



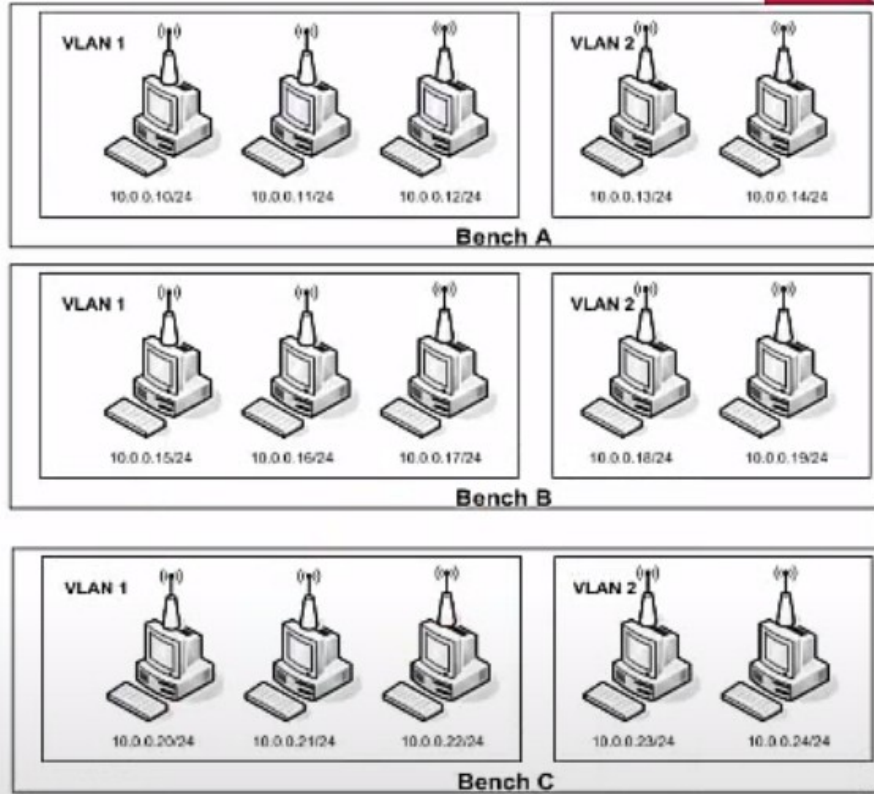
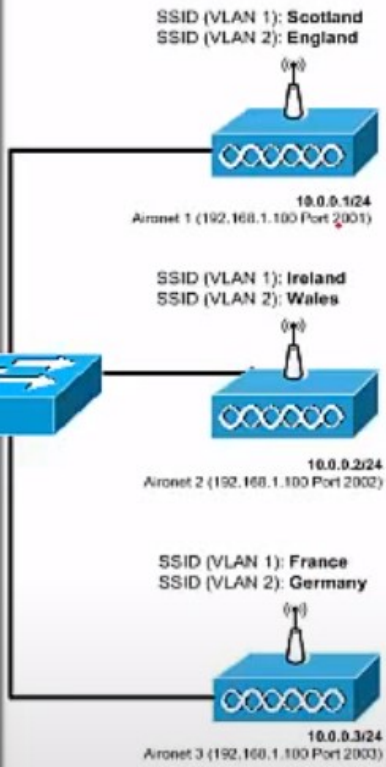
Module 13: WLAN Configuration

Switching, Routing, and
Wireless Essentials v7.0
(SRWE)



Opakování: každá VLAN má své SSID

Applied Cisco Networking
- Prof Bill Buchanan



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. |

13.1 Remote Site WLAN Configuration

Video – Configure a Wireless Network

This video will cover the following:

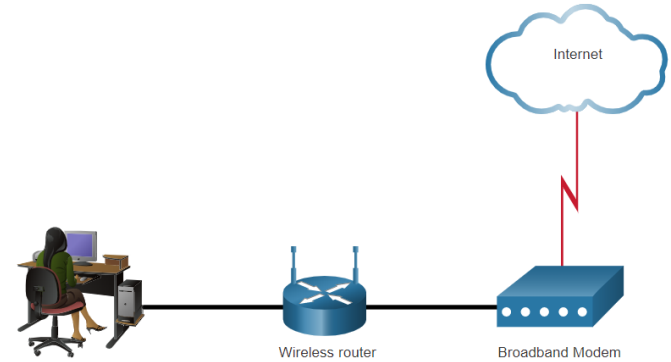
- Use the Wireless Router Web Page
- Change the Password
- Change the WAN and LAN settings
- Connect the Wireless Network

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.

Basic Wireless Setup

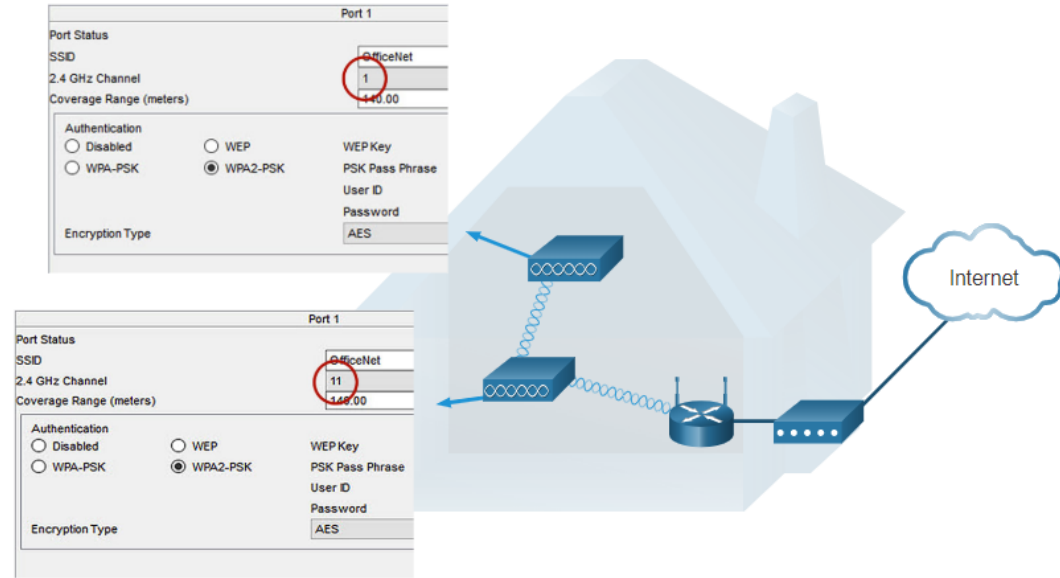
Basic wireless setup includes the following steps:

- 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.

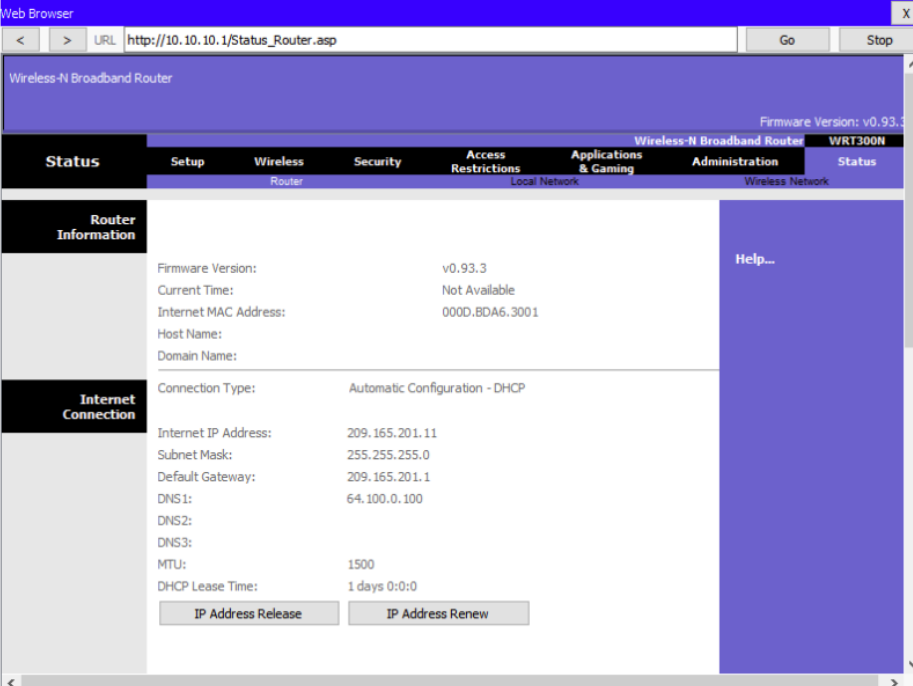
- If you want to extend the range beyond approximately **45 meters indoors and 90 meters outdoors**, you create a wireless mesh.
- Create the mesh by adding access points with the same settings, except using different channels to prevent interference.
- Extending a WLAN in a small office or home has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



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**.



