Lab 9: Configuring WLANs with DHCP Option 43 and Multiple SSIDs

Activity Objective:
- Implement campus network infrastructure to support wireless.
- Configure WLANs with DHCP option 43
- Configure WLC as a DHCP Proxy
- Configure multiple SSIDs that will tie into proper VLANs.

Note: Remove any existing configuration on all devices before you begin the lab.

Background

In this lab, you will configure the network infrastructure (Layer 2 and Layer 3 switches) to prepare for a wireless solution involving a wireless LAN (WLAN) controller and lightweight wireless access point (CAPWAP).

You will be configuring two SSIDs that will link into VLANs:
- SSID: dataxx is for Staff (Private), VLAN 2
- SSID: GUESTNET-x is for Guests (Public), VLAN 100
Lab 9: Configuring WLANs with DHCP Option 43 and Multiple SSIDs

**Required Tasks:**

1. Prepare the switches for the lab
2. Configure Multilayer and layer 2 switches
   a. Configure VLANs, trunks, and VTP.
   b. Configure SVIs
   c. Configure DHCP
   d. Configure infrastructure wireless support
   e. Enable IP routing on DLS1
3. Configure initial settings on the WLAN controller.
   a. Configure the basic WLC.
   b. Configure the WLC as a DHCP proxy
   c. Configure WLANs
4. Verification
5. Erase configuration on the WLC

**Step 1: Prepare the switches for the lab.**

a. Erase the startup-config file, delete the vlan.dat file, and reload each switch to clear the previous configurations.

b. Configure the switch hostnames as shown in the topology.

**Step 2: Configure VLANs, trunks, and VTP.**

VLAN 1 – Management VLAN for the WLC.
VLAN 50 – The CAPWAP is in this VLAN.
VLAN 2 and VLAN 100 – Hosts in the WLANs

a. Configure DLS1 as a VTP server, and ALS1 as a client in the VTP domain CMPN371.

DLS1(config)# vtp mode server
DLS1(config)# vtp domain CMPN371
DLS1(config)# vtp version 2
DLS1(config)# vlan 2,50,100

DLS1(config-vlan)# interface fastEthernet 0/8
DLS1(config-if)# switchport trunk encapsulation dot1q
DLS1(config-if)# switchport mode trunk

ALS1(config)# vtp mode client
ALS1(config)# interface fastEthernet 0/8
ALS1(config-if)# switchport mode trunk

b. Verify that VTP traffic has passed between the switches by comparing the non-zero VTP configuration revision using the show vtp status command.

DLS1# show vtp status
VTP Version : running VTP2
Lab 9: Configuring WLANs with DHCP Option 43 and Multiple SSIDs

<table>
<thead>
<tr>
<th>Configuration Revision</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum VLANs supported locally</td>
<td>1005</td>
</tr>
<tr>
<td>Number of existing VLANs</td>
<td>10</td>
</tr>
<tr>
<td>VTP Operating Mode</td>
<td>Server</td>
</tr>
<tr>
<td>VTP Domain Name</td>
<td>CMPN371</td>
</tr>
<tr>
<td>VTP Pruning Mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>VTP V2 Mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>VTP Traps Generation</td>
<td>Disabled</td>
</tr>
<tr>
<td>MD5 digest</td>
<td>0xE3 0x5B 0x2E 0x20 0x27 0xF9 0xF1 0x1B</td>
</tr>
<tr>
<td>Configuration last modified by 0.0.0.0 at 3-2-10 00:49:40</td>
<td></td>
</tr>
<tr>
<td>Local updater ID is 0.0.0.0 (no valid interface found)</td>
<td></td>
</tr>
</tbody>
</table>

ALS1# show vtp status
VTP Version : running VTP2
Configuration Revision : 1
Maximum VLANs supported locally : 255
Number of existing VLANs : 10
VTP Operating Mode : Client
VTP Domain Name : CMPN371
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xE3 0x5B 0x2E 0x20 0x27 0xF9 0xF1 0x1B
Configuration last modified by 0.0.0.0 at 3-2-10 00:49:40

Step 3: Configure SVIs.

Configure all the switch virtual interfaces (SVIs) shown in the diagram for DLS1.

DLS1(config)# interface vlan 1
DLS1(config-if)# ip address 172.16.1.1 255.255.255.0
DLS1(config-if)# no shutdown

DLS1(config-if)# interface vlan 2
DLS1(config-if)# ip address 172.16.2.1 255.255.255.0
DLS1(config-if)# no shutdown

DLS1(config-if)# interface vlan 50
DLS1(config-if)# ip address 172.16.50.1 255.255.255.0
DLS1(config-if)# no shutdown

DLS1(config-if)# interface vlan 100
DLS1(config-if)# ip address 172.16.100.1 255.255.255.0
DLS1(config-if)# no shutdown

Step 4: Configure DHCP.

