

WLAN Configuration



Module Objectives

Module Title: WLAN Configuration

Module Objective: Implement a WLAN using a wireless router and WLC.

Topic Title	Topic Objective
Remote Site WLAN Configuration	Configure a WLAN to support a remote site.
Configure a Basic WLAN on the WLC	Configure a WLC WLAN to use the management interface and WPA2 PSK authentication.
Configure a WPA2 Enterprise WLAN on the WLC	Configure a WLC WLAN to use a VLAN interface, a DHCP server, and WPA2 Enterprise authentication.
Troubleshoot WLAN Issues	Troubleshoot common wireless configuration issues.

Remote Site WLAN Configuration

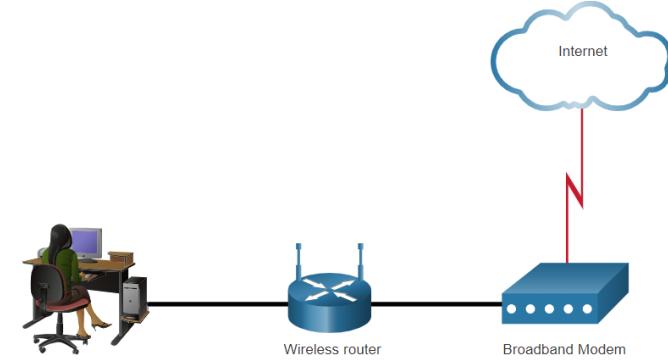
Remote Site WLAN Configuration

The Wireless Router

Remote workers, small branch offices, and home networks often use a small office and home router.

- These “integrated” routers typically include a switch for wired clients, a port for an internet connection (sometimes labeled “WAN”), and wireless components for wireless client access.
- These wireless routers typically provide WLAN security, DHCP services, integrated Name Address Translation (NAT), quality of service (QoS), as well as a variety of other features.
- The feature set will vary based on the router model.

Note: Cable or DSL modem configuration is usually done by the service provider's representative either on-site or remotely.



Log in to the Wireless Router

Most wireless routers are preconfigured to be connected to the network and provide services.

- Wireless router default IP addresses, usernames, and passwords can easily be found on the internet.
- Therefore, your first priority should be to change these defaults for security reasons.

To gain access to the wireless router's configuration GUI

- Open a web browser and enter the default IP address for your wireless router.
- The default IP address can be found in the documentation that came with the wireless router or you can search the internet.
- The word **admin** is commonly used as the default username and password.

Basic Network Setup

Basic network setup includes the following steps:

- Log in to the router from a web browser.
- Change the default administrative password.
- Log in with the new administrative password.
- Change the default DHCP IPv4 addresses.
- Renew the IP address.
- Log in to the router with the new IP address.

Remote Site WLAN Configuration

Basic Wireless Setup

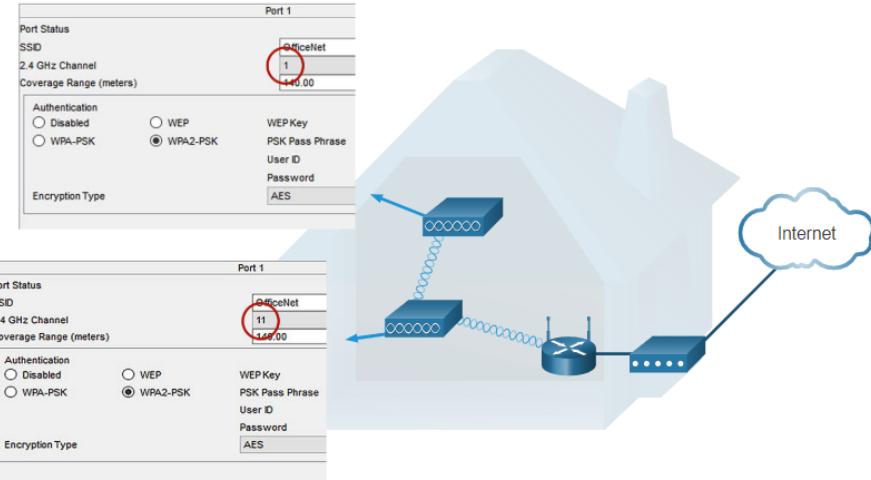
Basic wireless setup includes the following steps:

- View the WLAN defaults.
- Change the network mode, identifying which 802.11 standard is to be implemented.
- Configure the SSID.
- Configure the channel, ensuring there are no overlapping channels in use.
- Configure the security mode, selecting from Open, WPA, WPA2 Personal, WPA2 Enterprise, etc..
- Configure the passphrase, as required for the selected security mode.

Configure a Wireless Mesh Network

In a small office or home network, one wireless router may suffice to provide wireless access to all the clients.

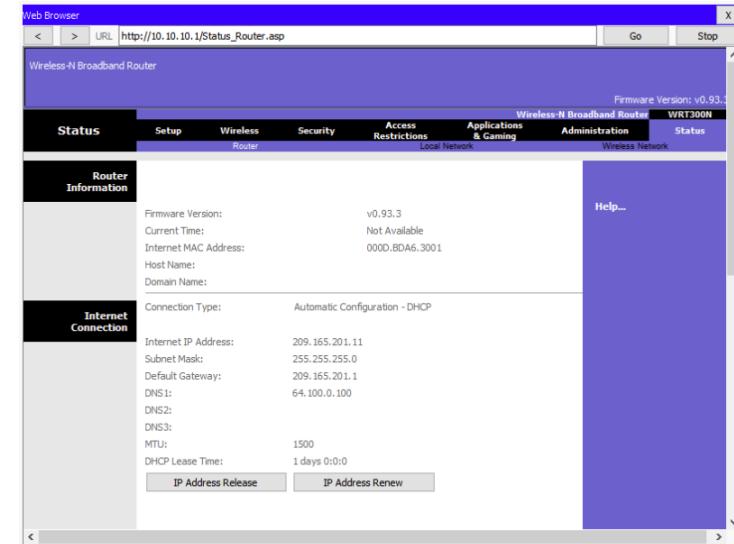
- If you want to extend the range beyond approximately 45 meters indoors and 90 meters outdoors, you create a wireless mesh.
- Create the mesh by adding access points with the same settings, except using different channels to prevent interference.
- Extending a WLAN in a small office or home has become increasingly easier.
- Manufacturers have made creating a wireless mesh network (WMN) simple through smartphone apps.



Remote Site WLAN Configuration NAT for IPv4

Typically, the wireless router is assigned a publicly routable address by the ISP and uses a private network address for addressing on the LAN.

- To allow hosts on the LAN to communicate with the outside world, the router will use a process called Network Address Translation (NAT).
- NAT translates a private (local) source IPv4 address to a public (global) address (the process is reversed for incoming packets).
- NAT makes sharing one public IPv4 address possible by tracking the source port numbers for every session established by a device.
- If your ISP has IPv6 enabled, you will see a unique IPv6 address for each device.



Remote Site WLAN Configuration

Quality of Service

Many wireless routers have an option for configuring Quality of Service (QoS).

- By configuring QoS, you can guarantee that certain traffic types, such as voice and video, are prioritized over traffic that is not as time-sensitive, such as email and web browsing.
- On some wireless routers, traffic can also be prioritized on specific ports.

