CCNA 2 v7.0 Curriculum: Module 13 – WLAN Configuration

itexamanswers.net/ccna-2-v7-0-curriculum-module-13-wlan-configuration.html

June 10, 2020

Contents

13.0 Introduction

13.0.1 Why should I take this module?

Welcome to WLAN Configuration!

Some of us remember getting on the internet using dial up. Dial up involved using your landline phone. Your landline phone was unavailable to make or receive calls while you were on the internet. Your dial up connection to the internet was very slow. It basically meant that, for most people, your computer was always in one place in your home or school.

Then we were able to connect to the internet without using our landlines. But our computers were still hardwired to the devices that connected them to the internet. Today we can connect to the internet using wireless devices that lets us take our phones, laptops, and tablets almost anywhere. It's nice to have this freedom of movement, but it requires special end and intermediary devices and a good understanding of wireless protocols. Want to know more? Then this is the module for you!

13.0.2 What will I learn to do in this module?

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

13.1.1 Video – Configure a Wireless Network

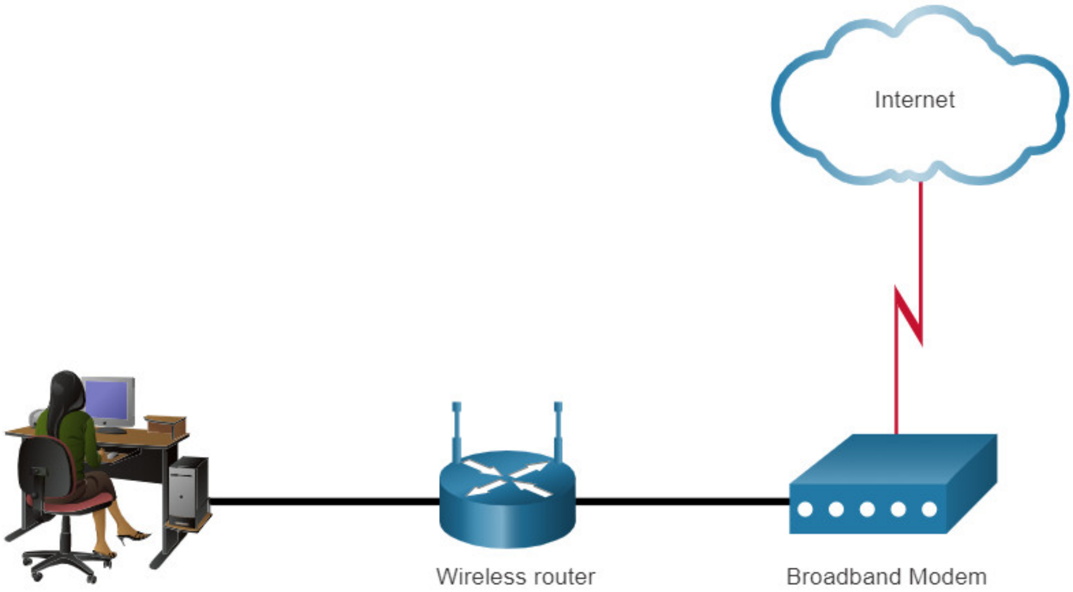
Click Play in the figure to view a demonstration of how to configure a wireless network.

13.1.2 The Wireless Router

Remote workers, small branch offices, and home networks often use a small office and home router. These routers are sometimes called an integrated router because they typically include a switch for wired clients, a port for an internet connection (sometimes labeled "WAN"), and wireless components for wireless client access, as shown for the Cisco Meraki MX64W in the figure. For the rest of this module, small office and home routers are referred to as wireless routers.

Cisco Meraki MX64W

The next figure shows a topology depicting the physical connection of a wired laptop to the wireless router, which is then connected to a cable or DSL modem for internet connectivity.



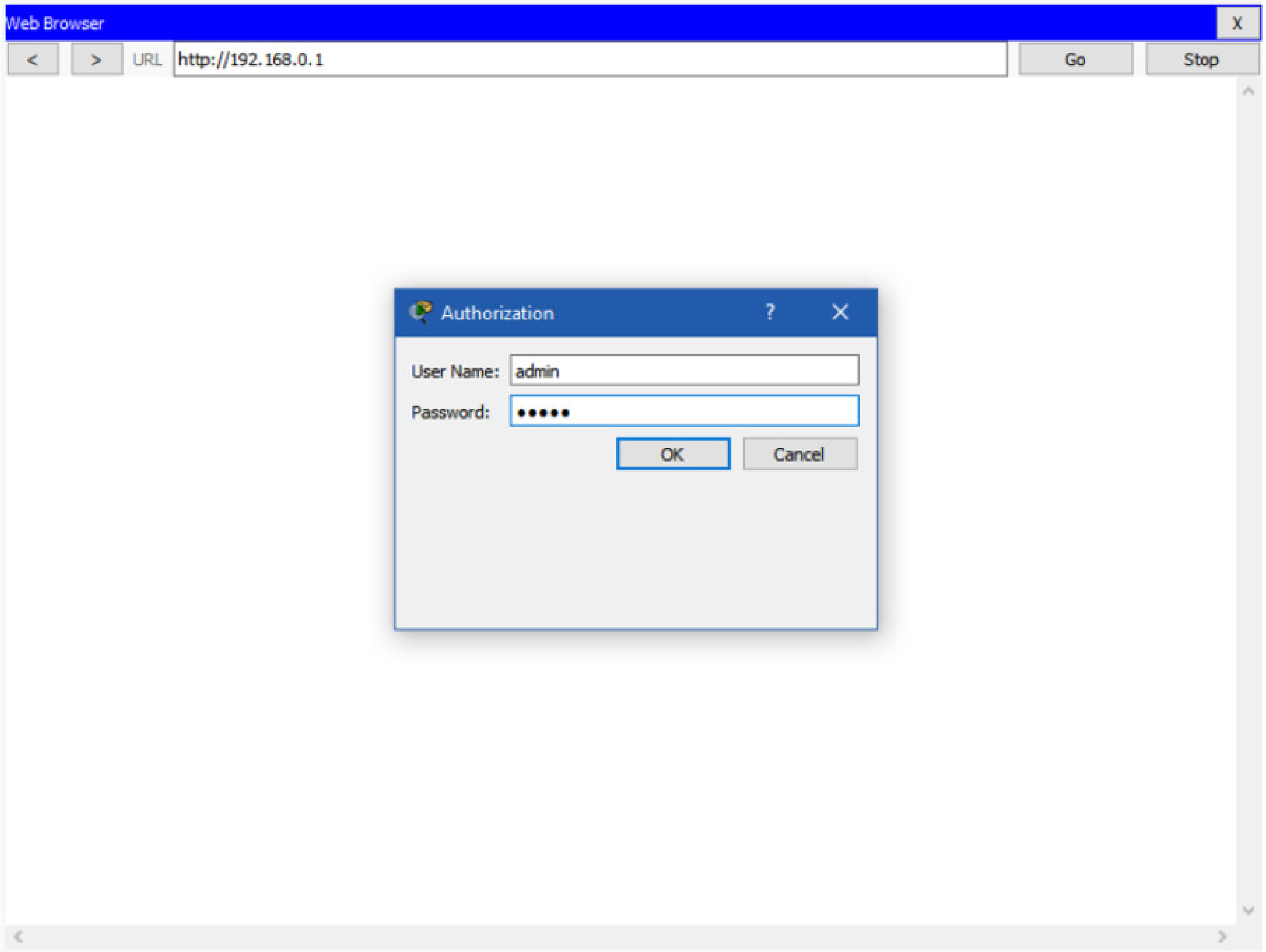
These wireless routers typically provide WLAN security, DHCP services, integrated Name Address Translation (NAT), quality of service (QoS), as well as a variety of other features. The feature set will vary based on the router model.

Note: Cable or DSL modem configuration is usually done by the service provider's representative either on-site or remotely through a walkthrough with you on the phone. If you buy the modem, it will come with documentation for how to connect it to your service provider which will most likely include contacting your service provider for more information.

