server is enabled (radio button selected), with a Start IP Address of 192.168.0.100, a Maximum number of Users set to 50, and an IP Address Range of 192.168.0.100 - 149.

c. Change **Router IP** to **192.168.20.1**

The screenshot shows the 'Router IP' configuration page. The IP Address is now set to 192.168.20.1, and the Subnet Mask is 255.255.255.0. Below the fields, there are tabs for 'DHCP' and 'Static'.

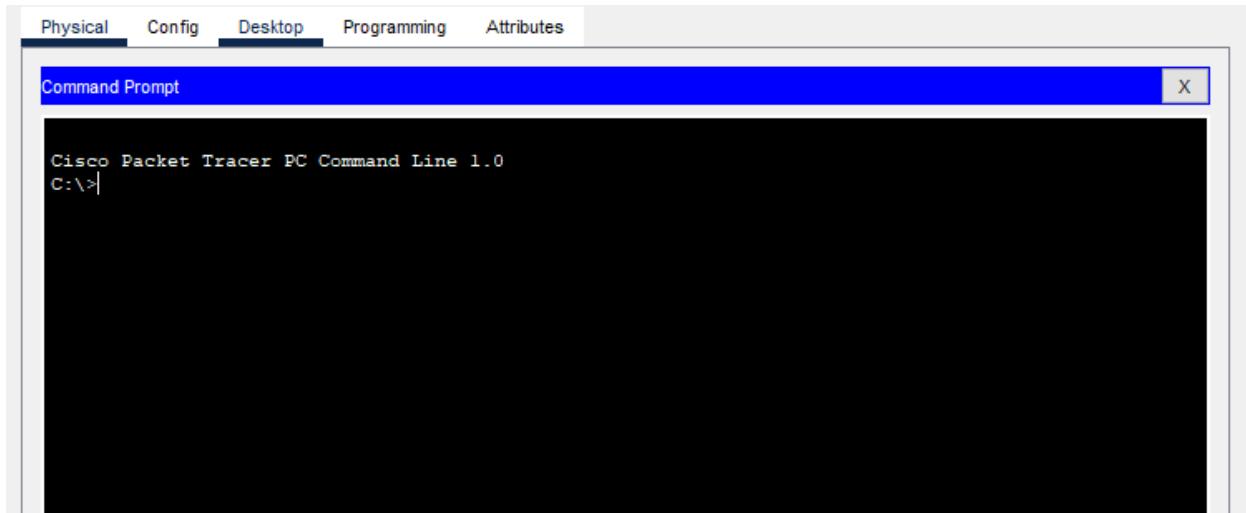
d. Add **10.1.1.10** as the **DNS Server** with the **DHCP** settings

The screenshot shows the 'DHCP' settings page. It includes fields for Client Lease Time (set to 0 minutes), Static DNS 1 (10.1.1.10), and Static DNS 2 (10.1.1.0).

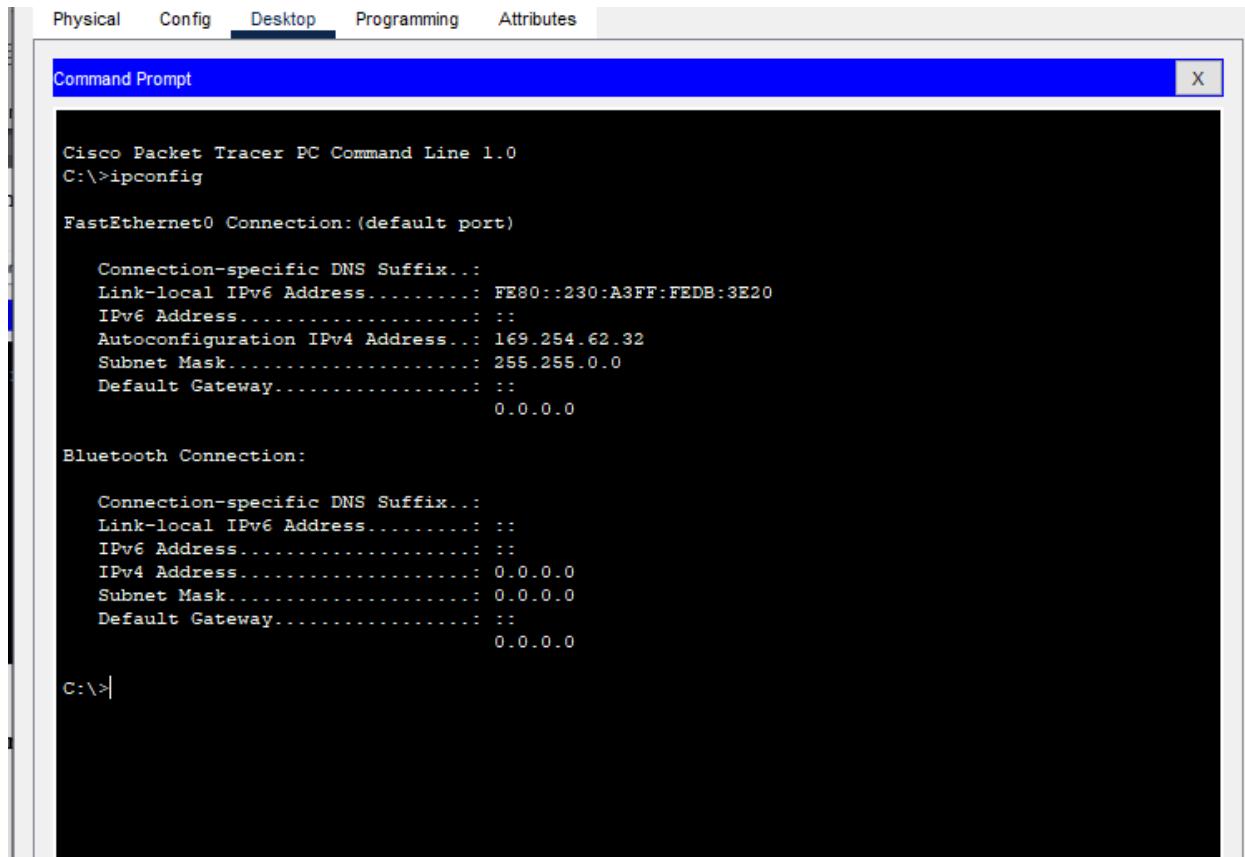
e. **Save Settings**

The screenshot shows the bottom navigation bar of the web interface. It features two buttons: 'Save Settings' and 'Cancel Changes'.

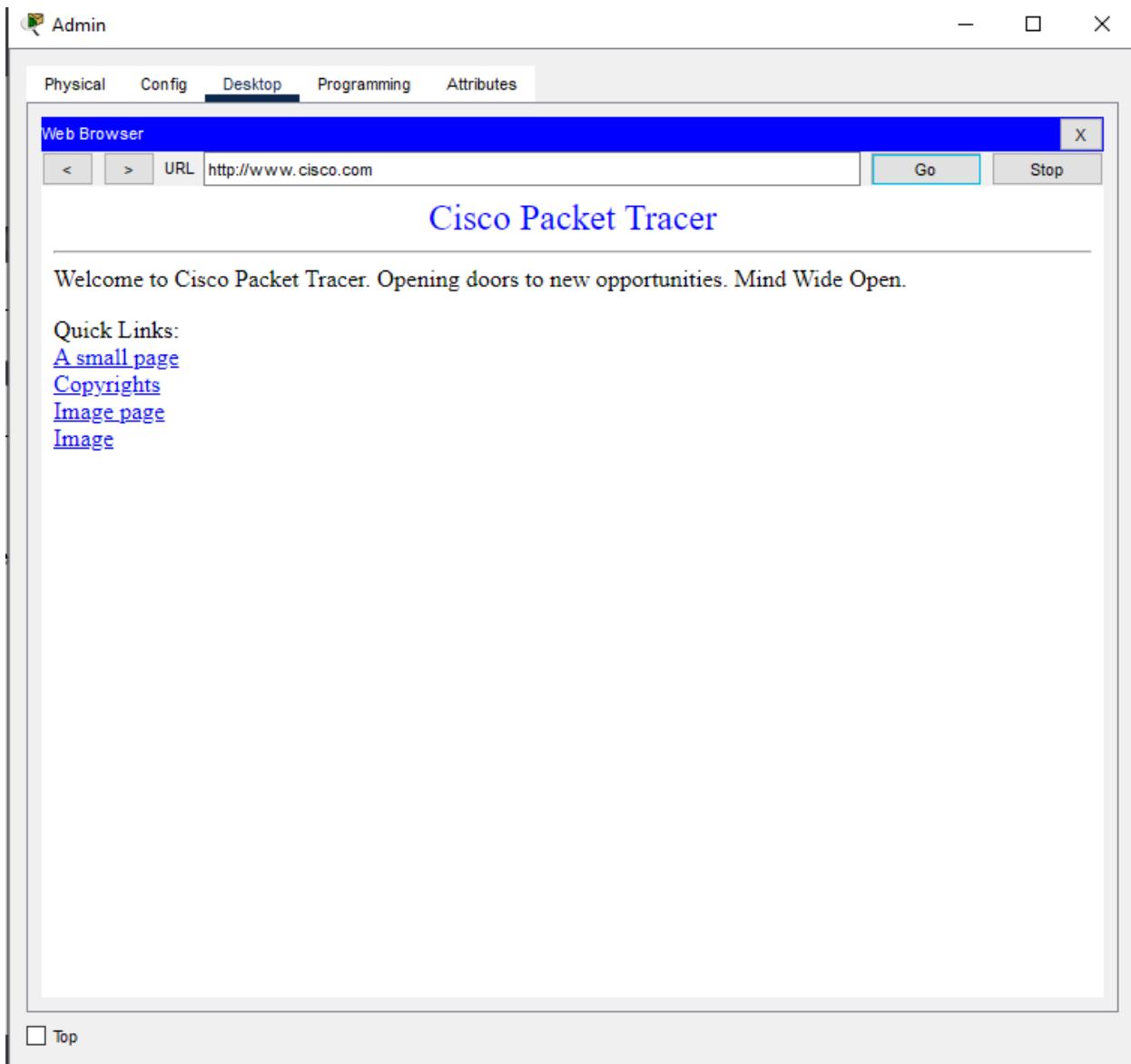
f. Navigate to Admin PC's **Command Prompt**



g. Type **ipconfig /renew** to force Admin to re-acquire its IP information via DHCP