The screenshot shows a user interface for configuring Quality of Service (QoS) on a network device. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' being selected. Below the tabs are buttons for 'Cancel' and 'Apply'. A main title 'QoS Setup' is centered above a table. To the left of the table is a vertical menu with links: 'Setup', 'Internet Setup', 'Wireless Setup', 'LAN Setup', 'QoS Setup' (which is highlighted with a blue arrow), 'Storage', 'Security', 'Administration', and 'Advanced Setup'. Below the table are buttons for 'Edit', 'Delete', and 'Delete All'. At the bottom center is a button labeled 'Add Priority Role'.

#	Qos Policy	Priority	Description
1	IP Phone	High	IP Phone applications
2	Counter Strike	High	Online Gaming Counter Strike
3	Netflix	High	Online Video Streaming Netflix
4	FTP	Medium	FTP Applications
5	WWW	Medium	WWW Applications
6	Gnutella	Low	Gnutella Applications
7	SMTP	Medium	SMTP Applications

Remote Site WLAN Configuration

Port Forwarding

Wireless routers typically block TCP and UDP ports to prevent unauthorized access in and out of a LAN.

- However, there are situations when specific ports must be opened so that certain programs and applications can communicate with devices on different networks.
- Port forwarding is a rule-based method of directing traffic between devices on separate networks.
- Port triggering allows the router to temporarily forward data through inbound ports to a specific device.
- You can use port triggering to forward data to a computer only when a designated port range is used to make an outbound request.

Packet Tracer – Configure a Wireless Network

In this Packet Tracer activity, you will complete the following objectives:

- Connect to a wireless router
- Configure the wireless router
- Connect a wired device to the wireless router
- Connect a wireless device to the wireless router
- Add an AP to the network to extend wireless coverage
- Update default router settings

Lab – Configure a Wireless Network

In this lab, you will configure basic settings on a wireless router and connect a PC to router wirelessly.

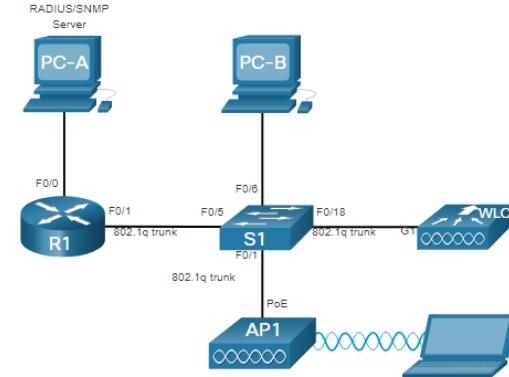
Configure a Basic WLAN on the WLC

Configure a Basic WLAN on the WLC

WLC Topology

The topology and addressing scheme used for this topic are shown in the figure and the table.

- The access point (AP) is a controller-based AP as opposed to an autonomous AP, so it requires no initial configuration and is often called lightweight APs (LAPs).
- LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC).
- Controller-based APs are useful in situations where many APs are required in the network.
- As more APs are added, each AP is automatically configured and managed by the WLC.



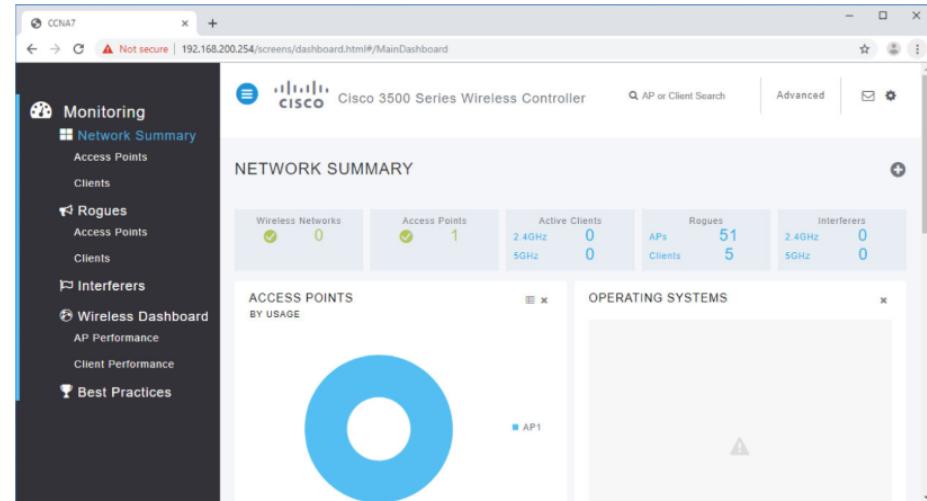
Device	Interface	IP Address	Subnet Mask
R1	F0/0	172.16.1.1	255.255.255.0
R1	F0/1.1	192.168.200.1	255.255.255.0
S1	VLAN 1	DHCP	
WLC	Management	192.168.200.254	255.255.255.0
AP1	Wired 0	192.168.200.3	255.255.255.0
PC-A	NIC	172.16.1.254	255.255.255.0
PC-B	NIC	DHCP	
Wireless Laptop	NIC	DHCP	

Configure a Basic WLAN on the WLC

Log in to the WLC

Configuring a wireless LAN controller (WLC) is not that much different from configuring a wireless router. The WLC controls APs and provides more services and management capabilities.

- The user logs into the WLC using credentials that were configured during initial setup.
- The **Network Summary** page is a dashboard that provides a quick overview of configured wireless networks, associated access points (APs), and active clients.
- You can also see the number of rogue access points and clients.



Configure a Basic WLAN on the WLC

View AP Information

Click **Access Points** from the left menu to view an overall picture of the AP's system information and performance.

- The AP is using IP address 192.168.200.3.
- Because Cisco Discovery Protocol (CDP) is active on this network, the WLC knows that the AP is connected to the FastEthernet 0/1 port on the switch.
- This AP in the topology is a Cisco Aironet 1815i which means you can use the command-line and a limited set of familiar IOS commands.

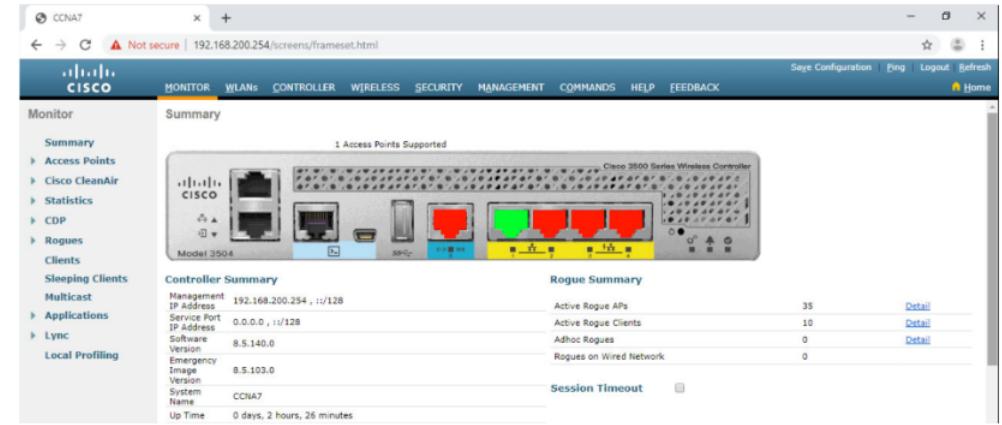
The screenshot shows the Cisco Wireless Local Controller (WLC) interface. On the left, a dark sidebar menu lists several monitoring and management sections: Monitoring, Network Summary, Access Points (selected), Clients, Rogues, Access Points, Clients, Interferers, Wireless Dashboard, AP Performance, Client Performance, and Best Practices. The main area is titled "ACCESS POINT VIEW". It displays a summary for "AP Name AP1" located in "default location". Key details include: MAC Address (2c:4f:52:60:37:e8), IP Address (192.168.200.3), CDP / LLDP (Switch, FastEthernet0/1), Ethernet Speed (100 Mbps), Model / Domain (AIR-AP1815I-B-K9 / 802.11bg:-A 802.11a:-B), Power status (PoE/Full Power), Serial Number (FCW2320NGDH), Groups (AP Group: default-group, Flex Group: default-flex-group), Mode / Sub-mode (Local / Not Configured), Max Capabilities (802.11n 2.4GHz, 802.11ac 5GHz, Spatial Streams : 2 (2.4GHz), 2 (5.0GHz), Max. Data Rate : 144 Mbps(2.4GHz), 867 Mbps(5.0GHz)), and Fabric (Disabled). To the right, a "PERFORMANCE SUMMARY" table provides data for both the 2.4GHz and 5GHz bands across various metrics like Number of clients, Channels, Configured Rate, Usage Traffic, Throughput, Transmit Power, Noise, Channel Utilization, Interference, Traffic, Air Quality, Admin Status, and Clean Air Status.