DHCP gives out dynamic IP addresses on a subnet to network devices or hosts rather than statically setting the addresses. This is useful when dealing with CAPWAPs, which usually do not have an initial configuration. The WLAN controller that the LAP associates with defines the configuration. A lightweight access point can dynamically receive an IP address and then communicate over IP with the WLAN controller.

a. Configure DLS1 to exclude the first 150 addresses from each subnet from DHCP to avoid conflicts with static IP addresses using the `ip dhcp excluded-address low-address [high-address]` global configuration command.
DLS1(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.150
DLS1(config)# ip dhcp excluded-address 172.16.2.1 172.16.2.150
DLS1(config)# ip dhcp excluded-address 172.16.50.1 172.16.50.150
DLS1(config)# ip dhcp excluded-address 172.16.100.1 172.16.100.150

b. To advertise on different subnets, create DHCP pools with the `ip dhcp pool name` command. After a pool is configured for a subnet, the DHCP server processes requests on that subnet, because it is enabled by default. From the DHCP pool prompt, set the network and mask to use with the `network address /mask` command. Set a default gateway with the `default-router address` command.

c. VLAN 50 also uses the `option` command, which allows you to specify a DHCP option. In this case, `option 43` is specified (a vendor-specific option), which gives the CAPWAP the IP address of the WLAN controller Manager interface. It is specified in a hexadecimal TLV (type, length, value) format. This configuration uses `f104ac100164`, which is made up of the following:

- **f1** is the hardcoded type of option.
- **04** represents the length of the value (an IP address is 4 octets).
- **ac100164** is the hexadecimal representation of 172.16.1.100, which is going to be the management interface address of the WLAN controller.

DLS1(config)# ip dhcp pool pool1
DLS1(dhcp-config)# network 172.16.1.0 /24
DLS1(dhcp-config)# default-router 172.16.1.1

DLS1(dhcp-config)# ip dhcp pool pool2
DLS1(dhcp-config)# network 172.16.2.0 /24
DLS1(dhcp-config)# default-router 172.16.2.1

DLS1(dhcp-config)# ip dhcp pool pool50
DLS1(dhcp-config)# network 172.16.50.0 /24
DLS1(dhcp-config)# default-router 172.16.50.1
DLS1(dhcp-config)# option 43 hex f104ac100164
DLS1(dhcp-config)# ip dhcp pool pool100
DLS1(dhcp-config)# network 172.16.100.0 /24
DLS1(dhcp-config)# default-router 172.16.100.1

### Step 5: Configure infrastructure wireless support.

On ALS1, configure IP Helper address for VLAN 2, VLAN 50 and VLAN 100.

DLS1 will route the traffic between the VLANs. Configure the interface on DLS1 that connects to the WLAN controller as an 802.1Q trunk.

DLS1(config)# interface fastEthernet 0/5
DLS1(config-if)# switchport trunk encapsulation dot1q
DLS1(config-if)# switchport mode trunk

### Configure IP helper-address on ALS1:

ALS1(config)# interface vlan 2
ALS1(config)# ip helper-address 172.16.2.1
ALS1(config)# interface vlan 50
Lab 9: Configuring WLANs with DHCP Option 43 and Multiple SSIDs

ALS1(config)# ip helper-address 172.16.50.1

ALS1(config)# interface vlan 100
ALS1(config)# ip helper-address 172.16.100.1

**Step 6: Enable IP routing on DLS1.**

a. Enabling IP routing on DLS1 lets DLS1 route between all subnets shown in the diagram. DLS1 can effectively route between all the VLANs configured because it has an SVI in each subnet.

DLS1(config)# ip routing

b. Each IP subnet is shown in the output of the show ip route command issued on DLS1.

DLS1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 6 subnets
   C     172.16.50.0 is directly connected, Vlan50
   C     172.16.1.0 is directly connected, Vlan1
   C     172.16.2.0 is directly connected, Vlan2
   C     172.16.100.0 is directly connected, Vlan100

**Note:** At this point. Full connectivity should have established. If not, troubleshooting the issue(s) before moving onto the next tasks.

**Step 7: Configure initial settings on the WLAN controller.**

On the WLC’s console screen, if you are asked to input **username** and **password**, there is an existing configuration. So you have to clean it up. Here’s HOW-TO:

1. Open WLC’s console screen – It is very important to have the WLC console screen opened before rebooting the WLC.

2. Reboot the controller.

3. When you are prompted for a username, enter **Recover-Config** (case sensitive) to restore the factory default configuration.