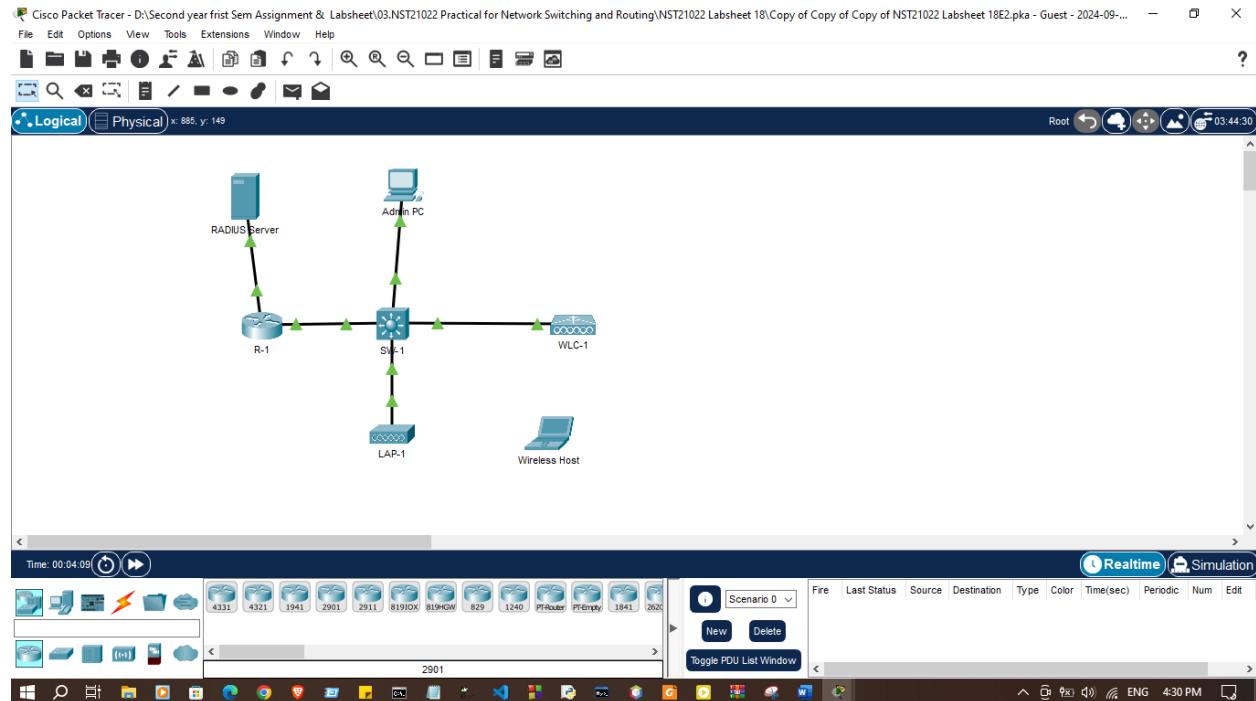
h. Verify that you can still navigate to www.cisco.com



Exercise 02:

Configure a WPA2 Enterprise WLAN on the WLC

Use “NST21022 Lab sheet 18E2.pka” file



Addressing Table

Device	Interface	IP Address
R1	G0/0/0.5	192.168.5.1/24
	G0/0/0.200	192.168.200.1/24
	G0/0/1	172.31.1.1/24
SW1	VLAN 200	192.168.200.100/24
LAP-1	G0	DHCP
WLC-1	Management	192.168.200.254/24
RADIUS/SNMP Server	NIC	172.31.1.254/24
Admin PC	NIC	192.168.200.200/24

Part 1: Create a new WLAN

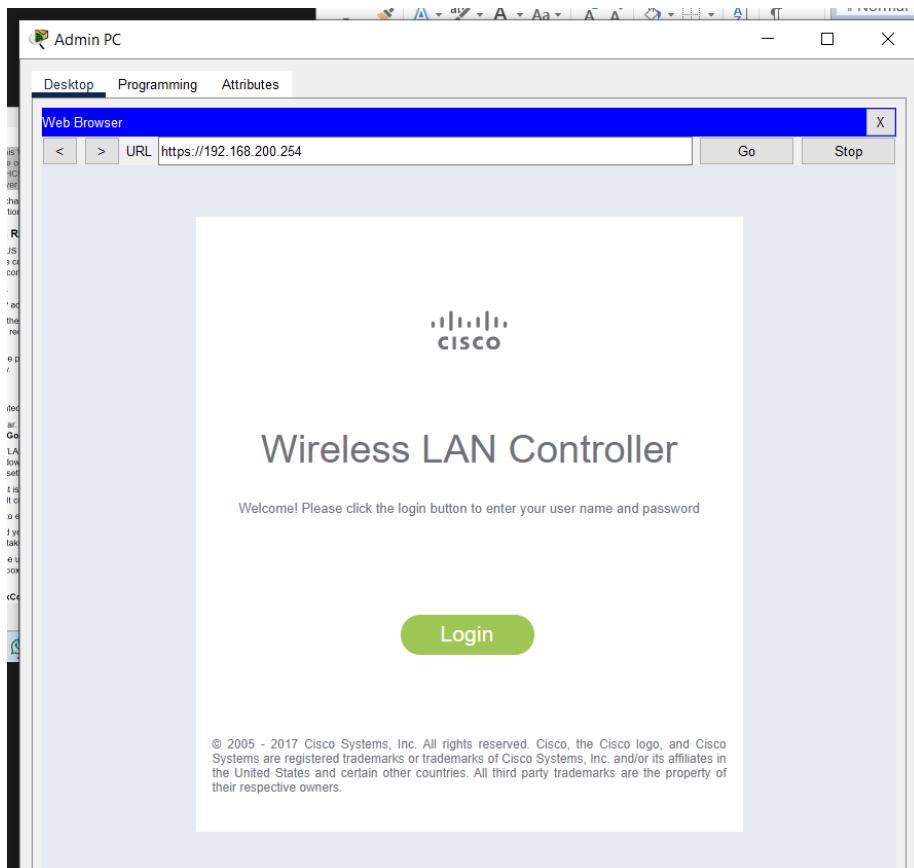
Step 1: Create a new VLAN interface.

Each WLAN requires a virtual interface on the WLC. These interfaces are known as dynamic interfaces.

The virtual interface is assigned a VLAN ID and traffic that uses the interface will be tagged as VLAN traffic. This is why connections between the

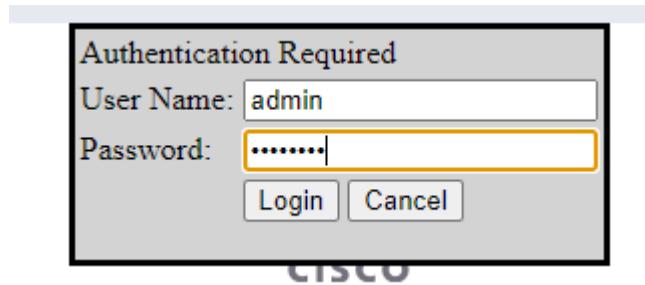
APs, the WLC, and the router are over trunk ports. For the traffic from multiple WLANs to be transported through the network, traffic for the WLAN VLANs must be trunked.

1. Open the browser from the desktop of Admin PC. Connect to the IP address of the WLC over HTTPS.



http → https change

2. Login with the username **admin** and password **Cisco123**.

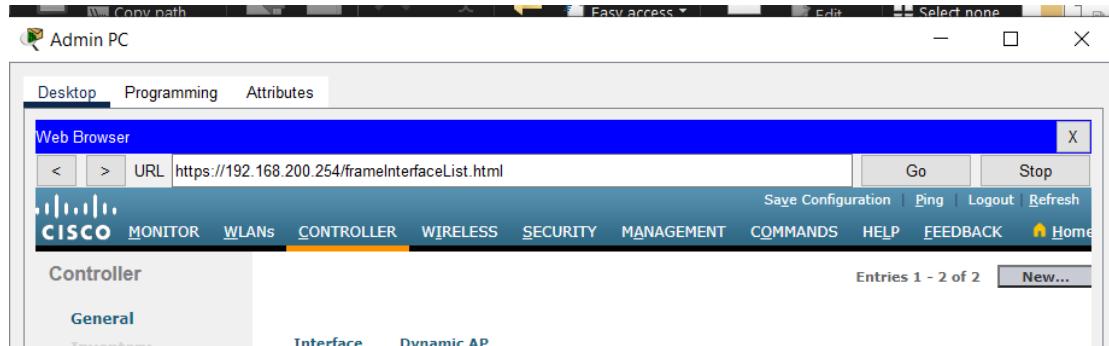


3. Click the **Controller** menu and then click **Interfaces** from the menu on the left. You will see the default virtual interface and the management interface to which you are connected.