13.1.3 Log in to the Wireless Router

Most wireless routers are ready for service out of the box. They are preconfigured to be connected to the network and provide services. For example, the wireless router uses DHCP to automatically provide addressing information to connected devices. However, wireless router default IP addresses, usernames, and passwords can easily be found on the internet. Just enter the search phrase "default wireless router IP address" or "default wireless router passwords" to see a listing of many websites that provide this information. For example, username and password for the wireless router in the figure is "admin". 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. In the address field, 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 figure shows the IPv4 address 192.168.0.1, which is a common default for many manufacturers. A security window prompts for authorization to access the router GUI. The word admin is commonly used as the default username and password. Again, check your wireless router's documentation or search the internet.



http://192.168.0.1

User Name: admin

Password: •••••

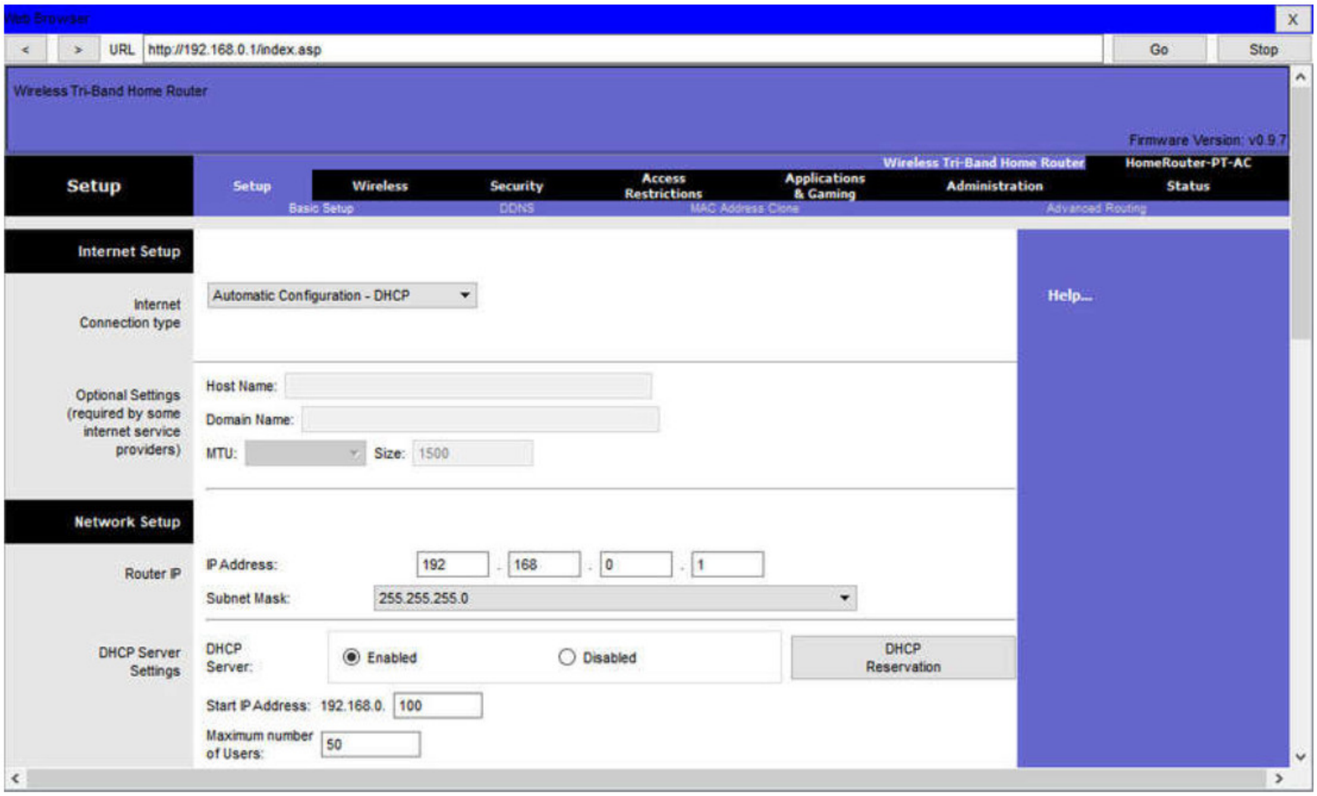
13.1.4 Basic Network Setup

Basic network setup includes the following steps:

1. Log in to the router from a web browser.
2. Change the default administrative password.
3. Log in with the new administrative password.
4. Change the default DHCP IPv4 addresses.
5. Renew the IP address.
6. Log in to the router with the new IP address.

Click each step for more information and an example GUI.

1. Log in to the router from a web browser.
After logging in, a GUI opens. The GUI will have tabs or menus to help you navigate to various router configuration tasks. It is often necessary to save the settings changed in one window before proceeding to another window. At this point, it is a best practice to make changes to the default settings.



URL http://192.168.0.1/index.asp

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU: Size: 1500

Network Setup

Router IP
IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255.255.255.0

DHCP Server Settings
DHCP Server: ● Enabled ○ Disabled
Start IP Address: 192.168.0. 100
Maximum number of Users: 50

13.1.5 Basic Wireless Setup

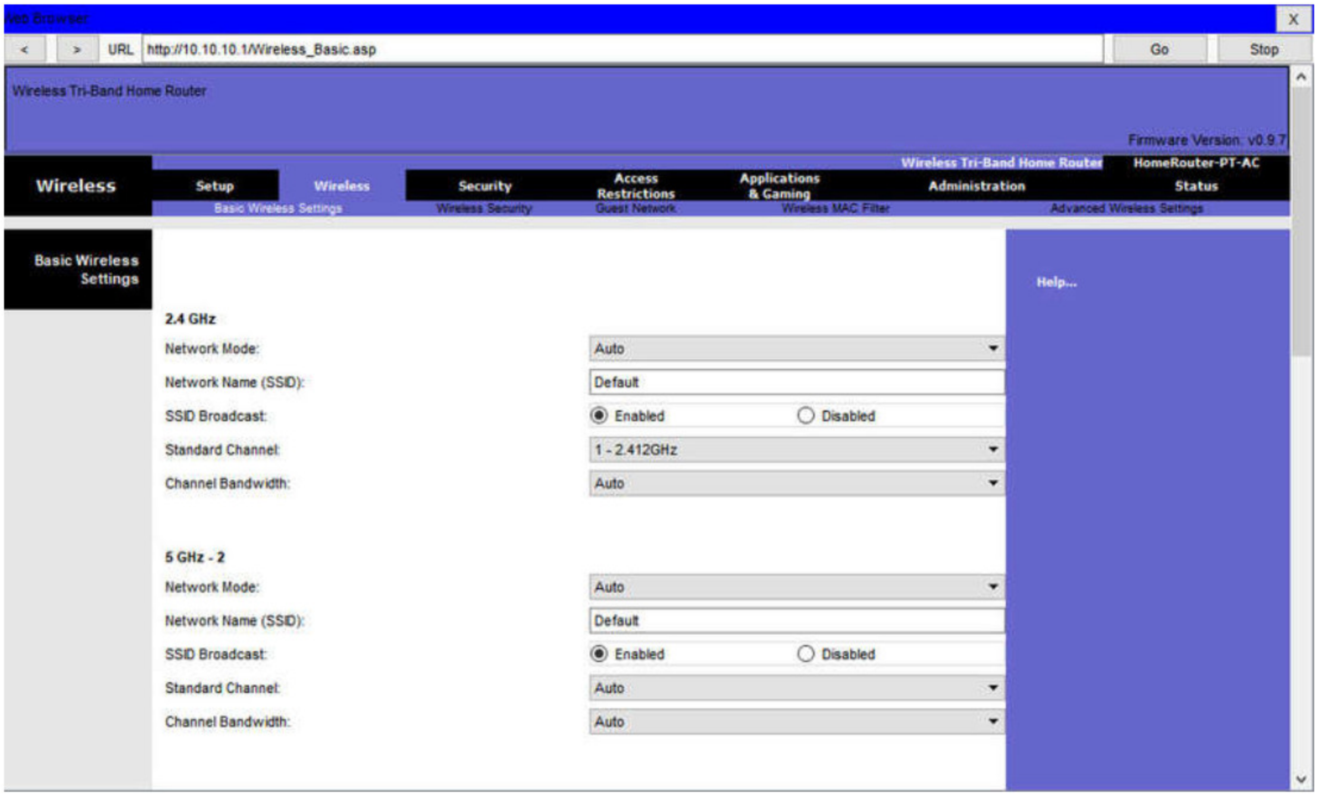
Basic wireless setup includes the following steps:

1. View the WLAN defaults.
2. Change the network mode.
3. Configure the SSID.
4. Configure the channel.
5. Configure the security mode.
6. Configure the passphrase.

Click each step for more information and an example GUI.

1. View the WLAN defaults.

Out of the box, a wireless router provides wireless access to devices using a default wireless network name and password. The network name is called the Service Set Identified (SSID). Locate the basic wireless settings for your router to change these defaults, as shown in the example.



