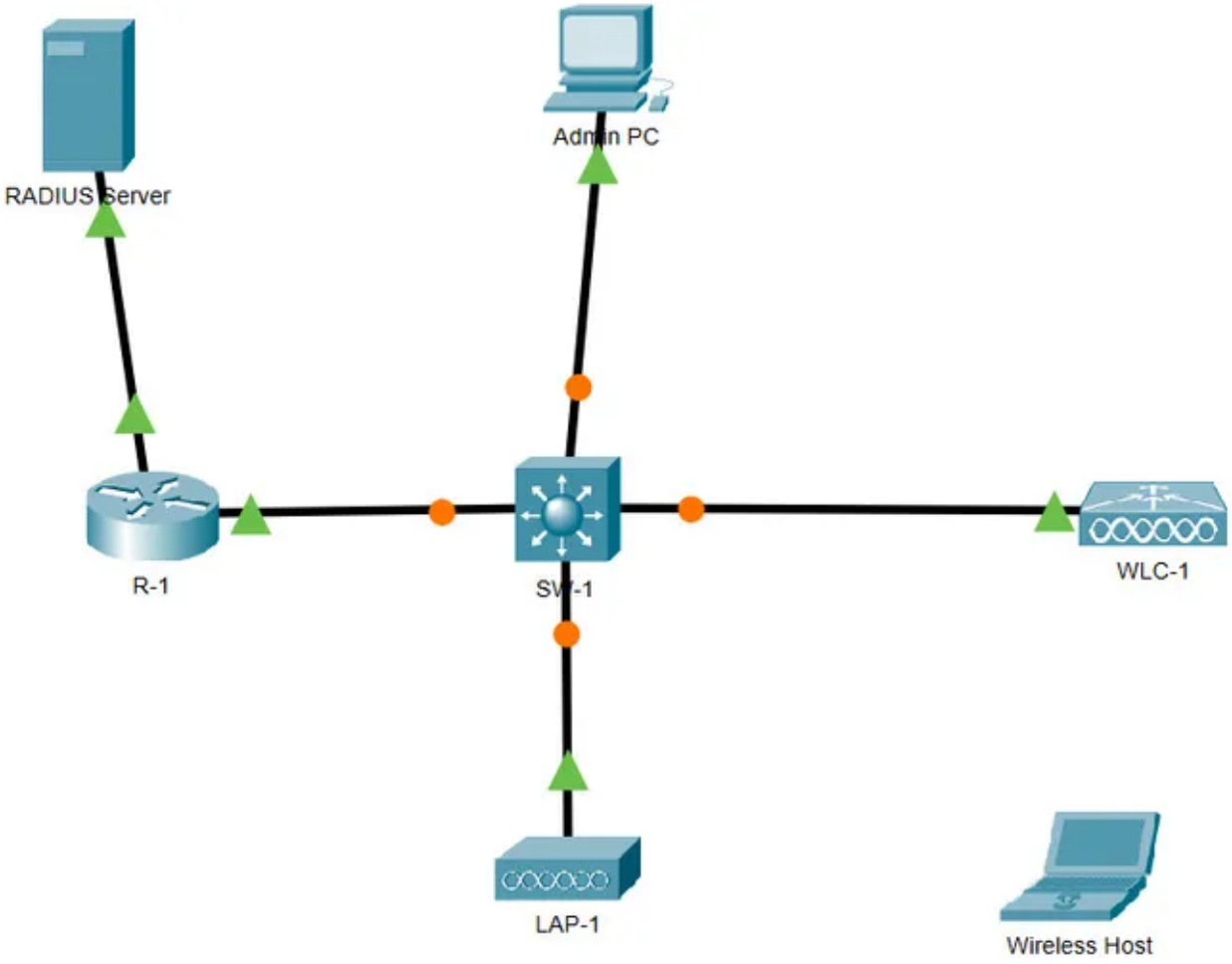
13.3.12 Packet Tracer – Configure a WPA2 Enterprise WLAN on the WLC (Instructor Version)



13.3.12 Packet Tracer – Configure a WPA2 Enterprise WLAN on the WLC

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

Objectives

- 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.

Background / Scenario

You have already configured and tested the WLC with an existing WLAN. You configured WPA2-PSK for that WLAN because it was to be used in a smaller business. You have been asked to configure and test a WLC topology that will be used in a larger enterprise. You know that WPA2-PSK does not scale well and is not appropriate to use in an enterprise network. This new topology will use a RADIUS server and WPA2- Enterprise to authenticate WLAN users. This allows administration of the user accounts from a central location and provides enhanced security and transparency because each account has its own username and password. In addition, user activity is logged on the server.

In this lab, you will create a new VLAN interface, use that interface to create a new WLAN, and secure that WLAN with WPA2-Enterprise. You will also configure the WLC to use the enterprise RADIUS server to authenticate users. In addition, you will configure the WLC to use a SNMP server.

Instructions

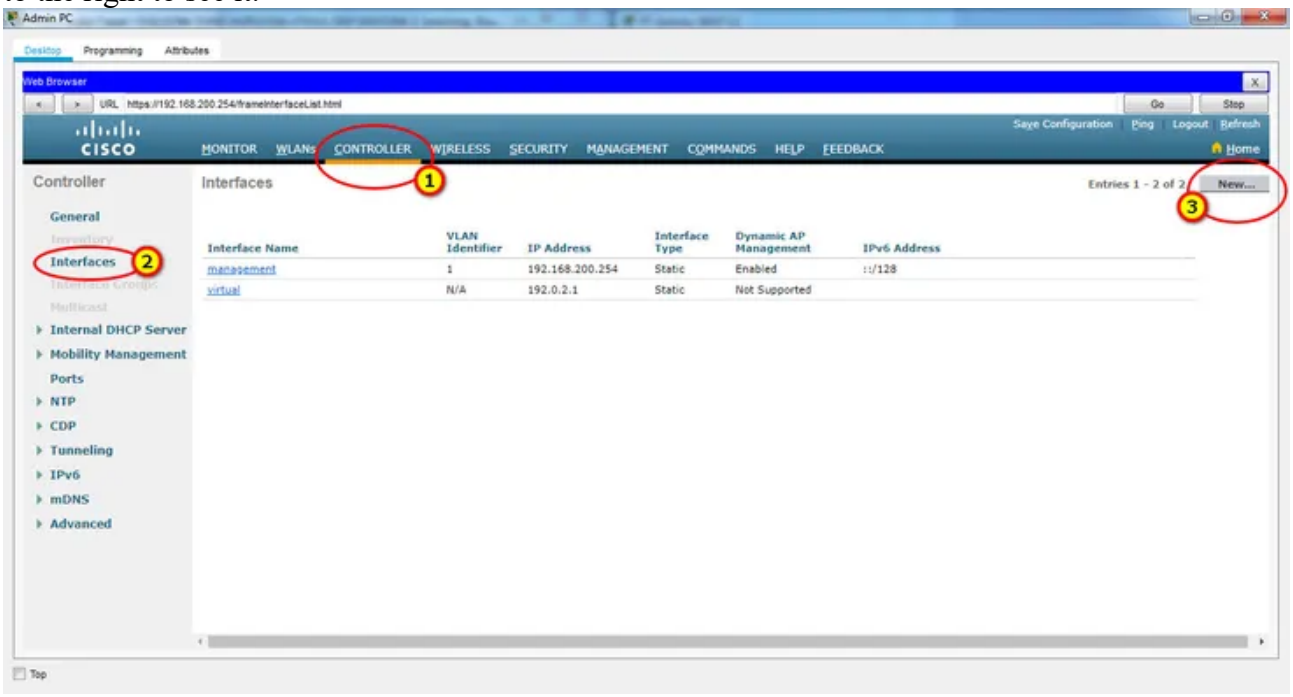
Part 1: Create a new WLAN

Step 1: Create a new VLAN interface.

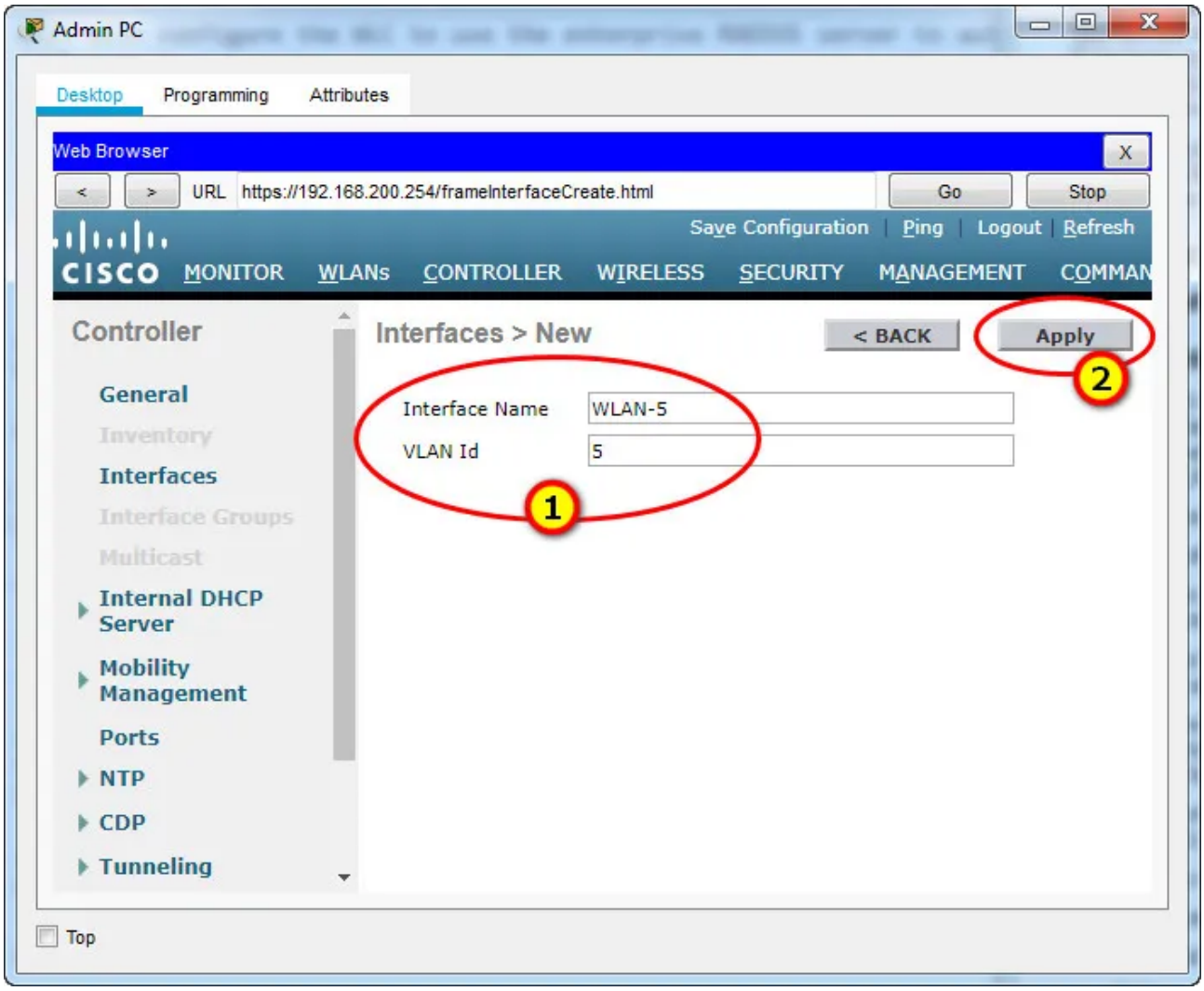
Each WLAN requires a virtual interface on the WLC. These interfaces are known as dynamic interfaces. The virtual interface is assigned a VLAN ID and traffic that uses the interface will be tagged as VLAN traffic. This is why connections between the APs, the WLC, and the router are over trunk ports. For the traffic from multiple WLANs to be transported through the network, traffic for the WLAN VLANs must be trunked.

a. Open the browser from the desktop of Admin PC. Connect to the IP address of the WLC over HTTPS. **https://192.168.200.254**
b. Login with the username **admin** and password **Cisco123.**
c. 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.

d. 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.