A screenshot of the Cisco Web UI. The title bar says 'Admin PC'. The navigation bar includes 'Desktop', 'Programming', and 'Attributes'. The main menu has items like 'Web Browser', 'Say Configuration', 'Ping', 'Logout', and 'Refresh'. The top navigation bar has links for 'CISCO', 'MONITOR', 'WLANS', 'CONTROLLER' (which is highlighted), 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. On the left, a sidebar menu under 'Controller' includes 'General', 'Inventory', 'Interfaces' (which is selected and highlighted in blue), 'Interface Groups', 'Multicast', and several expanded sections: 'Internal DHCP Server', 'Mobility Management', 'Ports', 'NTP', 'CDP', 'Tunneling', 'IPv6', 'mDNS', and 'Advanced'. The main content area is titled 'Interfaces' and shows a table with two rows:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic Manage
management	1	192.168.200.254	Static	Enabled
virtual	N/A	192.0.2.1	Static	Not Supp

4. Click the **New** button in the upper right-hand corner of the page. You may need to scroll the page to the right to see it.



5. Enter the name of the new interface. We will call it **WLAN-5**. Configure the **VLAN ID** as **5**. This is the VLAN that will carry traffic for the WLAN that we create later. Click **Apply**. This leads to a configuration screen for the VLAN interface.



6. First, configure the interface to use physical port number **1**. Multiple VLAN interfaces can use the same physical port because the physical interfaces are like dedicated trunk ports.

Physical Information

Port Number	<input type="text" value="1"/>
Backup Port	<input type="text" value="0"/>
Active Port	0
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	<input type="text" value="5"/>
-----------------	--------------------------------

7. Address the interface as follows:

IP Address: 192.168.5.254

Netmask: 255.255.255.0

Gateway: 192.168.5.1

Primary DHCP server: 192.168.5.1

Server Management

Interface Address

VLAN Identifier	<input type="text" value="5"/>
IP Address	<input type="text" value="192.168.5.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.5.1"/>

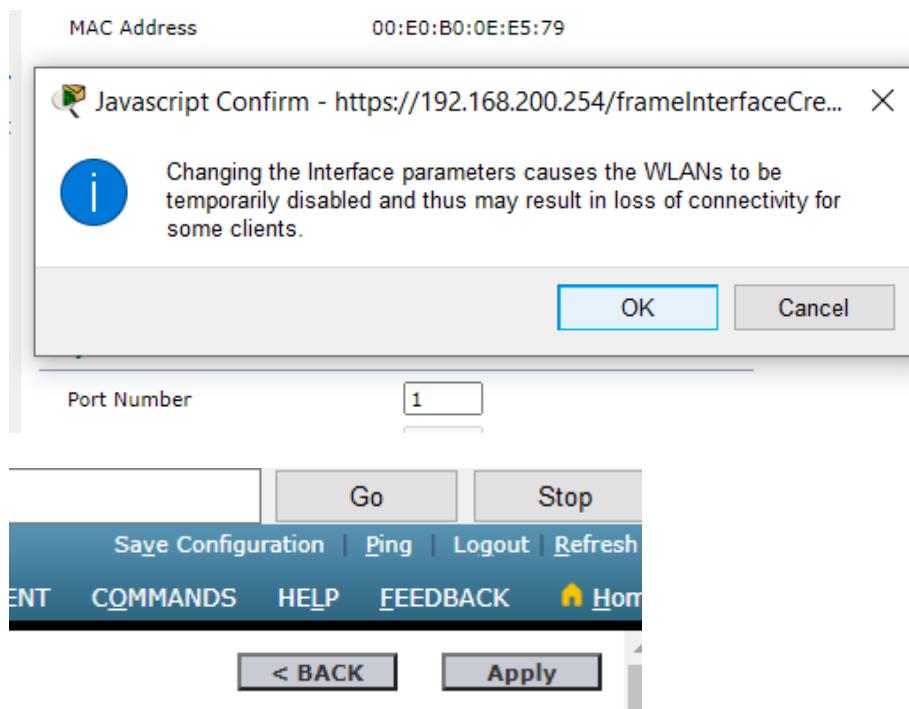
DHCP Information

Primary DHCP Server	<input type="text" value="192.168.5.1"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="text" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

User traffic for the WLAN that uses this VLAN interface will be on the 192.168.5.0/24 network. The default gateway is the address of an interface on router R-1. A DHCP pool has been configured on the router. The address that we configure here for DHCP tells the WLC to forward all DHCP requests that it receives from hosts on the WLAN to the DHCP server on the router.

8. Be sure to click **Apply** to enact your changes and click **OK** to respond to the warning message.

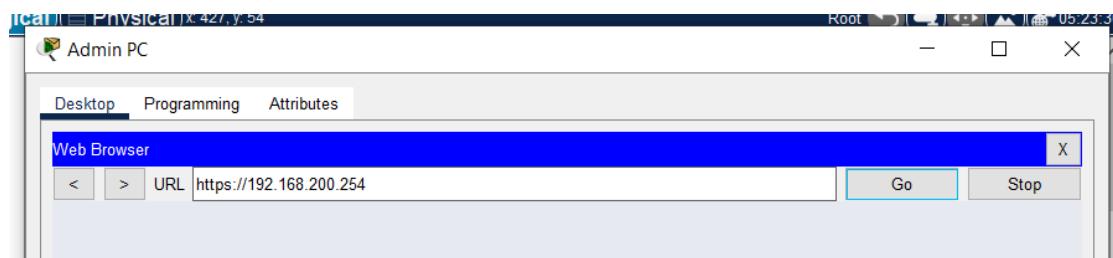
Click **Save Configuration** so that your configuration will be in effect when the WLC restarts.



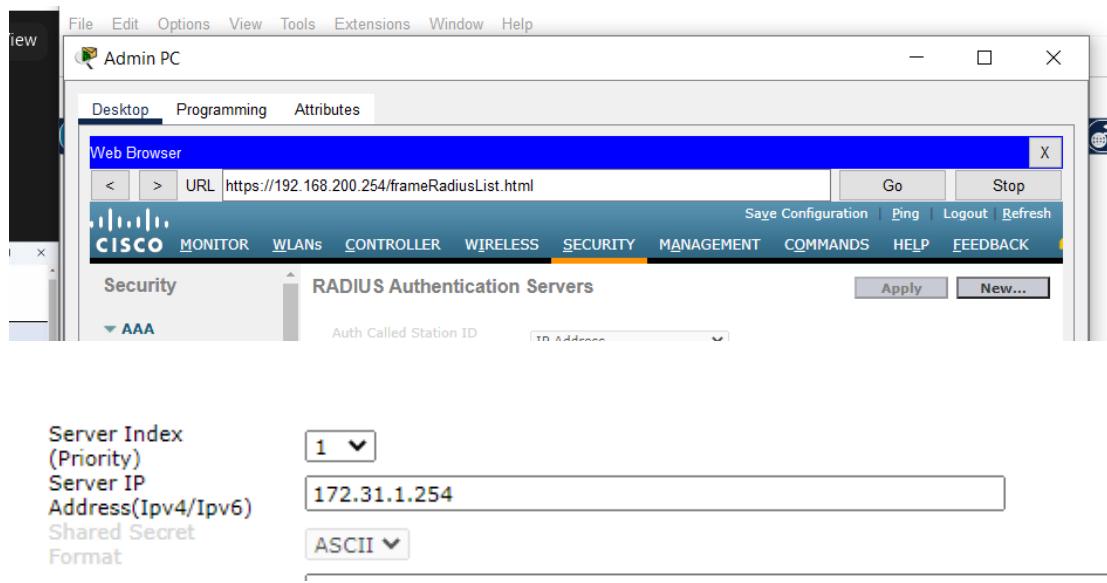
Step 2: Configure the WLC to use a RADIUS server.

WPA2-Enterprise uses an external RADIUS server to authenticate WLAN users. Individual user accounts with unique usernames and passwords can be configured on the RADIUS server. Before the WLC can use the services of the RADIUS server, the WLC must be configured with the server address.

1. Click the **Security** menu on the WLC.



2. Click the **New** button and enter the IP address of the RADIUS server in the

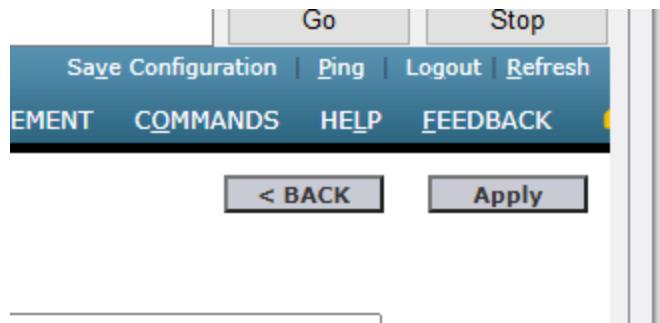


Server IP Address field.