URL http://10.10.10.1/Wireless_Basic.asp

Basic Wireless Settings

2.4 GHz

Network Mode: Auto

Network Name (SSID): Default

SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: 1 - 2.412GHz

Channel Bandwidth: Auto

5 GHz - 2

Network Mode: Auto

Network Name (SSID): Default

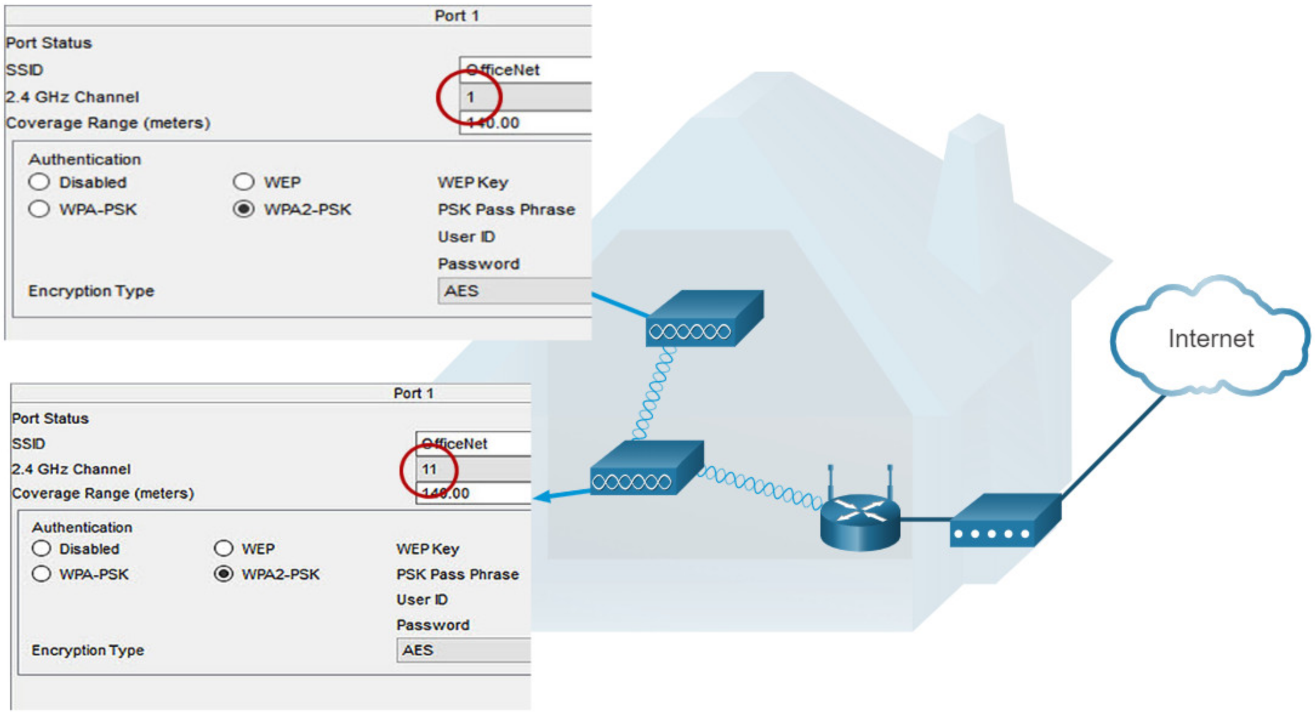
SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: Auto

Channel Bandwidth: Auto

13.1.6 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. However, if you want to extend the range beyond approximately 45 meters indoors and 90 meters outdoors, you can add wireless access points. As shown in the wireless mesh network in the figure, two access points are configured with the same WLAN settings from our previous example. Notice that the channels selected are 1 and 11 so that the access points do not interfere with channel 6 configured previously on the wireless router.



Port 1

Port Status

SSID OfficeNet

2.4 GHz Channel 1

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase

User ID

Password

Encryption Type AES

Port 1

Port Status

SSID OfficeNet

2.4 GHz Channel 11

Coverage Range (meters) 140.00

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase

User ID

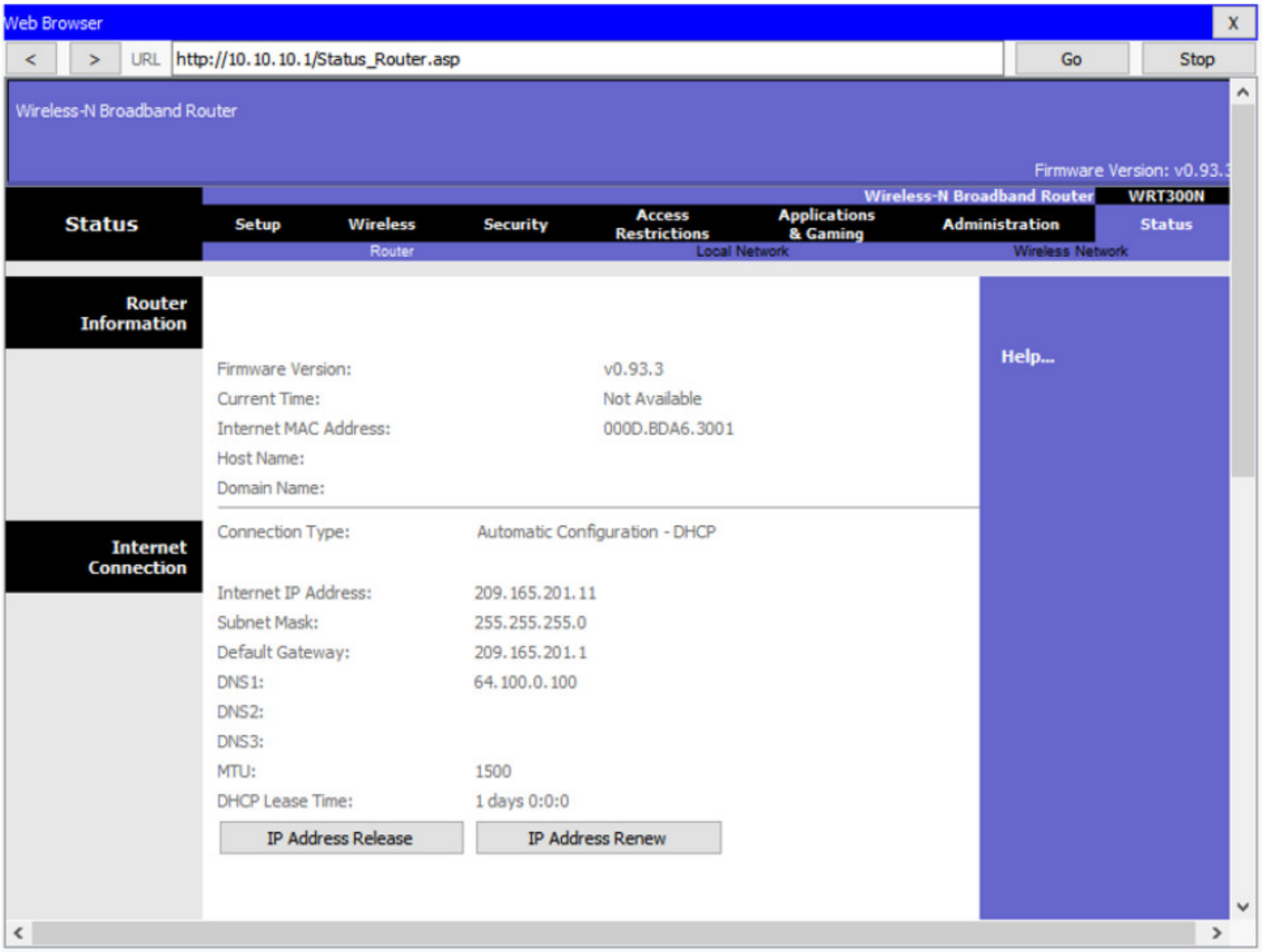
Password

Encryption Type AES

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. You buy the system, disperse the access points, plug them in, download the app, and configure your WMN in a few steps. Search the internet for “best wi-fi mesh network system” to find reviews of current offerings.

13.1.7 NAT for IPv4

On a wireless router, if you look for a page like the Status page shown in the figure, you will find the IPv4 addressing information that the router uses to send data to the internet. Notice that the IPv4 address is 209.165.201.11 is a different network than the 10.10.10.1 address assigned to the router’s LAN interface. All the devices on the router’s LAN will get assigned addresses with the 10.10.10 prefix.



Firmware Version:	v0.93.3
Current Time:	Not Available
Internet MAC Address:	000D.BDA6.3001
Host Name:	
Domain Name:	
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

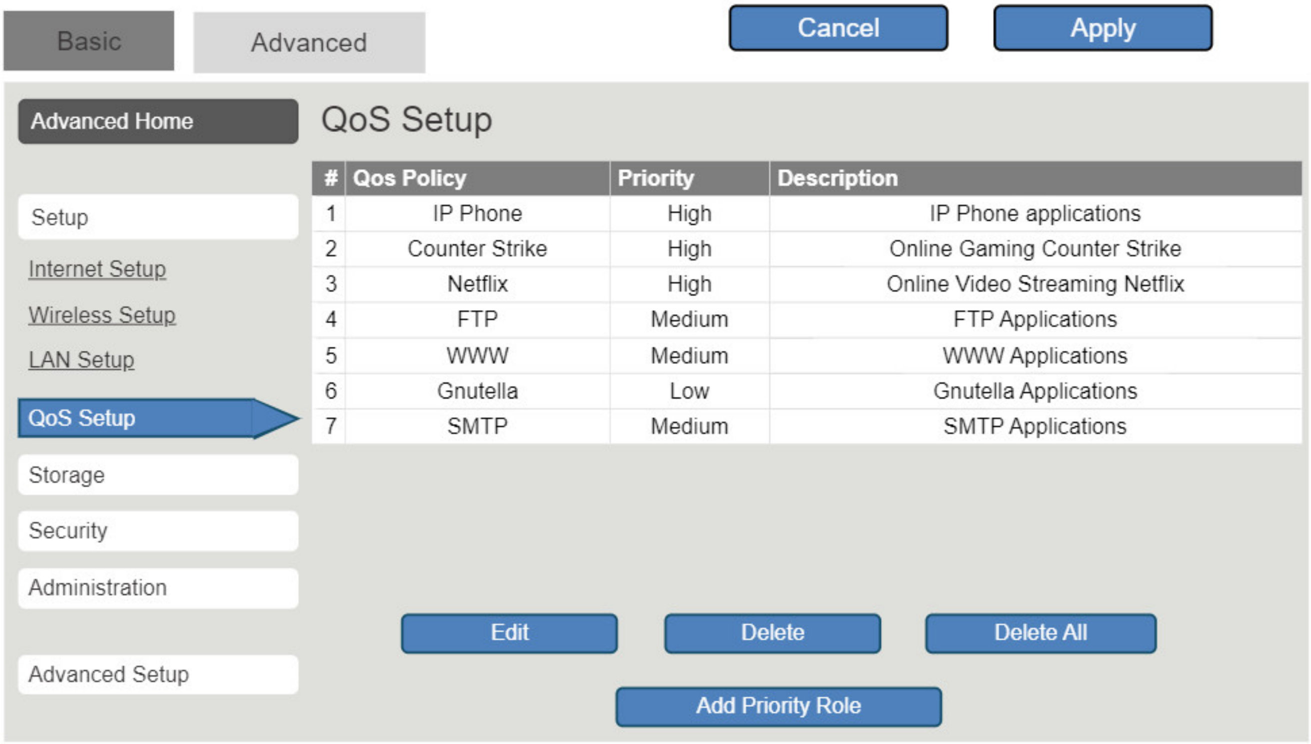
The 209.165.201.11 IPv4 address is publicly routable on the internet. Any address with the 10 in the first octet is a private IPv4 address and cannot be routed on the internet. Therefore, the router will use a process called Network Address Translation (NAT) to convert private IPv4 addresses to internet-routable IPv4 addresses. With NAT, a private (local) source IPv4 address is translated to a public (global) address. The process is reversed for incoming packets. The router is able to translate many internal IPv4 addresses into public addresses, by using NAT.

