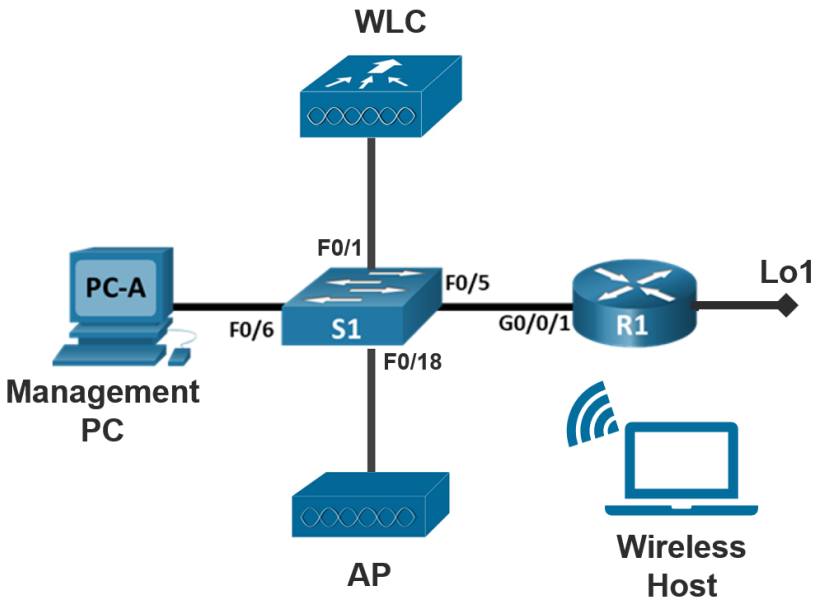
Module 13 Lab - Configure a Basic WLAN on the WLC



Addressing Table

Device	Interface	IP Address
R1	Lo1	10.10.10.1/24
	G0/0/1.1	192.168.200.1/24
	G0/0/1.20	172.16.20.1/24
S1	VLAN 20	172.16.20.2/24
	VLAN 1	192.168.200.2/24
AP	G0	DHCP
WLC	Management	192.168.200.3/24
	VLAN20	172.16.20.3/24
Management PC	NIC	192.168.200.4/24
Wireless Host	Wireless NIC	DHCP

Objectives

In this lab, you will explore some of the features of a wireless LAN controller. You will create a new WLAN on the controller and implement security on that LAN. Then you will configure a wireless host to connect to the new WLAN through an AP that is under the control of the WLC. Finally, you will verify connectivity.

- Connect to a wireless LAN controller GUI.
- Explain some of the information that is available on the WLC Monitor screen.
- Configure a WLAN on a wireless LAN controller.
- Implement security on a WLAN.
- Configure a wireless host to connect to a wireless LAN.

Background / Scenario

An organization is centralizing control of their wireless LAN by replacing their standalone access points with lightweight access points (AP) and a wireless LAN controller (WLC). You will be leading this project and you want to become familiar with the WLC and any potential challenges that may occur during the project. You will configure a WLC by adding a new wireless network and securing it with WPA-2 PSK security. To test the configuration, you will connect a laptop to the WLAN and ping devices on the network.

Required Resources

- 1 Routers (Cisco 2901 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 Cisco Wireless Controller (Cisco Firmware Release 8.3 image or comparable)
- 1 Cisco lightweight Access Point (Cisco Firmware Release 8.3 image or comparable)
- 1 PCs (Windows with a terminal emulation program, such as Tera Term)
- 1 PCs with Wireless NIC
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the Router and switch.

Step 1: Configure basic settings for router and switch.

a. Assign a device name to the router.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password and enable login.

e. Assign **cisco** as the VTY password and enable login.

f. Encrypt the plaintext passwords.

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

h. Save the running configuration to the startup configuration file.

i. Set the clock on the router to today's time and date.

Note: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command

Step 2: Configure Inter-VLAN Routing on R1

a. Activate interface G0/0/1 on the router.

b. Configure sub-interfaces for each VLAN as required by the IP addressing table. All sub-interfaces use 802.1Q encapsulation and are assigned the address from the IP address table. Ensure VLAN 1 is the native VLAN. Include a description for each sub-interface.

c. Create the Loopback interface 1 and configure IP Address from the Address table.

d. Verify the sub-interfaces are operational.

Step 3: Create VLANs on S1.

a. Create the required VLANs on S1 from the table above.

b. Configure and activate the interfaces VLAN 1 and VLAN 20 using IP addresses from the table above.

c. Assign port F0/18 on S1 to VLAN 20, configure it for static access mode.

Step 4: Manually configure S1's interfaces F0/1 and F0/5 as an 802.1Q trunk.

a. Change the switchport mode on the interface to force trunking.

b. As a part of the trunk configuration, set the native VLAN to 1.

c. As another part of trunk configuration, specify that VLANs 1, and 20 are allowed to cross the trunks.

d. Save the running configuration to the startup configuration file.

e. Verify trunking status.

Part 2: Configure and verify two DHCPv4 Servers on R1

In Part 2, you will configure and verify a DHCPv4 Server on R1. The DHCPv4 server will service two VLANs, VLAN1 and VLAN20.

Step 1: Configure R1 with DHCPv4 pools for the two supported subnets.

a. Exclude the first five useable addresses from each address pool.

b. Create the DHCP pools, VLAN1 and VLAN20

c. Specify the networks that this DHCP server is supporting (192.168.200.0/24 for VLAN1 and 172.16.20.0/24 for VLAN20).

d. Configure the domain name as ccna-lab.com

e. Configure the appropriate default gateway for each DHCP pool (192.168.200.1 for VLAN1 and 172.16.20.1 for VLAN20).

f. Configure the lease time for 2 days 12 hours and 30 minutes.

Step 2: Save your configuration

Save the running configuration to the startup configuration file.

Step 3: Verify the DHCPv4 Server configuration

a. Issue the command **show ip dhcp pool** to examine the pool details.

b. Issue the command **show ip dhcp bindings** to examine established DHCP address assignments.

c. Issue the command **show ip dhcp server statistics** to examine DHCP messages.

Part 3: Configure Cisco Wireless Controller and Lightweight Access Point

Now you will setup and create a new wireless LAN on the WLC and Access Point. You will configure the settings that are required for hosts to join the WLAN.

Step 1: Initial Setup for Wireless Controller.

The Controller needs to be first setup using CLI over a console cable. The Controller is connected to a console cable and powered on, the boot sequence showed starting all the services. Follow the setup wizard the inputs bellow (in red).

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:yes

System Name [Cisco_43:5c:04] (31 characters max): CNIT-134-WLC
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (3 to 24 characters): cisco123!
Re-enter Administrative Password                : cisco123!

Enable Link Aggregation (LAG) [yes][NO]: no

Management Interface IP Address: 192.168.200.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.200.1
Cleaning up Provisioning SSID
Management Interface VLAN Identifier (0 = untagged):0
Management Interface Port Num [1 to 4]: 1

Management Interface DHCP Server IP Address: 192.168.200.1

Virtual Gateway IP Address: 1.1.1.1
```

```
Multicast IP Address: 239.1.1.1

Mobility/RF Group Name: Mobi-134

Network Name (SSID): Management-[your name]

Configure DHCP Bridging Mode [yes][NO]: yes
Warning! Enabling Bridging mode will disable Internal DHCP server and DHCP Proxy
feature.
May require DHCP helper functionality on external switches.

Allow Static IP Addresses [YES][no]: yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes

Enter the date in MM/DD/YY format: 02/22/21
Enter the time in HH:MM:SS format: 16:49:00

Would you like to configure IPv6 parameters[YES][no]: no

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Cleaning up Provisioning SSID
```

```
Configuration saved!