3. The RADIUS server will authenticate the WLC before it will allow the WLC to access the user account information that is on the server. This requires a shared secret value. Use **Cisco123**. Confirm the shared secret and click **Apply**.

The screenshot shows the "Format" section of the RADIUS configuration. It includes fields for "Shared Secret" containing "*****" and "Confirm Shared Secret" also containing "*****". The "Confirm Shared Secret" field is highlighted with a yellow border.

Note: It is not a good practice to reuse passwords. This activity reuses passwords only to make the activity easier for you to complete and review.



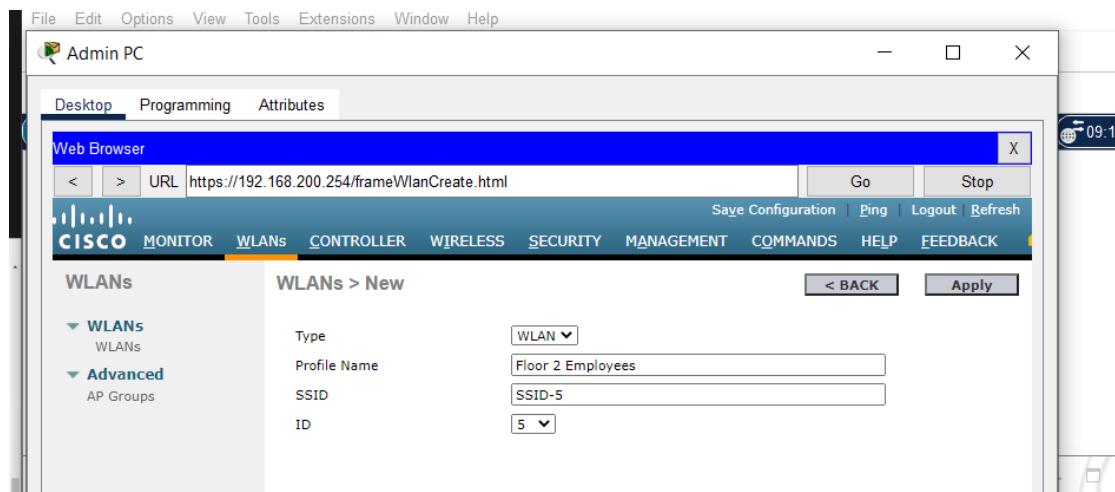
Step 3: Create a new WLAN.

Create a New WLAN. Use the newly created VLAN interface for the new WLAN.

1. Click the **WLANS** entry in the menu bar. Locate the dropdown box in the upper right-hand corner of the WLANS screen. It will say **Create New**. Click **Go** to create a new WLAN.

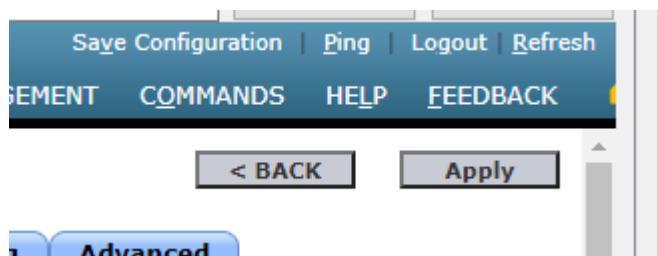


2. Enter the **Profile Name** of the new WLAN. Use the profile name **Floor 2 Employees**. Assign an SSID of **SSID-5** to the WLAN. Change the ID drop down to **5**. Hosts will need to use this SSID to join the network. When you are done, click **Apply** to accept your settings.



Note: The ID is an arbitrary value that is used as a label for the WLAN. In this case, we configured it as 5 to be consistent with VLAN for the WLAN. It could be any available value.

3. Click **Apply** so that the settings go into effect.



4. Now that the WLAN has been created you can configure features of the network. Click **Enabled** to make the WLAN functional. It is a common mistake to accidentally skip this step.

General Security QoS Policy-Mapping Advanced

Profile Name	Floor 2 Employees
Type	WLAN
SSID	SSID-5
Status	<input checked="" type="checkbox"/> Enabled

5. Choose the VLAN interface that will be used for the new WLAN. The WLC will use this interface for user traffic on the network. Click the drop-down box for Interface/Interface Group (G). Select the interface that we created in Step 1.

Radio Policy	All
Interface/Interface Group(G)	WLAN-5
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	

6. Go to the Advanced tab. Scroll to **FlexConnect** section of the interface.

- Click to enable **FlexConnect Local Switching** and **FlexConnect Local Auth**.

- Click **Apply** to enable the new WLAN. If you forget to do this, the WLAN will not operate.

Step 4: Configure WLAN security.

Instead of WPA2-PSK, we will configure the new WLAN to use WPA2-Enterprise.

- Click the WLAN ID of the newly created WLAN to continue configuring it, if necessary.



2. Click the Security tab. Under the Layer 2 tab, select **WPA+WPA2** from the dropdown box.

The screenshot shows the Cisco WebUI interface for managing WLANs. The URL in the browser is <https://192.168.200.254/frameWlanEdit.html>. The navigation bar includes Admin PC, Desktop, Programming, Attributes, and tabs for MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The main window displays 'WLANS' and 'WLANs > Edit 'Floor 2 Employees''. The 'Security' tab is active. Under the 'Layer 2' tab, the 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. Other options shown include 'MAC Filtering' (unchecked) and 'Protected Management Frame' (PMF, Disabled). Under 'WPA+WPA2 Parameters', both 'WPA Policy' and 'WPA2 Policy' checkboxes are unchecked. In the 'Authentication Key Management' section, '802.1X' has its 'Enable' checkbox checked, while 'CCKM' has its 'Enable' checkbox unchecked.

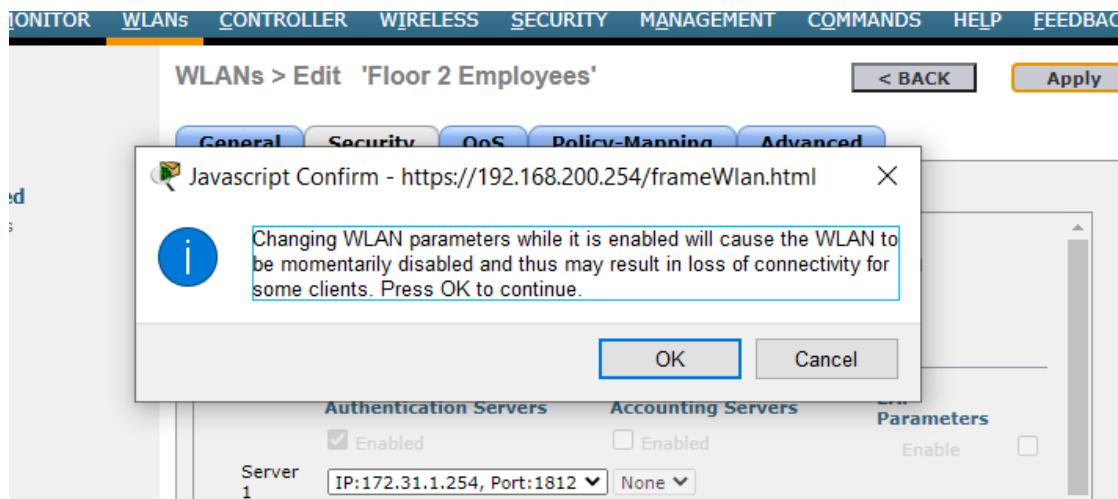
3. Under WPA+WPA2 Parameters, enable **WPA2 Policy**. Click **802.1X** under Authentication Key Management. This tells the WLC to use the 802.1X protocol to authenticate users externally.

The screenshot shows the configuration interface for a WLAN. The top navigation bar has tabs for 'Layer 2', 'Layer 3' (which is selected), and 'AAA Servers'. Under 'Layer 3', the 'Protected Management Frame' section has 'PMF' set to 'Disabled'. The 'WPA+WPA2 Parameters' section includes 'WPA Policy' (checked), 'WPA Encryption' (AES checked, TKIP unchecked), and 'WPA2 Policy' (unchecked). The 'Authentication Key Management' section shows '802.1X' enabled, 'CCKM' and 'PSK' disabled. A 'WPA gtk-randomize State' dropdown is set to 'Disable'.

4. Click the **AAA Servers** tab. Open the drop-down next to Server 1 in the Authentication Servers column and select the server that we configured in Step 2.

The screenshot shows the 'AAA Servers' tab configuration. The top navigation bar has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced' (selected). Under 'Advanced', the 'Radius Servers' section allows overriding default servers. It shows 'Authentication Servers' for 'Server 1' with IP:172.31.1.254, Port:1812 selected, and 'Accounting Servers' and 'EAP Parameters' both disabled. There are also fields for 'Server 2' and 'Server 3'.

5. Click **Apply** to enact this configuration. You have now configured the WLC to use the RADIUS sever to authenticate users that attempt to connect to the WLAN.