Once finishing up rebooting the controller, terminate auto-configuration.

**Caution:** Verify that the first selection you see is **system name**. When enabling the HyperTerminal/Tara term session to your controller, you might have pressed Enter to test the connection, and the setting you had at that time might have become the default selection. If
Lab 9: Configuring WLANs with DHCP Option 43 and Multiple SSIDs

that has become the default, and if the first selection you see is not System Name, then enter a hyphen (-) and press Enter go back to the System Name selection.

*** Repeat the procedure as many times as needed to get back to the System Name selection.

a. System name [Cisco_34:26:a3]: 2504-x (where x is your pod number)
b. Enter Administrative user name (24 characters max) :adminx (where x is your pod number)
c. Enter Administrative password (24 characters max) :Cmpn371
d. Re-enter Administrative password :Cmpn371
e. Enter the management interface information. The management interface communicates with the management workstation in VLAN 1. The interface number is 1, because this is the port trunked from the controller to the switch. The VLAN number is 0 for untagged. It is untagged because VLAN 1 is the native 802.1Q VLAN and is, therefore, sent untagged through 802.1Q trunks.

Management Interface IP Address: 172.16.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 172.16.1.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1

f. Configure the virtual gateway IP address as 1.1.1.1 (this is acceptable because you are not using this for routing). The virtual gateway IP address is typically a fictitious, unassigned IP address, such as the address we are using here, to be used by Layer 3 Security and Mobility managers.

Virtual Gateway IP Address: 1.1.1.1

g. Configure the mobility group podx, and network name as CMPN371-x. Configure DHCP Bridging Mode and allow static IP addresses, but do not configure a RADIUS server now.

Mobility/RF Group Name: podx (where x is your pod)
Network Name (SSID): CMPN371-x (where x is your pod)

Configure DHCP Bridging Mode [yes][no]: yes
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.

h. Use the defaults for the rest of the settings.

Enter Country Code (enter 'help' for a list of countries) [US]: CA
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
Configuration saved!
Resetting system with new configuration...

Note: Wireless equipment varies from country to country. Make sure to use the appropriate country code.
Note: Configure the time and date through the web interface.

Step 8: Configure the WLANs - Enabling DHCP Proxy

a. When the WLAN controller has finished restarting, log onto the web interface of the WLC.

b. From the controller web interface, in the upper menu, navigate to Controller>Advanced>DHCP, and check mark on “Enabling DHCP Proxy”

c. From the controller web interface, in the upper menu, navigate to WLANs> finding the WLAN that you just configured, and disable security settings on Layer 2 and 3.

d. Make sure you have the correct time and date on the WLC.

Step 9: Configure Staff WLAN

- Configure Staff WLAN with dynamic interface.
  - Parameters and values for the Staff WLAN:
    I. Interface Name: **Staff_VLAN**
    II. Port number: **1**
    III. VLAN ID: **2**
    IV. The IP address: **172.16.2.100/24**
    V. The gateway: **172.16.2.1/24**
    VI. Primary DHCP Server: **172.16.2.1/24**
    VII. SSID: **dataxx** (where x is your pod number)
    VIII. Profile Name: **Staff_Only**
    IX. Layer2 Security drop down arrow choose **None**.
Step 10: Configure Guest WLAN

- Configure Guest WLAN with dynamic interface.
- Parameters and values for the Guest WLAN:
  
  I. Interface Name: **GUEST_VLAN**
  II. Port number: **1**
  III. VLAN ID: **100**
  IV. The IP address: **172.16.100.100/24**
  V. The gateway: **172.16.100.1/24** (where x is your pod number)
  VI. Primary DHCP Server: **172.16.100.1/24**
  VII. SSID: **GUESTNET-X** (where x is your pod number)
  VIII. Profile Name: **Public_Guest_Access**
  IX. Layer2 Security drop down arrow choose **None**.

Step 11: Verification

- dataxx: 172.16.2.xx /24
- GUESTNET-X: 172.16.100.xx /24

On wireless clients, connecting to the both SSIDs, and issue ping commands. The ping should work between two hosts, If not troubleshooting the issue (s).
Reflection

Question 1: Explain how does option 43 work?

Question 2: If you chose Staff_VLAN interface instead of GUEST_VLAN, when you configured the GUEST WLAN. What are the consequences?

Question 3: What static interface (s) was provided by the WLC 2504 by default?

Question 4: List the dynamic interface (s) that you created in this lab.

Question 5: List top-level sections of the Cisco controller-2504. (Hint – Monitor, WLANs etc...)

Step 12: Erase WLC configuration

Please make sure this task is completed for other students.

Sign-off: