

Packet Tracer - Configure a WPA2 Enterprise WLAN on the WLC

Part 1: Create a new WLAN

Step 1: Create a new VLAN interface.

The screenshot shows the Cisco Packet Tracer interface with a network diagram on the left and the configuration window for the WLC on the right. The network diagram includes a RADIUS Server, Admin PC, R-1, S-1, WLC-1, LAP-1, and a Wireless Host. The configuration window is titled 'Admin PC' and shows the 'Web Browser' tab with the URL 'https://192.168.200.254/frameInterfaceEdit.html'. The 'Controller' tab is selected, and the 'Physical Information' section is expanded. The 'VLAN Identifier' is set to 5, and the 'IP Address' is 192.168.5.254. The 'Netmask' is 255.255.255.0, and the 'Gateway' is 192.168.5.1. The 'DHCP Information' section is also expanded, showing the 'Primary DHCP Server' as 192.168.5.1. The 'Access Control List' section is set to 'none'.

Step 2: Configure the WLC to use a RADIUS server

The screenshot shows the Cisco Packet Tracer interface with a network diagram on the left and the configuration window for the WLC on the right. The network diagram is the same as in the previous screenshot. The configuration window is titled 'Admin PC' and shows the 'Web Browser' tab with the URL 'https://192.168.200.254/frameRadiusLat.html'. The 'Security' tab is selected, and the 'RADIUS Authentication Servers' section is expanded. The 'Auth Called Station ID Type' is set to 'IP Address'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen'. The 'Framed MTU' is set to 1300. The 'Network User' table is shown with the following data:

| Network User | Management | Server Index | Server Address(Ipv4/Ipv6) | Port |
|--------------|-------------------------------------|--------------|---------------------------|------|
| | <input checked="" type="checkbox"/> | 1 | 173.31.1.254 | 1812 |

Step 3: Create a new WLAN.

Admin PC

Desktop Programming Attributes

Web Browser

URL: <https://192.168.200.254/frameWlanEdit.html> Go Stop

Save Configuration Ping Logout Refresh

CISCO MONITOR **WLANS** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

WLANS

- WLANS
- Advanced
 - AP Groups

WLANS > Edit 'Floor 2 Employees'

< BACK Apply

General Security QoS Policy-Mapping **Advanced**

Time(msecs) 100

FlexConnect

- FlexConnect Local Switching ☒ Enabled
- FlexConnect Local Auth ☒ Enabled
- Learn Client IP Address ☒ Enabled
- Vlan based Central Switching ☐ Enabled
- Central DHCP Processing ☐ Enabled
- Override DNS ☐ Enabled
- NAT-PAT ☐ Enabled
- Central Assoc ☐ Enabled

11k

- Assisted Roaming Prediction Optimization ☐ Enabled
- Neighbor List ☐ Enabled
- Neighbor List Dual Band ☐ Enabled

11v BSS Transition Support

- Universal AP Admin ☐
- BSS Transition ☐
- Disassociation Imminent ☐
- Disassociation Timer(0 to 3000 TBTT) 200
- Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40

Tunneling

- Tunnel Profile None

mDNS

- mDNS Snooping ☐ Enabled

Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured

Top

Step 4: Configure WLAN security

Admin PC

Desktop Programming Attributes

Web Browser

URL: <https://192.168.200.254/frameWlanEdit.html> Go Stop

Save Configuration Ping Logout Refresh

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

WLANs

- WLANs
- Advanced
 - AP Groups

WLANs > Edit 'Floor 2 Employees'

< BACK Apply

General Security QoS Policy-Mapping Advanced

Profile Name: Floor 2 Employees

Type: WLAN

SSID: SSID-5

Status: ☐ Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

Multicast Vlan Feature: ☐ Enabled

Broadcast SSID: ☒ Enabled

NAS-ID:

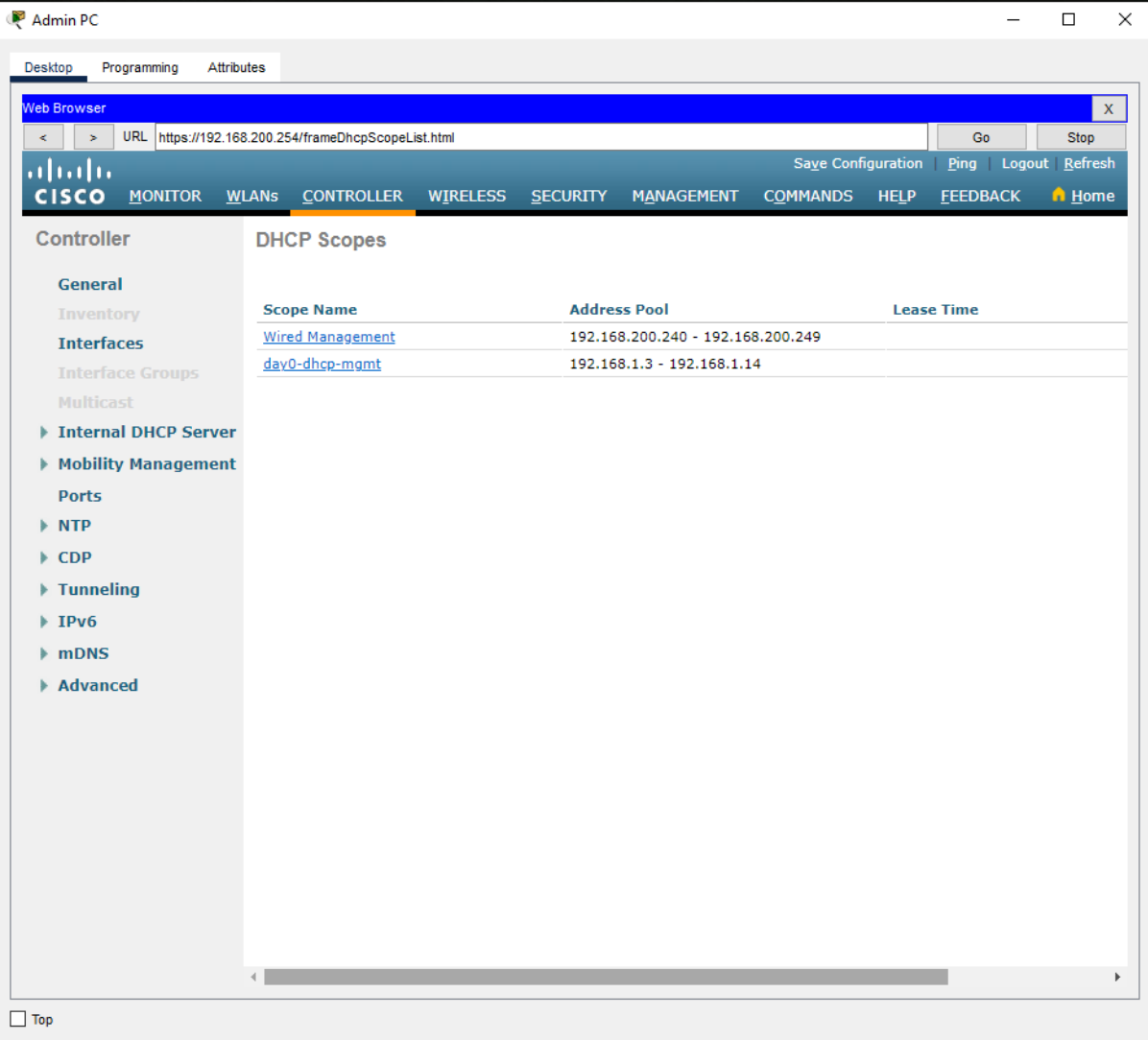
Foot Notes

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
- 2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
- 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 4 Client MFP is not active unless WPA2 is configured

Top

Part 2: Configure a DHCP Scope and SNMP

Step 1: Configure a DHCP Scope



The screenshot shows the Cisco Admin PC web interface. The browser window displays the URL `https://192.168.200.254/frameDhcpScopeList.html`. The interface includes a top navigation bar with tabs for Desktop, Programming, and Attributes. Below this is a Cisco logo and a menu with options: MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK, and Home. The main content area is titled "Controller" and "DHCP Scopes". On the left, there is a sidebar menu with options: General, Inventory, Interfaces, Interface Groups, Multicast, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, Tunneling, IPv6, mDNS, and Advanced. The main content area displays a table of DHCP Scopes.

| Scope Name | Address Pool | Lease Time |
|----------------------------------|-----------------------------------|------------|
| Wired Management | 192.168.200.240 - 192.168.200.249 | |
| day0-dhcp-mgmt | 192.168.1.3 - 192.168.1.14 | |

At the bottom left, there is a "Top" link.

Part 3: Connect Hosts to the Network

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

Wireless Host

Desktop

Programming

Attributes

Link Information

Connect

Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

| Wireless Network Name | CH | Signal |
|-----------------------|----|--------|
| SSID-5 | 1 | 63% |

Site Information

Wireless Mode

Infrastructure

Network Type

Mixed B/G/N

Radio Band

Auto

Security

WPA2-EAP

MAC Address

0000.0C43.9802

Refresh

Connect

2.4GHz



Adapter is Inactive

Wireless-N

 Notebook Adapter

Wireless Network Monitor v1.0

Model No. WPC300N

☐ Top

Step 2: Test Connectivity.

The image displays a Cisco Packet Tracer network simulation and a configuration window for a Wireless Host.

Network Diagram (Cisco Packet Tracer):

- The diagram shows a central switch, SW-1, connected to a router, R-1.
- R-1 is connected to a RADIUS Server and a Wireless Host.
- SW-1 is also connected to a Wireless LAN Controller (WLC-1) and a Laptop (LAP-1).
- The Wireless Host is shown at the bottom of the diagram.

Wireless Host Configuration Window:

The configuration window shows the following settings:

- Connection-specific DNS Suffix..:** FE80::2D0:97FF:FEB4:76A0
- Link-local IPv6 Address.....:** ::
- IPv6 Address.....:** ::
- Autoconfiguration IPv4 Address...:** 169.254.118.160
- Subnet Mask.....:** 255.255.0.0
- Default Gateway.....:** 0.0.0.0

The configuration window also shows the Bluetooth Connection settings, which are identical to the Wireless0 Connection settings.