Lab 4-3: Cisco Mobility Express

Lab Summary

CCNA 200-301 exam includes some newer wireless architecture topics. The questions are based on wireless fundamentals and configuration of access points. Cisco Mobility Express has a GUI that is accessed via web browser for deploying Cisco APs. The new architecture support dual role of controller and access point. The new CCNA exam will require you to know how to configure controllers and access points from web-based GUI only.

HTTP Secure Server

Configure HTTP server for web browser access and encryption to manage Cisco network devices. The following commands enable HTTP secure server on a wireless access point with local authentication.

> AP-1(config)# **ip http secure-server**
>
> AP-1(config)# **ip http authentication local**
>
> AP-1(config)# **end**
>
> AP-1(config)# **copy run start**
>
> AP-1(config)# **show run**

Cisco Mobility Express Management Access

- Initial configuration is via web browser access
- CiscoAirProvision SSID advertised by the master AP
- Password: **password**
- Enter **http://192.168.1.1** address from your web browser.
- The laptop is assigned an IP address from the subnet 192.168.1.0/24

Wireless LAN (WLAN)

1. WLAN ID, Profile Name and SSID
2. Security Settings: Open, WPA2-PSK, WPA2, Guest
3. DHCP Server: Controller / Server / Router
4. Enable VLAN Tagging: For Multiple SSID/VLANs and native VLAN
5. Firewall ACL: Only When VLAN Tagging Enabled
6. QoS: Platinum, Gold, Silver, Bronze

Access Points

1. AP Mode: AP/Controller
2. DHCP Enabled: yes/no
3. RF Band Selection: dual, 2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n/ac)
4. Channel Assignment: automatic (DCA), manual
5. Channel Width: 2.4 GHz (20 MHz), 5 GHz (Auto, 20 MHz, 40 MHz, 80 MHz)
6. Transmit Power: 1 to 8 (1 = highest) or automatic based on receiver signal

Switch Trunking

1. Enable Switch Port Trunk Mode
2. Configure Native VLAN
3. Configure VLAN Pruning (allowed VLANs)

WLAN Security

- Open authentication has no security

- WPA2-PSK (personal) has a passphrase configured on the controller and each client. There is no local or external authentication server.

- WPA2 (Enterprise) is the default and based on either a local controller authentication database or external RADIUS server. You would create LEAP users for local authentication. Configure the IP address of RADIUS server, UDP port 1812 and a shared secret ascii key)

- Guest security option is configured with WPA2-PSK or captive portal with a username and password login. You can configure security credentials on an internal or external web server and for 24 hour access. CMX cloud service is an option for guest authentication as well.

QoS (per VLAN)

NBAR2 enables real-time application layer monitoring and analysis of traffic to optimize performance

- Platinum (voice) - designed for voice over wireless
- Gold (video) - video applications
- Silver (best effort) - normal mixed bandwidth allocation for clients.
- Bronze (Background) - assigns lowest bandwidth for guests.

<u>Lab Notes</u>

Cisco Mobility Express architecture supports controller software on lightweight access points (LAP). That enables LAP operational mode or AP/Controller operational mode.

- AP configuration is available from Console (CLI), browser or Cisco DNA.

- AP controller mode is an overlay element of Cisco DNA architecture.

- Master AP = LAP + Controller

- The following access points support LAP Mode or LAP + Controller Mode: 4800, 3800, 2800, 1850, 1830, 1815, 1560, 1540

- The default system image on access points is AP mode only (CAPWAP).

- Cisco Mobility Express system image must be installed on an access point to support controller mode.

- Each WLAN has a unique WLAN ID, profile name (WLAN name), and SSID.

- The WLAN name and SSID can have up to 32 characters.

- The maximum number of WLANs per access point is 16.

- Different WLANs can be assigned to the same SSID as well using attributes.

- Create a unique profile name for each WLAN when creating WLAN with same SSID

- You cannot map a WLAN to VLAN0 or map VLAN 1002 to 1006.

- Dual-stack clients with static IPv4 addresses are not supported.

- Broadcast SSID is enabled

Master Controller Election

The master AP election is based on the following priority.

1. User-defined (manually configured)
2. **Then** access point with least client load
3. **Then** access point with lowest MAC address