PERFORMANCE SUMMARY		
	2.4GHz	5GHz
Number of clients	1	0
Channels	11	(100, 104, 108, 112)
Configured Rate	Min: 1 Mbps, Max: 144	Min: 6 Mbps, Max: 867 Mbps
Usage Traffic	709.4 MB	231.1 KB
Throughput	2.1 KB	0
Transmit Power	20 dBm	20 dBm
Noise	-90	-93 -95 -95 -95
Channel Utilization	9%	1%
Interference	7%	1%
Traffic	2%	0%
Air Quality	-	-
Admin Status	Enabled	Enabled
Clean Air Status	Not applicable	Not applicable

Configure a Basic WLAN on the WLC Advanced Settings

Most WLC will come with some basic settings and menus that users can quickly access to implement a variety of common configurations.

- However, as a network administrator, you will typically access the advanced settings.
- For the Cisco 3504 Wireless Controller, click **Advanced** in the upper right-hand corner to access the advanced **Summary** page.
- From here, you can access all the features of the WLC.



Configure a WLAN

Wireless LAN Controllers have Layer 2 switch ports and virtual interfaces that are created in software and are very similar to VLAN interfaces.

- Each physical port can support many APs and WLANs.
- The ports on the WLC are essentially trunk ports that can carry traffic from multiple VLANs to a switch for distribution to multiple APs.
- Each AP can support multiple WLANs.



Configure a WLAN (Cont.)

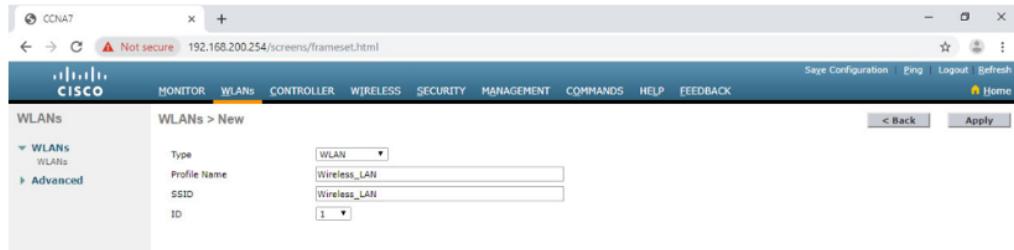
Basic WLAN configuration on the WLC includes the following steps:

1. Create the WLAN
2. Apply and Enable the WLAN
3. Select the Interface
4. Secure the WLAN
5. Verify the WLAN is Operational
6. Monitor the WLAN
7. View Wireless Client Information

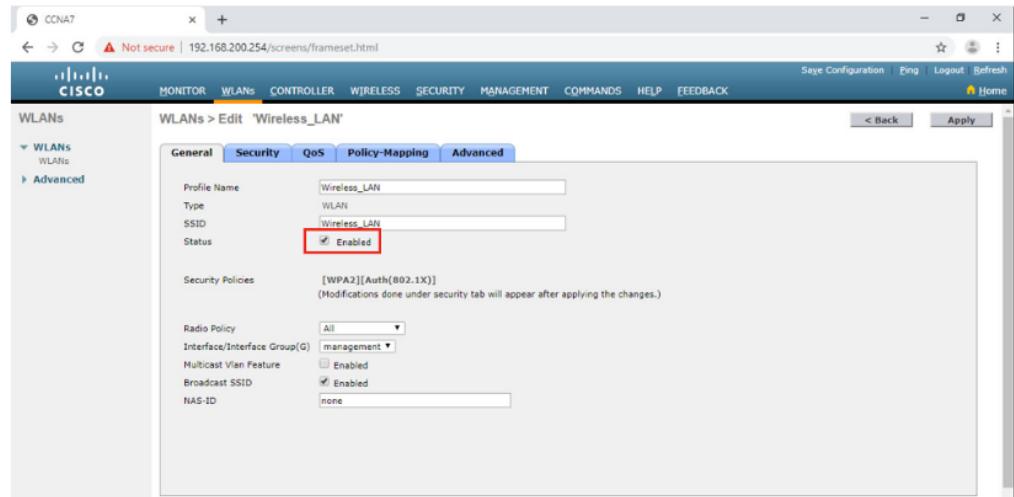
Configure a Basic WLAN on the WLC

Configure a WLAN (Cont.)

- Create the WLAN:** In the figure, a new WLAN with an SSID name **Wireless_LAN** is created.



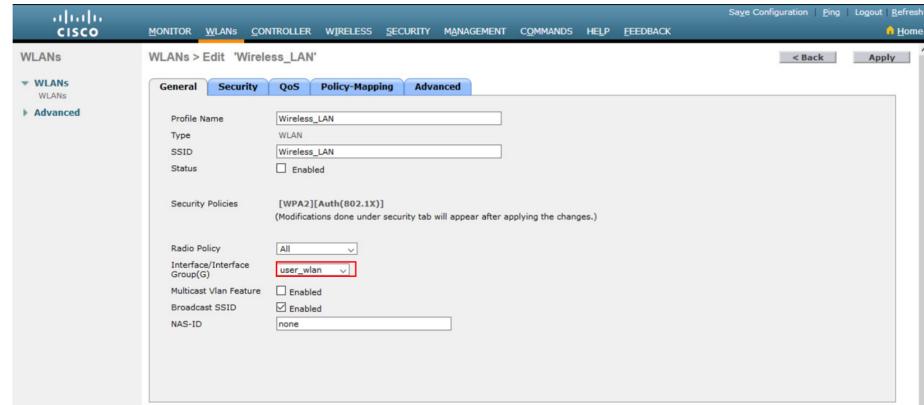
- Apply and Enable the WLAN:** Next the WLAN is enabled the WLAN settings are configured.