Some ISPs use private addressing to connect to customer devices. However, eventually, your traffic will leave the provider's network and be routed on the internet. To see the IP addresses for your devices, search the internet for "what is my IP address." Do this for other devices on the same network and you will see that they all share the same public IPv4 address. NAT makes this 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.

13.1.8 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 figure is a simplified mockup of a QoS interface based on a Netgear GUI. You will usually find the QoS settings in the advanced menus. If you have a wireless router available, investigate the QoS settings. Sometimes, these might be listed under “bandwidth control” or something similar. Consult the wireless router’s documentation or search the internet for “qos settings” for your router’s make and model.



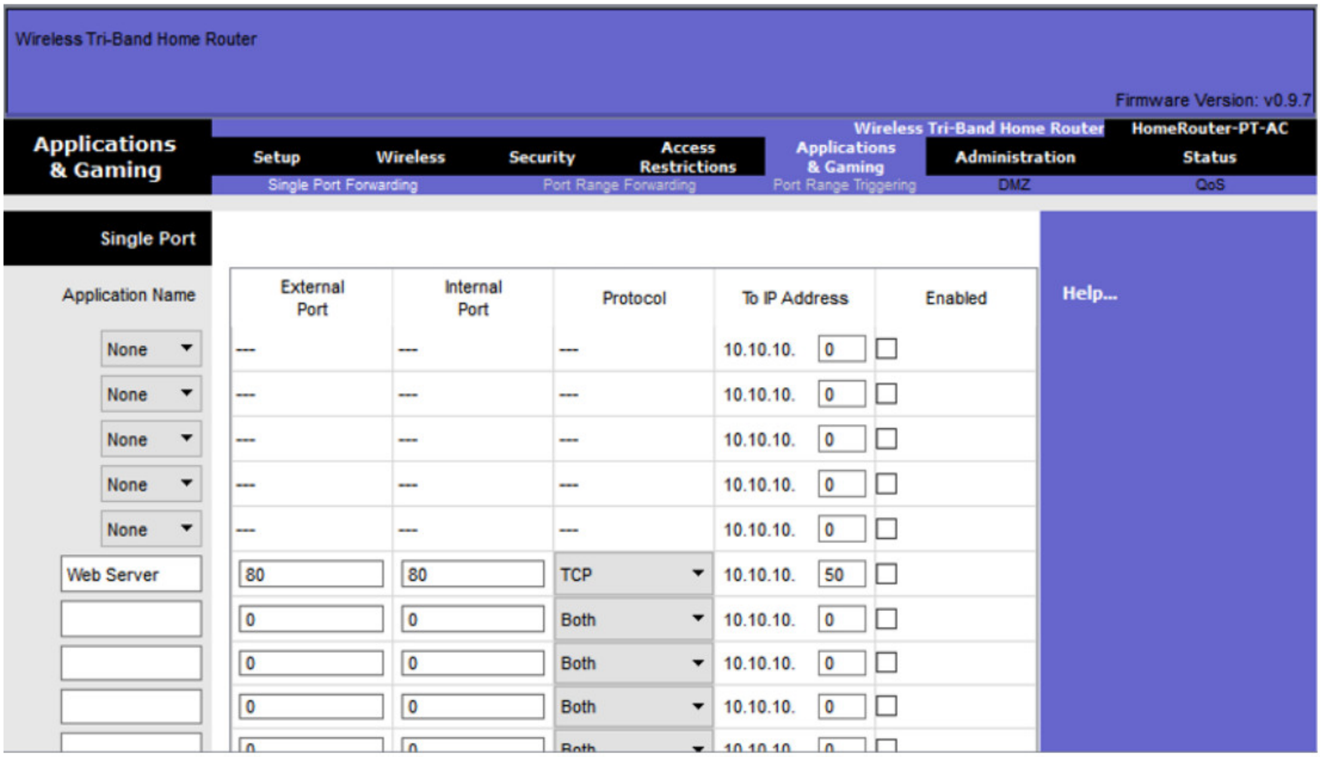
QoS Setup

#	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

13.1.9 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.

When traffic reaches the router, the router determines if the traffic should be forwarded to a certain device based on the port number found with the traffic. For example, a router might be configured to forward port 80, which is associated with HTTP. When the router receives a packet with the destination port of 80, the router forwards the traffic to the server inside the network that serves web pages. In the figure, port forwarding is enabled for port 80 and is associated with the web server at IPv4 address 10.10.10.50.



Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
None ▼	---	---	---	10.10.10. 0	□
None ▼	---	---	---	10.10.10. 0	□
None ▼	---	---	---	10.10.10. 0	□
None ▼	---	---	---	10.10.10. 0	□
None ▼	---	---	---	10.10.10. 0	□
Web Server	80	80	TCP ▼	10.10.10. 50	□
	0	0	Both ▼	10.10.10. 0	□
	0	0	Both ▼	10.10.10. 0	□
	0	0	Both ▼	10.10.10. 0	□
	0	0	Both ▼	10.10.10. 0	□

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. For example, a video game might use ports 27000 to 27100 for connecting with other players. These are the trigger ports. A chat client might use port 56 for connecting the same players so that they can interact with each other. In this instance, if there is gaming traffic on an outbound port within the triggered port range, inbound chat traffic on port 56 is forwarded to the computer that is being used to play the video game and chat with friends. When the game is over and the triggered ports are no longer in use, port 56 is no longer allowed to send traffic of any type to this computer.

13.1.10 Packet Tracer – Configure a Wireless Network

In this activity, you will configure a wireless router and an access point to accept wireless clients and route IP packets.

13.1.10 Packet Tracer – Configure a Wireless Network

13.1.11 Lab – Configure a Wireless Network

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

13.1.11 Lab – Configure a Wireless Network

13.2 Configure a Basic WLAN on the WLC

13.2.1 Video – Configure a Basic WLAN on the WLC

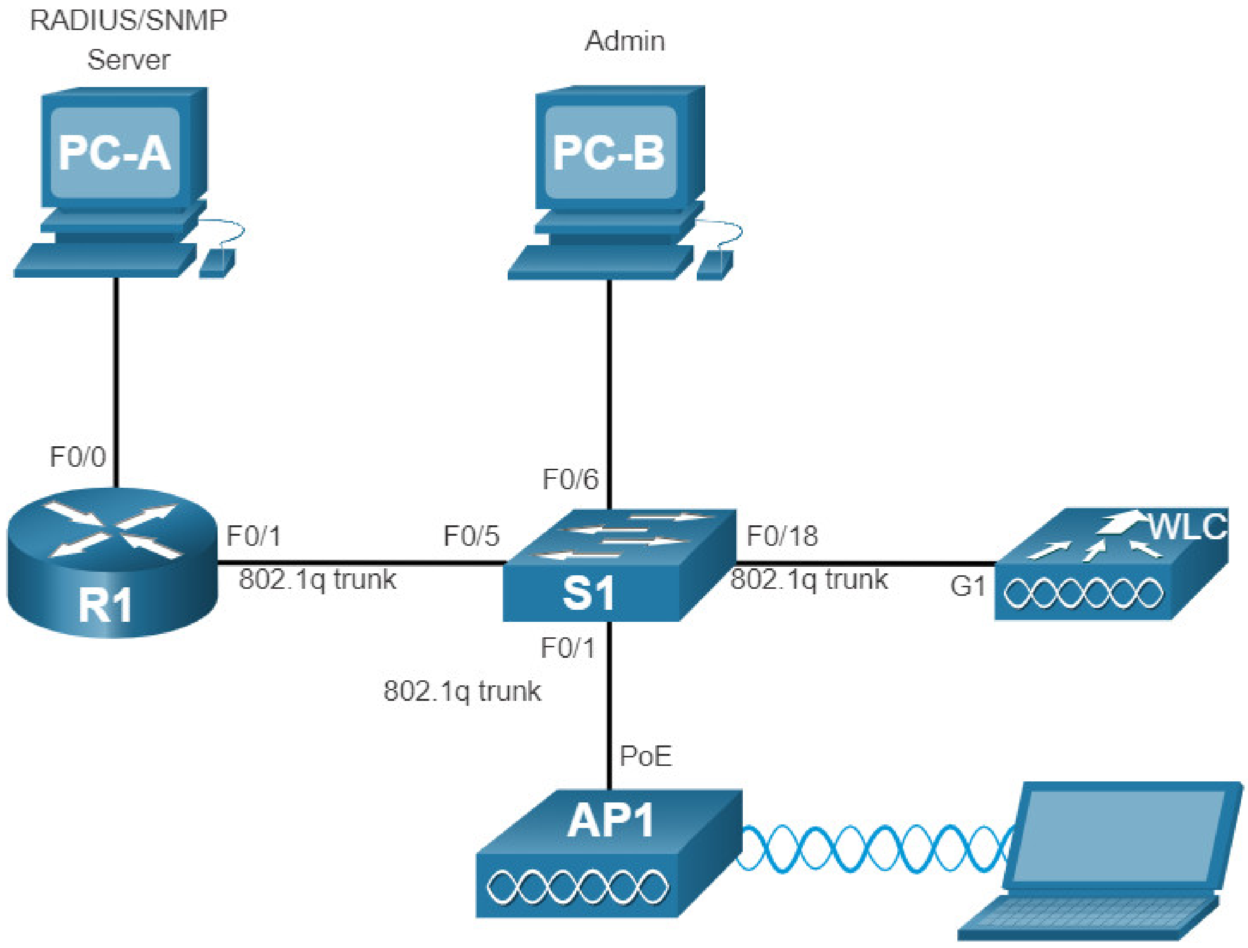
In the previous topic you learned about remote site WLAN configuration. This topic is about configuring a basic WLAN on the WLC.