The screenshot shows a web browser window with the URL `http://10.10.10.1/Status_Router.asp`. The page title is "Wireless-N Broadband Router" and the firmware version is v0.93.3. The page is divided into several sections:

- Router Information:**
 - Firmware Version: v0.93.3
 - Current Time: Not Available
 - Internet MAC Address: 000D.BDA6.3001
 - Host Name:
 - Domain Name:
- Internet Connection:**
 - Connection Type: Automatic Configuration - DHCP
 - Internet IP Address: 209.165.201.11
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 209.165.201.1
 - DNS1: 64.100.0.100
 - DNS2:
 - DNS3:
 - MTU: 1500
 - DHCP Lease Time: 1 days 0:0:0

Buttons for "IP Address Release" and "IP Address Renew" are visible at the bottom of the Internet Connection section.

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.**

Basic Advanced Cancel Apply

Advanced Home QoS Setup

| # | 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 |

Edit Delete Delete All Add Priority Role

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 13.1.11 – Configure a Wireless Network

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

13.2 Configure a Basic WLAN on the WLC

Video – Configure a Basic WLAN on the WLC

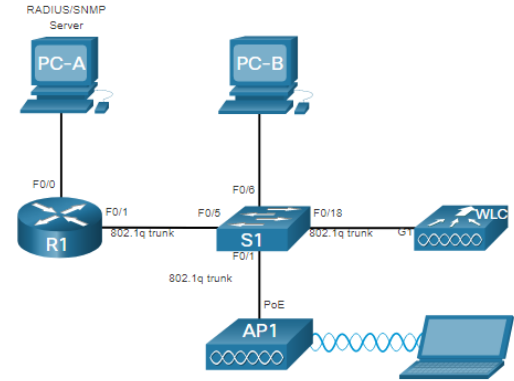
This video will cover the following:

- Review the topology
- Access the GUI for the WLAN controller
- Information about the wireless network on the Network summary screen
- Configure a new WLAN
- Secure the new WLAN

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**.

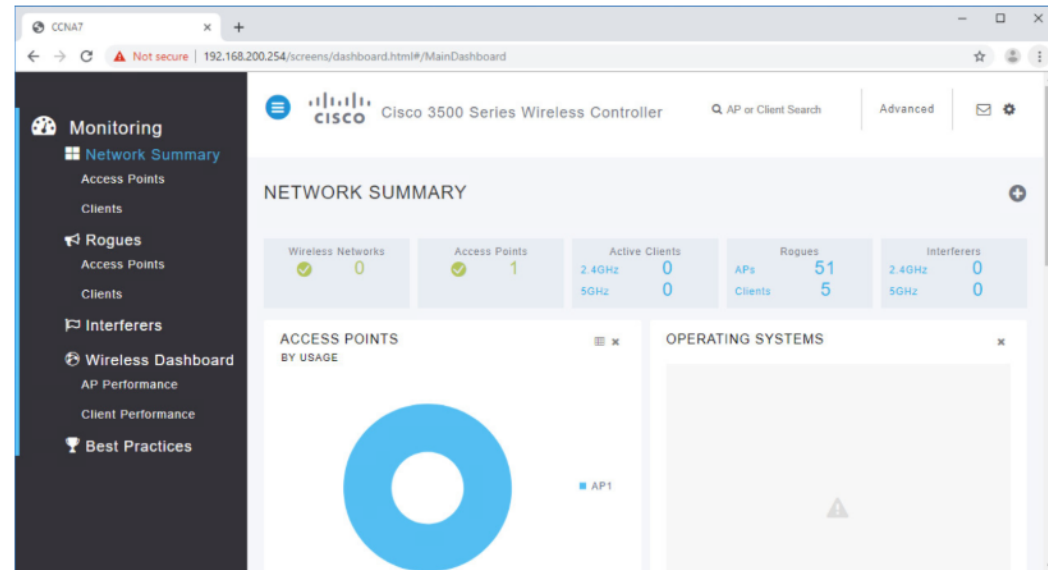


| Device | Interface | IP Address | Subnet Mask |
|-----------------|------------|-----------------|---------------|
| R1 | F0/0 | 172.16.1.1 | 255.255.255.0 |
| R1 | F0/1.1 | 192.168.200.1 | 255.255.255.0 |
| S1 | VLAN 1 | DHCP | |
| WLC | Management | 192.168.200.254 | 255.255.255.0 |
| AP1 | Wired 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 | |

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.

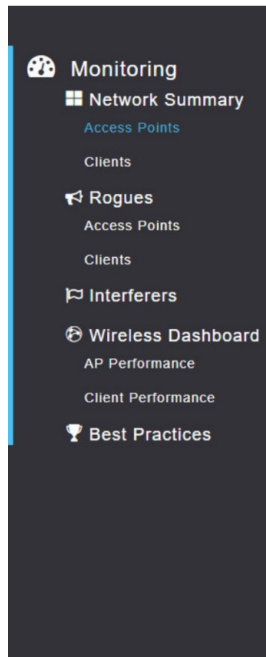
- The user logs into the WLC using credentials that were configured during initial setup.
- The **Network Summary** page is a dashboard that provides a **quick overview** of configured wireless networks, associated access points (APs), and active clients.
- You can also see the **number of rogue access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



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.



- Monitoring
 - Network Summary
 - Access Points
 - Clients
 - Rogues
 - Access Points
 - Clients
 - Interferers
 - Wireless Dashboard
 - AP Performance
 - Client Performance
 - Best Practices

ACCESS POINT VIEW

GENERAL

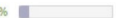

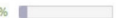

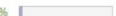



AP Name
AP1

Location
default location

| | |
|------------------|--|
| 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) |
| Fabric | Disabled |

PERFORMANCE SUMMARY

| | 2.4GHz | 5GHz |
|---------------------|--|--|
| Number of clients | 1 | 0 |
| Channels | 11 | (100, 104, 108, 112) |
| Configured Rate | Min: 1 Mbps, Max: 144 Mbps | 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 |

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.

The screenshot displays the Cisco Wireless Controller (WLC) Advanced Summary page. The page is titled "Summary" and shows the following information:

Controller Summary

| | |
|-------------------------|-----------------------------|
| Management IP Address | 192.168.200.254, ::/128 |
| Service Port IP Address | 0.0.0.0, ::/128 |
| Software Version | 8.5.140.0 |
| Emergency Image Version | 8.5.103.0 |
| System Name | CCNA7 |
| Up Time | 0 days, 2 hours, 25 minutes |

Rogue Summary

| | | |
|-------------------------|----|------------------------|
| Active Rogue APs | 35 | Detail |
| Active Rogue Clients | 10 | Detail |
| Adhoc Rogues | 0 | Detail |
| Rogues on Wired Network | 0 | |

Session Timeout [icon]

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.)

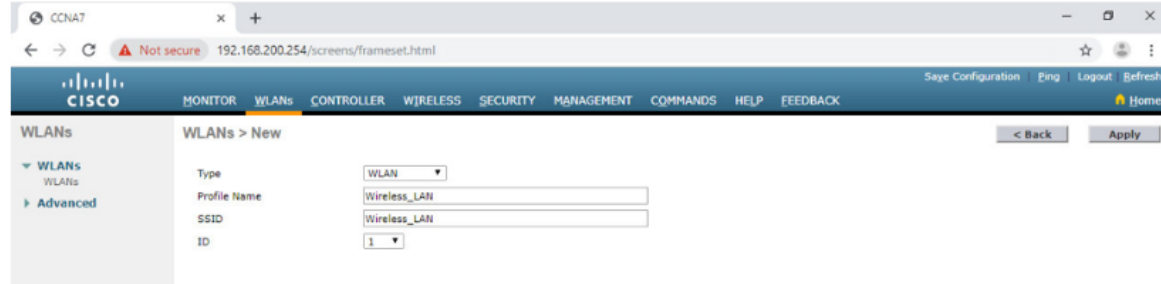
Basic WLAN configuration on the WLC includes the following steps:

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.)

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

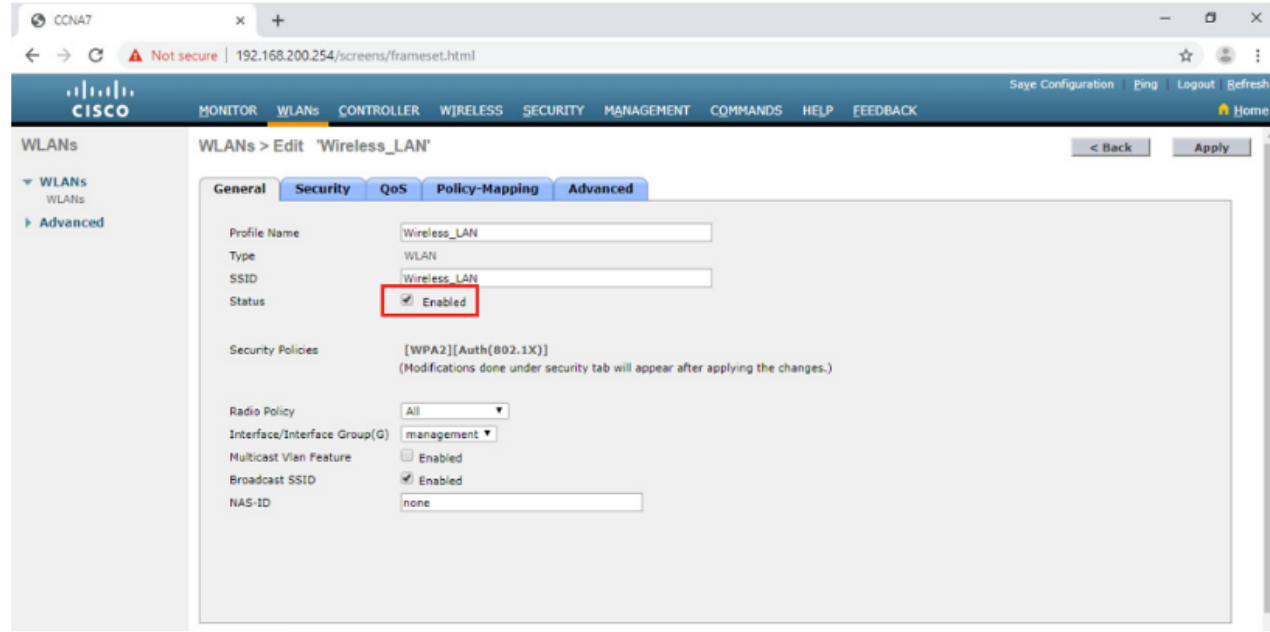


The screenshot shows the 'WLANs > New' configuration page in a web browser. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. On the left, there is a sidebar with 'WLANs' and 'Advanced' options. The main content area contains the following fields:

| | |
|--------------|--------------|
| Type | WLAN |
| Profile Name | Wireless_LAN |
| SSID | Wireless_LAN |
| ID | 1 |

Buttons for '< Back' and 'Apply' are visible at the top right.

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



The screenshot shows the 'WLANs > Edit 'Wireless_LAN'' configuration page in a web browser. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. On the left, there is a sidebar with 'WLANs' and 'Advanced' options. The main content area has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is selected, showing the following fields:

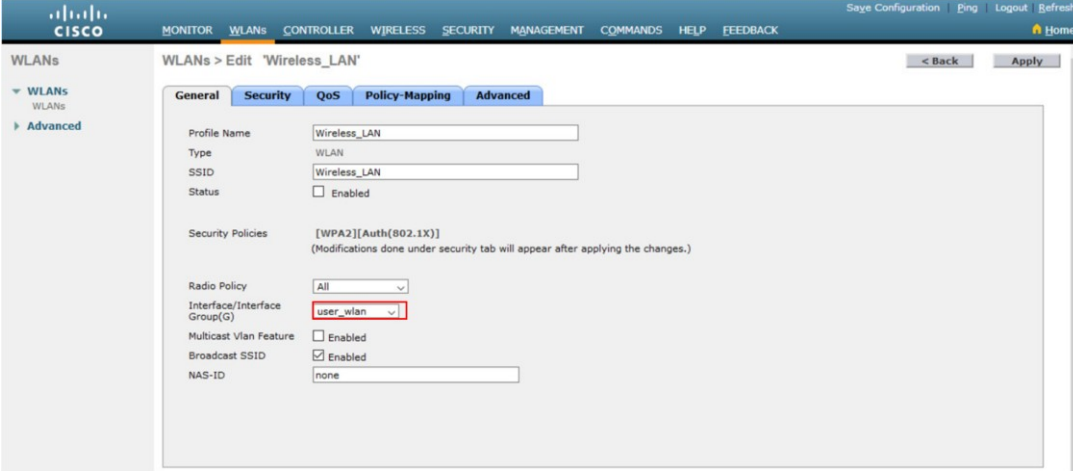
| | |
|------------------------------|---|
| Profile Name | Wireless_LAN |
| Type | WLAN |
| SSID | Wireless_LAN |
| Status | <input checked="" type="checkbox"/> Enabled |
| Security Policies | [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | management |
| Multicast Vlan Feature | <input type="checkbox"/> Enabled |
| Broadcast SSID | <input checked="" type="checkbox"/> Enabled |
| NAS-ID | none |

Buttons for '< Back' and 'Apply' are visible at the top right. The 'Status' field is highlighted with a red box.

Configure a WLAN (Cont.)

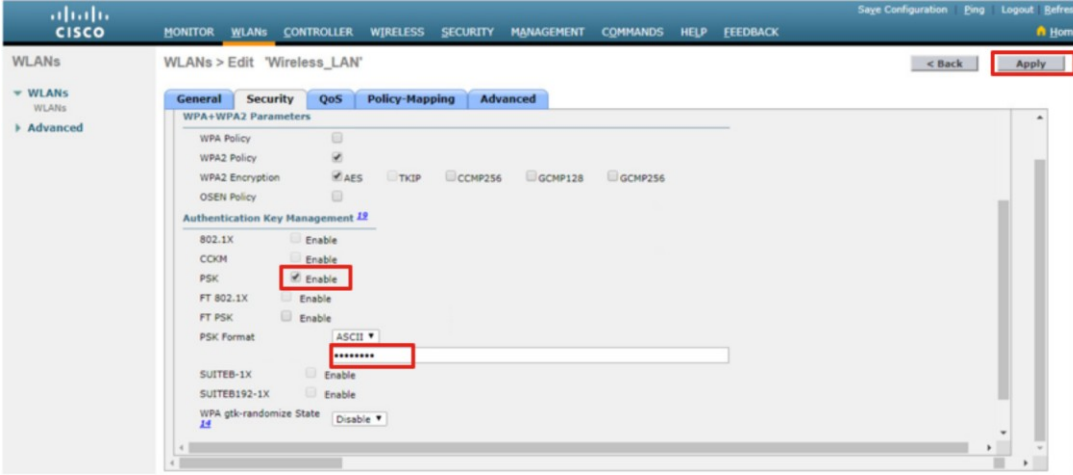
3. **Select the Interface:** The interface that will carry the WLAN traffic must be selected.

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



The screenshot shows the Cisco configuration interface for a WLAN named 'Wireless_LAN'. The 'General' tab is selected. The configuration includes:

- Profile Name: Wireless_LAN
- Type: WLAN
- SSID: Wireless_LAN
- 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): user_wlan
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: none



The screenshot shows the Cisco configuration interface for the same WLAN, now on the 'Security' tab. The configuration includes:

- WPA+WPA2 Parameters:
 - WPA Policy:
 - WPA2 Policy:
 - WPA2 Encryption: AES, TKIP, CCMP256, GCM128, GCM256
 - OSN Policy:
- Authentication Key Management [?](#)
 - 802.1X: Enable
 - COXN: Enable
 - PSK: Enable
 - FT 802.1X: Enable
 - FT PSK: Enable
 - PSK Format: ASCII, *****
 - SUITB-1X: Enable
 - SUITB192-1X: Enable
 - WPA gtk-randomize State: [?](#) Disable

Configure a WLAN (Cont.)

5. Verify the WLAN is Operational:

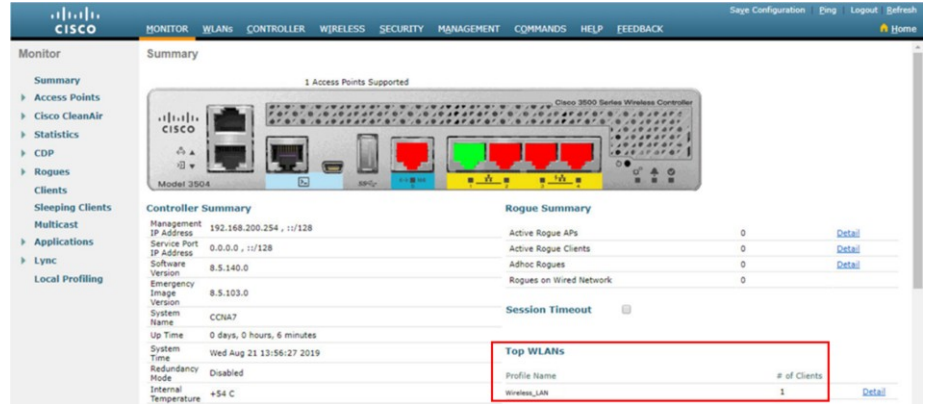
The **WLANs** menu on the left is used to view the newly configured WLAN and its settings.



The screenshot shows the Cisco configuration interface for WLANs. The 'WLANs' menu item in the left sidebar is highlighted with a red box. The main content area displays a table of WLANs with the following data:

| 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.