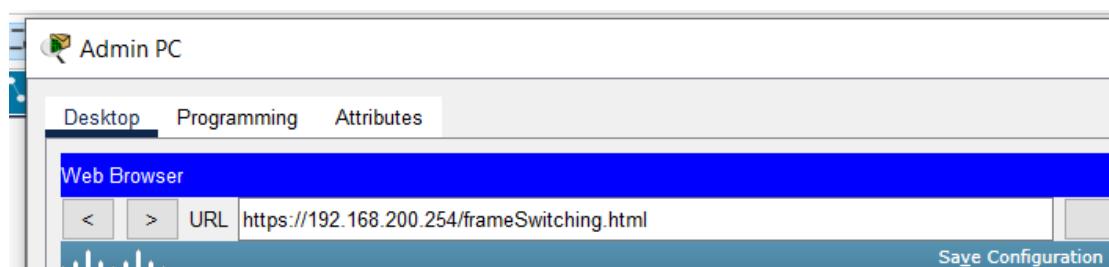


Part 2: Configure a DHCP Scope and SNMP Step 1:

Configure a DHCP Scope.

The WLC offers its own internal DHCP server. Cisco recommends that the WLAN DHCP server not be used for high-volume DHCP services, such as that required by larger user WLANs. However, in smaller networks, the DHCP server can be used to provide IP addresses to LAPs that are connected to the wired management network.

1. Should be connected to the WLC GUI from Admin PC.



2. Click the **Controller** menu and then click **Interfaces**.

:o Packet Tracer - E:\Campus Lecture\Subject\2nd Year\1 st SEMESTER\NST 21022 Practical for Network Swit...

The screenshot shows a Cisco Controller interface window titled "Admin PC". The URL in the browser is <https://192.168.200.254/frameInterfaceList.html>. The navigation bar includes "Desktop", "Programming", "Attributes", "Web Browser", "Save Configuration", and tabs for "CISCO", "MONITOR", "WLANS", "CONTROLLER" (which is selected), "WIRELESS", "SECURITY", "MANAGEMENT", and "COMMANDS". On the left, a sidebar under "Controller" has links for "General", "Inventory", "Interfaces" (which is selected), "Interface Groups", "Multicast", and "Internal DHCP Server". The main content area is titled "Interfaces" and displays a table:

Interface Name	VLAN Identifier	IP Address
WLAN-5	5	192.168.5.254
management	1	192.168.200.254
virtual	N/A	192.0.2.1

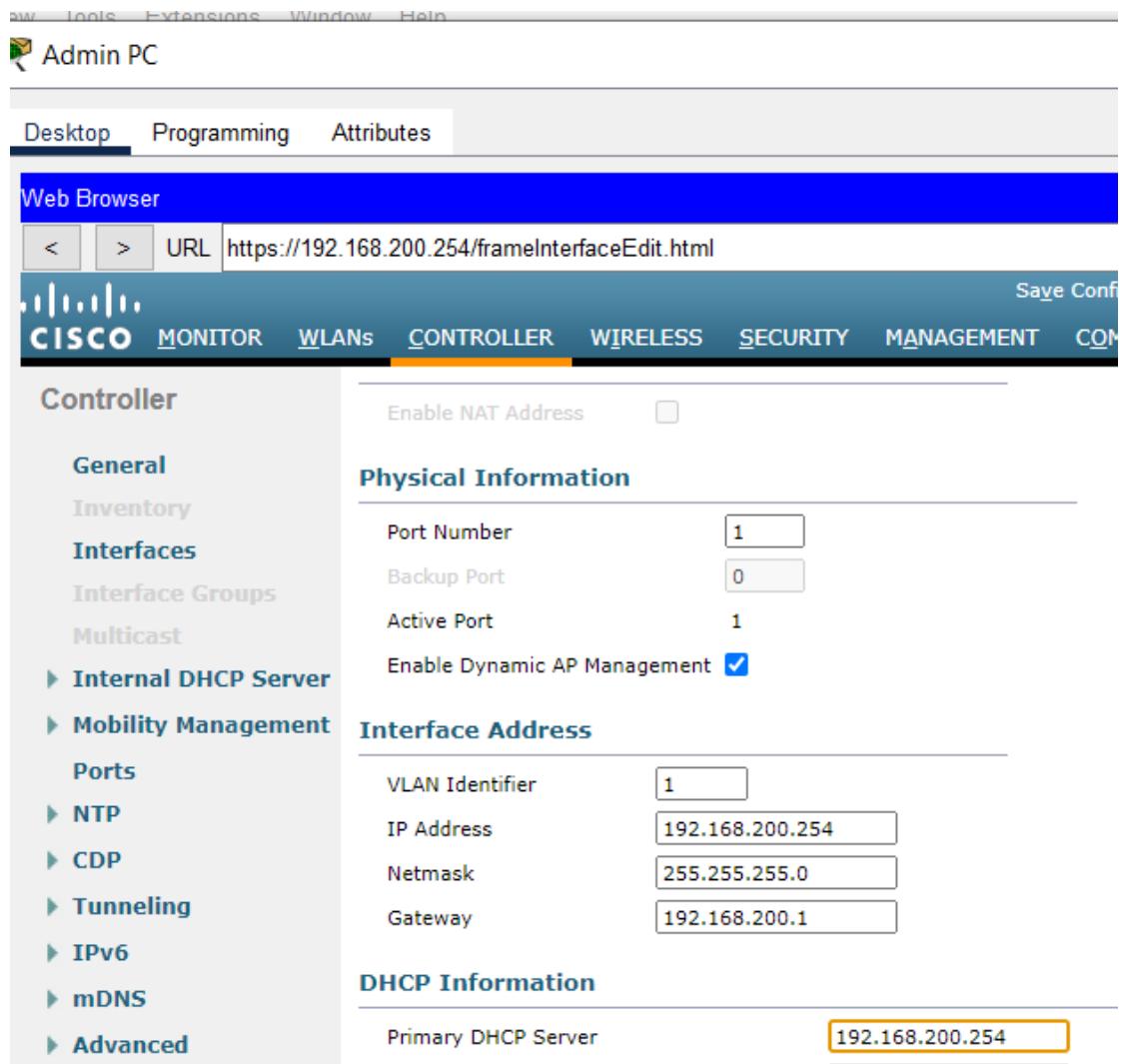
3. Click the **management** Interface. Record its addressing information here.

IP address:

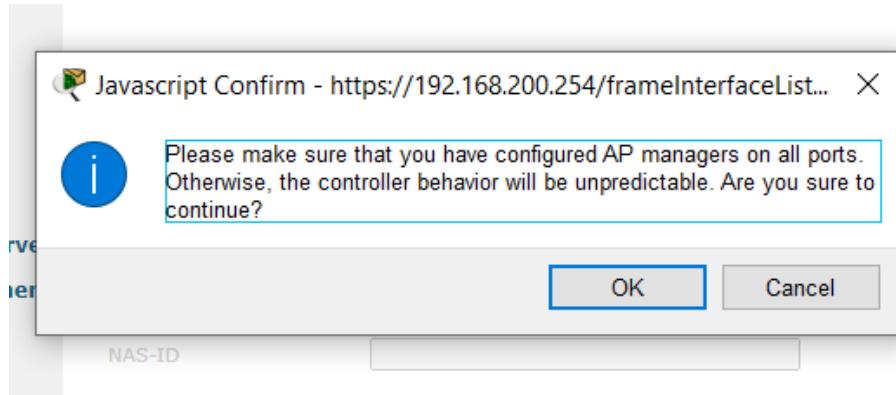
Netmask:

Gateway:

Primary DHCP server:



4. We want the WLC to use its own DHCP sever to provide addressing to devices on the wireless management network, such as lightweight APs. For this reason, enter the IP address of the WLC management interface as the primary DHCP server address. Click **Apply**. Click **OK** to acknowledge any warning messages that appear.

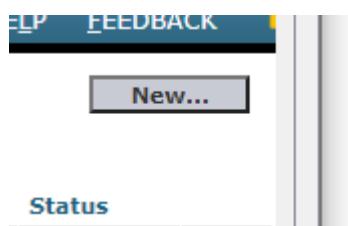


5. In the left-hand menu, expand the **Internal DHCP Server** section. Click **DHCP Scope**.

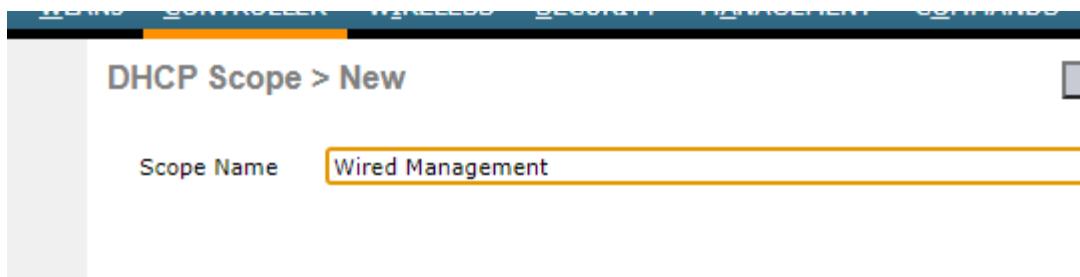
A screenshot of the Cisco Wireless Local Controller (WLC) interface. The top navigation bar includes links for MONITOR, WIANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar under the "Controller" heading has several sections: General, Inventory, Interfaces, Interface Groups, Multicast, Internal DHCP Server (which is expanded to show DHCP Scope and DHCP Allocated Leases), Mobility Management (Ports, NTP, CDP, Tunneling, and IEEE 802.1Q), and Status. The main content area is titled "DHCP Scopes" and displays a table with one entry:

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

6. To create a DHCP scope, click the **New...** button.



7. Name the scope **Wired Management**. You will configure this DHCP scope to provide addresses to the wired infrastructure network that connects the Admin PC, WLC-1, and LAP-1.