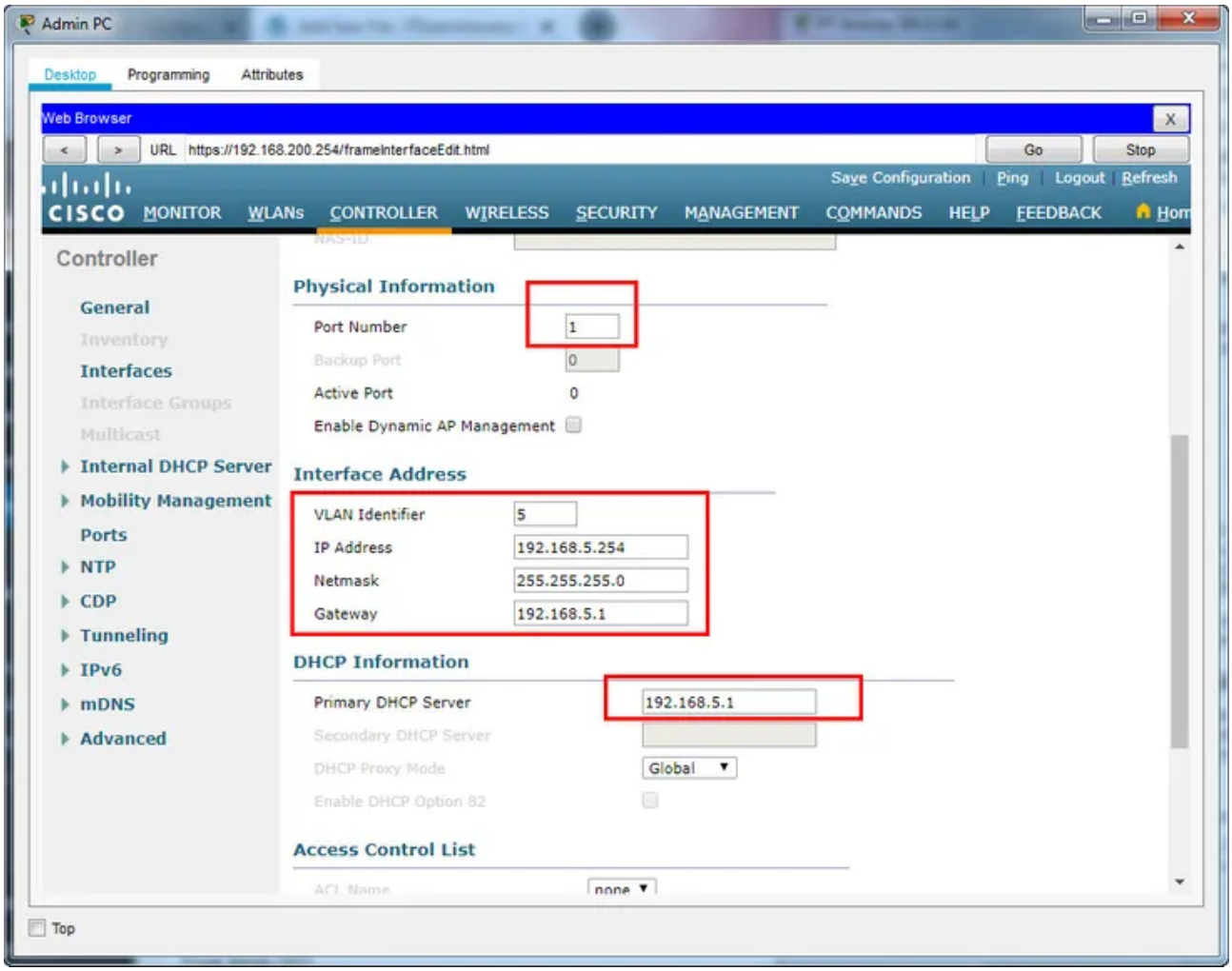


e. Enter the name of the new interface. We will call it **WLAN-5.** Configure the VLAN ID as **5**. This is the VLAN that will carry traffic for the WLAN that we create later. Click **Apply.** This leads to a configuration screen for the VLAN interface.



f. 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.
g. Address the interface as follows:

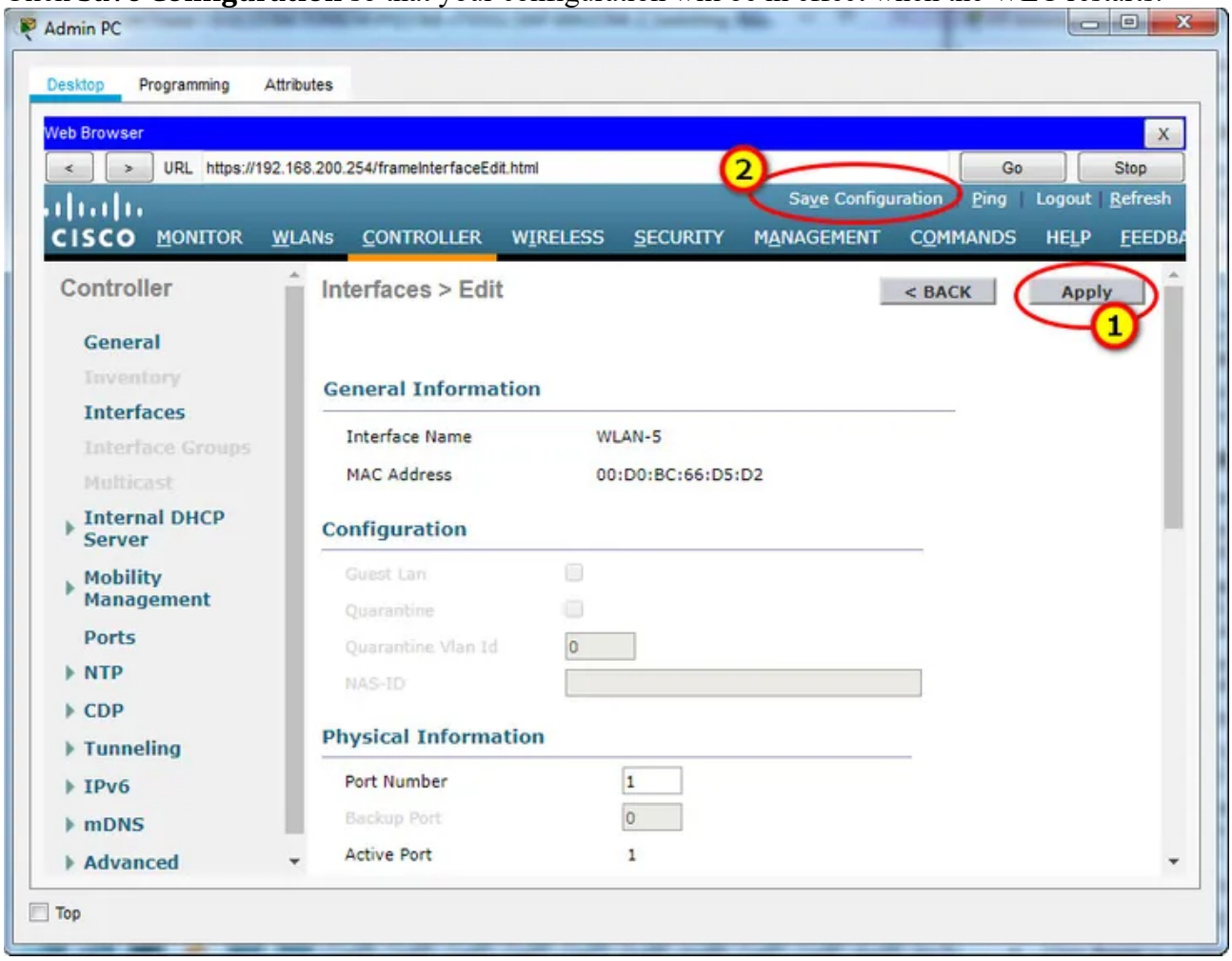
IP Address: **192.168.5.254**
Netmask: **255.255.255.0**
Gateway: **192.168.5.1**
Primary DHCP server: **192.168.5.1**



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.

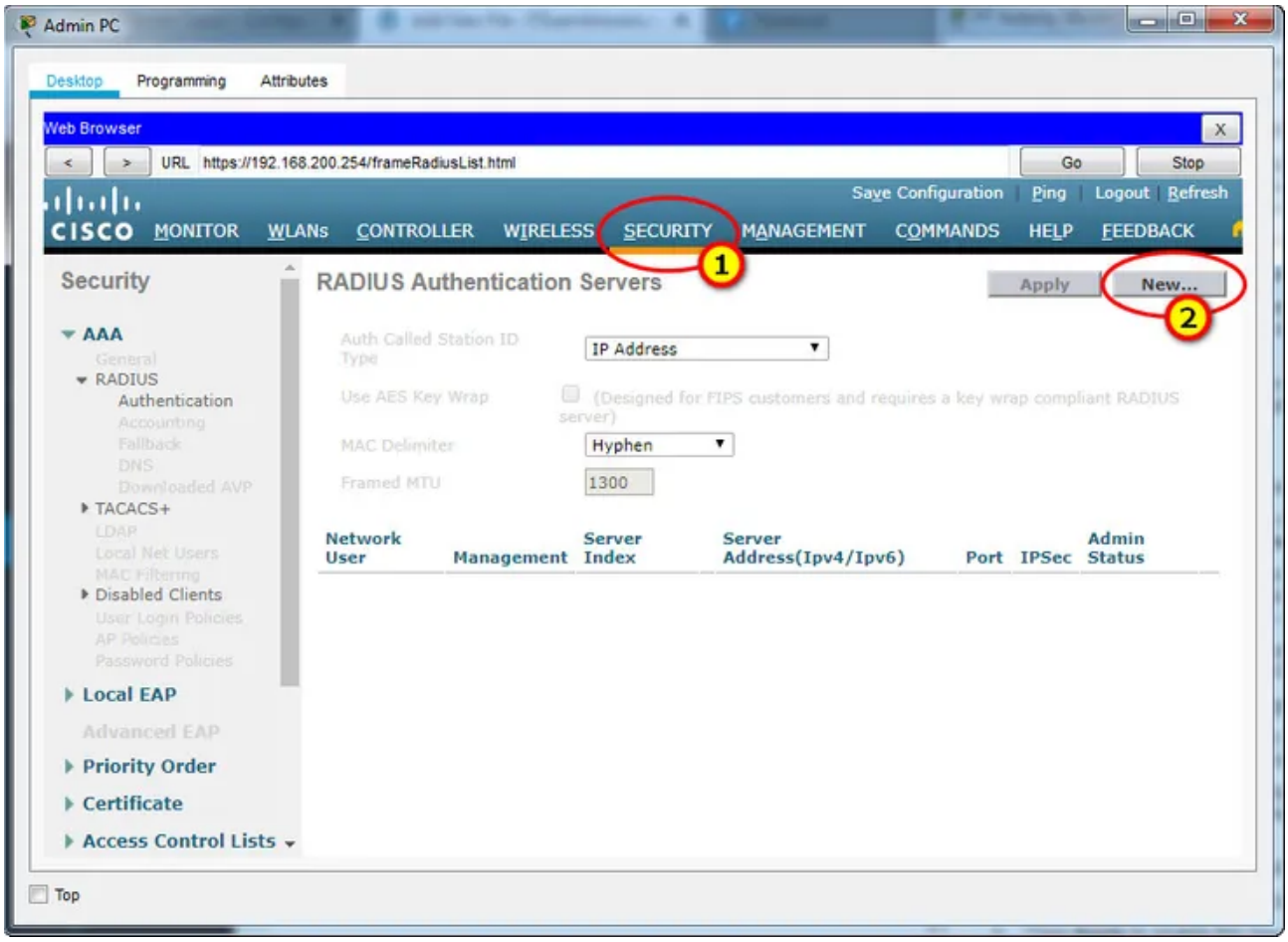
h. Be sure to click **Apply** to enact your changes and click **OK** to respond to the warning message. Click **Save Configuration** so that your configuration will be in effect when the WLC restarts.