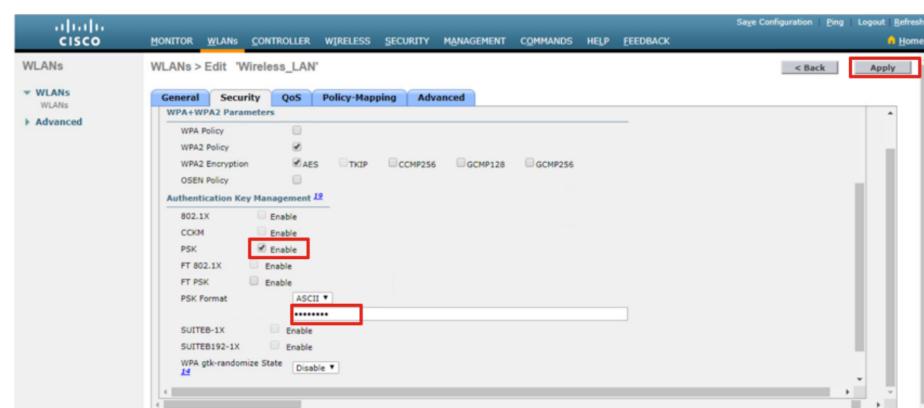
Configure a Basic WLAN on the WLC

Configure a WLAN (Cont.)

3. **Select the Interface:** The interface that will carry the WLAN traffic must be selected.



4. **Secure the WLAN:** The Security tab is used to access all the available options for securing the LAN.



Configure a Basic WLAN on the WLC

Configure a WLAN (Cont.)

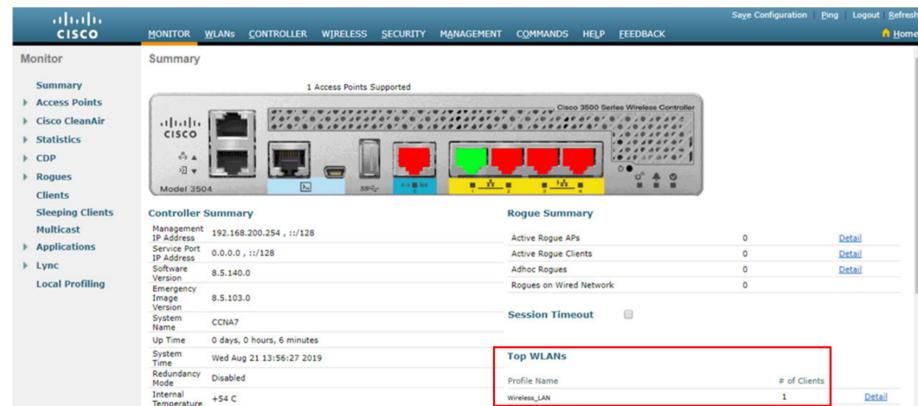
5. Verify the WLAN is Operational:

The **WLANs** menu on the left is used to view the newly configured WLAN and its settings.

The screenshot shows the 'WLANs' configuration page. The left sidebar has 'WLANs' expanded, with 'WLANs' selected. The main area displays a table with one row for 'Wireless_LAN'. The columns are: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The table shows: WLAN ID 1, Type WLAN, Profile Name Wireless_LAN, WLAN SSID Wireless_LAN, Admin Status Enabled, and Security Policies [WPA2][Auth(PSK)].

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Wireless_LAN	Wireless_LAN	Enabled	[WPA2][Auth(PSK)]

6. Monitor the WLAN: The Monitor tab is used to access the advanced Summary page and confirm that the **Wireless_LAN** now has one client using its services.



Configure a Basic WLAN on the WLC

Configure a WLAN (Cont.)

7. View Wireless Client Details:

Click **Clients** in the left menu to view more information about the clients connected to the WLAN.



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes links for 'Say Configuration', 'Ping', 'Logout', and 'Refresh'. The main menu has tabs for 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. On the left, a sidebar under 'Monitor' has a 'Summary' section and links for 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', and 'Rogues'. The 'Clients' link is highlighted with a red box. The main content area is titled 'Clients' and shows one entry. The table columns are 'Client MAC Addr', 'IP Address(Ipv4/Ipv6)', 'AP Name', 'WLAN Profile', and 'WLAN SSID'. The single entry is: Client MAC Addr 00:13:ce:57:7c:67, IP Address 192.168.5.2, AP Name AP1, WLAN Profile Wireless_LAN, and WLAN SSID Wireless_LAN. A note at the bottom right says 'Entries 1 - 1 of 1'.

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID
00:13:ce:57:7c:67	192.168.5.2	AP1	Wireless_LAN	Wireless_LAN

Packet Tracer – Configure a Basic WLAN on the WLC

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.

Configure a WPA2 Enterprise WLAN on the WLC

Configure a WPA2 Enterprise WLAN on the WLC Video – Define an SNMP and RADIUS Server on the WLC

This video will cover the following:

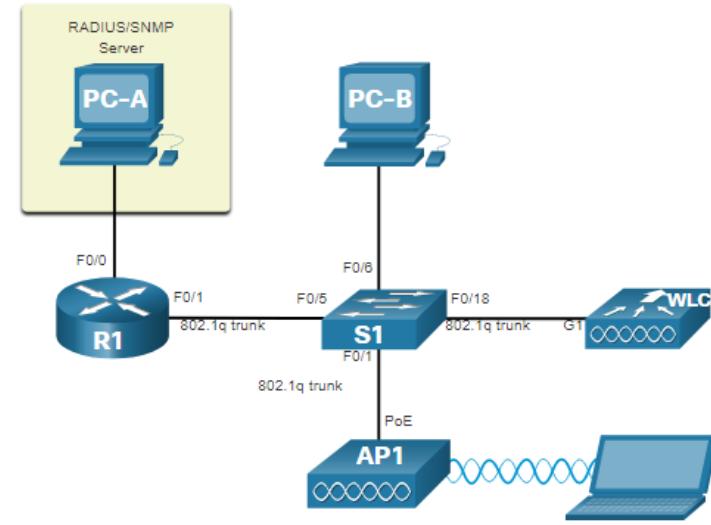
- Configure the WLAN controller to send SNMP traps to an external server
- Configure the WLAN controller to use an external RADIUS server to authenticate WLAN users
- Verify connectivity with the RADIUS server

Configure a WPA2 Enterprise WLAN on the WLC SNMP and RADIUS

PC-A is running Simple Network Management Protocol (SNMP) and Remote Authentication Dial-In User Service (RADIUS) server software.

- The network administrator wants the WLC to forward all SNMP log messages (i.e., traps) to the SNMP server.
- The network administrator wants to use a RADIUS server for authentication, authorization, and accounting (AAA) services.
- Users will enter their username and password credentials which will be verified by the RADIUS server.
- The RADIUS server is required for WLANs that are using WPA2 Enterprise authentication.

Note: SNMP server and RADIUS server configuration is beyond the scope of this module.

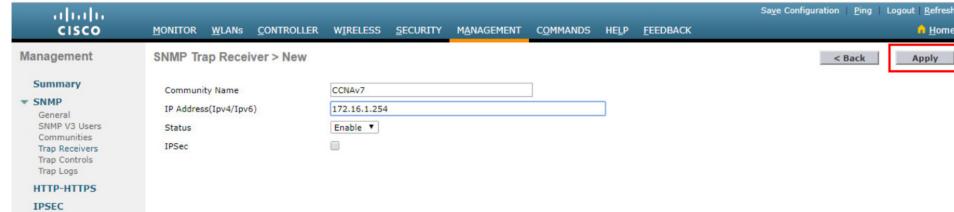


Configure a WPA2 Enterprise WLAN on the WLC

Configure SNMP Server Information

To enable SNMP and configure settings:

1. Click the **MANAGEMENT** tab to access a variety of management features.
 2. Click **SNMP** to expand the sub-menus.
 3. Click **Trap Receivers**.
 4. Click **New...** to configure a new SNMP trap receiver.
-
- Enter the SNMP Community name and the IP address (IPv4 or IPv6) for the SNMP server and then click **Apply**.
 - The WLC will now forward SNMP log messages to the SNMP server.