Click Play in the figure to view a demonstration of configuring a Cisco 3504 WLC with basic WLAN connectivity.

13.2.2 WLC Topology

The topology and addressing scheme used for the videos and 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. Recall that controller-based APs require no initial configuration and are 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.

Topology



The AP is PoE, which means it is powered over the Ethernet cable that is attached to the switch.

Addressing Table

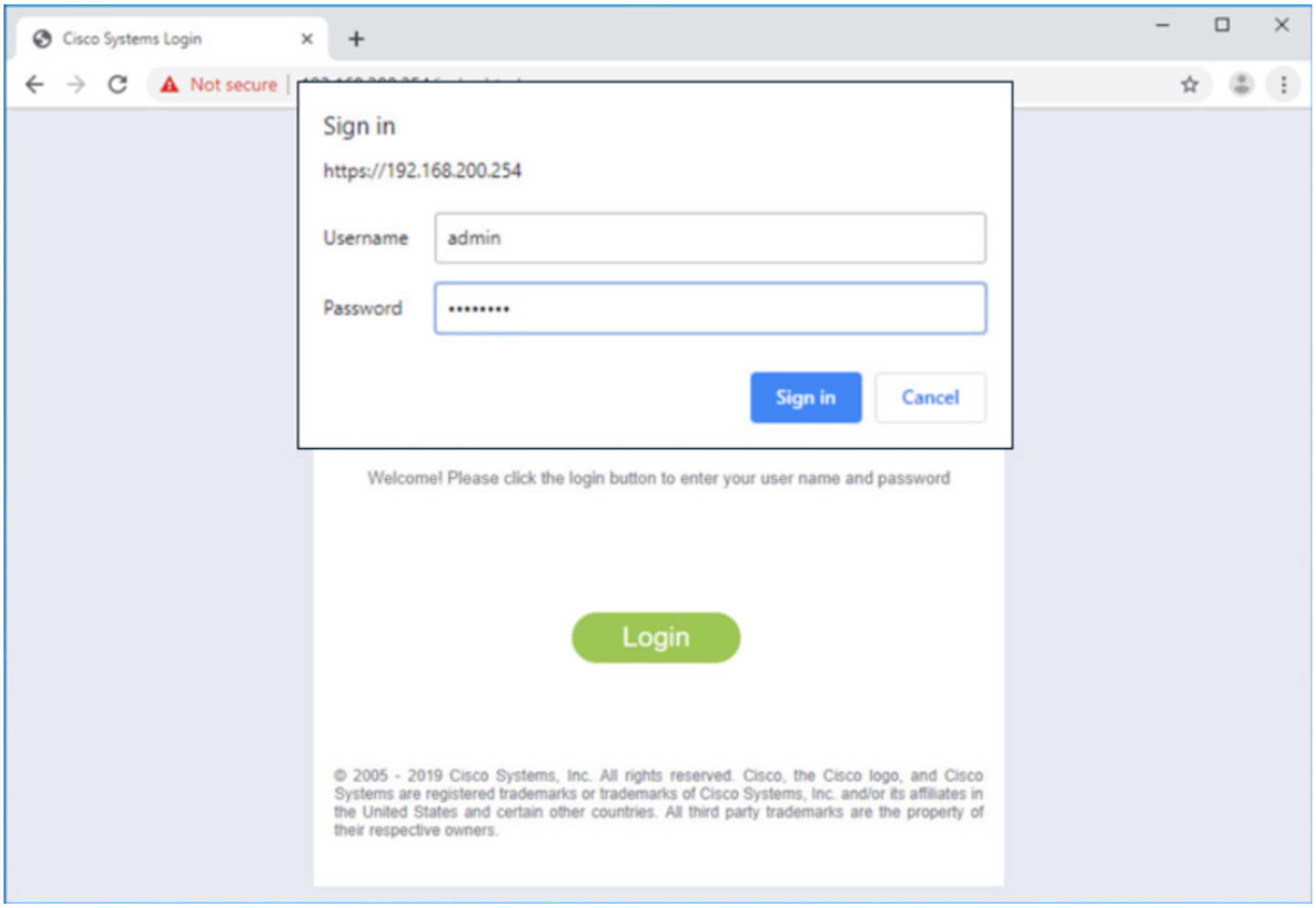
Device	Interface	IP Address	Subnet Mask
R1	F0/0	172.16.1.1	255.255.255.0
R1	F0/1.1	192.168.200.1	255.255.255.0
S1	VLAN 1	DHCP	
WLC	Management	192.168.200.254	255.255.255.0
AP1	Wired 0	192.168.200.3	255.255.255.0
PC-A	NIC	172.16.1.254	255.255.255.0
PC-B	NIC	DHCP	
Wireless Laptop	NIC	DHCP	

13.2.3 Log in to the WLC

Configuring a wireless LAN controller (WLC) is not that much different from configuring a wireless router. The big difference is that a WLC controls APs and provides more services and management capabilities, many of which are beyond the scope of this module.

Note: The figures in this topic that show the graphical user interface (GUI) and menus are from a Cisco 3504 Wireless Controller. However, other WLC models will have similar menus and features.

The figure shows the user logging into the WLC with credentials that were configured during initial setup.



Sign in

https://192.168.200.254

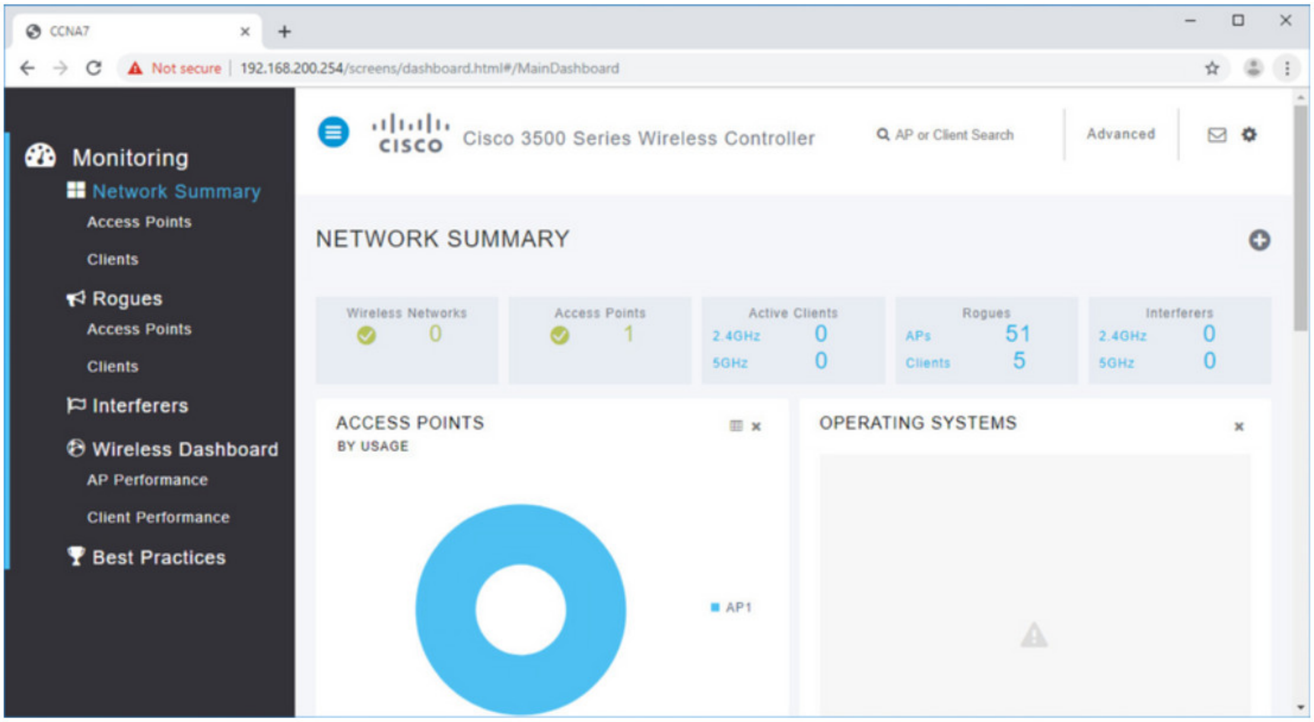
Username: admin

Password: ••••••••

Welcome! Please click the login button to enter your user name and password

© 2005 - 2019 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

The **Network Summary** page is a dashboard that provides a quick overview of the number of configured wireless networks, associated access points (APs), and active clients. You can also see the number of rogue access points and clients, as shown in the figure.

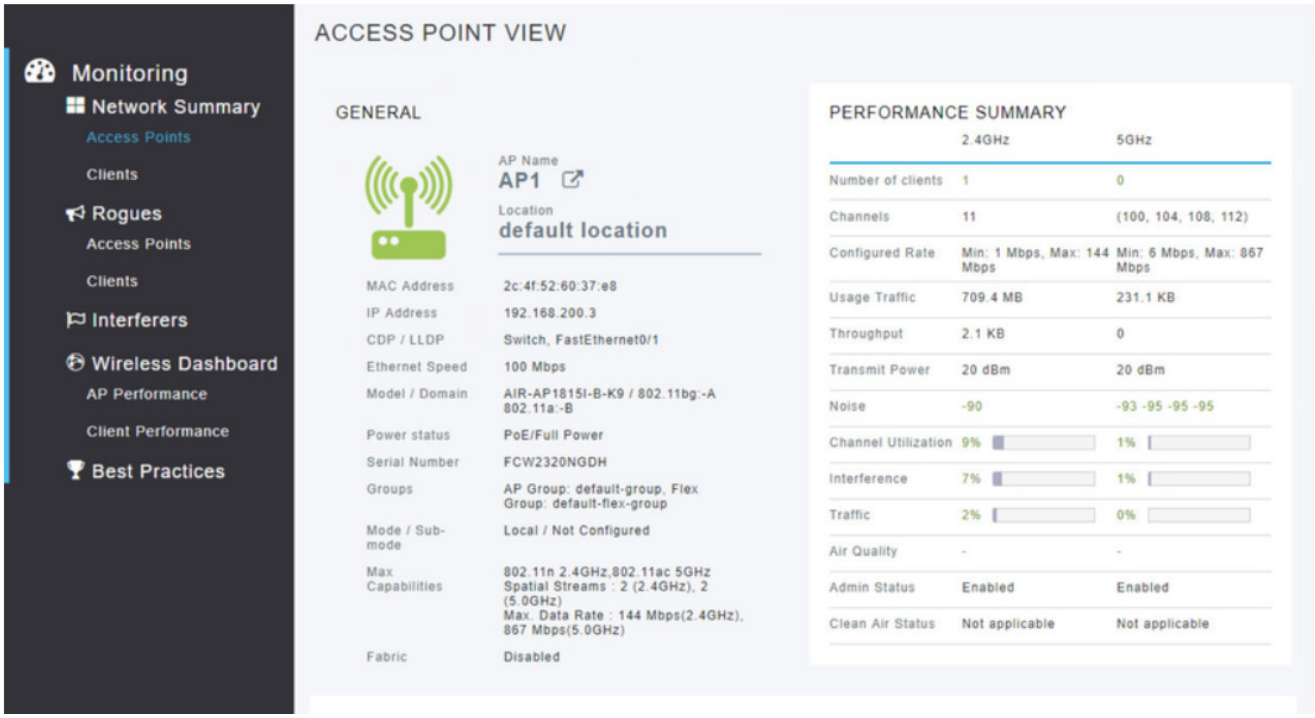


NETWORK SUMMARY

Wireless Networks	Access Points	Active Clients		Rogues		Interferers	
✓ 0	✓ 1	2.4GHz	0	APs	51	2.4GHz	0
		5GHz	0	Clients	5	5GHz	0

13.2.4 View AP Information

Click **Access Points** from the left menu to view an overall picture of the AP's system information and performance, as shown in the next figure. 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.



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

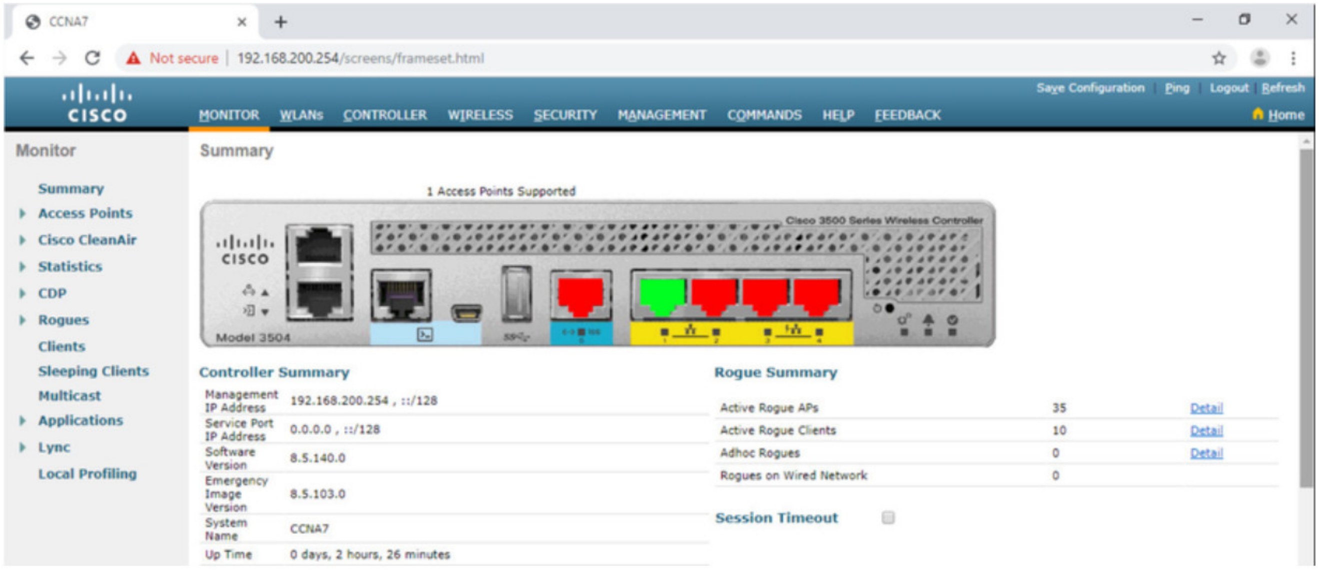
	2.4GHz	5GHz
Number of clients	1	0
Channels	11	(100, 104, 108, 112)
Configured Rate	Min: 1 Mbps, Max: 144 Mbps	Min: 6 Mbps, Max: 867 Mbps
Usage Traffic	709.4 MB	231.1 KB
Throughput	2.1 KB	0
Transmit Power	20 dBm	20 dBm
Noise	-90	-93 -95 -95 -95
Channel Utilization	9%	1%
Interference	7%	1%
Traffic	2%	0%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

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. In the example, the network administrator pinged the default gateway, pinged the WLC, and verified the wired interface.

```
AP1# ping 192.168.200.1
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1069812.242/1071814.785/1073817.215 ms
AP1# ping 192.168.200.254
Sending 5, 100-byte ICMP Echos to 192.168.200.254, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1055820.953/1057820.738/1059819.928 ms
AP1# show interface wired 0
wired0    Link encap:Ethernet  HWaddr 2C:4F:52:60:37:E8
          inet addr:192.168.200.3  Bcast:192.168.200.255  Mask:255.255.255.255
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:2478 errors:0 dropped:3 overruns:0 frame:0
          TX packets:1494 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:80
          RX bytes:207632 (202.7 KiB)  TX bytes:300872 (293.8 KiB)
AP1#
```

13.2.5 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, as shown in the figure. From here, you can access all the features of the WLC.


CCNA7
Not secure | 192.168.200.254/screens/frameset.html
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
Cisco 3500 Series Wireless Controller
Model 3504

Summary

1 Access Points Supported

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, 26 minutes

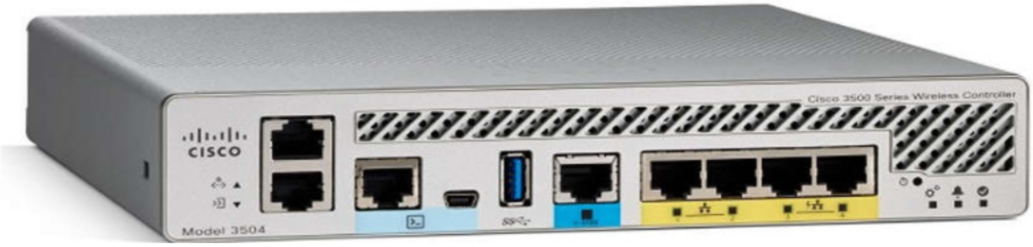
Rogue Summary

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

Session Timeout □

13.2.6 Configure a WLAN

Wireless LAN Controllers have ports and interfaces. Ports are the sockets for the physical connections to the wired network. They resemble switch ports. Interfaces are virtual. They are created in software and are very similar to VLAN interfaces. In fact, each interface that will carry traffic from a WLAN is configured on the WLC as a different VLAN. The Cisco 3504 WLC can support 150 access points and 4096 VLANs, however it only has five physical ports, as shown in the figure. This means that 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.



Basic WLAN configuration on the WLC includes the following steps:

1. Create the WLAN
2. Apply and Enable the WLAN
3. Select the Interface

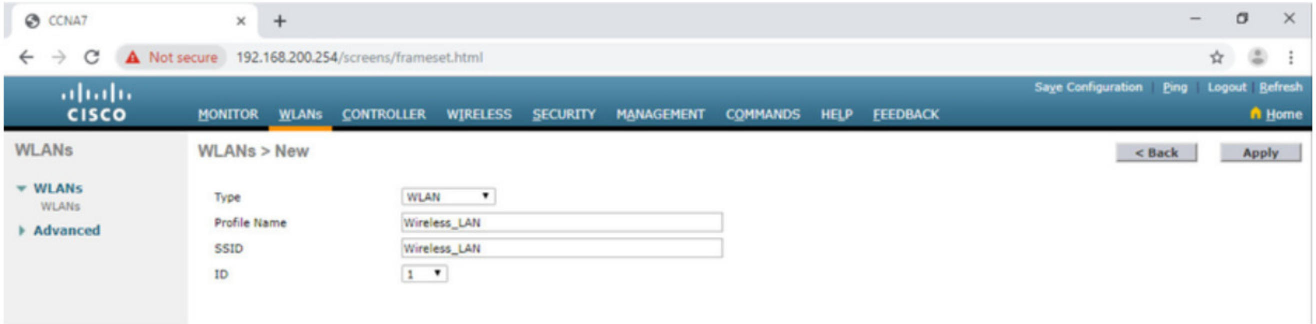
4. Secure the WLAN
5. Verify the WLAN is Operational
6. Monitor the WLAN
7. View Wireless Client Information

Click each step for more information and an example GUI.

- 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 Details

1. Create the WLAN

In the figure, the administrator is creating a new WLAN that will use **Wireless_LAN** as the name and service set identifier (SSID). The ID is an arbitrary value that is used to identify the WLAN in display output on the WLC.



WLANs > New

Type: WLAN
Profile Name: Wireless_LAN
SSID: Wireless_LAN
ID: 1

13.2.7 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.

13.2.7 Packet Tracer – Configure a Basic WLAN on the WLC

13.3 Configure a WPA2 Enterprise WLAN on the WLC

13.3.1 Video – Define an SNMP and RADIUS Server on the WLC

The previous topic covered configuring a basic WLAN on the WLC. Now you will learn about configuring a WPA2 Enterprise WLAN.

Click Play in the figure to view a demonstration of configuring SNMP and RADIUS services on the WLC.

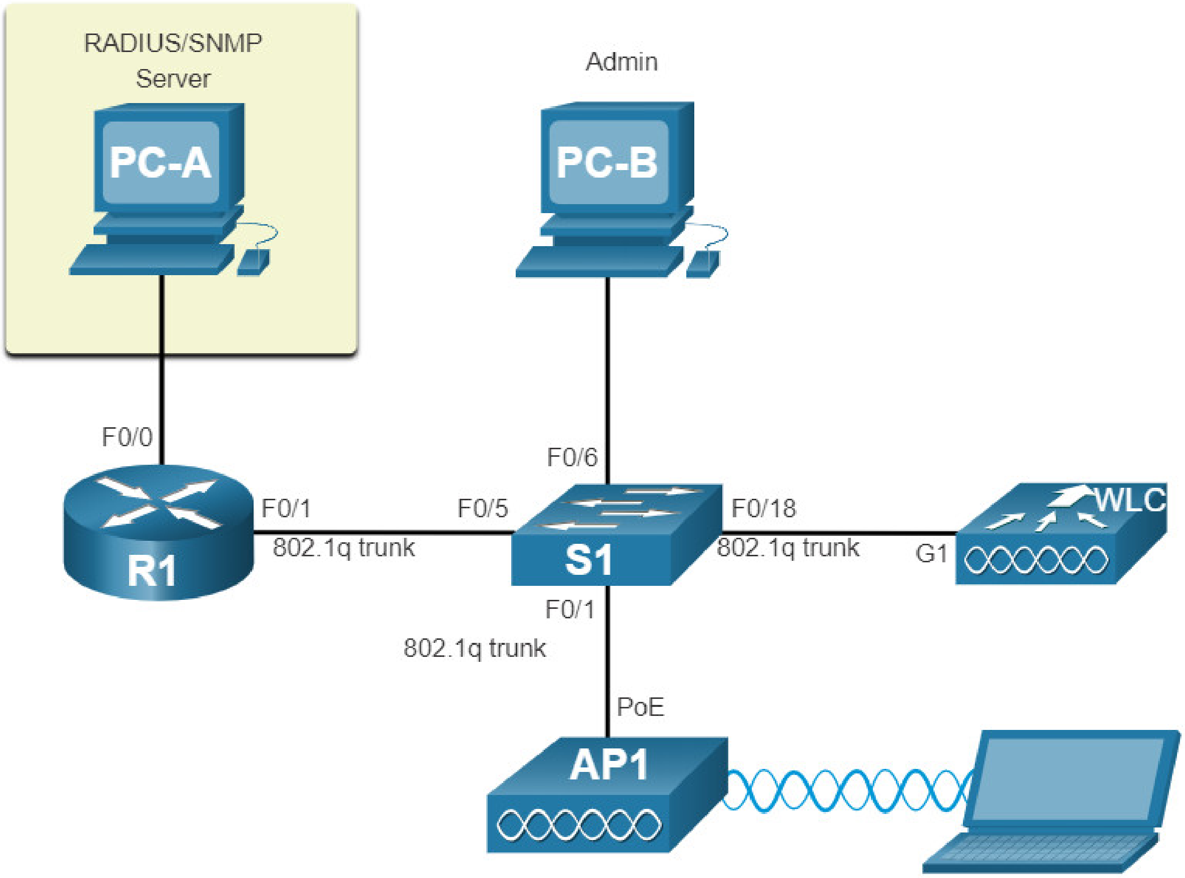
13.3.2 SNMP and RADIUS

In the figure, PC-A is running Simple Network Management Protocol (SNMP) and Remote Authentication Dial-In User Service (RADIUS) server software. SNMP is used to monitor the network. The network administrator wants the WLC to forward all SNMP log messages, called traps, to the SNMP server.

In addition, for WLAN user authentication, the network administrator wants to use a RADIUS server for authentication, authorization, and accounting (AAA) services. Instead of entering a publicly known pre-shared key to authenticate, as they do with WPA2-PSK, users will enter their own username and password credentials. The credentials will be verified by the RADIUS server. This way, individual user access can be tracked and audited if necessary and user accounts can be added or modified from a central location. The RADIUS server is required for WLANs that are using WPA2 Enterprise authentication.

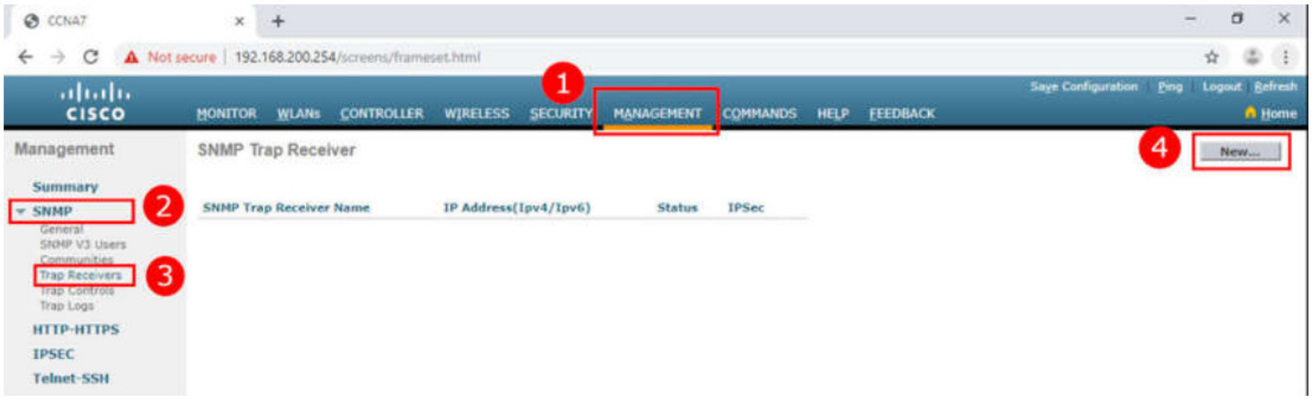
Note: SNMP server and RADIUS server configuration is beyond the scope of this module.