8. Click **Apply** to create the new DHCP scope.
9. Click the new scope in the DHCP Scopes table to configure addressing information for the scope. Enter the following information.

Scope Name	Address Pool
Wired Management	0.0.0.0 - 0.0.0.0

Pool Start Address: 192.168.200.240

Pool End Address: 192.168.200.249

Status: Enabled

Provide the values for **Network**, **Netmask**, and **Default Routers** from the information you gathered in Step 1.3. (**Step 1 . 3 eke Netmask add krrnna**)

The screenshot shows the 'frameDhcpScopeEdit.html' configuration page for a Cisco WLC. The configuration details are as follows:

Setting	Value
Scope Name	Wired Management
Pool Start Address	192.168.200.240
Pool End Address	192.168.200.249
Network	192.168.200.0
Netmask	255.255.255.0
Lease Time (seconds)	86400
Default Routers	192.168.200.1
DNS Domain Name	Not Supported
DNS Servers	0.0.0.0
Netbios Name Servers	0.0.0.0
Status	Enabled

10. Click **Apply** to activate the configuration. Click **Save Configuration** in the upper-right-hand corner of the WLC interface to save your work so that it is available when the WLC restarts.



The internal DHCP server will now provide an address to LAP-1 after a brief delay. When LAP-1 has its IP address, the CAPWAP tunnel will be established and LAP-1 will be able to provide access to the Floor 2 Employees (SSID-5) WLAN. If you move the mouse over LAP-1 in the topology, you should see its IP address, the status of the CAPWAP tunnel, and the WLAN that LAP-1 is providing access to.

Step 2: Configure SNMP.

1. Click the **Management** menu in the WLC GUI and expand the entry for **SNMP** in the left-hand menu.

The screenshot shows the WLC Management interface. The left sidebar has a tree view with 'Management' expanded, showing 'Summary', 'SNMP' (which is expanded to show 'General', 'SNMP V3 Users', 'Communities', 'Trap Receivers', 'Trap Controls', and 'Trap Logs'), and other options like 'HTTP-HTTPS', 'IPSEC', 'Telnet-SSH', 'Serial Port', 'Local Management', 'Users', and 'User Sessions'. The main content area is titled 'Summary' and contains a table of SNMP configuration settings:

SNMP Protocols	v1:Enabled v2c:Enabled v3:Enabled
Syslog	Disabled
HTTP Mode	Disabled
HTTPS Mode	Enabled
New Telnet Sessions Allowed	No
New SSH Sessions Allowed	No
Management via Wireless	Disabled

2. Click **Trap Receivers** and then **New...**

The screenshot shows the 'SNMP Trap Receiver' configuration page. At the top right is a 'New...' button. Below it is a table with columns: 'SNMP Trap Receiver Name', 'IP Address(Ipv4/Ipv6)', 'Status', and 'IPSec'. There are currently no entries in the table.

3. Enter the community string as **WLAN_SNMP** and the IP address of the server at

172.31.1.254.

SNMP Trap Receiver > New

Community Name: WLAN_SNMP

IP Address(Ipv4/Ipv6): 172.31.1.254

Status: Enable

IPSec:

< Back Apply

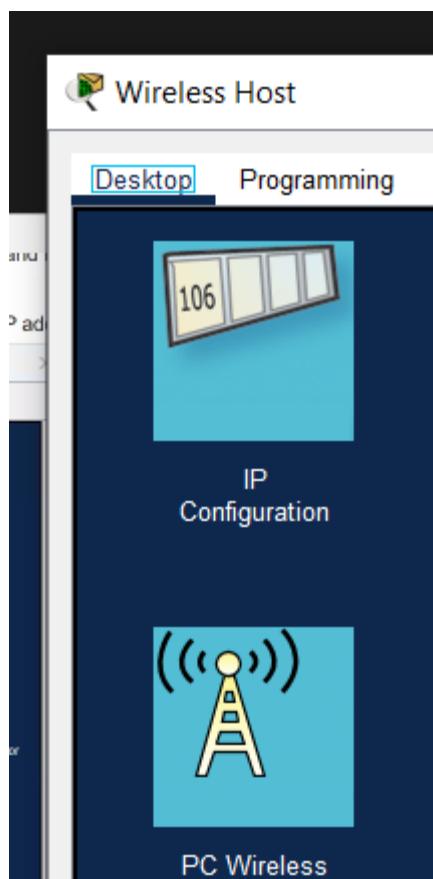
3. Click **Apply** to finish the configuration.

Part 3: Connect Hosts to the Network

Step 1: Configure a host to connect to the enterprise network.

In the Packet Tracer PC Wireless client app, you must configure a WLAN Profile in order to attach to a WPA2-Enterprise WLAN.

1. Click Wireless Host and open the **PC Wireless** app.



2. Click the **Profiles** tab and then click **New** to create a new profile. Name the profile **WLC NET**.

To connect to a network, select the profile name then click the **Connect** button. To create or edit a profile, use the menu bar at the bottom of the screen.

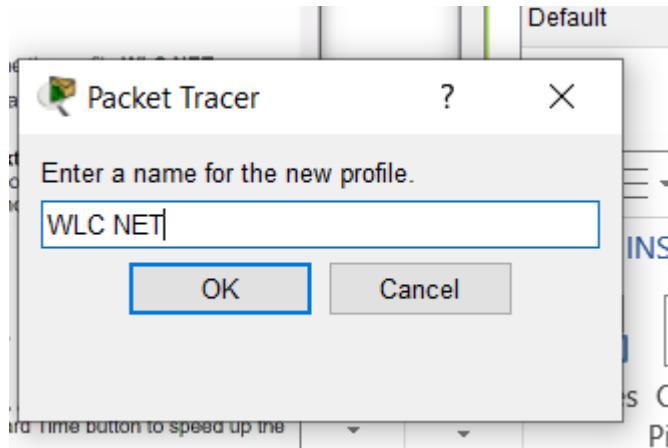
Profile	Wireless Network Name
Default	Default

Site Information	
Wireless Mode	Infrastructure
Wide Channel	Auto
Standard Channel	Auto
Security	Disable
Authentication	Auto

2.4GHz

Adapter is Inactive

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



3. Highlight the Wireless Network Name for the WLAN that we created earlier and click **Advanced Setup**.



4. Verify that the SSID for the wireless LAN is present and then click Next. Wireless Host should see SSID-5.
 5. If it does not, move the mouse over LAP-1 to verify that it is communicating with the WLC. The popup box should indicate that LAP-1 is aware of SSID-5. If it is not, check the WLC configuration. You can also manually enter the SSID.

Creating a Profile

Wireless Mode

Please choose the Wireless Mode that best suits your needs.

Infrastructure Mode Select Infrastructure Mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode Select Ad-Hoc Mode if you want to connect to another wireless device directly without using a wireless router or access point.

Please enter the wireless network name (SSID) for your wireless network.
The wireless network name is shared by all devices in a wireless network and is case-sensitive.

Wireless Network Name **SSID-5**

| Back | Next

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

Creating a Profile

Network Settings

Obtain network settings automatically (DHCP)
Select this option to have your network settings assigned automatically.

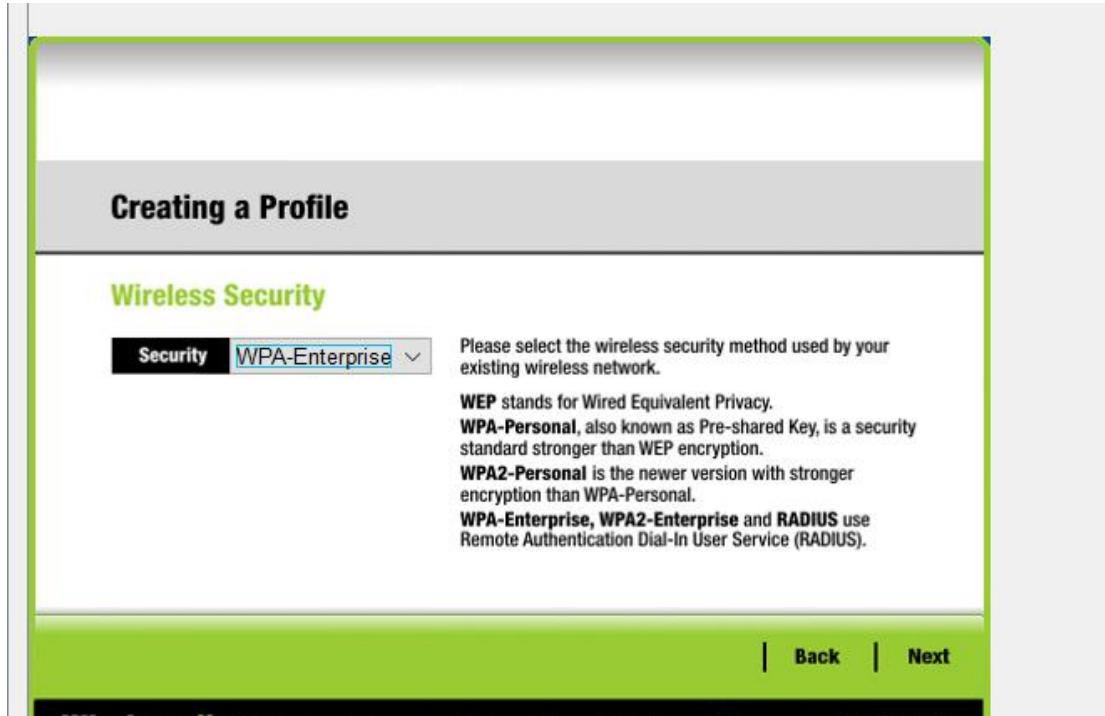
Specify network settings
Select this option to specify the network settings for the adapter.