Configure a WPA2 Enterprise WLAN on the WLC

Configure RADIUS Server Information

To configure the WLC with the RADIUS server information:

1. Click **SECURITY**.
 2. Click **RADIUS**
 3. Click **Authentication**
 4. Click **New...** to add PC-A as the RADIUS server.
-
- Enter the IPv4 address for PC-A and the shared secret that will be used between the WLC and the RADIUS server and then click **Apply**.

The image consists of two screenshots of the Cisco Wireless Local Controller (WLC) web interface. Both screenshots show the 'RADIUS Authentication Servers' configuration page under the 'SECURITY' tab.

Screenshot 1 (Left): Shows the main configuration page for RADIUS servers. The 'Auth Called Station ID Type' dropdown is set to 'AP MAC Address:SSID'. The 'Use AES Key Wrap' checkbox is checked. Other settings include 'MAC Delimiter' (Hyphen), 'Framed HTU' (1300), and a table for 'Network User Management' with columns for 'User', 'Management', 'Tunnel Proxy', 'Server Index', 'Server Address(Ipv4/Ipv6)', 'Port', 'IPSec', and 'Admin Status'. A sidebar on the left shows the 'AAA' configuration tree with 'Authentication' selected. A red box highlights the 'SECURITY' tab at the top, and numbered circles 1 through 4 point to the tabs, the 'New...' button, and the 'Apply' button respectively.

Screenshot 2 (Right): Shows the detailed configuration for a new RADIUS server entry. The 'Server Index (Priority)' is set to 1, and the 'Server IP Address(Ipv4/Ipv6)' is 172.16.1.254. The 'Shared Secret Format' is set to 'ASCII'. The 'Shared Secret' field contains '*****'. The 'Confirm Shared Secret' field also contains '*****'. The 'Key Wrap' checkbox is checked. Other settings include 'Port Number' (1812), 'Server Status' (Enabled), 'Support for CoA' (Disabled), 'Server Timeout' (5 seconds), 'Network User Management' (Enable), and 'Management Retransmit Timeout' (5 seconds). A red box highlights the 'Apply' button at the bottom right.

Configure a WPA2 Enterprise WLAN on the WLC

Configure RADIUS Server Information (Cont.)

After clicking **Apply**, the list of configured **RADIUS Authentication Servers** refreshes with the new server listed.



The screenshot shows the Cisco Wireless Local Controller (WLC) interface under the 'SECURITY' tab. In the left sidebar, under 'AAA', the 'RADIUS' section is expanded, showing options like Authentication, Accounting, Fallback, DRNG, and Downloaded AVP. Below this, 'TACACS+' and 'LDAP' sections are partially visible. The main pane displays 'RADIUS Authentication Servers' settings. Under 'Auth Called Station ID Type', 'AP MAC Address:SSID' is selected. The 'Use AES Key Wrap' checkbox is checked, with a note '(Designed for FIPS customers and requires a key wrap compliant RADIUS server)'. 'MAC Delimiter' is set to 'Hyphen' and 'Framed MTU' is set to '1300'. A table lists the configured RADIUS servers:

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	172.16.1.254	1812	Disabled	Enabled

Configure a WPA2 Enterprise WLAN on the WLC

Video – Configure a VLAN for a New WLAN

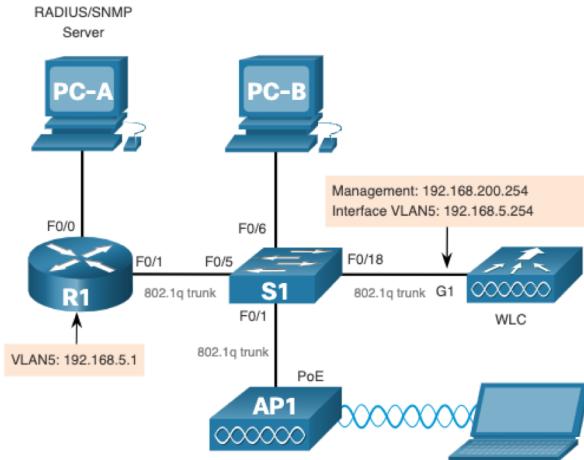
This video will cover the following:

- Review the topology
- Deploy a new VLAN interface
- Associate the new VLAN interface with a WLAN

Configure a WPA2 Enterprise WLAN on the WLC Topology with VLAN 5 Addressing

Each WLAN configured on the WLC needs its own virtual interface.

- The WLC has five physical data ports that can be configured to support multiple WLANs and virtual interface.
- The new WLAN will use interface VLAN 5 and network 192.168.5.0/24 and therefore R1 has been configured for VLAN 5 as shown in the topology and **show ip interface brief** output.



```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    172.16.1.1     YES manual up       up
FastEthernet0/1    unassigned      YES unset  up       up
FastEthernet0/1.1  192.168.200.1  YES manual up       up
FastEthernet0/1.5  192.168.5.254 YES manual up       up
(output omitted)
R1#
```

Configure a New Interface

VLAN interface configuration on the WLC includes the following steps:

1. Create a new interface.
2. Configure the VLAN name and ID.
3. Configure the port and interface address.
4. Configure the DHCP server address.
5. Apply and Confirm.
6. Verify Interfaces.

Configure a WPA2 Enterprise WLAN on the WLC

Configure a New Interface (Cont.)

1. Create a new interface:
Click **CONTROLLER** >
Interfaces > **New...**



The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar has tabs: MONITOR, WLAN, CONTROLLER (which is highlighted with a red box and circled with a red number 1), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. Below the navigation is a search bar and links for 'Say Configuration', 'Ping', 'Logout', 'Refresh', 'Home', and 'Entries 1 - 5 of 5'. On the left, a sidebar menu includes: General, Icons, Inventory, **Interfaces** (highlighted with a red box and circled with a red number 2), Interface Groups, Multicast, Network Routes, and Fabric Configuration. The main content area is titled 'Interfaces' and lists five entries:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.200.254	Static	Enabled	::/128
redundancy-management	untagged	0.0.0.0	Static	Not Supported	
redundancy-port	untagged	0.0.0.0	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

2. Configure the VLAN name and ID: In the example, the new interface is named **vlan5**, the VLAN ID is **5**, and applied.



The screenshot shows the 'Interfaces > New' configuration dialog. The top navigation bar is identical to the previous screen. The left sidebar shows 'Controller' and 'Interfaces' (highlighted with a red box). The main form has fields for 'Interface Name' (set to 'vlan5') and 'VLAN Id' (set to '5'). At the bottom right is a red-bordered 'Apply' button.

Configure a WPA2 Enterprise WLAN on the WLC

Configure a New Interface (Cont.)

