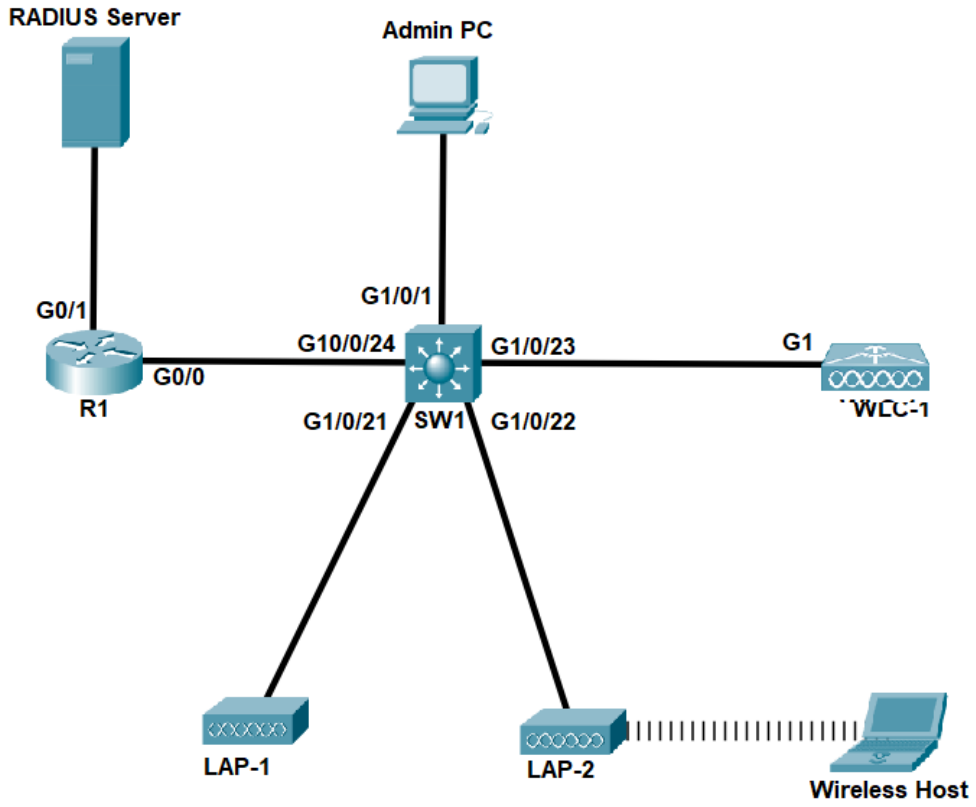
Networking Academy

Shaun Lim

Lab 5.2 Configure a WPA2 Enterprise WLAN on a WLC



Addressing Table

Device	Device Model	Interface	IP Address	Gateway
R1	Cisco 2901	G0/0/0.5	192.168.5.1/24	N/A
		G0/0/0.200	192.168.200.1/24	N/A
		G0/0/1	172.31.1.1/24	N/A
SW1	Cisco 3650	VLAN 200	192.168.200.100/24	N/A
LAP-1	Cisco 3702i	G0	192.168.200.251/24	192.168.200.1
LAP-2	Cisco 3702i	G0	192.168.200.252/24	192.168.200.1
WLC-1	Cisco 3504	Management	192.168.200.2/24	192.168.200.1
		WLAN-5 (dynamic)	192.168.5.2/24	N/A
RADIUS Server	Generic server host	NIC	172.31.1.254/24	172.31.1.1

Device	Device Model	Interface	IP Address	Gateway
Admin PC	Generic PC host	NIC	192.168.200.200/24	1921.68.200.1`
Wireless Host	Generic laptop	Wireless NIC	DHCP	

Objectives

In this activity, you will configure a new WLAN on a wireless LAN controller (WLC), including the VLAN interface that it will use. You will configure the WLAN to use a RADIUS server and WPA2-Enterprise to authenticate users.

- Build the topology and perform initial configurations
- Integrate WLCs and APs
- Configure a new WLAN on a WLC.
- Secure a WLAN with WPA2-Enterprise .
- Connect hosts to the new WLAN.

Background / Scenario

Wireless controllers (WLC) can reduce the administrative overhead of managing WLANs in a large network by centralizing the management and configuration of WLANs on multiple lightweight access points. To improve security due to the potentially large number of users connecting the WLAN, such type of deployments also often utilize AAA services such as RADIUS to provide individualized user logins through WPA enterprise mode.

This 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 management VLAN for device administration and also a user VLAN that will serve as the network for wireless users. You will also configure the WLC to use the enterprise RADIUS server to authenticate users connecting to the WLAN using WPA2.

Instructions

Part 1: Build the Network

In part 1, you will build the WLAN topology including the distribution system.

Step 1: Cable the network

Cable the network according to the topology diagram above. As some succeeding configurations of this activity are device-model specific, pay attention to device model indicated in the addressing table above when selecting devices to add to the topology.

Step 2: Configure the switch

SW1 will serve as the distribution switch of the network.

a. Create the following VLANs on SW1: **VLAN 5 (Users) VLAN 200 (Management)**

b. Create the **VLAN 200** interface and assign it the address **192.168.200.100**

c. Configure the interface connected to **R1** as a **trunk.** Since SW1 is a Layer 3 switch, the trunk encapsulation needs to be manually specified as 802.1q

```
SW1(config)#int range g1/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
```

d. Assign the interface connected **to Admin PC** as an access port of **VLAN 200**

Step 3: Configure the router

R1 will serve as default gateway and provide interVLAN routing to all VLANs of the newtork including the WLAN to be created. At the same time, it will also provide DHCP services to the WLAN.

a. Configure router interfaces and subinterfaces according to the addressing table

b. Create a DHCP pool named **WLAN_POOL** with the following settings:

Excluded addresses: 192.168.5.1 – 192.168.5.10

Network: 192.168.5.0/24

Default gateway: 192.168.5.1

Step 4: Configure the RADIUS server

The RADIUS server needs to be configured with the profile for the WLC and with user accounts. This allows the AAA service to recognize the WLC as a legitimate AAA client when it later contacts the RAIUD server to authenticate users attempting to connect to the WLAN.

a. Open the **RADIUS server** and configure its IP Address and default gateway. Ensure that it can ping the router.

b. Go to the **Services** tab and click on **AAA** on the services menu to configure RADIUS settings

c. **Enable** the service on port **1812.** Select the **On** radio button and input the port number

d. Register the WLC as an AAA client:

1) Under Network Configuration, input the following:

Client Name: **WLC1**

Client IP: **192.168.200.2**

Secret: **Cisco123**

2) Click Add

e. Create a user account:

1) Under user, input the following:

Username: **user1**

Password: **User1Pass**

2) Click Add

Step 5: Configure IP addresses of remaining devices

Configure the IP address and default gateway of the **Admin PC, WLC-1, LAP-1,** and **LAP-2** according to the addressing table.

Part 2: Interface the WLCs and APs

Wireless LAN Controller and lightweight APs physical ports rely on trunk links to communicate with the network and carry traffic from WLANs into the correct VLANs. In Part 2, you will configure the switch with the correct settings to interface with the WLC and APs, as well as perform initial settings on the WLC

Step 1: Configure SW1 trunk links to the WLC and LAPs

WLC and LAP ports function as trunk connections, which allow them to carry traffic for multiple WLANs corresponding to 1 VLAN each. In this step, you will set the SW1 ports connected to these devices as trunk using the management VLAN as the native VLAN.

Setting the management VLAN as the native VLAN of the WLC and LAP trunks is normally not a requirement on real networks; however due to a Packet Tracer issue, this additional step is necessary in order for the WLC management GUI to be accessible to a host browser.

a. Configure the port connected to WLC-1 **(G1/0/23)** as a **trunk** and set the management VLAN as its native VLAN.

```
SW1(config)#int range g1/23
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 200
```

b. Similarly configure trunking on ports connected to LAPs and turn on Power over Ethernet (PoE). This allows the LAPs to draw power from their Ethernet connection to the switch

```
SW1(config-if)#interface range g1/0/21-22
SW1(config-if-range)# switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport trunk native vlan 200
SW1(config-if-range)#power inline auto
```

Why would Power over Ethernet (PoE) be a usefu feature to have on a switch when integrating WLAN devices in the network?

> PoE is a useful feature to have on a switch when integrating WLAN devices in a network because it simplifies deployment of wireless access points by allowing both power and data to be supplied over a single Ethernet cable. In addition, PoE offers flexibility, as devices can be placed in locations that would prove difficult to have a power supply in, such as walls or ceilings.

c. Test that the Admin PC can ping the WLC and LAPs. Recheck trunk interface settings on the switch and IP addressing on the Admin PC, WLC and LAPs if pings do not work.

Step 2: Perform Initial WLC Setup

The management GUI of a WLC can be accessed using a browser similar to wireless router. When configuring a WLC for the first time, an administrator will need to do so using HTTP, then configure initial device settings using an initial setup menu.

a. Using the browser of the Admin PC, input the IP address of **WLC-1**in the navigation bar and wait for the initial login page to load. This may take a few minutes to load. You may use the fast forward feature of Packet Tracer to speed up this process.

b. When the page loads, create an administrator account. Use the user name **‘admin’** and password ‘**Cisco123**’. Retype the password to confirm then click **Start.**

c. The succeeding menu shows the required basic settings of the WLC. Under controller setup, use the following values:

System Name: **WLC1**

Management IP Address: **192.168.200.2**

Subnet Mask**: 255.255.255.0**

Default Gateway: **192.168.200.1**

Leave other parameters at default values then click **Next.**

d. Under the Wireless Network Creation menu, configure a new dummy network. This WLAN is placed on the same VLAN as device management interfaces hence we are merely doing so to fulfill initial setting requirements. We will be deleting this WLAN later and recreating a new one for the User VLAN. Use the following settings:

Network Name: **Dummy**

Passphrase / Confirm Passphrase: **Dummy123**

Leave other parameters at default values then click **Next.**

e. Leave the Advanced setting menu at default values and click **Next**

f. Recheck settings then click **Apply** to finish the initial setup and **OK** to allow the WLC to reboot.

g. Once initial settings are configured, The Web GUI of the WLC will no be accessible using HTTPS instead of HTTP. Wait a few seconds for the link lights of the WLC to turn green then change the URL in the browser navigation bar of **Admin PC** to https://192.168.200.2 to reconnect to **WLC-1.**

h. Click on the login button then supply the username and password configured to login. You will be brought to the WLC monitoring summary page.