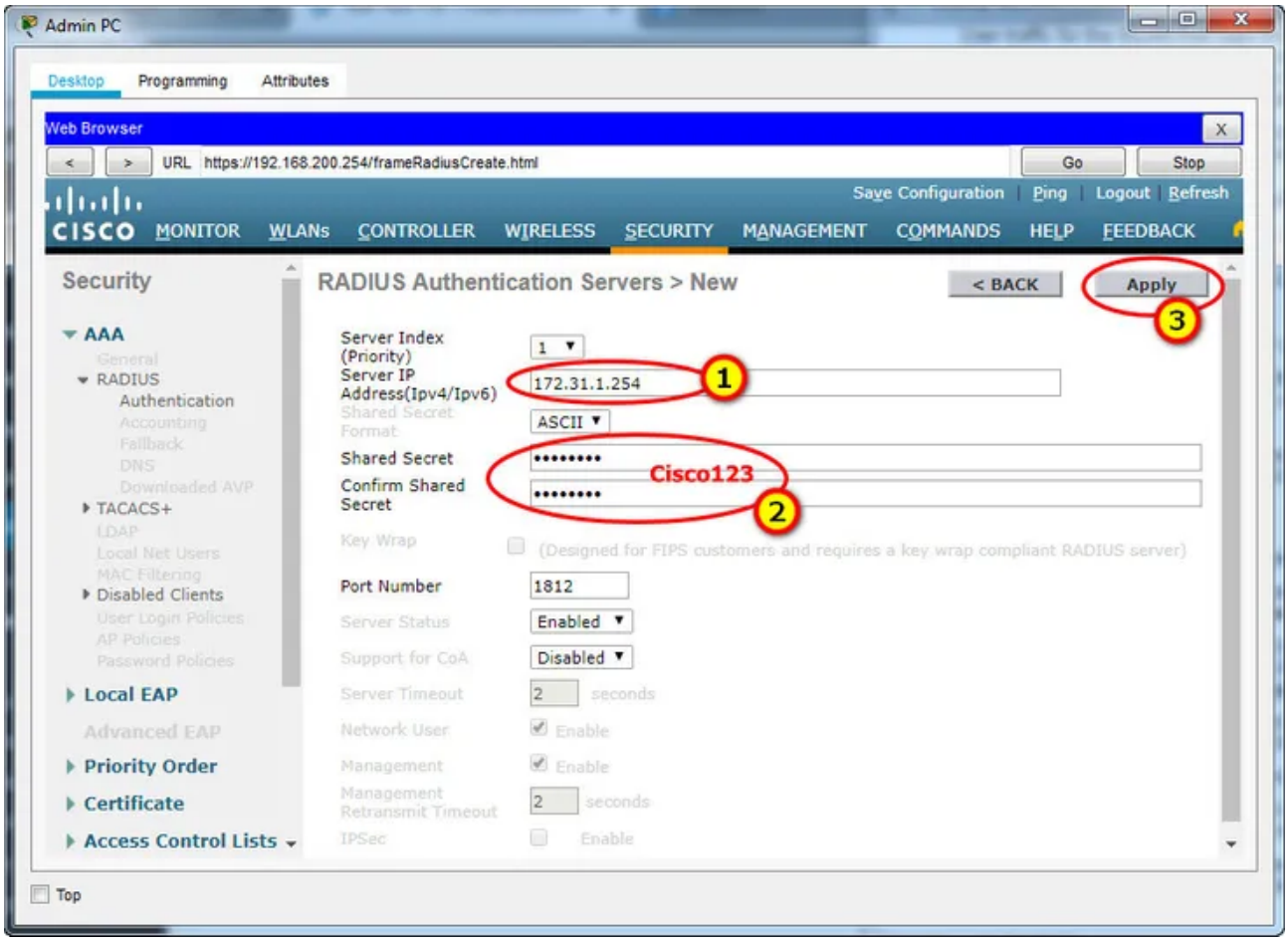
Step 2: Configure the WLC to use a RADIUS server.

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.

a. Click the **Security** menu on the WLC.
b. Click the **New** button and enter the IP address of the RADIUS server in the Server IP Address field.



c. 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.**

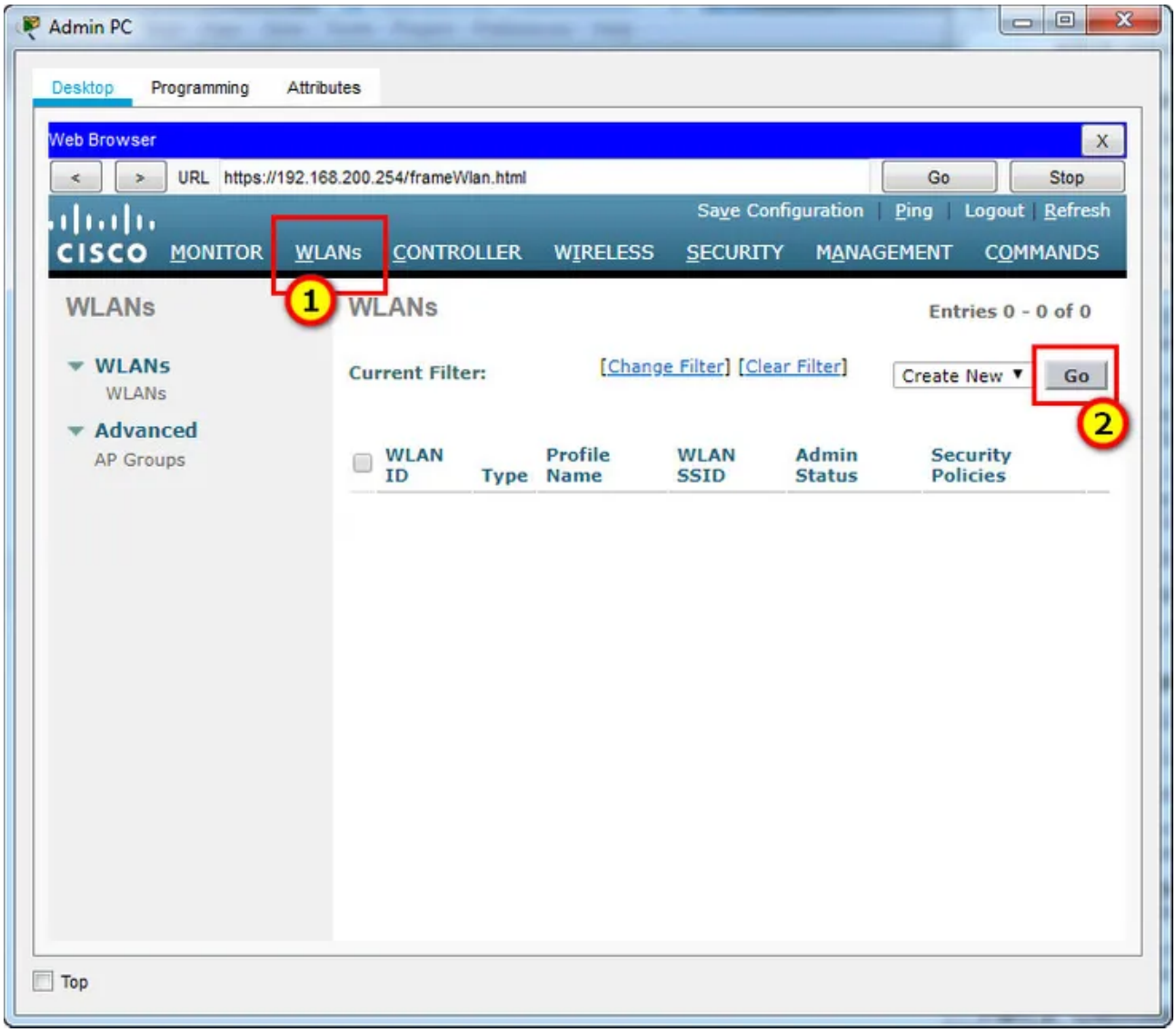


Note: It is not a good practice to reuse passwords. This activity reuses passwords only to make the activity easier for you to complete and review.

Step 3: Create a new WLAN.

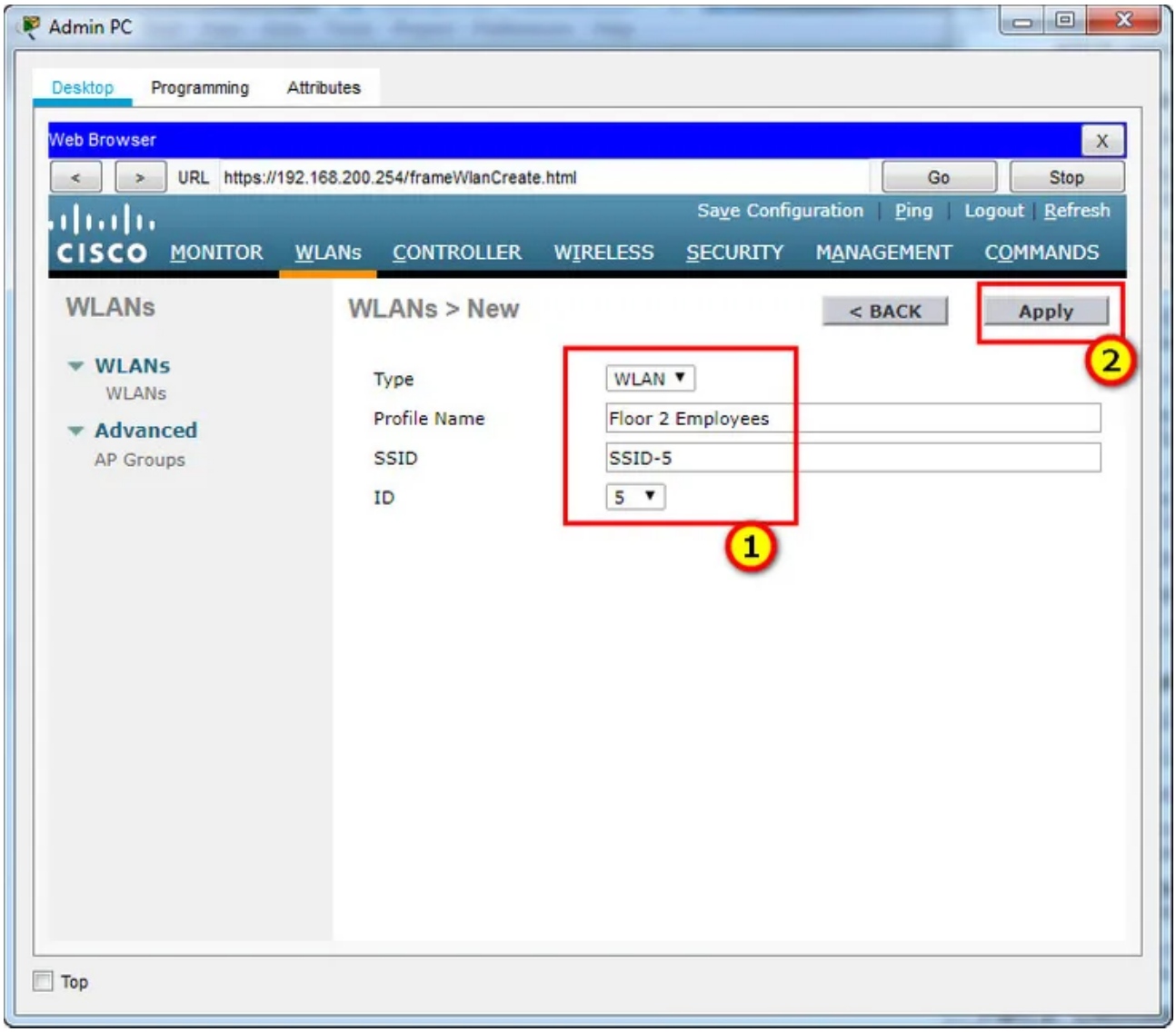
Create a New WLAN. Use the newly created VLAN interface for the new WLAN.

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



b. 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.



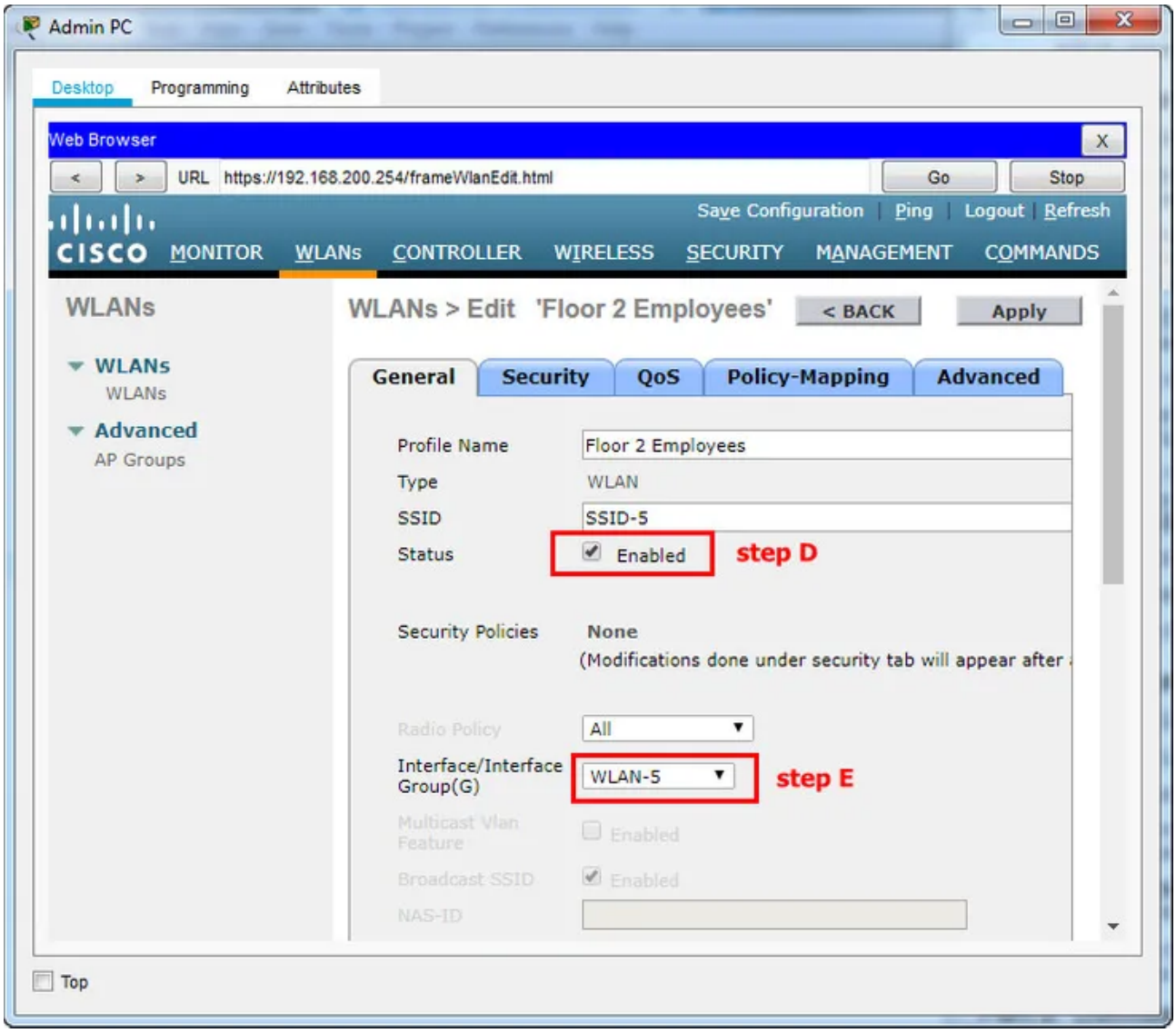
Note: The ID is an arbitrary value that is used as a label for the WLAN. In this case, we configured it as 5 to be consistent with VLAN for the WLAN. It could be any available value.