3. Configure the port and interface address: On the interface Edit page, configure the physical port number (i.e., the WLC G1 interface is Port Number 1 on the WLC), the VLAN 5 interface addressing (i.e., 192.168.5.254/24), and the default gateway (i.e., 192.168.5.1)

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes links for Monitor, WLANs (highlighted in orange), Controller, Wireless, Security, Management, Commands, Help, and Feedback. The left sidebar lists various configuration categories: General, Icons, Inventory, Interfaces (selected), Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, Internal DHCP Server, Mobility Management, and Ports. Under Ports, sub-options like NTP, CDP, PMIPv6, Tunnelling, IPv6, mDNS, and Advanced are listed. The main content area is titled "Interfaces > Edit" and shows the configuration for "vlan5". The "General Information" section displays the Interface Name as "vlan5" and the MAC Address as "70:18:a7:c8:cc:f1". The "Configuration" section includes fields for Guest Lan (unchecked), Quarantine (unchecked), Quarantine Vlan Id (set to 0), and NAS-ID (set to none). The "Physical Information" section shows the Port Number set to "1" (highlighted with a red box). The "Interface Address" section shows the VLAN Identifier set to "5" (highlighted with a red box), and the IP Address, Netmask, and Gateway fields all set to "192.168.5.1" (all three fields highlighted with red boxes).

Configure a WPA2 Enterprise WLAN on the WLC

Configure a New Interface (Cont.)

4. Configure the DHCP server

address: The example configures a primary DHCP server at IPv4 address 192.168.5.1 which is the default gateway router address which is enabled as a DHCP server.

The screenshot shows the Cisco Wireless Local Controller (WLC) web interface under the 'CONTROLLER' tab. In the 'Interface Address' section, the 'IP Address' field is set to 192.168.5.254. In the 'DHCP Information' section, the 'Primary DHCP Server' field is highlighted with a red box and contains the value 192.168.5.1. Other fields include 'Secondary DHCP Server' (empty), 'DHCP Proxy Mode' (set to 'Global'), and two unchecked checkboxes for 'Enable DHCP Option 82' and 'Enable DHCP Option 6 OpenDNS'.

5. Apply and Confirm: Scroll to the top and click **Apply** and then click **OK** for the warning message.

A confirmation dialog box titled 'CCNA7' is displayed over the WLC interface. It shows the URL as 'Not secure | 192.168.200.254/screens/frameset.html'. The message reads: '192.168.200.254 says Changing the interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.' At the bottom are 'OK' and 'Cancel' buttons.

Configure a WPA2 Enterprise WLAN on the WLC

Configure a New Interface (Cont.)

6. Verify Interfaces: Click Interfaces to verify that the new **vlan5** interface is shown in the list of interfaces with its IPv4 address.



The screenshot shows the Cisco Wireless Local Controller (WLC) web interface. The top navigation bar includes links for 'Say Configuration', 'Ping', 'Logout', and 'Refresh'. On the far right, there's a 'Home' icon. Below the navigation, a secondary menu on the left lists categories: General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, and Redundancy. The 'Interfaces' link under 'General' is currently selected. The main content area displays a table titled 'Interfaces' with the following data:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.200.254	Static	Enabled	::/128
redundancy-management	untagged	0.0.0.0	Static	Not Supported	
redundancy-port	untagged	0.0.0.0	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
user_wlan	10	192.168.10.254	Dynamic	Disabled	::/128
virtual	N/A	1.1.1.1	Static	Not Supported	
vlan5	5	192.168.5.254	Dynamic	Disabled	::/128

Entries 1 - 7 of 7

Configure a WPA2 Enterprise WLAN on the WLC

Video – Configure a DHCP Scope

This video will cover the following:

- Review the topology
- Explain the role of the WLC DHCP server
- Create a new DHCP scope

Configure a DHCP Scope

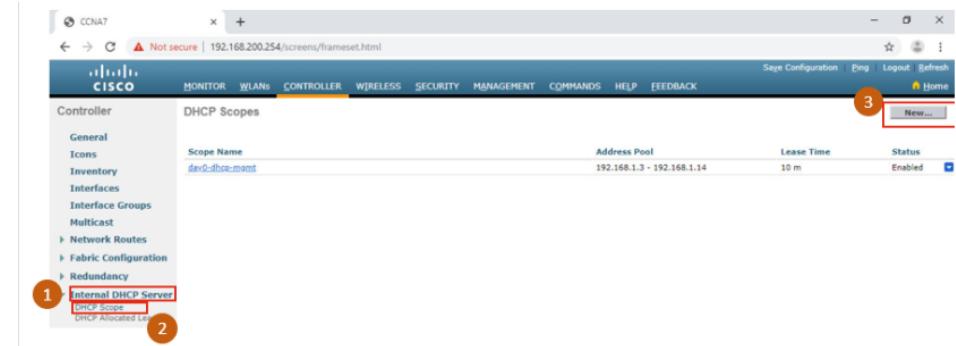
DHCP scope configuration includes the following steps:

1. Create a new DHCP scope.
2. Name the DHCP scope.
3. Verify the new DHCP scope.
4. Configure and enable the new DHCP scope.
5. Verify the enable DHCP scope

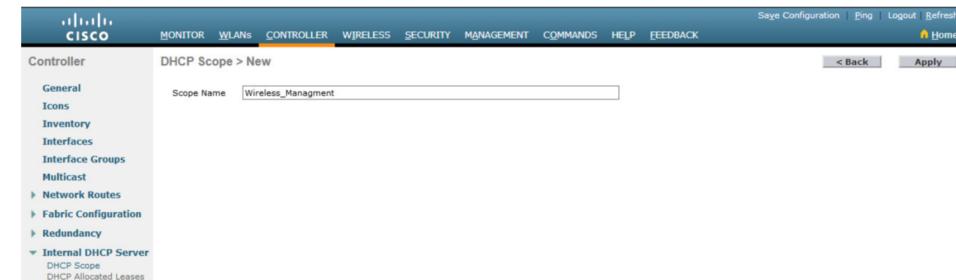
Configure a WPA2 Enterprise WLAN on the WLC

Configure a DHCP Scope (Cont.)

1. **Create a new DHCP scope:** To configure a new DHCP scope, click Internal DHCP Server > DHCP Scope > New....



2. **Name the DHCP scope:** The scope is named **Wireless_Management** and then applied.



Configure a WPA2 Enterprise WLAN on the WLC

Configure a DHCP Scope (Cont.)

3. **Verify the new DHCP scope:** In the **DHCP Scopes** page click the new Scope Name to configure the DHCP scope.
4. **Configure and enable the new DHCP scope:** On the Edit screen for the **Wireless_Management** scope, configure a pool of addresses (i.e., 192.168.200.240/24 to .249), the default router IPv4 address (i.e., 192.168.200.1), then **Enabled** and **Apply**.

Scope Name	Address Pool	Lease Time	St
Wireless_Management	0.0.0 - 0.0.0 192.168.1.3 - 192.168.1.14	1 d 1 d	Dir En

The screenshot shows the 'Edit' screen for the 'Wireless_Management' DHCP scope. The configuration fields are as follows:

- Scope Name: Wireless_Management
- Pool Start Address: 192.168.200.240
- Pool End Address: 192.168.200.249
- Network: 192.168.200.0
- Netmask: 255.255.255.0
- Lease Time (seconds): 86400
- Default Routers: 192.168.200.1
- DNS Domain Name: (empty)
- DNS Servers: 0.0.0.0
- Netbios Name Servers: 0.0.0.0
- Status: Enabled

Configure a WPA2 Enterprise WLAN on the WLC

Configure a DHCP Scope (Cont.)

5. Verify the enable DHCP scope: The network administrator is returned to the **DHCP Scopes** page and can verify the scope is ready to be allocated to a new WLAN.

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANs, **CONTROLLER**, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the far right, there are links for Save Configuration, Ping, Logout, Refresh, and Home. The left sidebar has a tree view with nodes like General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, and Internal DHCP Server, with the latter expanded to show sub-options for DHCP Scope and DHCP Allocated Leases. The main content area is titled "DHCP Scopes". It displays a table with one row for a scope named "Wireless_Management". The table columns include Scope Name, Address Pool, Lease Time, and Status. The "Address Pool" column shows the range 192.168.200.240 - 192.168.200.249, which is highlighted with a red border. The "Lease Time" column shows "1 d". The "Status" column shows "Enabled".

Scope Name	Address Pool	Lease Time	Status
Wireless_Management day0-dhcp-mgmt	192.168.200.240 - 192.168.200.249 192.168.1.3 - 192.168.1.14	1 d 1 d	Enabled Enabled

Video – Configure a WPA2 Enterprise WLAN

This video will cover the following:

- Review the topology
- Create a WLAN
- Configure the WLC to use the RADIUS server
- Secure the new WLAN with WPA2-Enterprise
- Verify WPA2-Enterprise Security

Configure a WPA2 Enterprise WLAN

By default, all newly created WLANs on the WLC will use WPA2 with Advanced Encryption System (AES).

- 802.1X is the default key management protocol used to communicate with the RADIUS server.
- Next, create a new WLAN to use interface **vlan5**.

Configuring a new WLAN on the WLC includes the following steps:

1. Create a new WLAN.
2. Configure the WLAN name and SSID.
3. Enable the WLAN for VLAN 5.
4. Verify AES and 802.1X defaults.
5. Configure WLAN security to use the RADIUS server.
6. Verify the new WLAN is available.

Configure a WPA2 Enterprise WLAN on the WLC

Configure a WPA2 Enterprise WLAN (Cont.)

1. **Create a new WLAN:** Click the **WLANS** tab and then **Go** to create a new WLAN.

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANS (which is highlighted with a red box), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. Below the navigation is a search bar with 'Not secure | 192.168.200.254/screens/frameset.html'. The main content area is titled 'WLANS' and shows a table with one row. The columns are 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'. The row contains values: 1, WLAN, Wireless_Lab, Wireless_Lab, Enabled, and [WPA2][Auth(PSK)]. At the bottom right of the table, there is a 'Create New' button with a red box around it, and a 'Go!' button next to it.

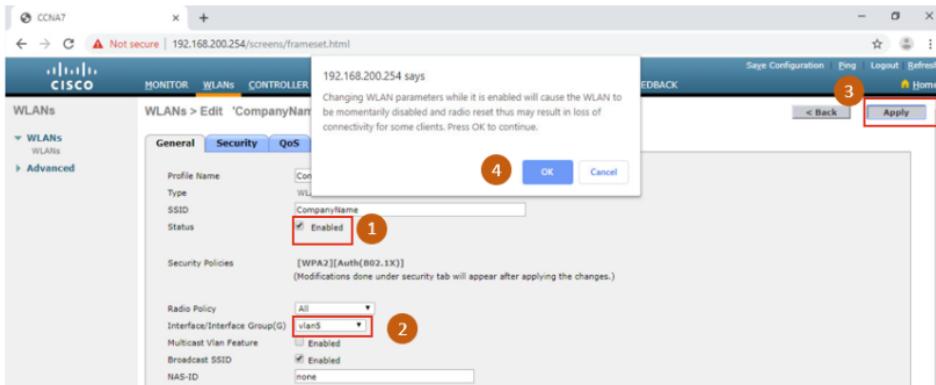
2. **Configure the WLAN name and SSID:** Enter the profile name and SSID, choose an ID of 5, and then click **Apply** to create the new WLAN.

The screenshot shows the 'WLANS > New' configuration page. The left sidebar has 'WLANS' selected. The main form has fields for 'Type' (set to 'WLAN'), 'Profile Name' (containing 'CompanyName'), 'SSID' (containing 'CompanyName'), and 'ID' (set to '5'). A red box highlights the 'Apply' button at the bottom right of the form.

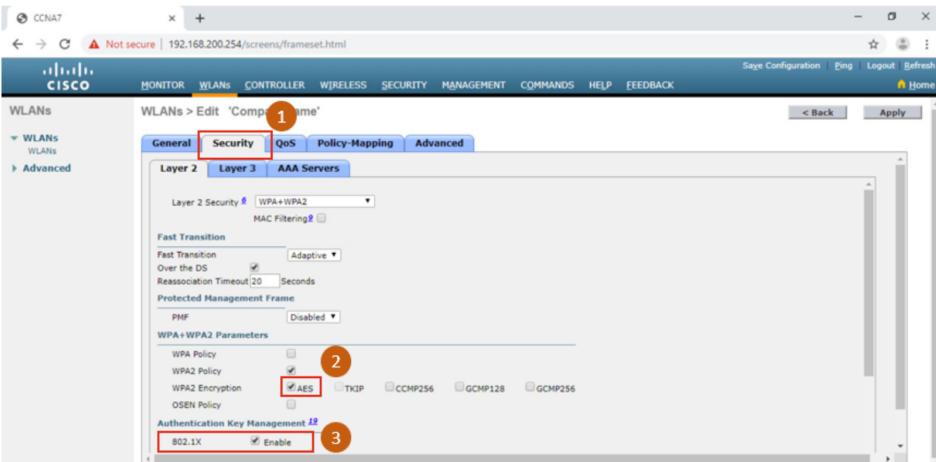
Configure a WPA2 Enterprise WLAN on the WLC

Configure a WPA2 Enterprise WLAN (Cont.)

3. **Enable the WLAN for VLAN 5:** Once the WLAN, change the status to **Enabled**, choose **vlan5** from the Interface/Interface Group(G) dropdown list, and then click **Apply** and click **OK** to accept the popup message.



4. **Verify AES and 802.1X defaults:** Click the **Security** tab to view the default security configuration for the new WLAN.



Configure a WPA2 Enterprise WLAN on the WLC

Configure a WPA2 Enterprise WLAN (Cont.)

5. **Configure the RADIUS server:** To select the RADIUS server that will be used to authenticate WLAN users, click the **AAA Servers** tab and in the dropdown box, select the RADIUS server that was configured on the WLC previously, and then **Apply** your changes.

The screenshot shows the 'WLANs > Edit 'CompanyName'' page. The 'AAA Servers' tab is selected. Under 'Authentication Servers', there is a table with one row highlighted. The first column is labeled 'Server' and contains '1'. The second column is labeled 'IP' and contains '172.16.1.254'. The third column is labeled 'Port' and contains '1812'. A red box highlights this row, and a red circle with the number '2' is placed over the 'IP' field. Another red box highlights the 'Apply' button in the top right corner, and a red circle with the number '3' is placed over it. The 'Policy-Mapping' tab is also highlighted with a red circle and the number '1'.

6. **Verify that the new WLAN is available:** To verify that the new WLAN is listed and enabled click on the **WLANS** submenu.

The screenshot shows the 'WLANS' page. The 'WLANS' submenu is selected, indicated by a red box. The table lists two WLANs: 'Wireless_LAN' and 'CompanyName'. The 'CompanyName' row is highlighted with a red box. The columns are: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The 'CompanyName' row has '1' in the WLAN ID column, 'WLAN' in the Type column, 'Wireless_LAN' in the Profile Name column, 'Wireless_LAN' in the WLAN SSID column, 'Enabled' in the Admin Status column, and '[WPA2][Auth(PSK)]' in the Security Policies column. The 'WLANS' tab is also highlighted with a red circle and the number '1'.

Configure a WPA2 Enterprise WLAN on the WLC

Packet Tracer – Configure a WPA2 Enterprise WLAN on the WLC

In this Packet Tracer 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. You will also configure the WLC to use an SNMP server.

- Configure a new VLAN interface on a WLC.
- Configure a new WLAN on a WLC.
- Configure a new scope on the WLC internal DHCP server.
- Configure the WLC with SNMP settings.
- Configure the WLC to use a RADIUS server to authenticate WLAN users.
- Secure a WLAN with WPA2-Enterprise.
- Connect hosts to the new WLC.

Ví[^ à| ^• @ [oÝ ŠOË Ássues

Troubleshooting Approaches

Network problems can be simple or complex, and can result from a combination of hardware, software, and connectivity issues.

- Technicians must be able to analyze the problem and determine the cause of the error before they can resolve the network issue.
- This process is called troubleshooting.

Troubleshooting any sort of network problem should follow a systematic approach.

A common and efficient troubleshooting methodology is based on the scientific method and can be broken into the six main steps shown in the table on the next slide.

Troubleshooting Approaches (Cont.)

Step	Title	Description
1	Identify the Problem	The first step in the troubleshooting process is to identify the problem. While tools can be used in this step, a conversation with the user is often very helpful.
2	Establish a Theory of Probable Causes	After you have talked to the user and identified the problem, you can try and establish a theory of probable causes. This step often yields more than a few probable causes to the problem.
3	Test the Theory to Determine Cause	Based on the probable causes, test your theories to determine which one is the cause of the problem. A technician will often apply a quick procedure to test and see if it solves the problem. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
4	Establish a Plan of Action to Resolve the Problem and Implement the Solution	After you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution.
5	Verify Full System Functionality and Implement Preventive Measures	After you have corrected the problem, verify full functionality and, if applicable, implement preventive measures.
6	Document Findings, Actions, and Outcomes	In the final step of the troubleshooting process, document your findings, actions, and outcomes. This is very important for future reference.

Wireless Client Not Connecting

If there is no connectivity, check the following:

- Confirm the network configuration on the PC using the **ipconfig** command.
- Confirm that the device can connect to the wired network. Ping a known IP address.
- If needed, reload drivers as appropriate for the client or try a different wireless NIC.
- If the wireless NIC of the client is working, check the security mode and encryption settings on the client.

If the PC is operational but the wireless connection is performing poorly, check the following:

- Is the PC out of the planned coverage area (BSA)?
- Check the channel settings on the wireless client.
- Check for interference with the 2.4 GHz band.

Wireless Client Not Connecting (Cont.)

Next, ensure that all the devices are actually in place.

- Consider a possible physical security issue.
- Is there power to all devices and are they powered on?

Finally, inspect links between cabled devices looking for bad connectors or damaged or missing cables.

- If the physical plant is in place, verify the wired LAN by pinging devices, including the AP.
- If connectivity still fails at this point, perhaps something is wrong with the AP or its configuration.
- When the user PC is eliminated as the source of the problem, and the physical status of devices is confirmed, begin investigating the performance of the AP.
- Check the power status of the AP.

Troubleshooting When the Network Is Slow

To optimize and increase the bandwidth of 802.11 dual-band routers and APs, either:

- **Upgrade your wireless clients** - Older 802.11b, 802.11g, and even 802.11n devices can slow the entire WLAN. For the best performance, all wireless devices should support the same highest acceptable standard.
- **Split the traffic** - The easiest way to improve wireless performance is to split the wireless traffic between the 802.11n 2.4 GHz band and the 5 GHz band. Therefore, 802.11n (or better) can use the two bands as two separate wireless networks to help manage the traffic.

There are several reasons for using a split-the-traffic approach:

- The 2.4 GHz band may be suitable for basic Internet traffic that is not time-sensitive.
- The bandwidth may still be shared with other nearby WLANs.
- The 5 GHz band is much less crowded than the 2.4 GHz band; ideal for streaming multimedia.
- The 5 GHz band has more channels; therefore, the channel chosen is likely interference-free.

Troubleshooting When the Network Is Slow (Cont.)

By default, dual-band routers and APs use the same network name on both the 2.4 GHz band and the 5 GHz band.

- It may be useful to segment the traffic.
- The simplest way to segment traffic is to rename one of the wireless networks.

To improve the range of a wireless network, ensure the wireless router or AP location is free of obstructions, such as furniture, fixtures, and tall appliances.

- These block the signal, which shortens the range of the WLAN.
- If this still does not solve the problem, then a Wi-Fi Range Extender or deploying the Powerline wireless technology may be used.

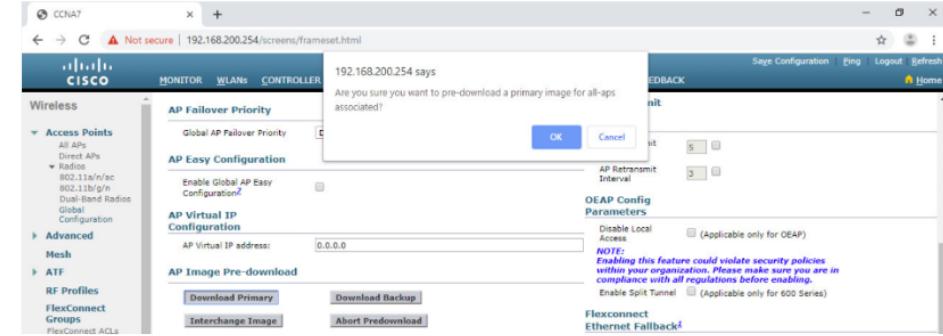
Troubleshoot WLAN Issues

Updating Firmware

Most wireless routers and APs offer upgradable firmware that should be periodically verified.

On a WLC, there will most likely be the ability to upgrade the firmware on all APs that the WLC controls.

- In the figure, the firmware image that will be used to upgrade all the APs is downloaded.
- On a Cisco 3504 Wireless Controller, click **WIRELESS > Access Points > Global Configuration** and then scroll to the bottom of the page for the AP Image Pre-download section.



Packet Tracer – Troubleshoot WLAN Issues

In this Packet Tracer, you will complete the following objectives:

- Troubleshoot wireless LAN connectivity issues in a home network.
- Troubleshoot wireless LAN connectivity issues in an enterprise network.

T [å` |^ÁÚ! æ&cð&^

Packet Tracer – WLAN Configuration

In this Packet Tracer activity, you will configure both a wireless home router and a WLC-based network. You will implement both WPA2-PSK and WPA2-Enterprise security.

- Configure a home router to provide Wi-Fi connectivity to a variety of devices.
- Configure WPA2-PSK security on a home router.
- Configure interfaces on a WLC.
- Configure WPA2-PSK security on a WLAN and connect hosts to the WLAN.
- Configure WPA2-Enterprise on a WLAN and connect hosts to the WLAN.
- Verify connectivity.