Part 3: Create a new WLAN

In Part 3, you will create a new WLAN associated with VLAN 5 of the network which uses WPA2-Enterprise mode to authenticate users. This task involves registering the RADIUS server details on the WLC, creating a new VLAn interface, creating the new WLAN and settings its wireless and security configurations

Step 1: 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. This must match the scret used earlier to register the WLC on the RAIUD server. 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 2: 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.

a. 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.

b. 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.

c. Enter the name of the new interface. We will call it **WLAN-5** to make it more convenient in remembering which VLAN this interface belongs to. Configure the VLAN ID as **5**. This is the User VLAN that will carry traffic for the WLAN that we create later. Click **Apply**. This leads to a configuration screen for the VLAN interface.

d. First, configure the interface to use physical port number **1** since we are using the port to connect the WLC to the network switch. Multiple VLAN interfaces can use the same physical port because the physical interfaces are like dedicated trunk ports.

e. Address the interface as follows:

IP Address: **192.168.5.2**

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. Since the router is configured as a DHCP server for VLAN 5 hosts, 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 service on the router.

f. Be sure to click **Apply** to enact your changes and click **OK** to respond to the warning message. Click **Save Configuration** on the upper right area of the horizontal menu bar so that your configuration will be in effect when the WLC restarts.

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. This brings up the list of the existing WLANs on WLC. Click on the **Remove** link for the Dummy WLAN (rightmost of the table entry) created earlier.

b. 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.

c. 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.

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

e. 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.

f. 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 2.

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

h. Click to enable **FlexConnect Local Switching**. This allows the WLC to automatically configure switching and VLAN operations on detected access points.

Step 4: Configure WLAN security.

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

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

b. 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.

c. 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 1.

d. 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.

Step 5: Verify LAP Status.

Once a WLAN is created and enabled, its settings are automatically coordinated with LAPs recognized by the WLC.

Mouse over **LAP-1** and **LAP2** and observe the CAPWAP status and list of provided WLANs. What does the output tell you?

> The CAPWAP status for both LAP-1 and LAP-2 says “Connected to 192.168.200.2”, meaning both are connected to WLC-1’s management VLAN.

* If it does not show a working CAPWAP connection or a list of WLANs provided, check the WLC configuration.

Part 4: 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 using the **Physical** tab, install a WPC300N wireless NIC module. Refer to lab activity 5.1 if you need a step-by-step instruction to do so.

b. Open the **PC Wireless** app and click the **Profiles** tab and then click **New** to create a new profile. Name the profile **WLC NET**.

c. Click **Advanced Setup**. And input the SSID of the WLAN present and then click **Next**..

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

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

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

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

h. 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 or LAP-2. You can click the Fast Forward Time button to speed up the process if it seems to be taking too long.

Step 2: Test Connectivity.

a. Close the PC Wireless app.

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

What network should the address be in? Explain.

The address should be in the network 192.168.5.0, however it will not be assigned the addresses 192.168.5.1 to 192.168.5.10 since it was defined as excluded addresses, but the remaining addresses can be assigned to the devices connected to the WLAN. This is because the WLAN was configured to use DHCP.

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

Reflection Questions

1. What are the advantages of using a wireless LAN controller to manage a WLAN in a large organization?

   The advantages of using a Wireless LAN controller to manage a WLAN in a large organization is it simplifies the management of multiple access points, as well as making use of various security protocols to make the network more secure.

2. The RADIUS server uses a dual authentication mechanism which validates both the WLC as an AAA client and the user who is logging in to the network? Why do think is this mechanism necessary?

   The dual authentication mechanism is needed to ensure that only authorized users can access it and prevents rogue attackers from accessing the server. This is also so that there will not be any rogue devices that can infiltrate the network.

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

   WPA2-Enterprise has plenty of advantages over WPA2-PSK for large organizations. Firstly, it enables personalized and centralized control over Wi-Fi network access, requiring users to authenticate via their login credentials. Secondly, WPA2-Enterprise enhances security by utilizing a RADIUS server for authentication, employing more complex EAP protocol variants for authentication, and generating unique keying material between client and access point. Lastly, it ensures that users never handle encryption keys directly; these keys are securely generated per user session after authentication, preventing unauthorized access to the network key from user devices.