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

d. Now that the WLAN has been created you can configure features of the network.

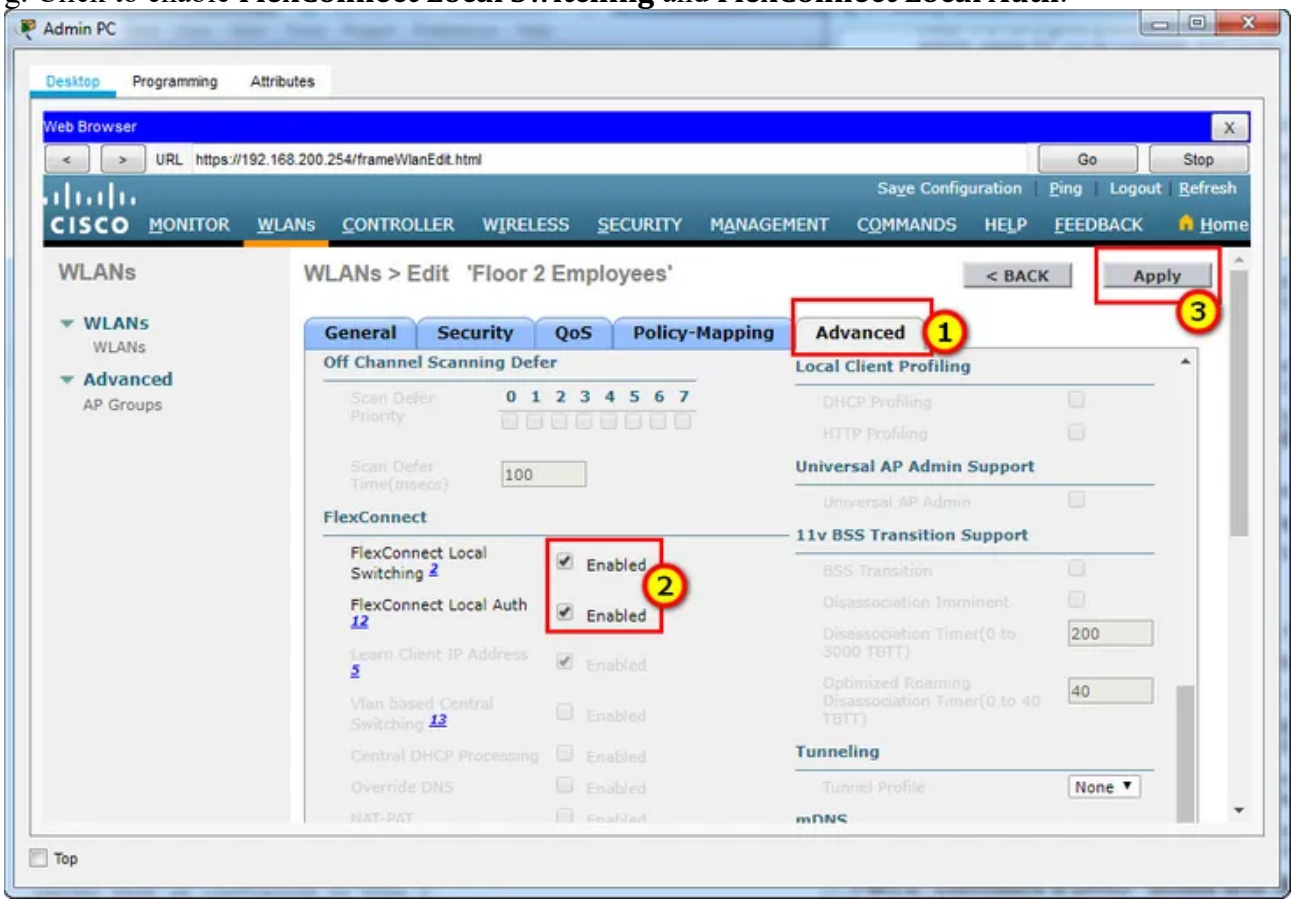
Click **Enabled** to make the WLAN functional. It is a common mistake to accidentally skip this step.

e. 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**.



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

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

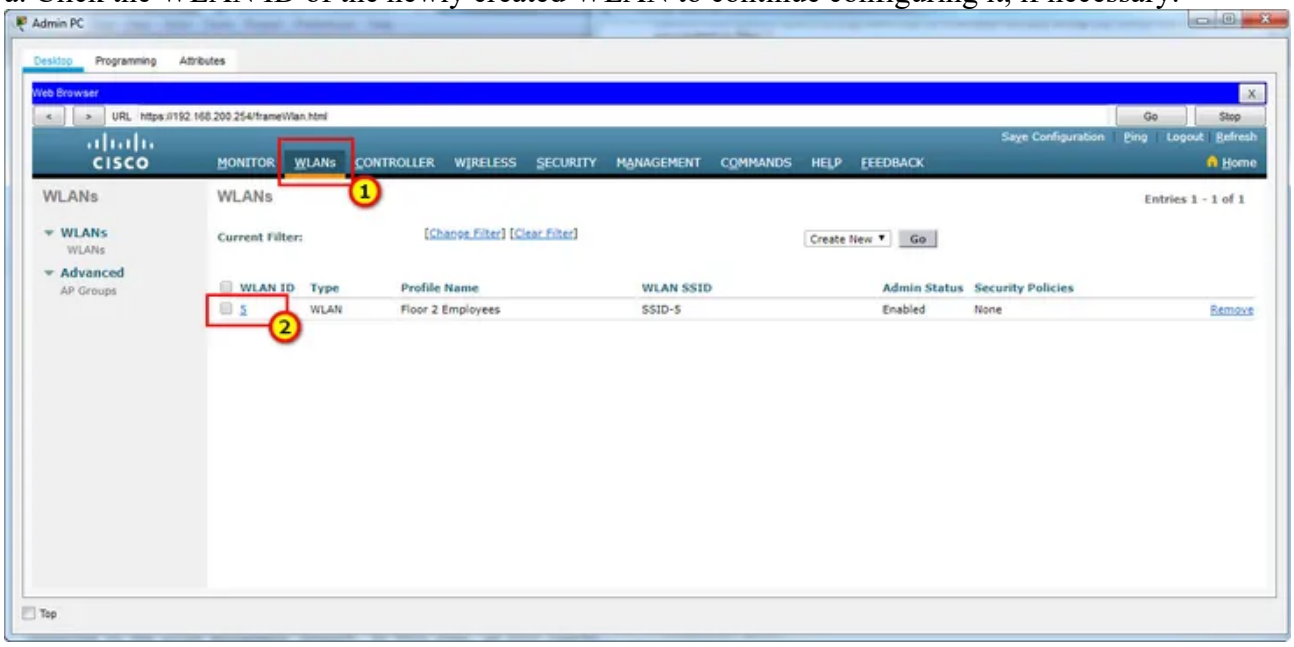


h. Click **Apply** to enable the new WLAN. If you forget to do this, the WLAN will not operate.

Step 4: Configure WLAN security.

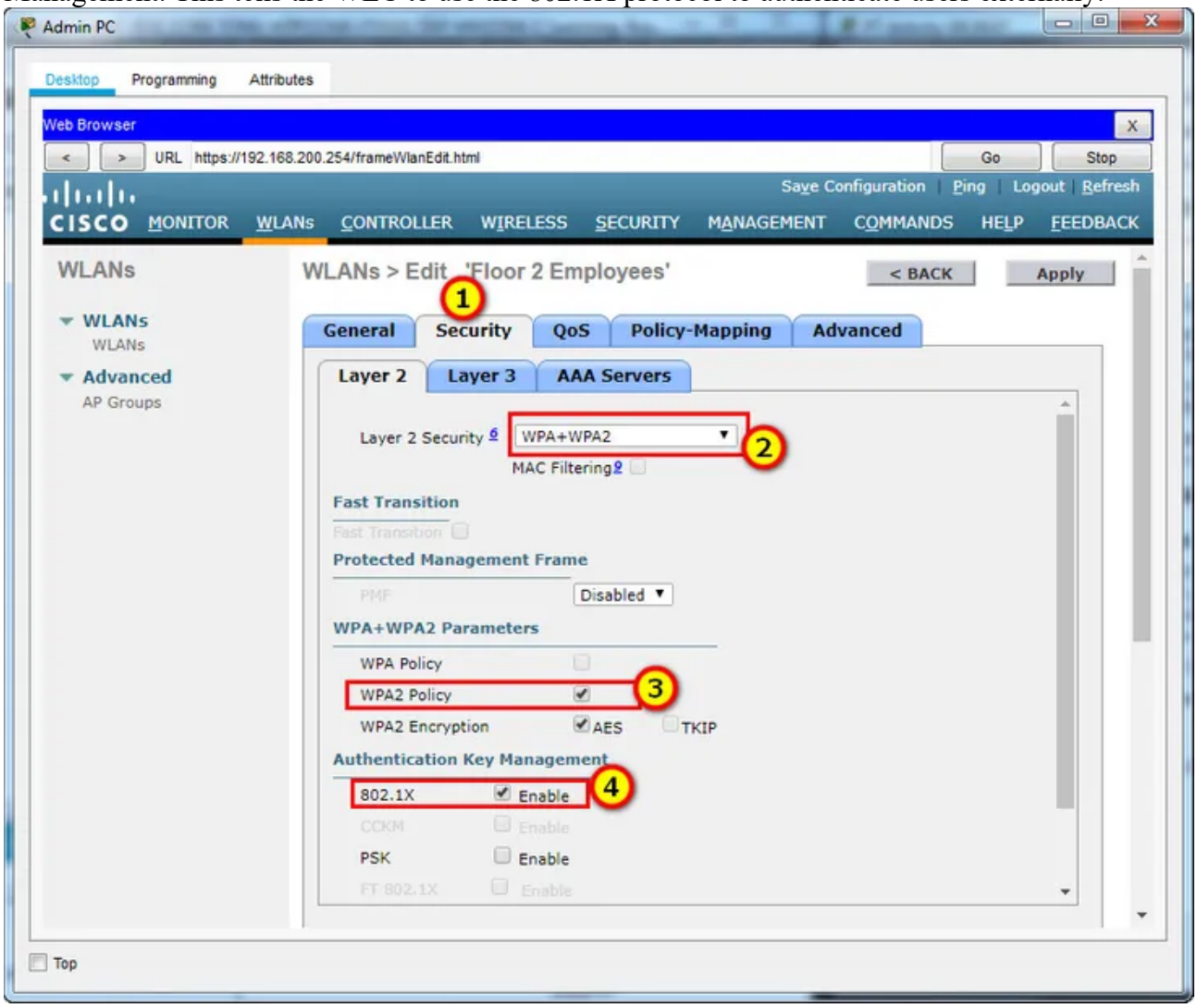
Instead of WPA2-PSK, we will configure the new WLAN to use WPA2-Enterprise.