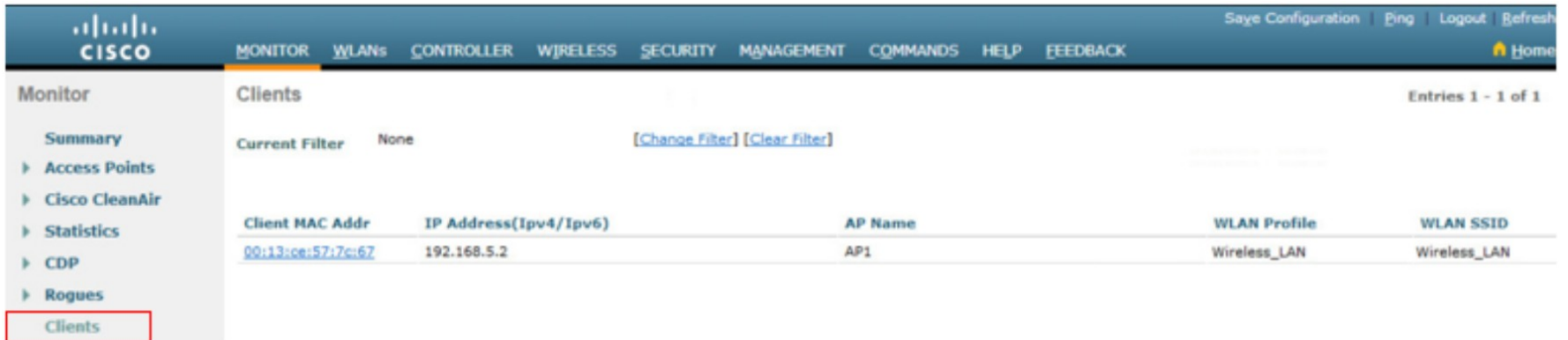


The screenshot shows the Cisco Monitor interface for the WLAN. The 'Monitor' tab is selected, and the 'Summary' page is displayed. The 'Top WLANs' table at the bottom right is highlighted with a red box and contains the following data:

| Profile Name | # of Clients |
|--------------|--------------|
| Wireless_LAN | 1 |

Configure a WLAN (Cont.)

- View Wireless Client Details:** Click **Clients** in the left menu to view more information about the clients connected to the WLAN.



The screenshot displays the Cisco WLC GUI. The top navigation bar includes the Cisco logo and menu items: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The right side of the top bar contains links for Save Configuration, Ping, Logout, Refresh, and Home. The left sidebar menu is expanded to show 'Clients', which is highlighted with a red rectangular box. Other menu items include Monitor, Summary, Access Points, Cisco CleanAir, Statistics, CDP, and Rogues. The main content area is titled 'Clients' and shows 'Entries 1 - 1 of 1'. Below the title, there is a 'Current Filter' section set to 'None' with links for '[Change Filter]' and '[Clear Filter]'. A table lists the client details:

| 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.

13.3 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:

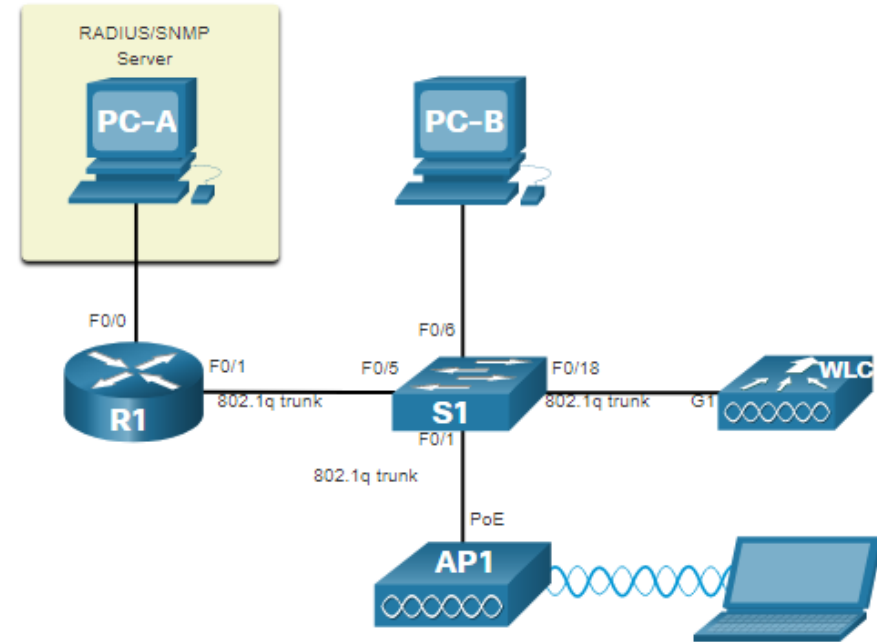
- Configure the WLAN controller to send SNMP traps to an external server
- Configure the WLAN controller to use an external RADIUS server to authenticate WLAN users
- Verify connectivity with the RADIUS server

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**.

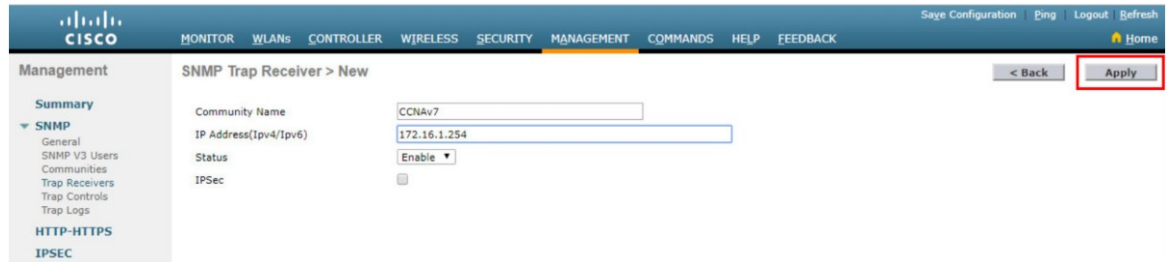
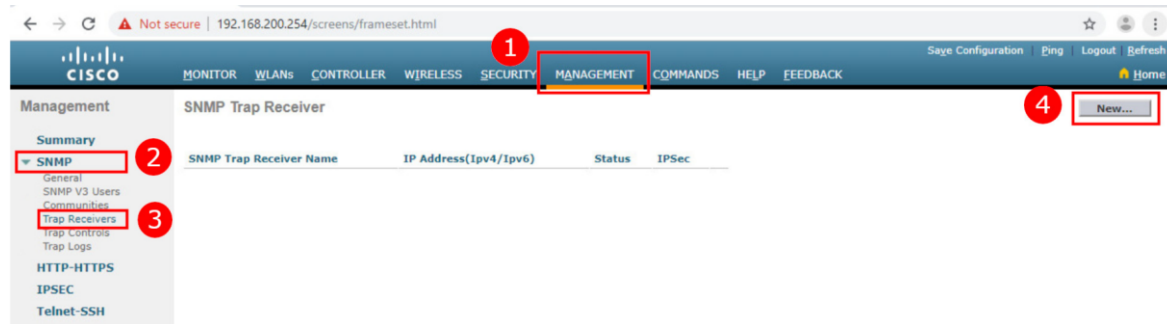
Note: SNMP server and RADIUS server configuration is beyond the scope of this module.



Configure 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.



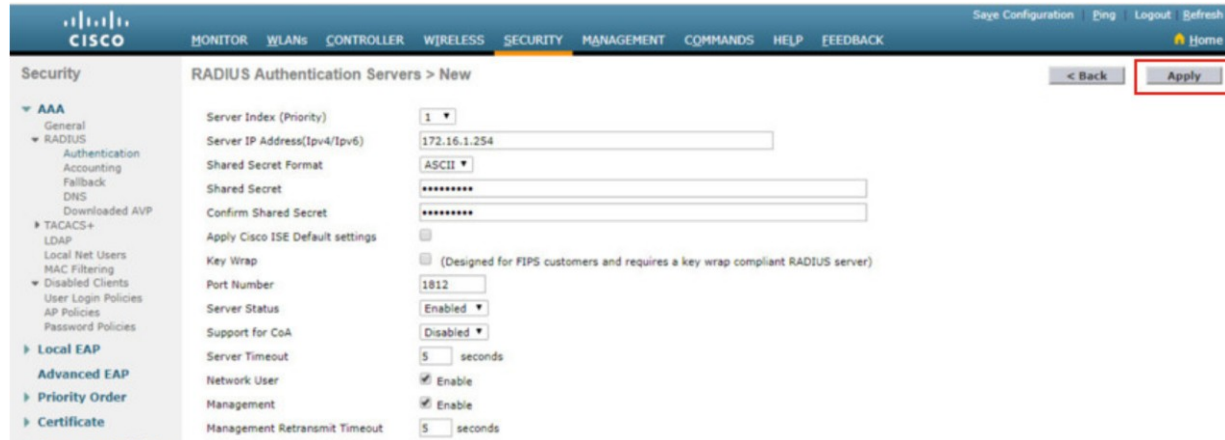
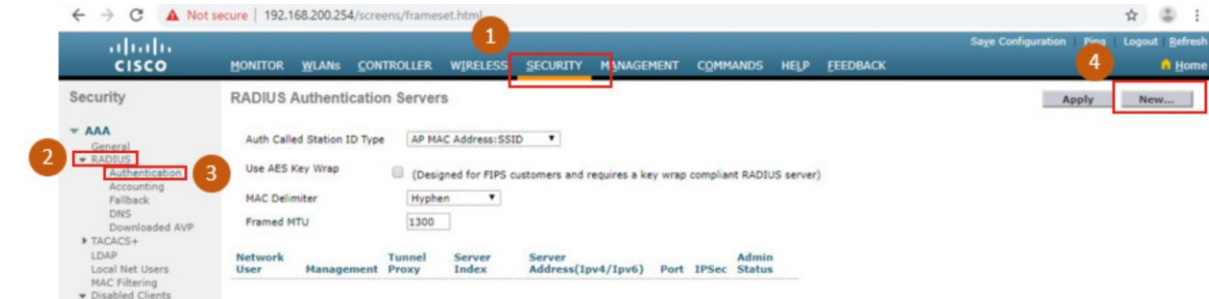
- Enter the SNMP Community name and the IP address (IPv4 or IPv6) for the SNMP server and then click **Apply**.
- The WLC will now forward SNMP log messages to the SNMP server.

Configure 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.



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 configuration interface for RADIUS Authentication Servers. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY' (highlighted), 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Security' menu with 'AAA' expanded to 'RADIUS'. The main content area is titled 'RADIUS Authentication Servers' and contains the following configuration options:

- Auth Called Station ID Type: AP MAC Address:SSID
- Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- MAC Delimiter: Hyphen
- Framed MTU: 1300

Below the configuration options is a table of configured RADIUS Authentication Servers. The table has the following columns: Network User, Management, Tunnel Proxy, Server Index, Server Address(Ipv4/Ipv6), Port, IPSec, and Admin Status. A single server is listed with the following details:

| 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 |

Video – Configure a VLAN for a New WLAN

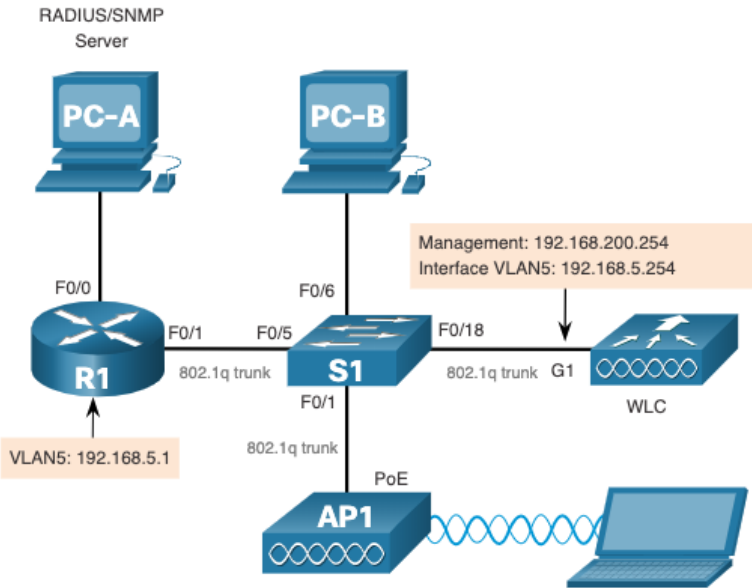
This video will cover the following:

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

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...**

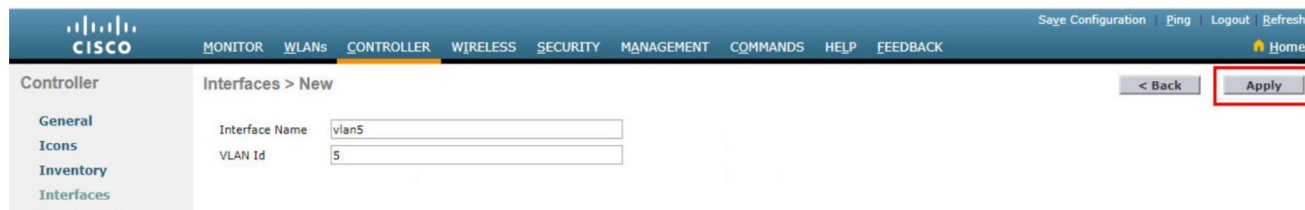


The screenshot shows the Cisco WLC Controller configuration page. The browser address bar shows the URL <https://192.168.200.254/s/frameset.html>. The navigation menu includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The CONTROLLER tab is selected and highlighted with a red box and a red circle containing the number 1. The left sidebar shows the Controller configuration tree with General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, and Fabric Configuration. The Interfaces section is selected and highlighted with a red box and a red circle containing the number 2. The main content area displays a table of 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 |
| virtual | N/A | 192.0.2.1 | Static | Not Supported | |

The table has 5 entries, and a 'New...' button is visible in the top right corner, highlighted with a red box and a red circle containing the number 3.

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 Cisco WLC Controller configuration page for creating a new interface. The navigation menu is the same as in the previous screenshot. The CONTROLLER tab is selected. The left sidebar shows the Controller configuration tree with General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, and Fabric Configuration. The Interfaces section is selected. The main content area displays the 'Interfaces > New' form with the following fields:

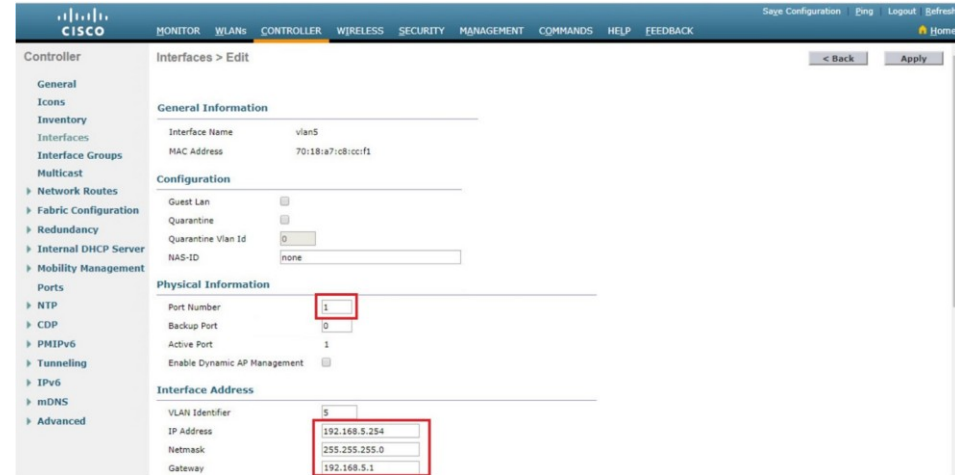
Interface Name:

VLAN Id:

The form has a '< Back' button and an 'Apply' button, both highlighted with red boxes.

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)

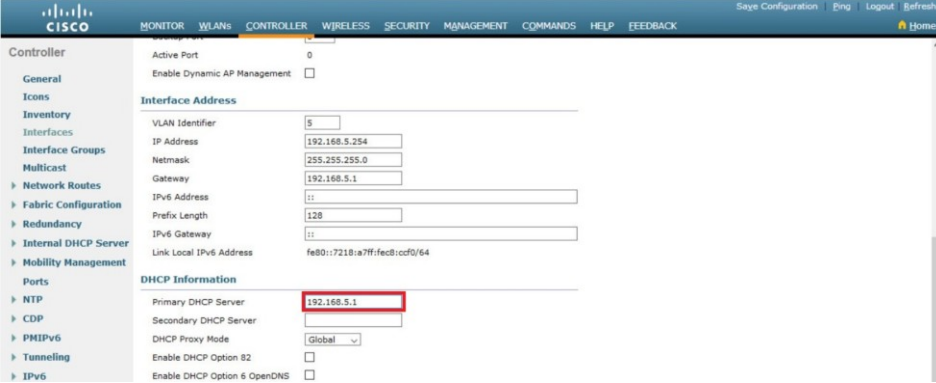


The screenshot shows the Cisco Controller configuration page for an interface. The page is titled "Interfaces > Edit" and has a navigation bar at the top with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar contains a navigation menu with categories like General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, PHIPv6, Tunneling, IPv6, mDNS, and Advanced. The main content area is divided into sections: General Information, Configuration, Physical Information, and Interface Address. The Physical Information section has a red box around the Port Number field, which is set to 1. The Interface Address section has a red box around the IP Address, Netmask, and Gateway fields, which are set to 192.168.5.254, 255.255.255.0, and 192.168.5.1 respectively. The VLAN Identifier field is also set to 5.

| Section | Field | Value |
|----------------------|--------------------|--------------------------|
| General Information | Interface Name | vlan5 |
| | MAC Address | 70:18:a7:c8:cc:ff |
| Configuration | Guest Lan | <input type="checkbox"/> |
| | Quarantine | <input type="checkbox"/> |
| | Quarantine Vlan Id | 0 |
| Physical Information | Port Number | 1 |
| | Backup Port | 0 |
| | Active Port | 1 |
| Interface Address | VLAN Identifier | 5 |
| | IP Address | 192.168.5.254 |
| | Netmask | 255.255.255.0 |
| | Gateway | 192.168.5.1 |

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.



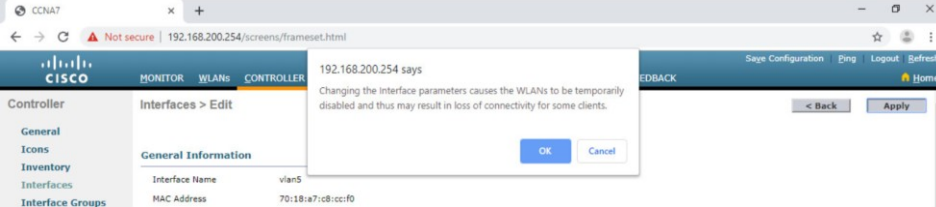
The screenshot shows the Cisco Controller configuration page for a new interface. The 'Interface Address' section is visible, with the following fields:

| Field | Value |
|-------------------------|------------------------------|
| VLAN Identifier | 5 |
| IP Address | 192.168.5.254 |
| Netmask | 255.255.255.0 |
| Gateway | 192.168.5.1 |
| IPv6 Address | |
| Prefix Length | 128 |
| IPv6 Gateway | |
| Link Local IPv6 Address | fe80::7218:a7ff:fedc:ccf0/64 |

The 'DHCP Information' section is also visible, with the following fields:

| Field | Value |
|------------------------------|--------------------------|
| Primary DHCP Server | 192.168.5.1 |
| Secondary DHCP Server | |
| DHCP Proxy Mode | Global |
| Enable DHCP Option 82 | <input type="checkbox"/> |
| Enable DHCP Option 6 OpenDNS | <input type="checkbox"/> |

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



The screenshot shows the Cisco Controller configuration page for a new interface, with a warning message displayed. The warning 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." The warning message has an 'OK' button and a 'Cancel' button. The configuration page is partially visible in the background, showing the 'General Information' section with the following fields:

| Field | Value |
|----------------|-------------------|
| Interface Name | vlan5 |
| MAC Address | 70:18:a7:c8:cc:f0 |

Configure a New Interface (Cont.)

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



The screenshot displays the Cisco Controller web interface. The top navigation bar includes the Cisco logo, a menu with options like MONITOR, WLANs, CONTROLLER (highlighted), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK, and utility links for Save Configuration, Ping, Logout, Refresh, and Home. The left sidebar shows a navigation tree with 'Interfaces' selected. The main content area shows a table of interfaces.

| 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 |

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

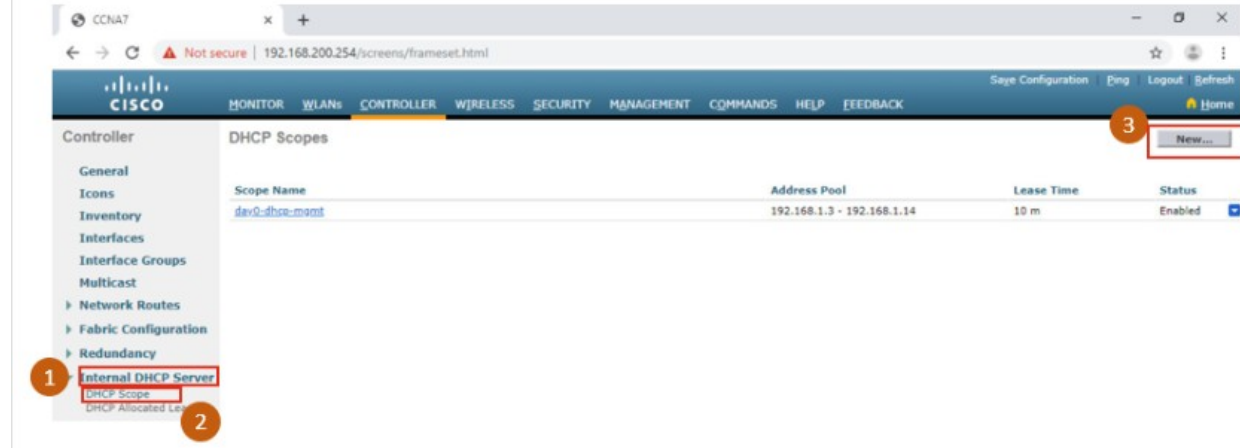
Configure a DHCP Scope

DHCP scope configuration includes the following steps:

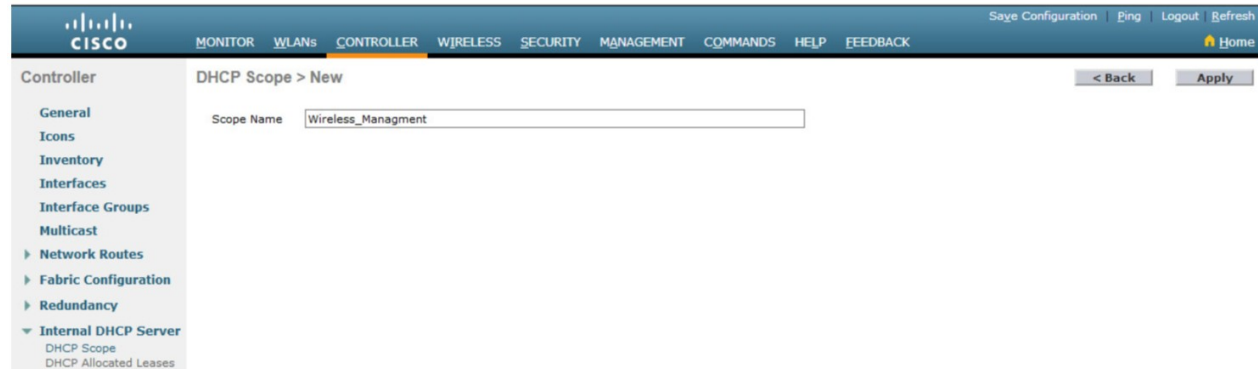
1. Create a new DHCP scope.
2. Name the DHCP scope.
3. Verify the new DHCP scope.
4. Configure and enable the new DHCP scope.
5. Verify the enable DHCP scope

Configure a DHCP Scope (Cont.)

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



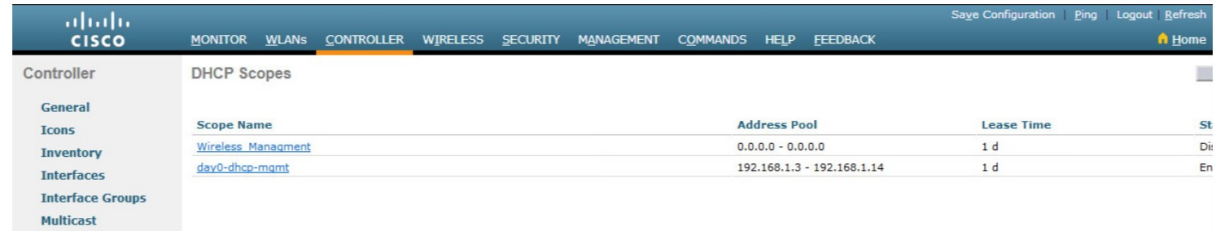
2. **Name the DHCP scope:** The scope is named **Wireless_Managment** and then applied.



Configure a DHCP Scope (Cont.)

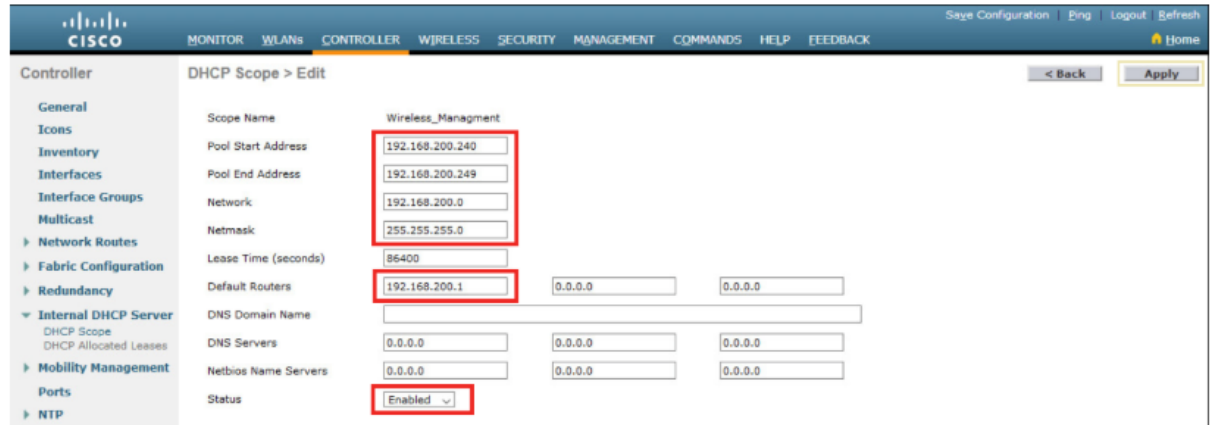
3. **Verify the new DHCP scope:**
In the **DHCP Scopes** page click the new Scope Name to configure the DHCP scope.

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**.



The screenshot shows the Cisco Controller interface for DHCP Scopes. The table lists the following scopes:

| Scope Name | Address Pool | Lease Time | Status |
|-------------------------------------|----------------------------|------------|----------|
| Wireless_Management | 0.0.0.0 - 0.0.0.0 | 1 d | Disabled |
| day0-dhcp-mgmt | 192.168.1.3 - 192.168.1.14 | 1 d | Enabled |

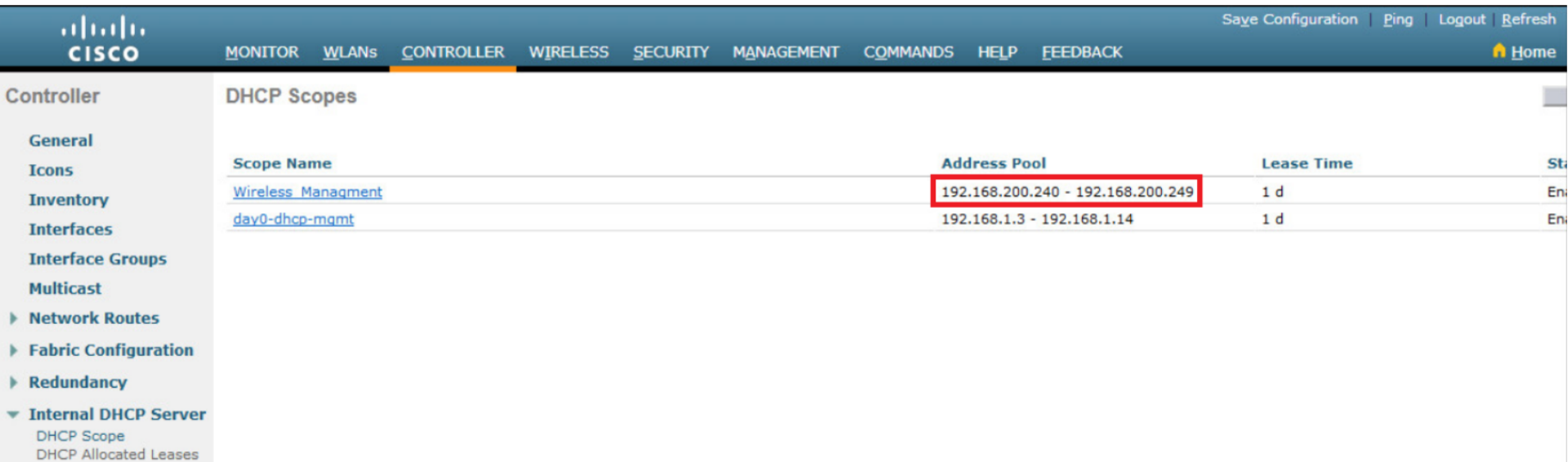


The screenshot shows the configuration page for the DHCP Scope 'Wireless_Management'. The following fields are highlighted with red boxes:

- Pool Start Address: 192.168.200.240
- Pool End Address: 192.168.200.249
- Network: 192.168.200.0
- Netmask: 255.255.255.0
- Default Router: 192.168.200.1
- Status: Enabled

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 DHCP Scopes configuration page. The 'CONTROLLER' tab is selected in the top navigation bar. The left sidebar shows the 'Internal DHCP Server' section expanded. The main content area displays a table of DHCP scopes. The 'Wireless_Management' scope is highlighted, and its 'Address Pool' is circled in red.

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

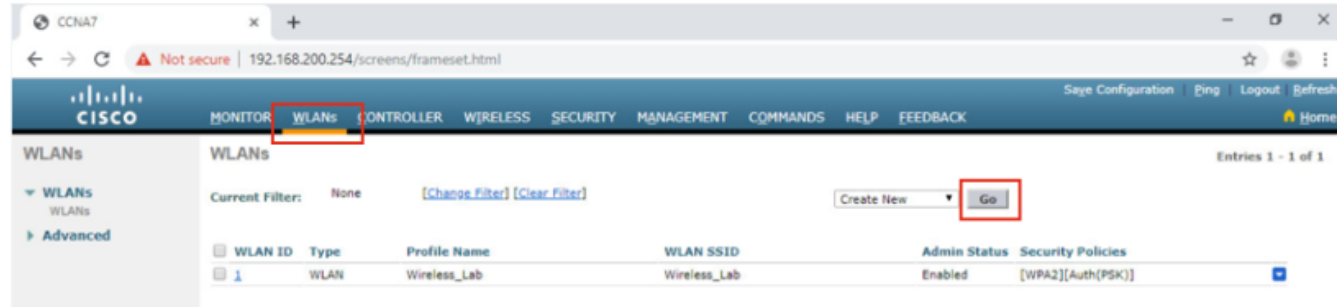
- 802.1X is the default key management protocol used to communicate with the RADIUS server.
- Next, create a new WLAN to use interface **vlan5**.

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

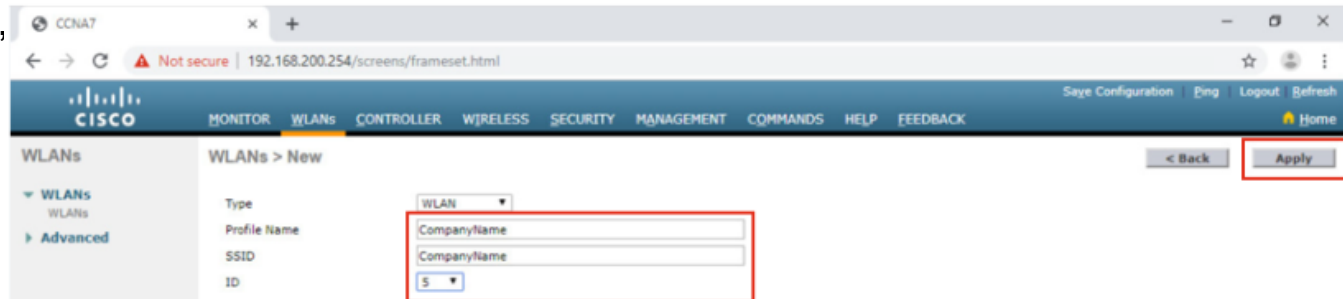
1. Create a new WLAN.
2. Configure the WLAN name and SSID.
3. Enable the WLAN for VLAN 5.
4. Verify AES and 802.1X defaults.
5. Configure WLAN security to use the RADIUS server.
6. Verify the new WLAN is available.

Configure a WPA2 Enterprise WLAN (Cont.)

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



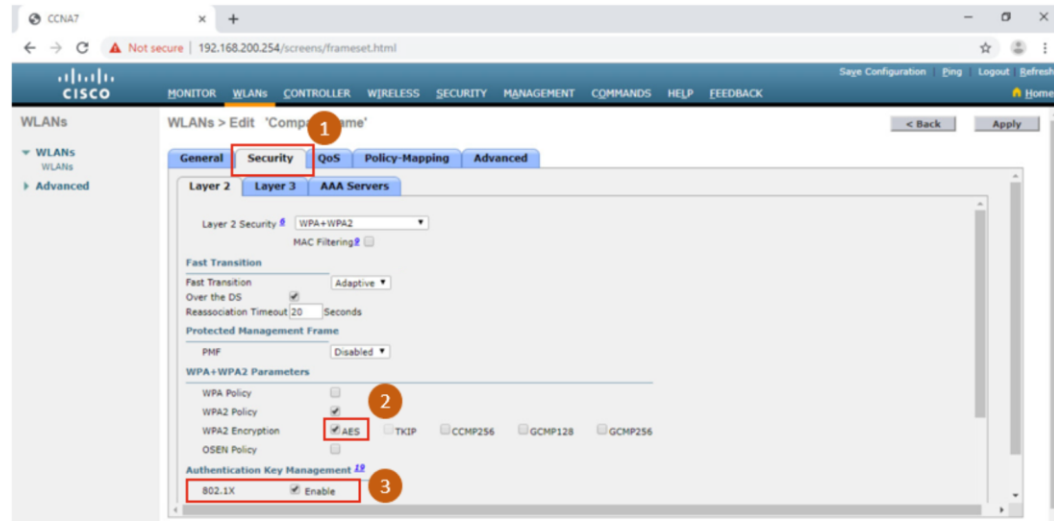
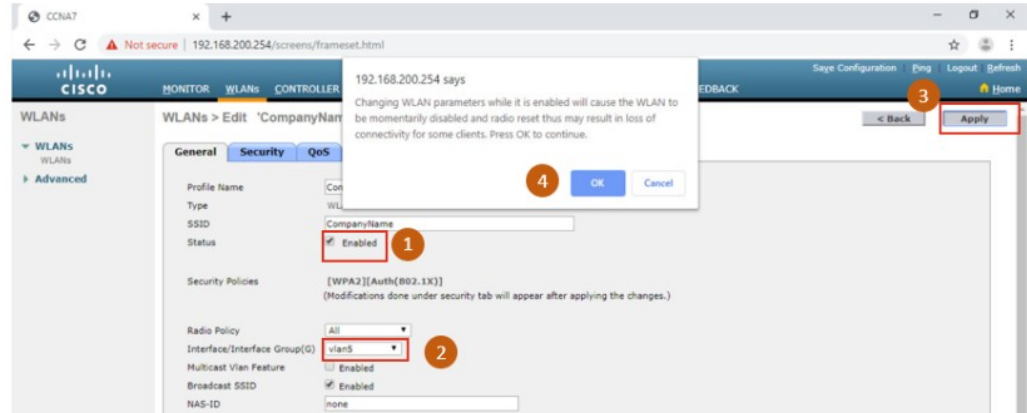
2. **Configure the WLAN name and SSID:** Enter the profile name and SSID, choose an **ID of 5**, and then click **Apply** to create the new WLAN.



Configure a WPA2 Enterprise WLAN (Cont.)

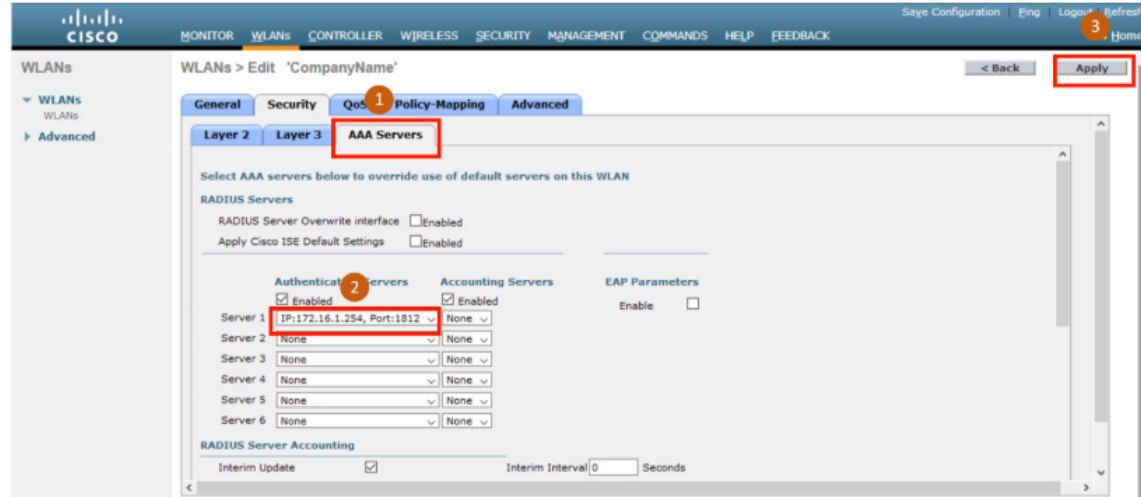
3. **Enable the WLAN for VLAN 5:** Once the WLAN, change the status to **Enabled**, choose **vlan5** from the Interface/Interface Group(G) dropdown list, and then click **Apply** and click **OK** to accept the popup message.

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 (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 'AAA Servers' configuration page for a WLAN. The 'AAA Servers' tab is selected, and the 'Server 1' dropdown menu is open, showing the selected IP address 'IP:172.16.1.254, Port:1812'. The 'Apply' button is highlighted in the top right corner.

WLANs > Edit 'CompanyName'

General Security **QoS-1 AAA Servers** Policy-Mapping Advanced

Layer 2 Layer 3

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Apply Cisco ISE Default Settings Enabled

Authenticating Servers Accounting Servers EAP Parameters

Enabled Enabled Enable

| Server | Authenticating Servers | Accounting Servers | EAP Parameters |
|----------|----------------------------|--------------------|---------------------------------|
| Server 1 | IP:172.16.1.254, Port:1812 | None | Enable <input type="checkbox"/> |
| Server 2 | None | None | |
| Server 3 | None | None | |
| Server 4 | None | None | |
| Server 5 | None | None | |
| Server 6 | None | None | |

RADIUS Server Accounting

Interim Update Interim Interval 0 Seconds

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' configuration page. The 'WLANs' submenu is highlighted in the left sidebar. The main area displays a table of configured WLANs.

WLANs

WLANs

Current Filter: None [Change Filter] [Clear Filter] Create New Go

| WLAN ID | Type | Profile Name | WLAN SSID | Admin Status | Security Policies |
|---------|------|--------------|--------------|--------------|----------------------|
| 1 | WLAN | Wireless_LAN | Wireless_LAN | Enabled | [WPA2][Auth(PSK)] |
| 5 | WLAN | CompanyName | CompanyName | Enabled | [WPA2][Auth(802.1X)] |

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.

13.4 Troubleshoot WLAN Issues

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.

Cisco Linksys RE1000 Wireless-N WiFi Range Extender



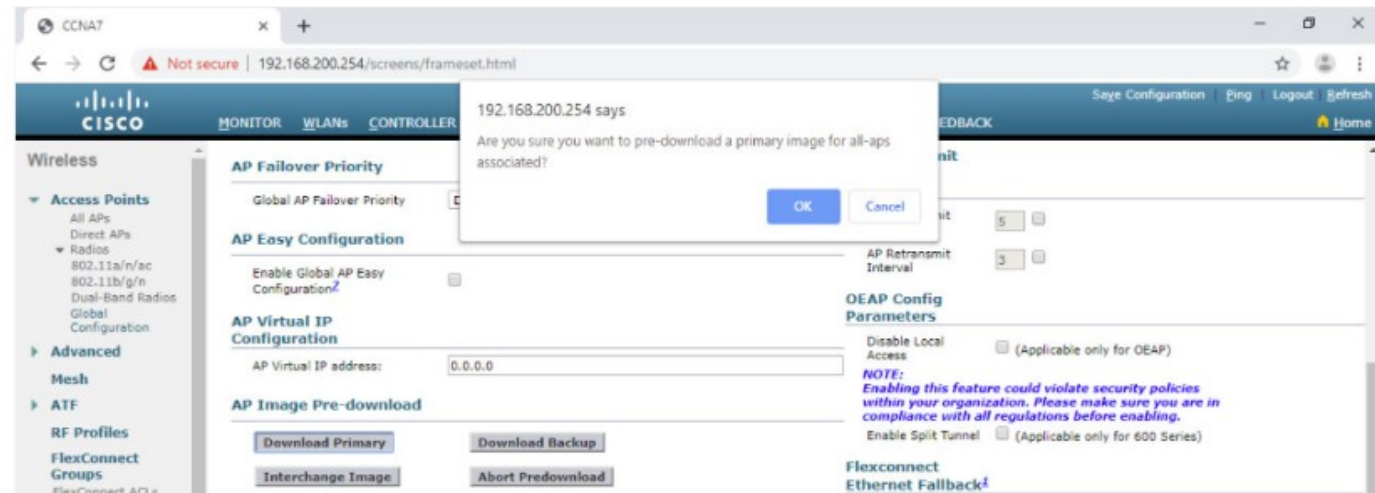
Troubleshoot WLAN Issues

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.

13.5 Module Practice and Summary

Module 13: Osvědčené postupy

Téma 13.1

Zeptejte se studentů nebo uspořádejte diskusi ve třídě
Proč byste měli pravidelně měnit pověření na vašem bezdrátovém routeru? Jakou hodnotu podle vás QoS poskytne domácímu uživateli?

Téma 13.2

Co si myslíte, že je jednou z výhod nasazení sítě pomocí WLC?
Jaký protokol používá WLC k získání informací o AP?

Téma 13.3

Co je podle vás nevýhodou centralizovaného ověřování pomocí protokolu RADIUS?
Proč byste zakázali vysílání vašeho SSID?

Téma 13.4

Proč je udržování aktualizovaného firmwaru tak důležité pro zabezpečení sítě?
Mnoho bezdrátových směrovačů umožňuje majiteli provozovat několik různých bezdrátových sítí; jednu v pásmu 2,4 GHz a druhou v pásmu 5 GHz. Jakou výhodu by to mohlo poskytnout?

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.

What Did I Learn In This Module?

- Remote workers, small branch offices, and home networks often use a wireless router, which typically include a switch for wired clients, a port for an internet connection (sometimes labeled “WAN”), and wireless components for wireless client access.
- Most wireless routers are preconfigured to be connected to the network and provide services. The wireless router uses DHCP to automatically provide addressing information to connected devices.
- Your first priority should be to change the username and password of your wireless router.
- If you want to extend the range beyond approximately 45 meters indoors and 90 meters outdoors, you can add wireless access points.
- The router will use a process called Network Address Translation (NAT) to convert private IPv4 addresses to internet-routable IPv4 addresses.
- 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.
- Lightweight APs (LAPs) use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC).

What Did I Learn In This Module? (Cont.)

- Configuring a wireless LAN controller (WLC) is similar to configuring a wireless router except that a WLC controls APs and provides more services and management capabilities. Use the WLC interface to view an overall picture of the AP's system information and performance, to access advanced settings and to configure a WLAN.
- SNMP is used to monitor the network. The WLC is set to forward all SNMP log messages, called traps, to the SNMP server.
- For WLAN user authentication, a RADIUS server is used for authentication, accounting, and auditing (AAA) services. Individual user access can be tracked and audited.
- Use the WLC interface to configure SNMP server and RADIUS server information, VLAN interfaces, DHCP scope, and a WPA2 Enterprise WLAN.
- There are six steps to the troubleshooting process.
- When troubleshooting a WLAN, a process of elimination is recommended. Common problems are: no connectivity and poorly performing wireless connection when the PC is operational.
- To optimize and increase the bandwidth of 802.11 dual-band routers and APs, either: upgrade your wireless clients or split the traffic.
- Most wireless routers and APs offer upgradable firmware. Firmware releases may contain fixes for common problems reported by customers as well as security vulnerabilities. You should periodically check the router or AP for updated firmware.

youtube

13.1.11 Lab - Configure a Wireless Network

<https://www.youtube.com/watch?v=F5A9cG22Sfw>