Resetting system with new configuration...
```

Step 2: WLC web interface login.

After the Controller has reloaded, you can access its web interface at ***http://192.168.200.3***. Use the username **cisco** and password **cisco123!** that you just setup above to login.

Step 3: Create VLAN 20 on WLC.

a. From the WLC GUI choose **Advance**, choose **Controller > Interfaces**. The **Interfaces** page lists all the interfaces that are configured on the WLC in order to create a new dynamic interface, click **New**.

b. Enter the Interface Name as ***VLAN20*** and VLAN Identifier as ***20*** and click **Apply**.

c. Enter the parameters specific to this VLAN. Some of the parameters include the IP Address (***172.16.20.3***), Netmask (***255.255.255.0***), Gateway (***172.16.20.1***), and the DHCP server IP address (***192.168.200.1***), Port Number (***1***) and click **Apply.**

d. Verify the interface configuration. Click the **Controller** tab in the menu at the top of the window and choose **Interfaces** from the menu on the left.

Step 4: Create WLAN for VLAN 20 on WLC.

a. Click the **WLAN** stab in the menu at the top of the window and click **Create New**.

b. Enter the Service set identifier (SSID) ***[Your Name -VL20]*** and Profile Name ***[Your Name -VL20]*** and click **Apply**.

c. Select ***VLAN 20*** from the **Interface/Interface Group(G)** drop-down menu at the bottom of the window and click **Apply**. In this case, SSID ***[Your Name -VL20]*** is tied to Interface Name VLAN 20.

d. Click the **Security** tab. Under the **Layer 2** tab, select **WPA+WPA2** from the **Layer 2 Security** drop down box. This will reveal the WPA parameters.

e. Click the checkbox next to **WPA2 Policy**. This will reveal additional security settings. Under **Authentication Key Management**, enable **PSK**.

f. Now you can enter the pre-shared key that will be used by hosts to join the WLAN. Use **cisco123!** as the passphrase.

g. Click **Apply** to save these settings.

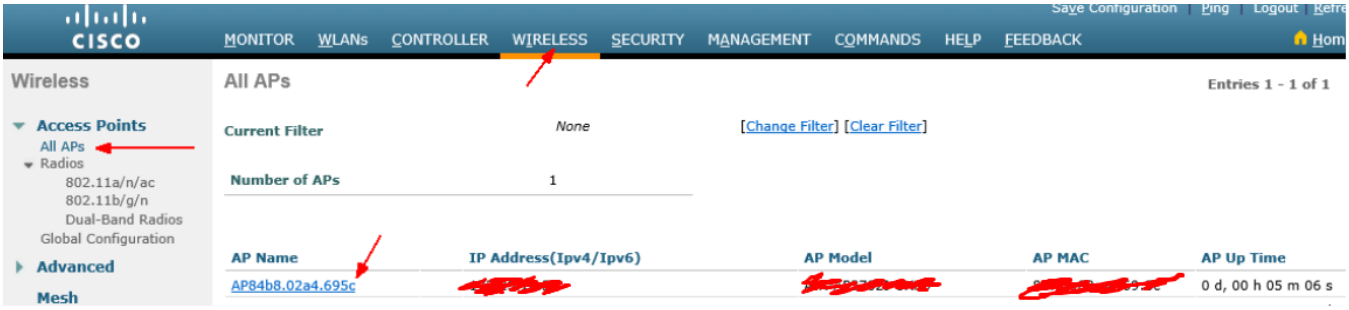
Step 5: Setup for Lightweight Access Points.

This is the beauty of deploying a controller-based system. The configuration on a LAP is minimum. All it needs is connecting to the same network of the WLC's management so that it can reports to the Controller. Once all the LAP is registered with the Controller, you can forget about it.

a. Connect the AP to a VLAN1's Port on S1 (it is on the same broadcast domain with the WLC)

b. Connect the LAP with Console cable, and power it on. You are going to see some log messages about getting an IP from the DHCP server.

c. As soon as the LAP is auto configured, the magic happens. You'll see bunch of log messages coming out of the console and the LED turns Blue, Red, Green and flashing. The LAP is now registering with the Controller; the Controller tells it to upgrade its code if it finds code version inconsistency. After about 3 to 5 minutes, the first LAP appears in your Controller's management console.



d. Connect the AP to a Port ***F0/18*** on S1 and wait until you see the AP appears in your Controller's management console (again).

Part 4: Connect a Wireless Host to the WLAN

Step 1: Connect to the network and verify connectivity.

a. On **Wireless Host** Select the SSID ***[Your Name -VL20]*** and click the **Connect** button. ***Take a screenshot (for submission)***

b. Enter the pre-shared key that you configured for the WLAN and click **Connect**.

c. Open Command Prompt and enter *ipconfig /all* to verify the wireless IP Address. ***Take a screenshot (for submission)***

d. From Wireless Host, ping the WLAN default gateway and the Loopback interface of R1 to verify that the laptop has full connectivity. **Take a screenshot (for submission)**

e. Repeat these steps with the SSID ***Management-[your name]***. ***Take screenshots (for submission).***