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

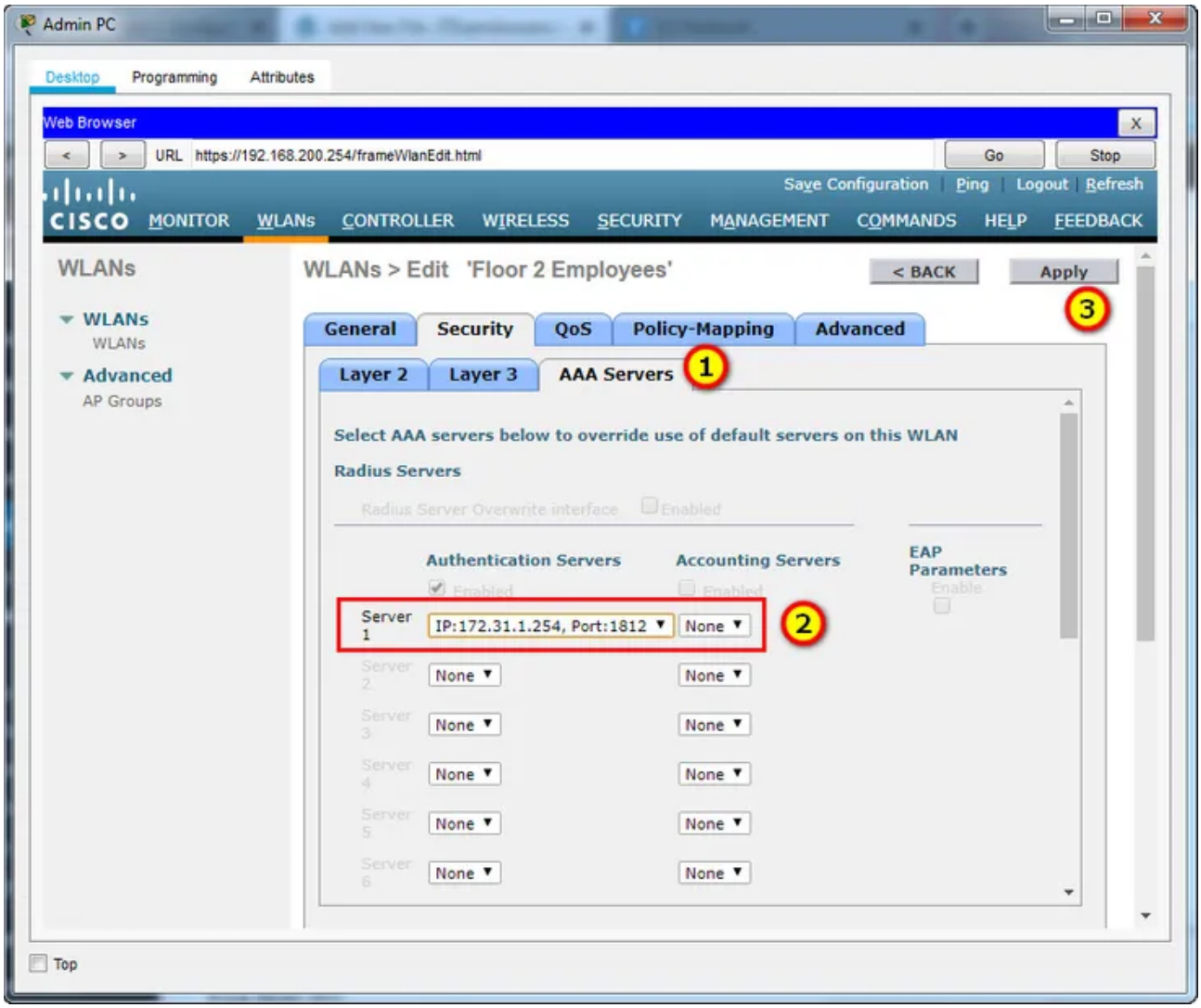


b. Click the Security tab. Under the Layer 2 tab, select **WPA+WPA2** from the drop-down box.

c. 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.



d. 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.



e. 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.

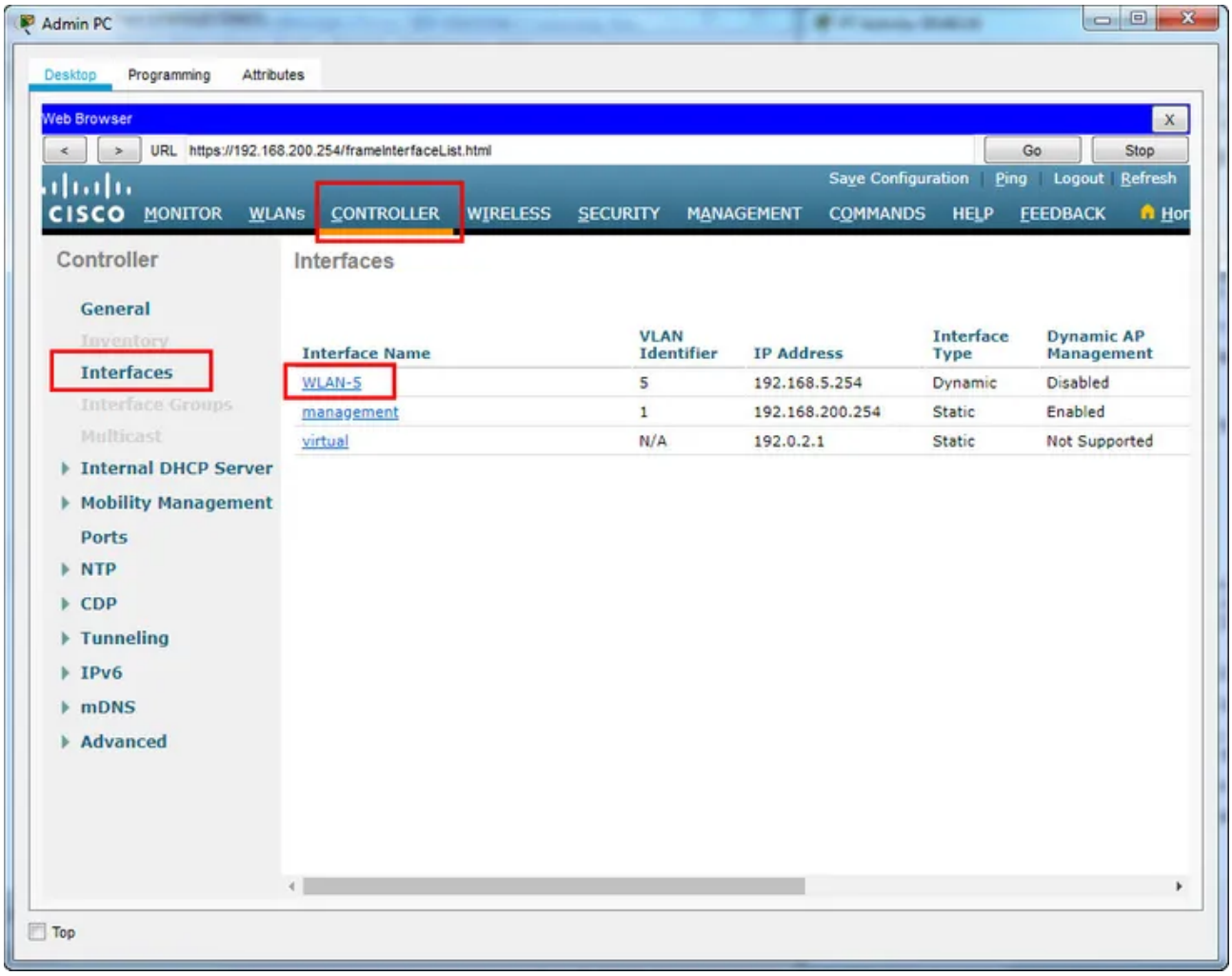
Part 2: Configure a DHCP Scope and SNMP

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. In this step, we will configure a DHCP scope on the WLC and use it to address LAP-1.

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

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



What interfaces are present?

WLAN-5, management, and virtual.

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

IP address:

192.168.200.254

Netmask:

255.255.255.0

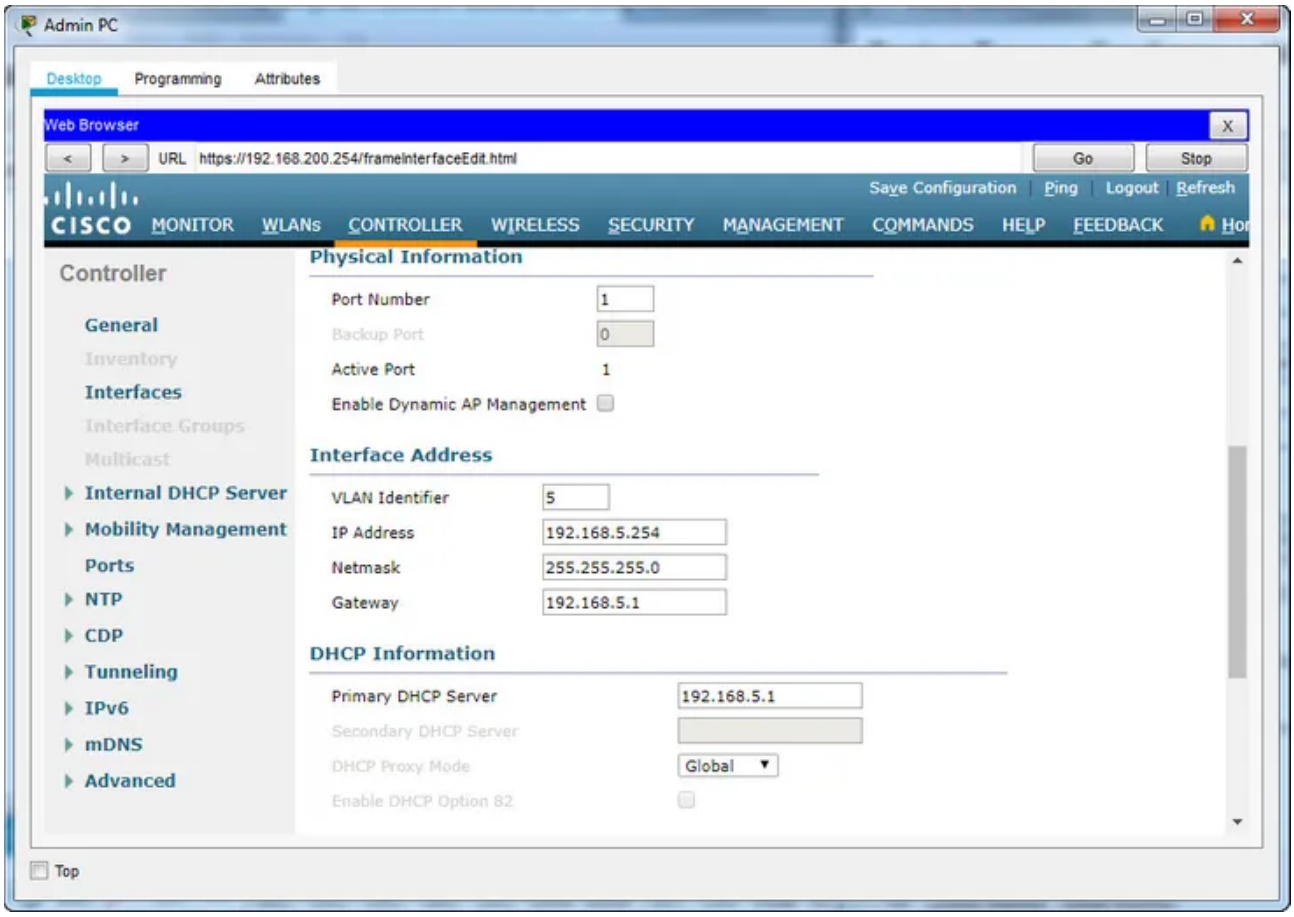
Gateway:

192.168.200.1

Primary DHCP server:

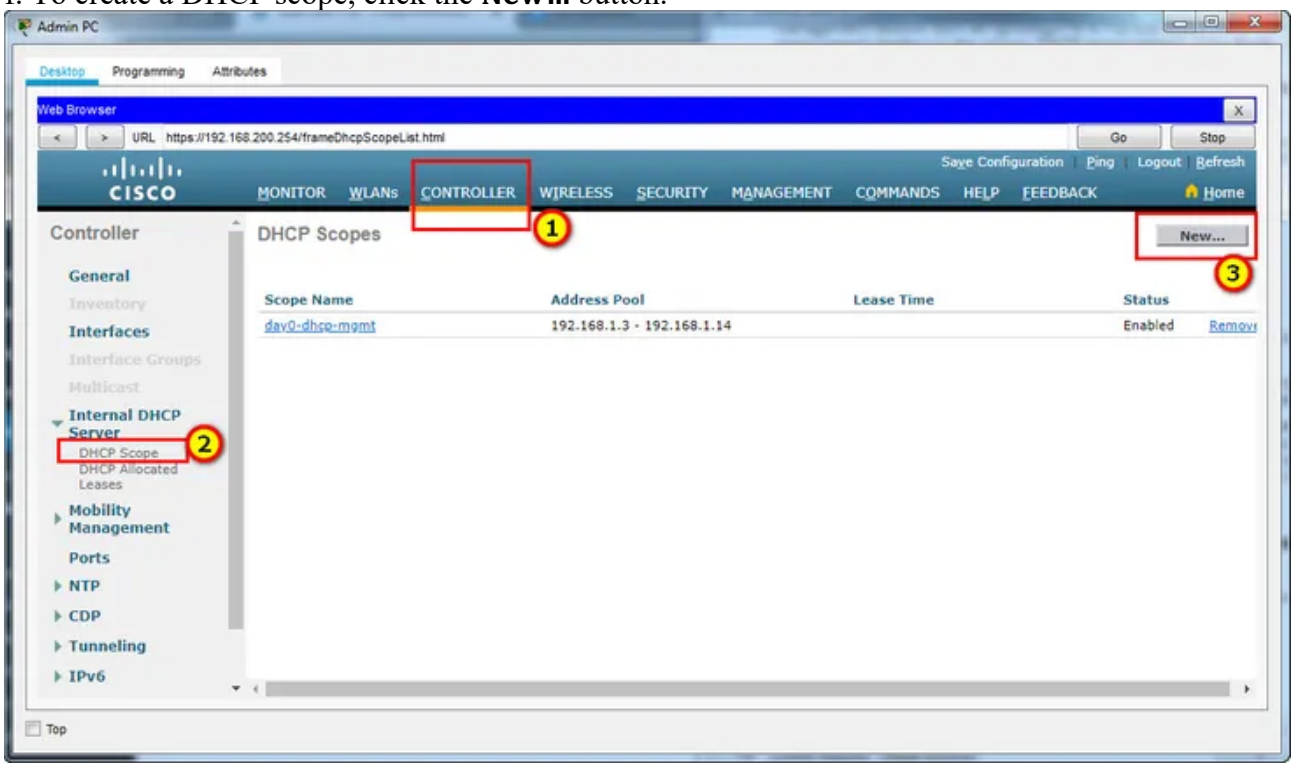
none specified

d. 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.



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

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

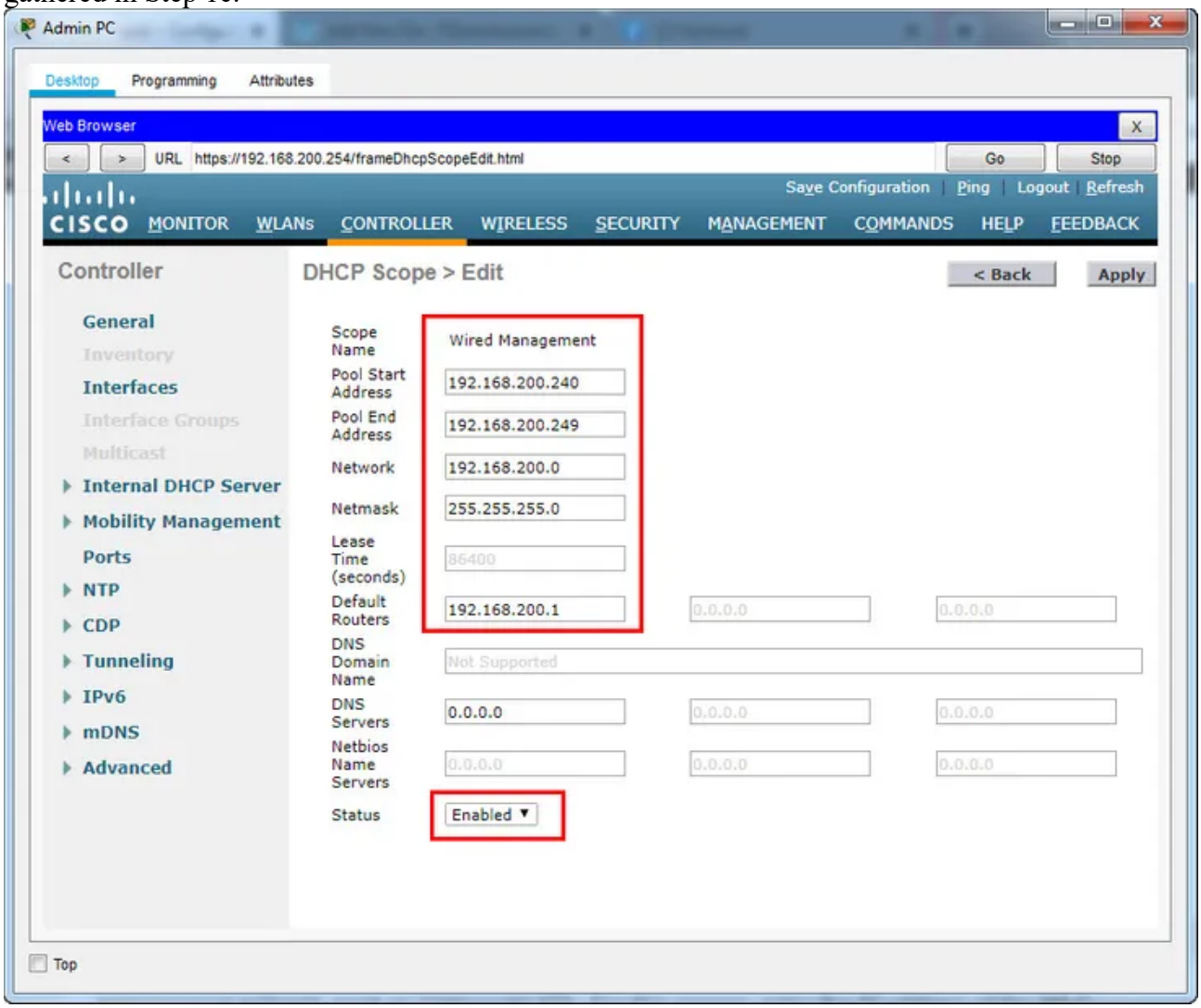


g. Name the scope **Wired Management**. You will configure this DHCP scope to provide addresses to the wired infrastructure network that connects the Admin PC, WLC-1, and LAP-1.

h. Click **Apply** to create the new DHCP scope.

i. Click the new scope in the DHCP Scopes table to configure addressing information for the scope. Enter the following information.

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 1c.

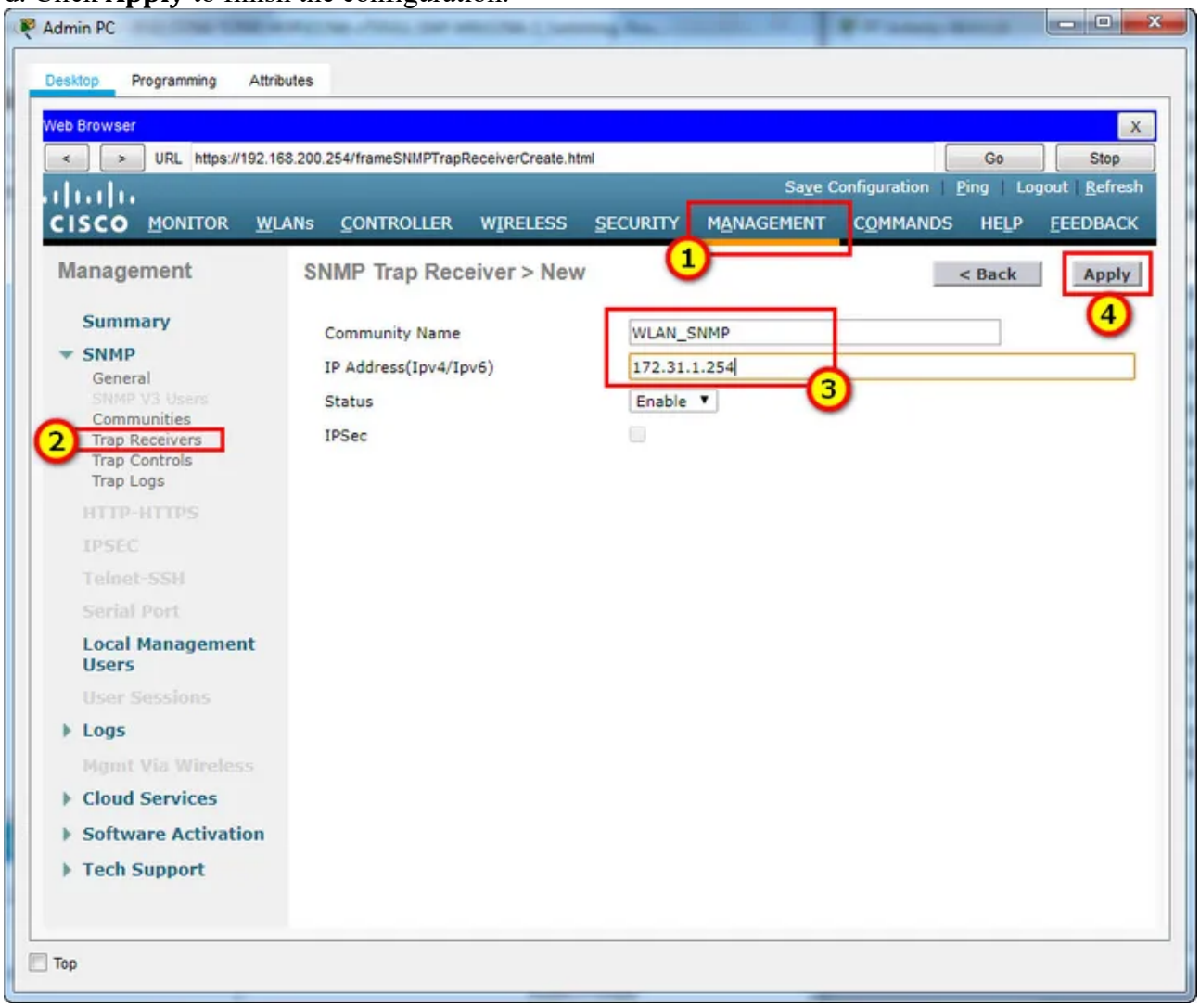


j. Click **Apply** to activate the configuration. Click **Save Configuration** in the upper-right-hand corner of the WLC interface to save your work so that it is available when the WLC restarts.
The internal DHCP server will now provide an address to LAP-1 after a brief delay. When LAP-1 has its IP 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

a. Click the **Management** menu in the WLC GUI and expand the entry for **SNMP** in the left-hand menu.
b. Click **Trap Receivers** and then **New…**
c. Enter the community string as **WLAN_SNMP** and the IP address of the server at **172.31.1.254.**