IP Address DNS 1
Subnet Mask DNS 2
Default Gateway

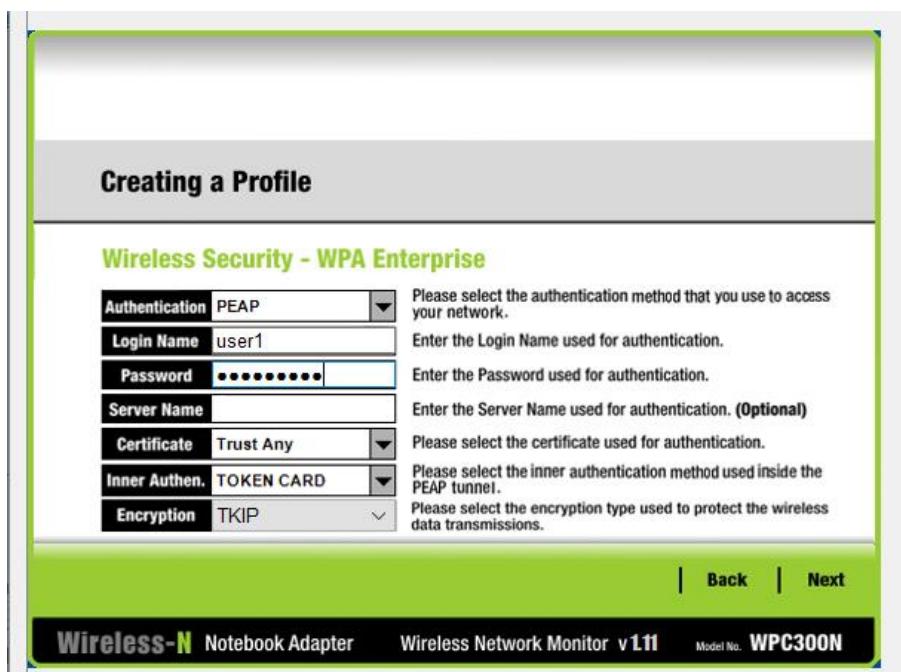
| Back | Next

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

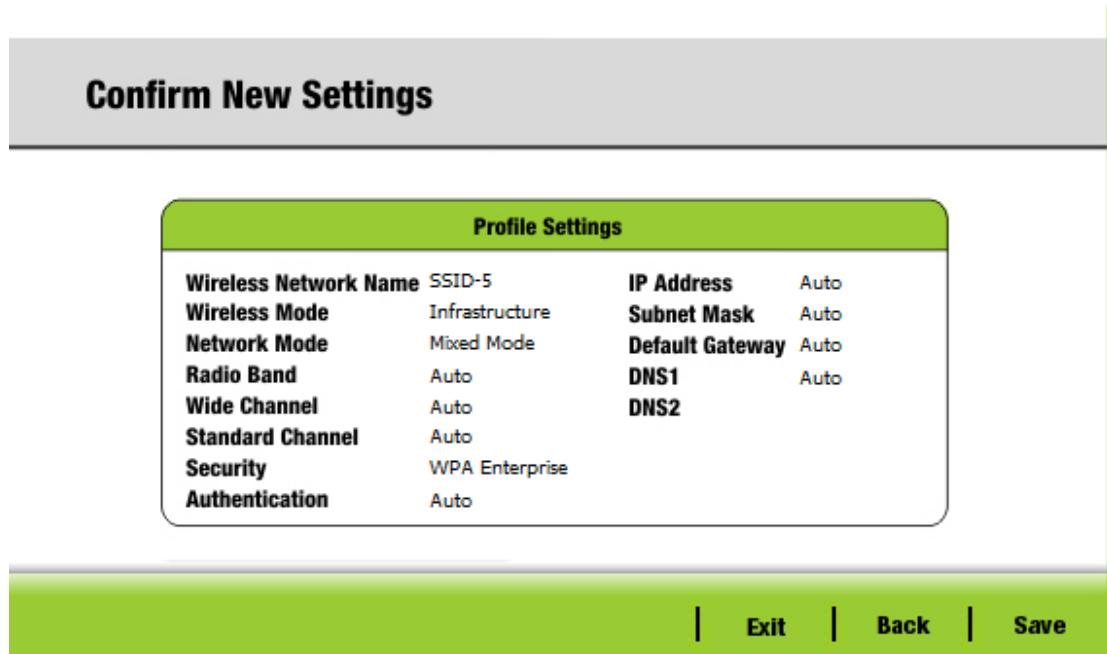
- Verify that the DHCP network setting is selected and click **Next**.
- In the Security drop down box, select **WPA2-Enterprise**. Click **Next**.



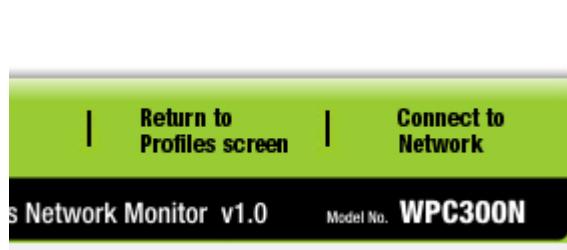
- Enter login name **user1** and the password **User1Pass** and click **Next**.



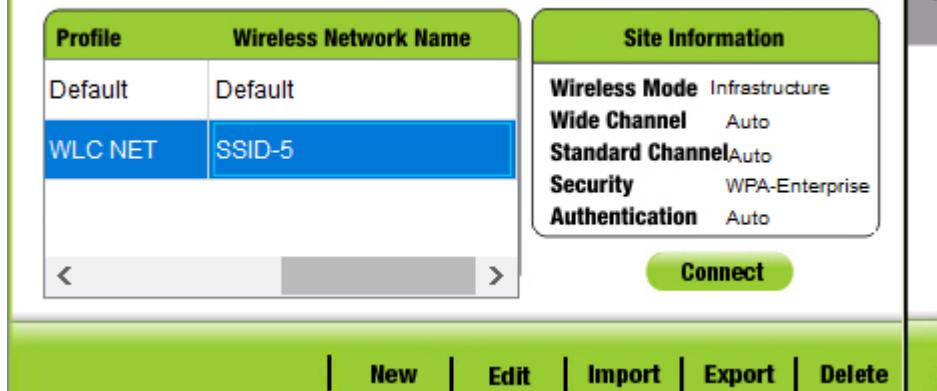
8. Verify the Profile Settings and click **Save**.



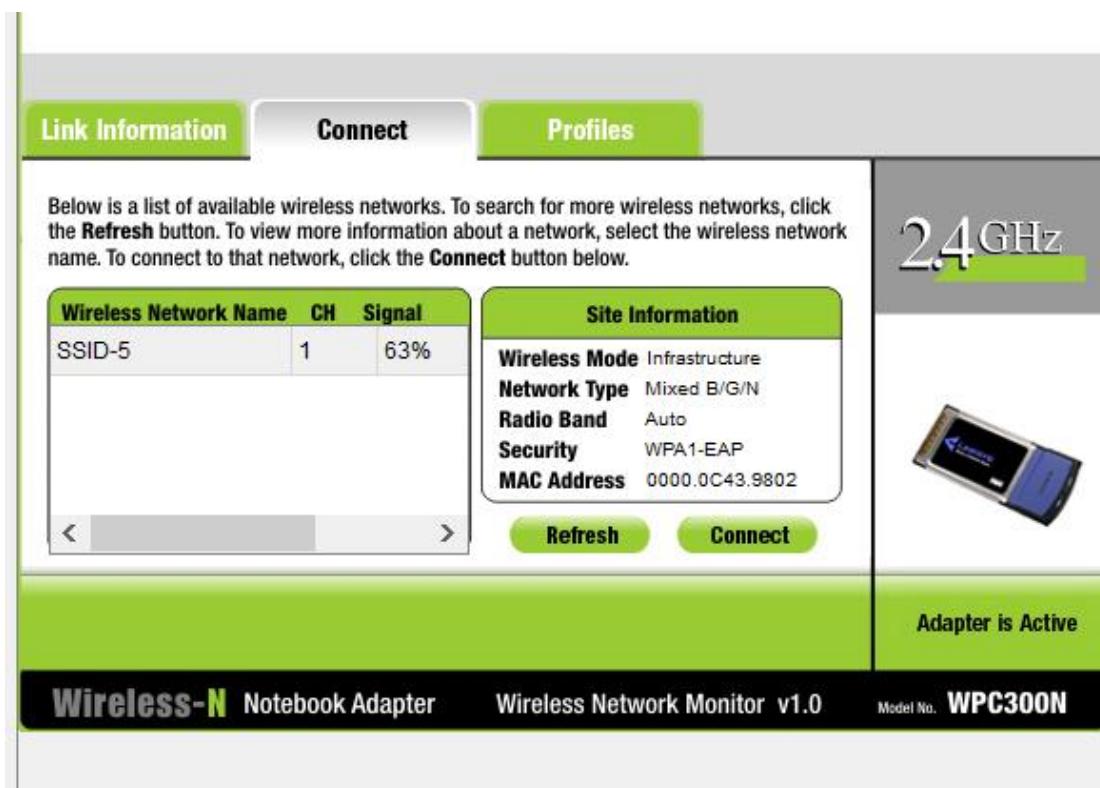
9. Select the **WLC NET** profile and click the **Connect to Network** button. After a brief delay, you should see the Wireless Host connect to LAP-1. You can click the Fast Forward Time button to speed up the process if it seems to be taking too long.



or edit a profile, use the menu bar at the bottom of the screen.