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



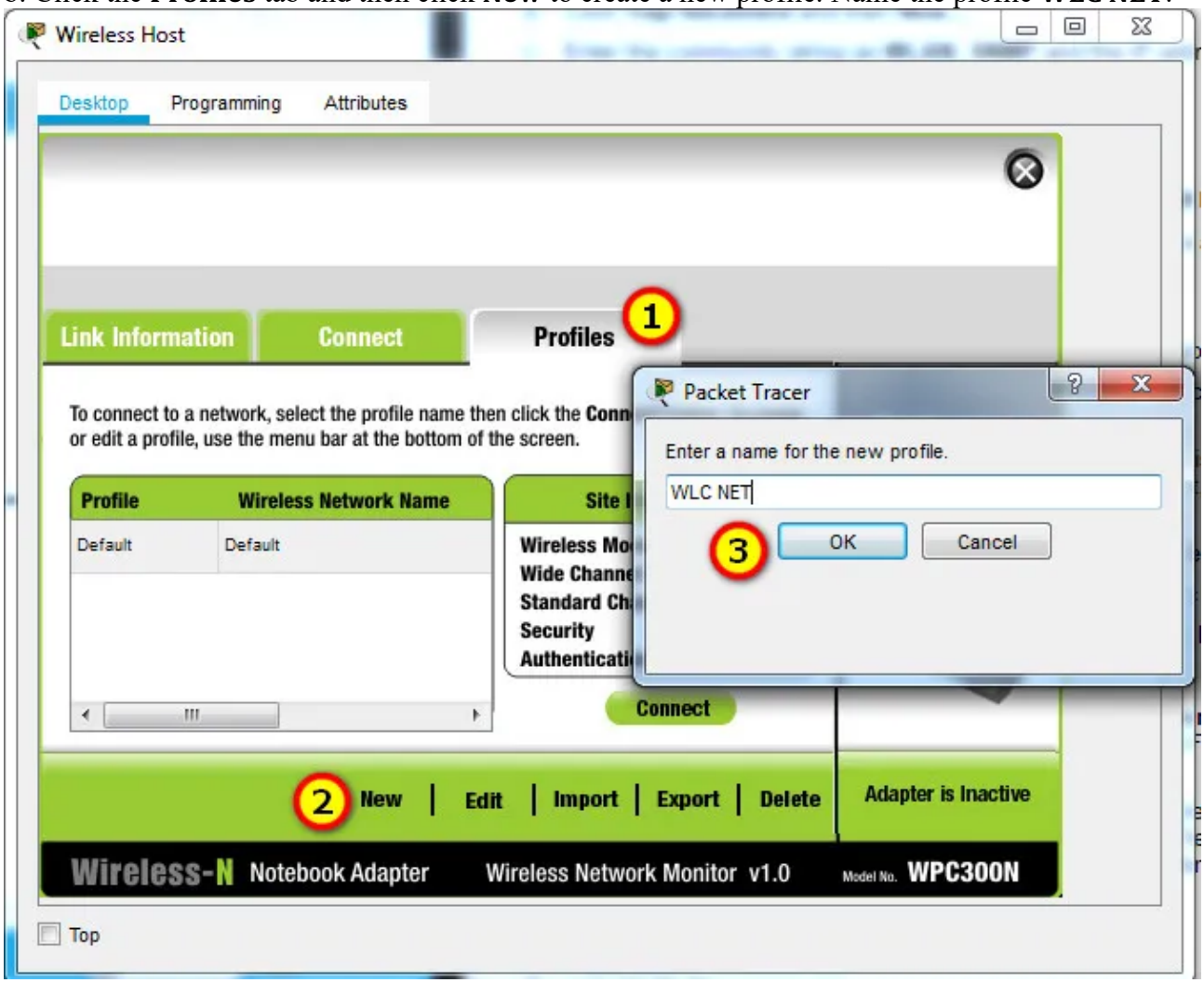
Part 3: Connect Hosts to the Network

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

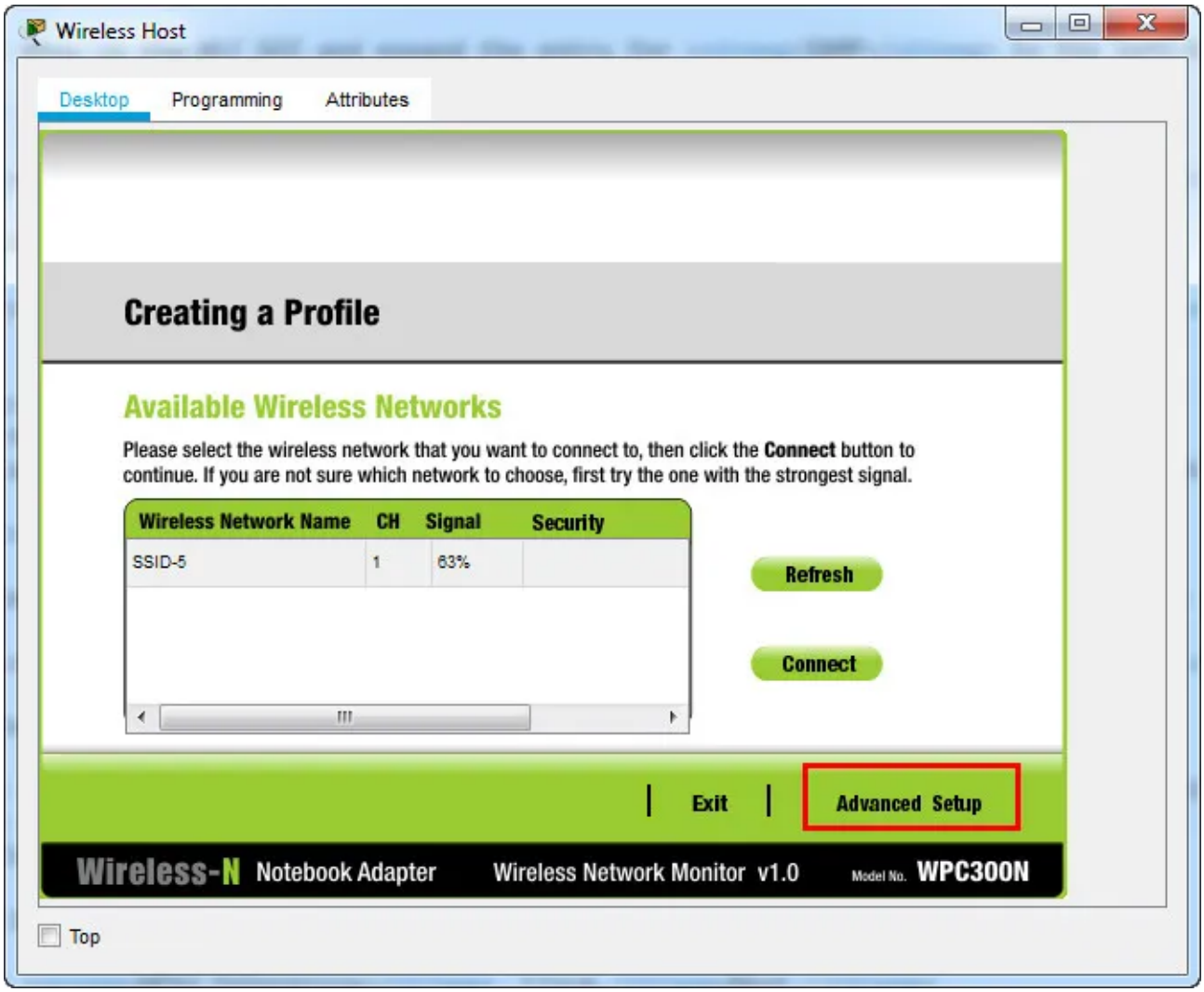
In the Packet Tracer PC Wireless client app, you must configure a WLAN Profile in order to attach to a WPA2-Enterprise WLAN.

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

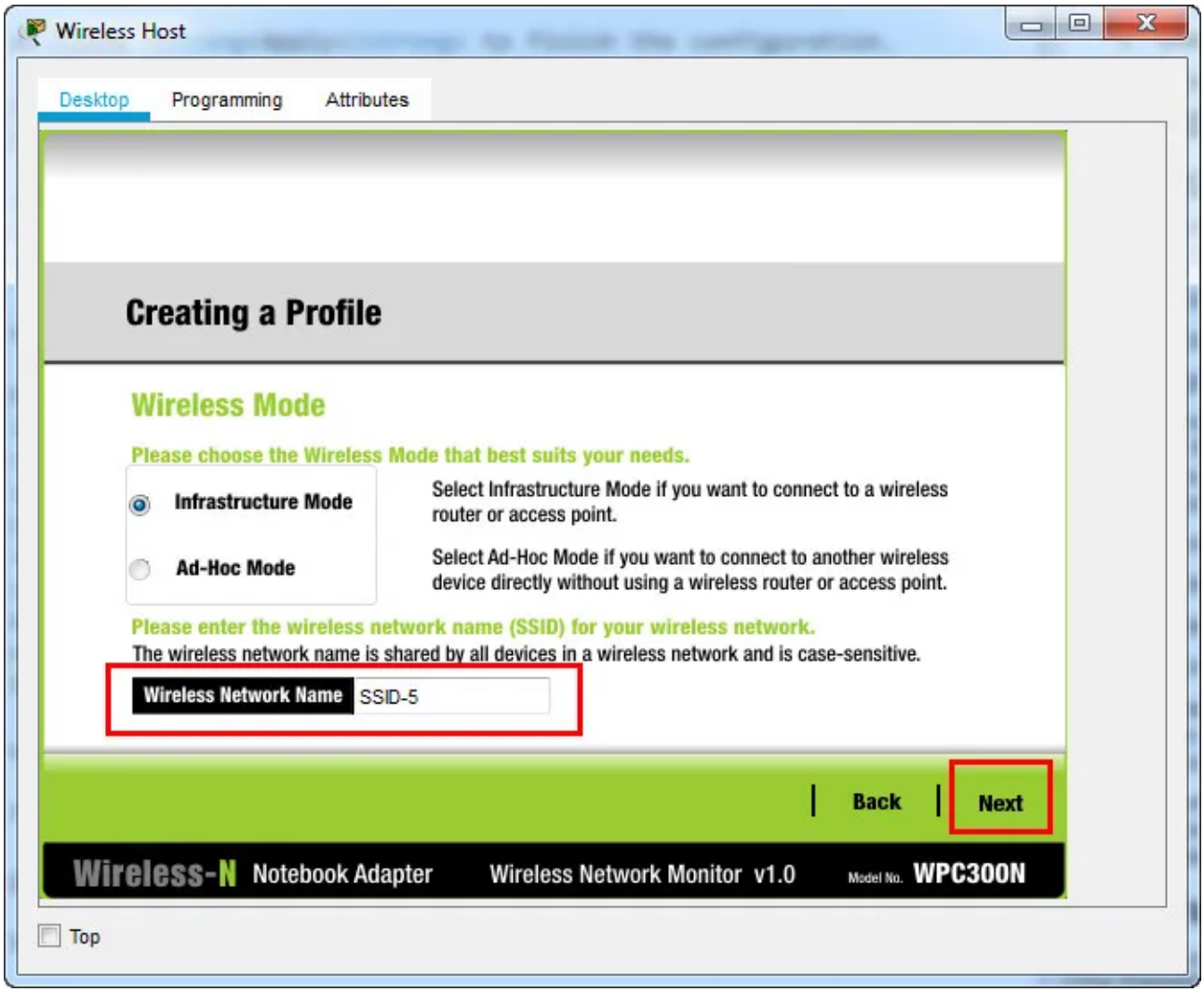
b. Click the **Profiles** tab and then click **New** to create a new profile. Name the profile **WLC NET**.



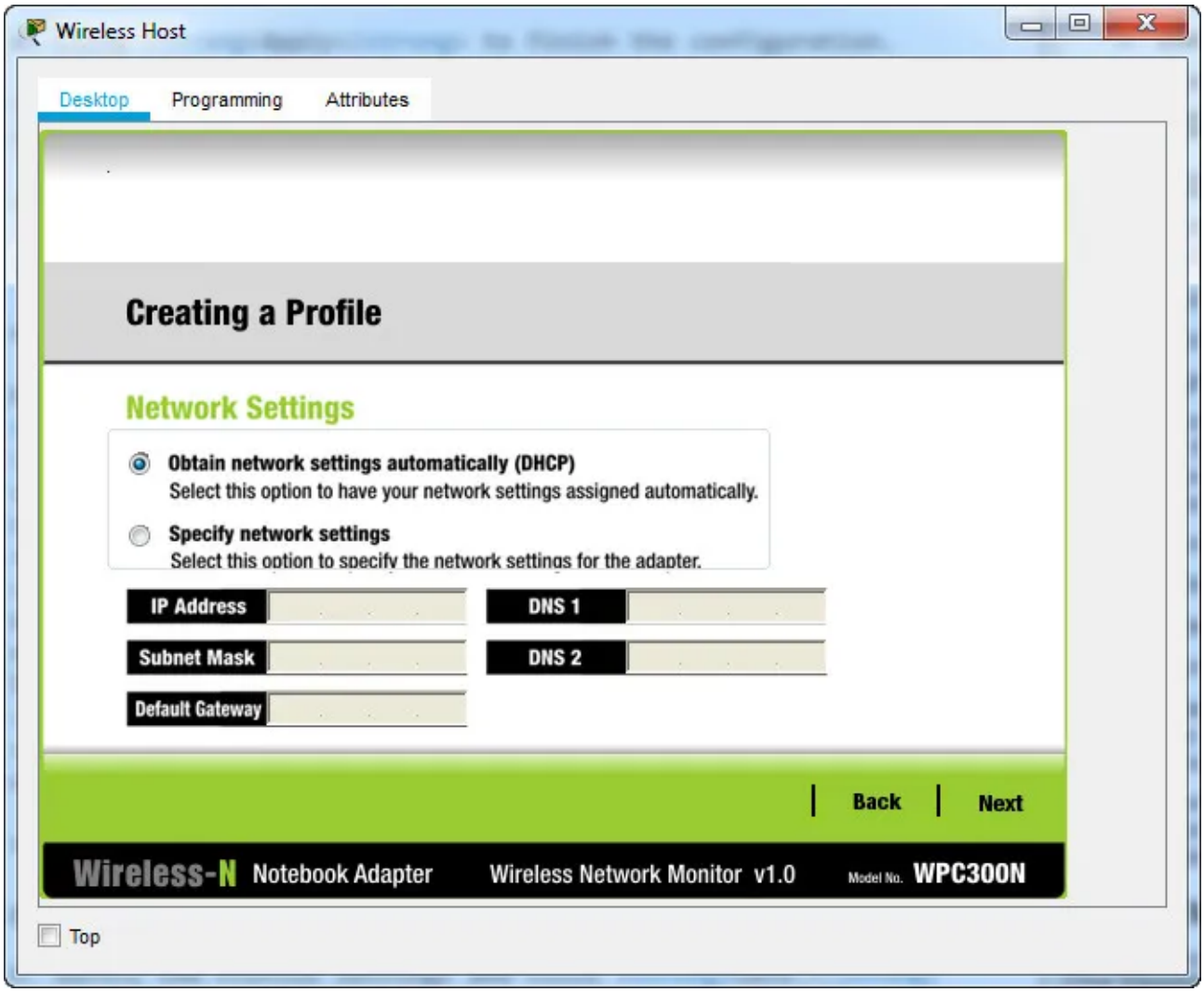
c. Highlight the Wireless Network Name for the WLAN that we created earlier and click **Advanced Setup.**



d. Verify that the SSID for the wireless LAN is present and then click **Next.** Wireless Host should see SSID-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.

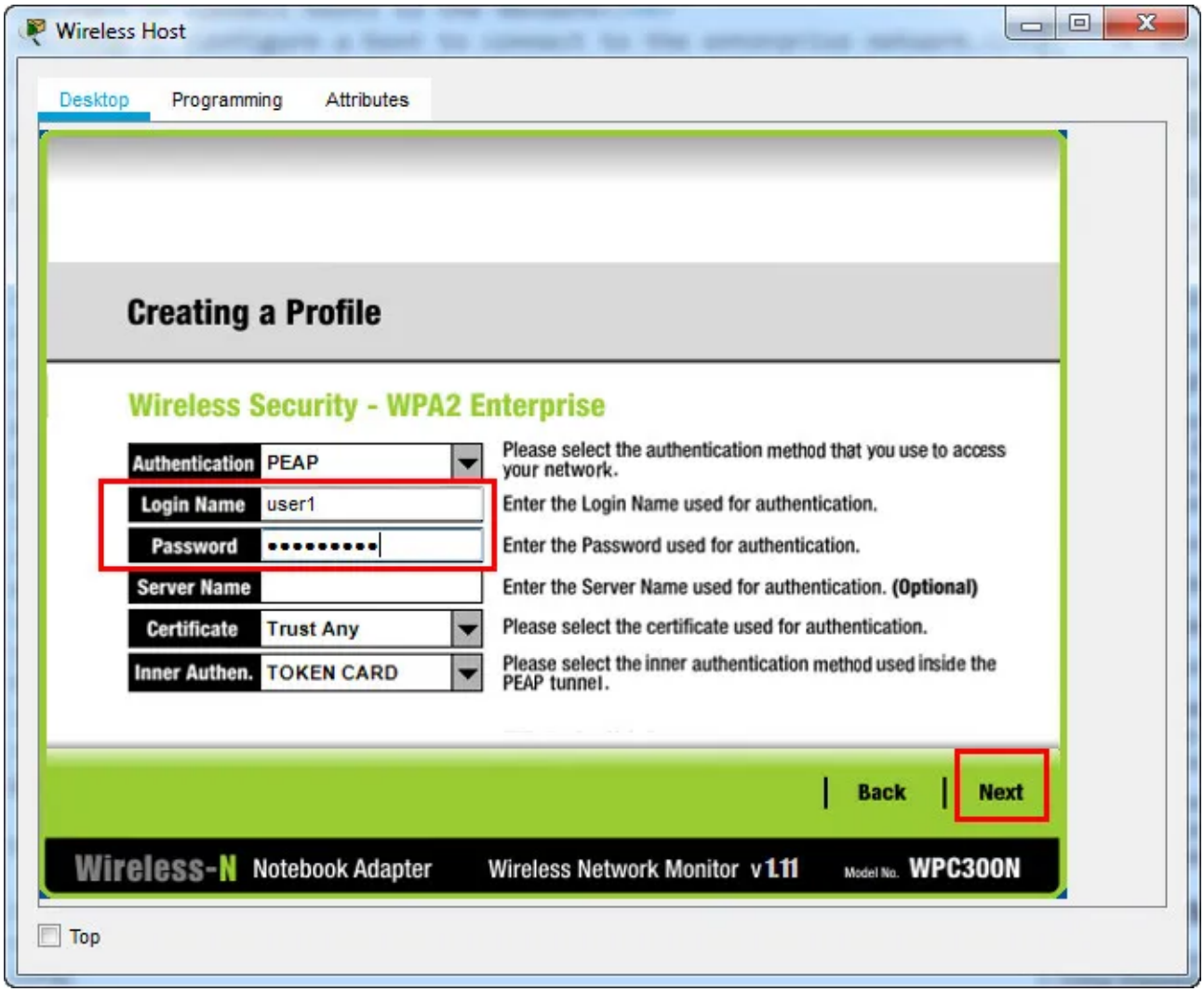


e. Verify that the DHCP network setting is selected and click **Next.**



f. In the Security drop down box, select **WPA2-Enterprise**. Click **Next.**

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

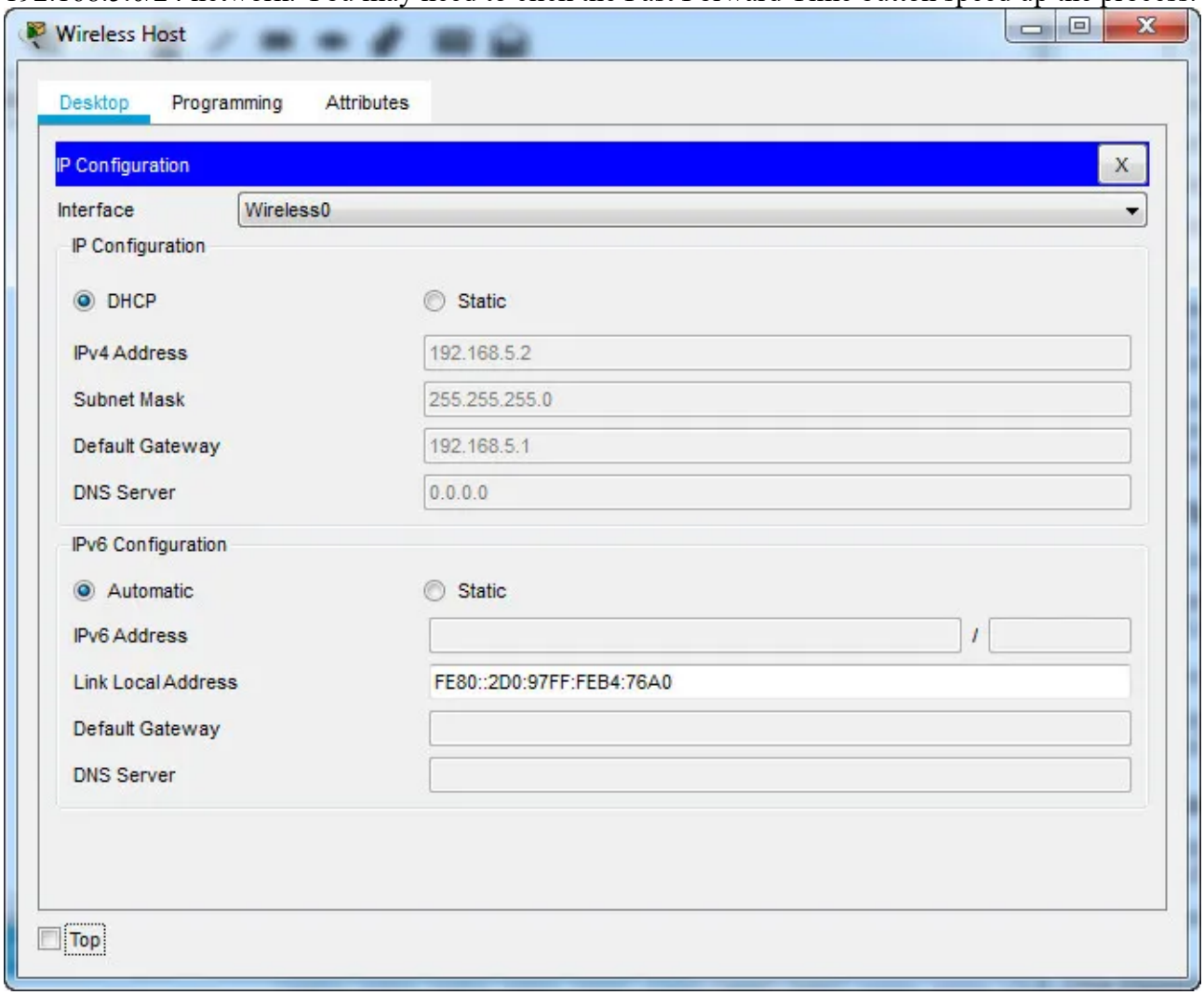


h. Verify the Profile Settings and click **Save.**

i. 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.

j. 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.

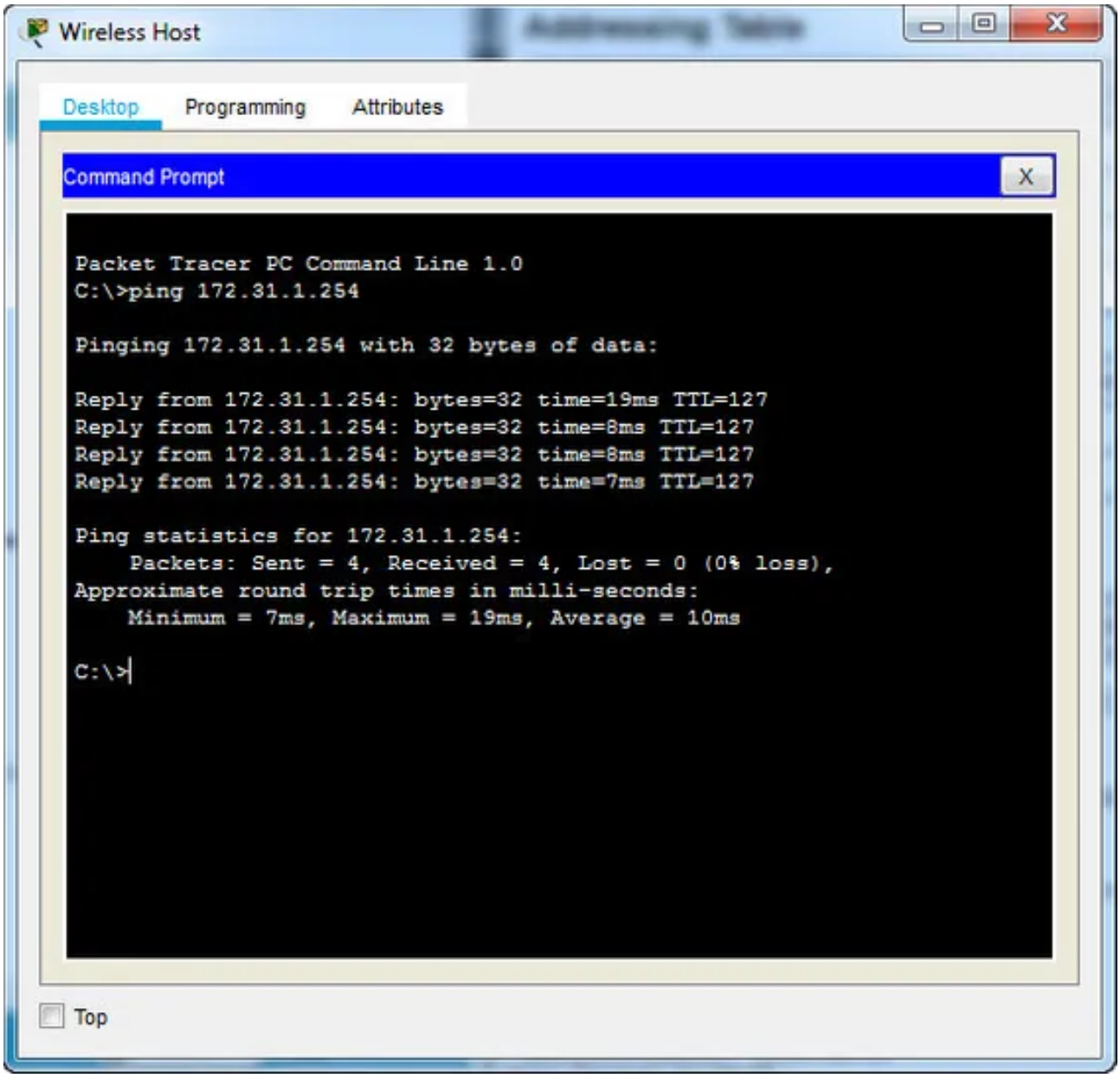
a. Close the PC Wireless app.

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

What network should the address be in? Explain.

The address should be in the 192.168.5.0/24 network. The interface was configured to get its IP address from 192.168.5.1. That is the router subinterface address for VLAN 5. DHCP is running on the router to provide addresses to wireless hosts.

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



Ping RADIUS Server

Reflection Questions

1. The RADIUS server uses a dual authentication mechanism. What two things are authenticated by the RADIUS server? Why do think this is necessary?

The RADIUS server authenticates both the WLC and the wireless host. The WLC makes the authentication request on behalf of the wireless host. It is necessary authenticate the WLC because it is important to protect the RADIUS server tables of usernames and passwords from intrusions by unauthorized devices. This is why a shared secret is required during configuration of the WLC to use the RADIUS server.

2. What are the advantages of WPA2-Enterprise over WPA2-PSK?

WPA2-PSK requires all hosts to use the same password. In addition, a username is not required. This means that it is more difficult to monitor when users connect to

and log out of the network. In addition, because so many hosts are using the same password, it is easier for a threat actor to steal the password and gain access to the network. Finally, if the PSK password needs to be changed, all users must be informed of the new password. This also creates a higher probability that the password will be stolen. WPA2-Enterprise using RADIUS allows for creation and administration of multiple unique user accounts. User behavior can easily be audited from the logs kept by the RADIUS server. In addition, users can easily be deleted or added as staffing in the enterprise changes.