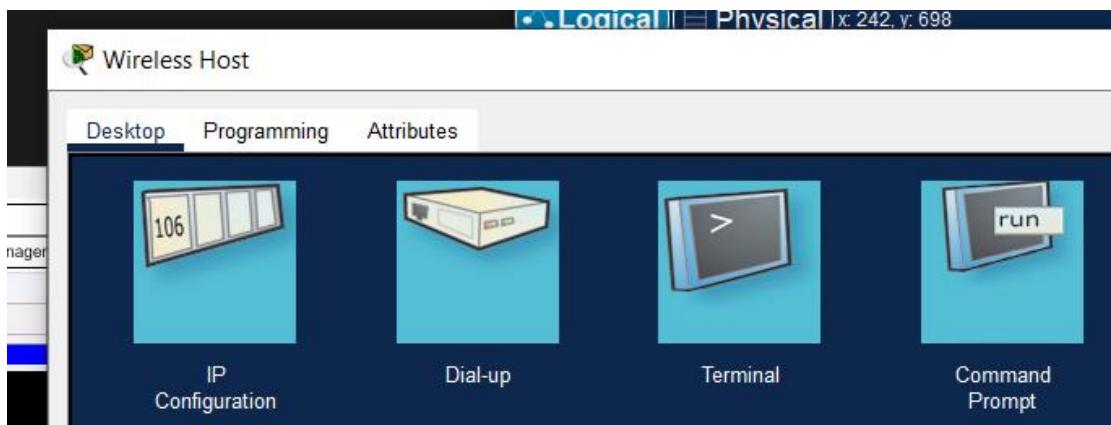
Select and Click Connect Refresh and select wireless network and connect



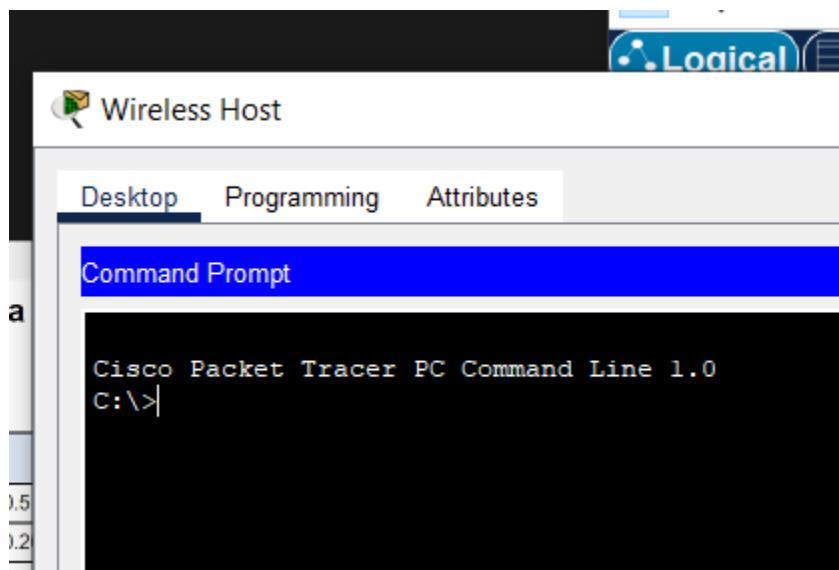
10. Confirm that Wireless Host has connected to the WLAN. Wireless Host should receive an IP address from the DHCP server that is configured for hosts on R1. The address will be in the 192.168.5.0/24 network. You may need to click the Fast Forward Time button speed up the process.

Step 2: Test Connectivity.

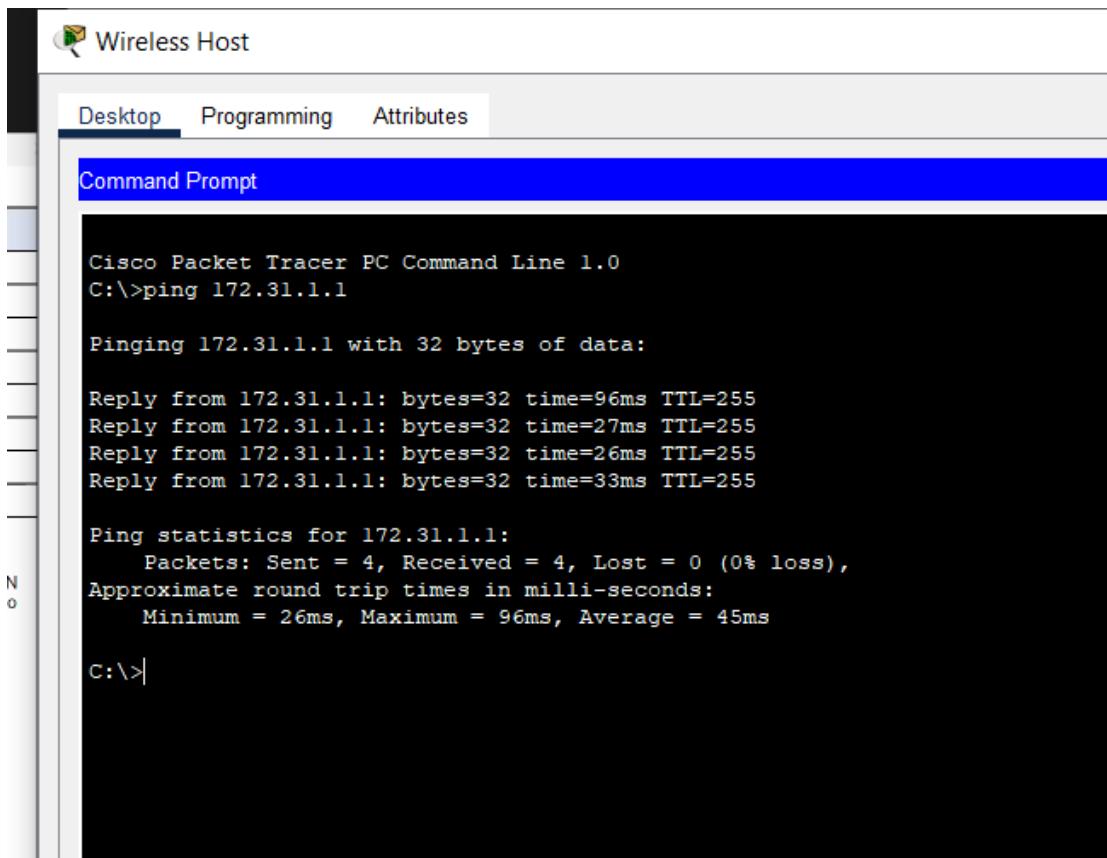
1. Close the PC Wireless app.



2. Open a command prompt and confirm that Wireless Host laptop has obtained an IP address from the WLAN network.



3. Ping the default gateway, SW1, and the RADIUS server. Success indicates full connectivity within this topology.



The screenshot shows the Cisco Packet Tracer Command Line interface. The title bar says "Wireless Host". The menu bar has "Desktop", "Programming", and "Attributes". The main window is titled "Command Prompt". The command entered was "C:\>ping 172.31.1.1". The output shows the ping results for the IP address 172.31.1.1, including four replies with TTL=255 and round-trip times ranging from 26ms to 96ms. The statistics show 4 packets sent, 4 received, and 0% loss. The prompt "C:\>" is visible at the bottom.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.31.1.1

Pinging 172.31.1.1 with 32 bytes of data:

Reply from 172.31.1.1: bytes=32 time=96ms TTL=255
Reply from 172.31.1.1: bytes=32 time=27ms TTL=255
Reply from 172.31.1.1: bytes=32 time=26ms TTL=255
Reply from 172.31.1.1: bytes=32 time=33ms TTL=255

Ping statistics for 172.31.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 96ms, Average = 45ms

C:\>
```

Discussion

- In this lab session, we focused on configuring and securing a wireless network using a wireless router and Wireless LAN Controller (WLC). First, we set up a wireless router and

connected wireless devices to it, ensuring basic wireless connectivity. To extend coverage, we added an access point to expand the network's reach. On the WLC, we configured a new VLAN interface to segment network traffic, then created a new WLAN for wireless clients. We also set up a new DHCP scope on the WLC's internal DHCP server to automatically assign IP addresses to wireless clients. To improve monitoring, we configured SNMP settings on the WLC, followed by integrating a RADIUS server for secure user authentication. Finally, we secured the WLAN using WPA2-Enterprise and connected hosts to the new WLAN, ensuring both security and smooth wireless access across the network.