Topology



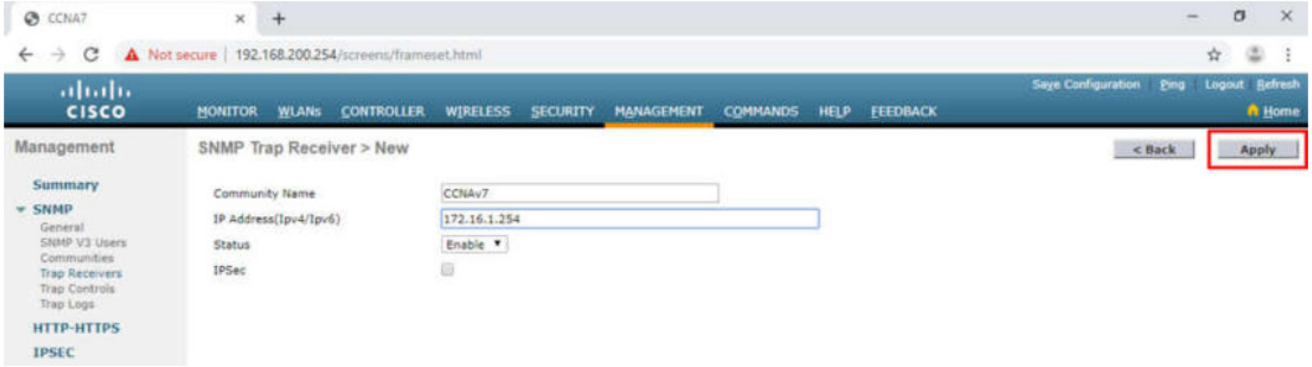
13.3.3 Configure SNMP Server Information

Click the **MANAGEMENT** tab to access a variety of management features. SNMP is listed at the top of the menu on the left. Click **SNMP** to expand the sub-menus, and then click **Trap Receivers**. Click **New...** to configure a new SNMP trap receiver, as shown in the figure.



1. Click **MANAGEMENT**
2. Click **SNMP**
3. Click **Trap Receivers**
4. Click **New...**

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

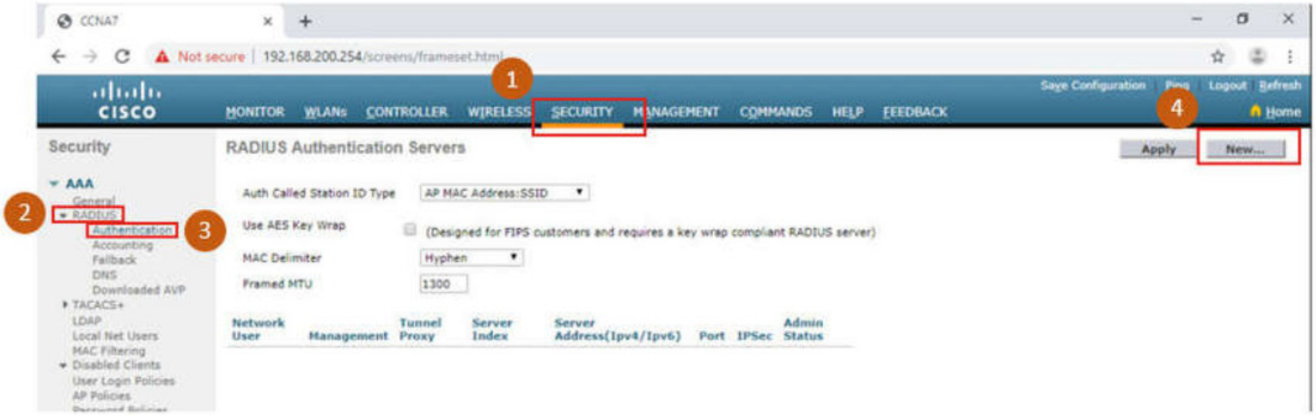

CCNA7
Not secure | 192.168.200.254/screens/frameset.html
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Management
SNMP Trap Receiver > New
< Back
Apply
Summary
SNMP
General
SNMP V3 Users
Communities
Trap Receivers
Trap Controls
Trap Logs
HTTP-HTTPS
IPSEC

Community Name: CCNAv7
IP Address(Ipv4/Ipv6): 172.16.1.254
Status: Enable
IPSec: □

13.3.4 Configure RADIUS Server Information

In our example configuration, the network administrator wants to configure a WLAN using WPA2 Enterprise, as opposed to WPA2 Personal or WPA2 PSK. Authentication will be handled by the RADIUS server running on PC-A.

To configure the WLC with the RADIUS server information, click the **SECURITY** tab > **RADIUS** > **Authentication**. No RADIUS servers are currently configured.
Click **New...** to add PC-A as the RADIUS server.



RADIUS Authentication Servers

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)

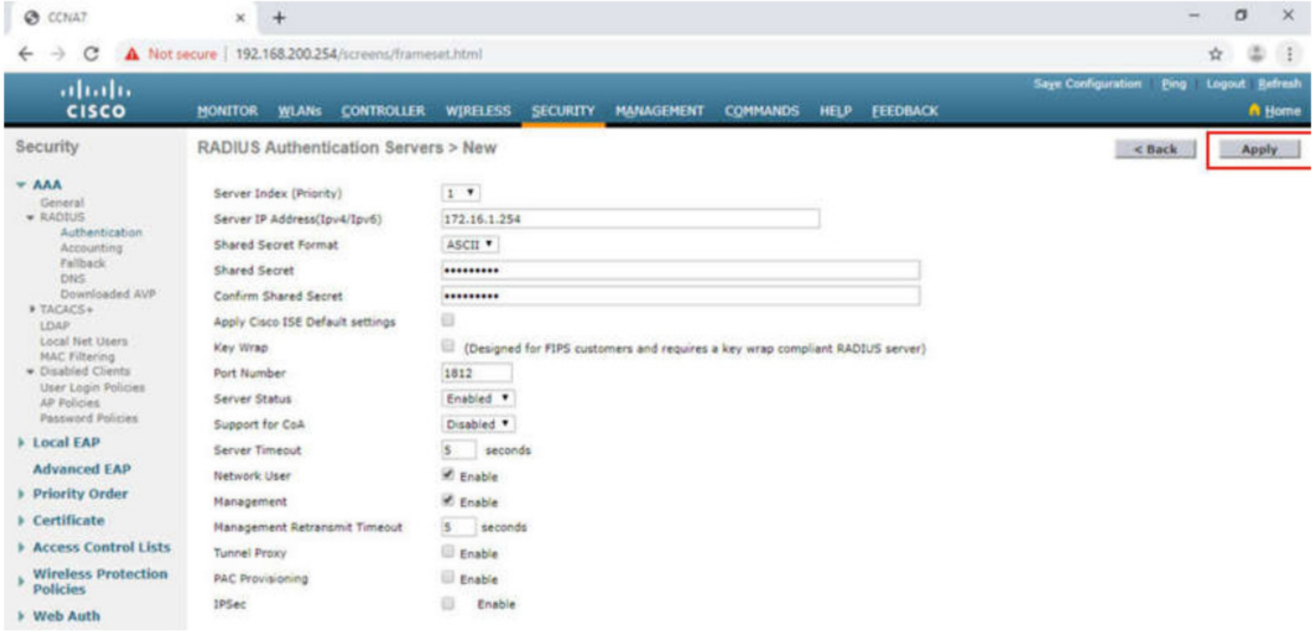
MAC Delimiter: Hyphen

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status

1. Click **SECURITY**
2. Click **RADIUS**
3. Click **Authentication**
4. Click **New...**

Enter the IPv4 address for PC-A and the shared secret. This is the password used between the WLC and the RADIUS server. It is not for users. Click **Apply**, as shown in the figure.



RADIUS Authentication Servers > New

Server Index (Priority): 1

Server IP Address(Ipv4/Ipv6): 172.16.1.254

Shared Secret Format: ASCII

Shared Secret: •••••••••

Confirm Shared Secret: •••••••••

Apply Cisco ISE Default settings: ☐

Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for CoA: Disabled

Server Timeout: 5 seconds

Network User: ☑ Enable

Management: ☑ Enable

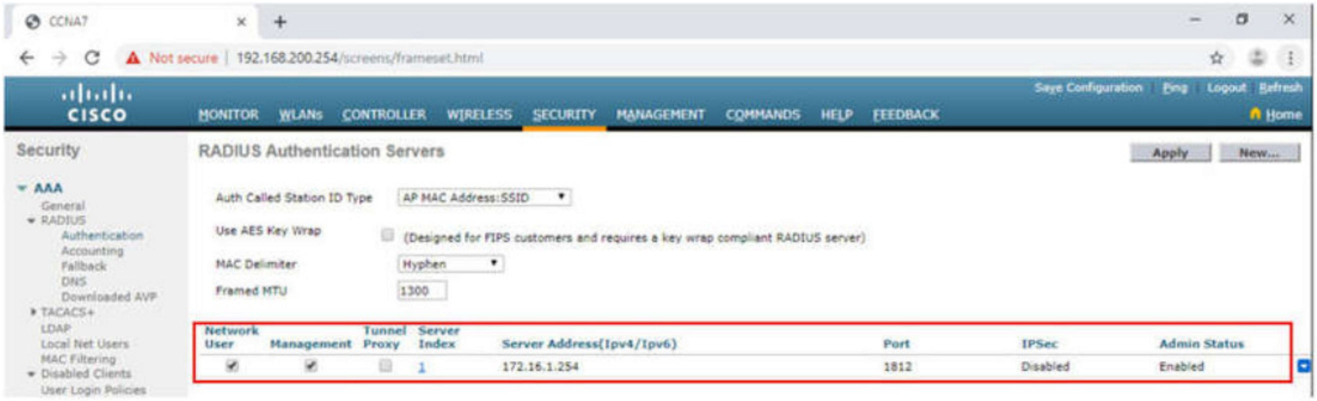
Management Retransmit Timeout: 5 seconds

Tunnel Proxy: ☐ Enable

PAC Provisioning: ☐ Enable

IPSec: ☐ Enable

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



RADIUS Authentication Servers

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

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	□	1	172.16.1.254	1812	Disabled	Enabled

13.3.5 Video – Configure a VLAN for a New WLAN

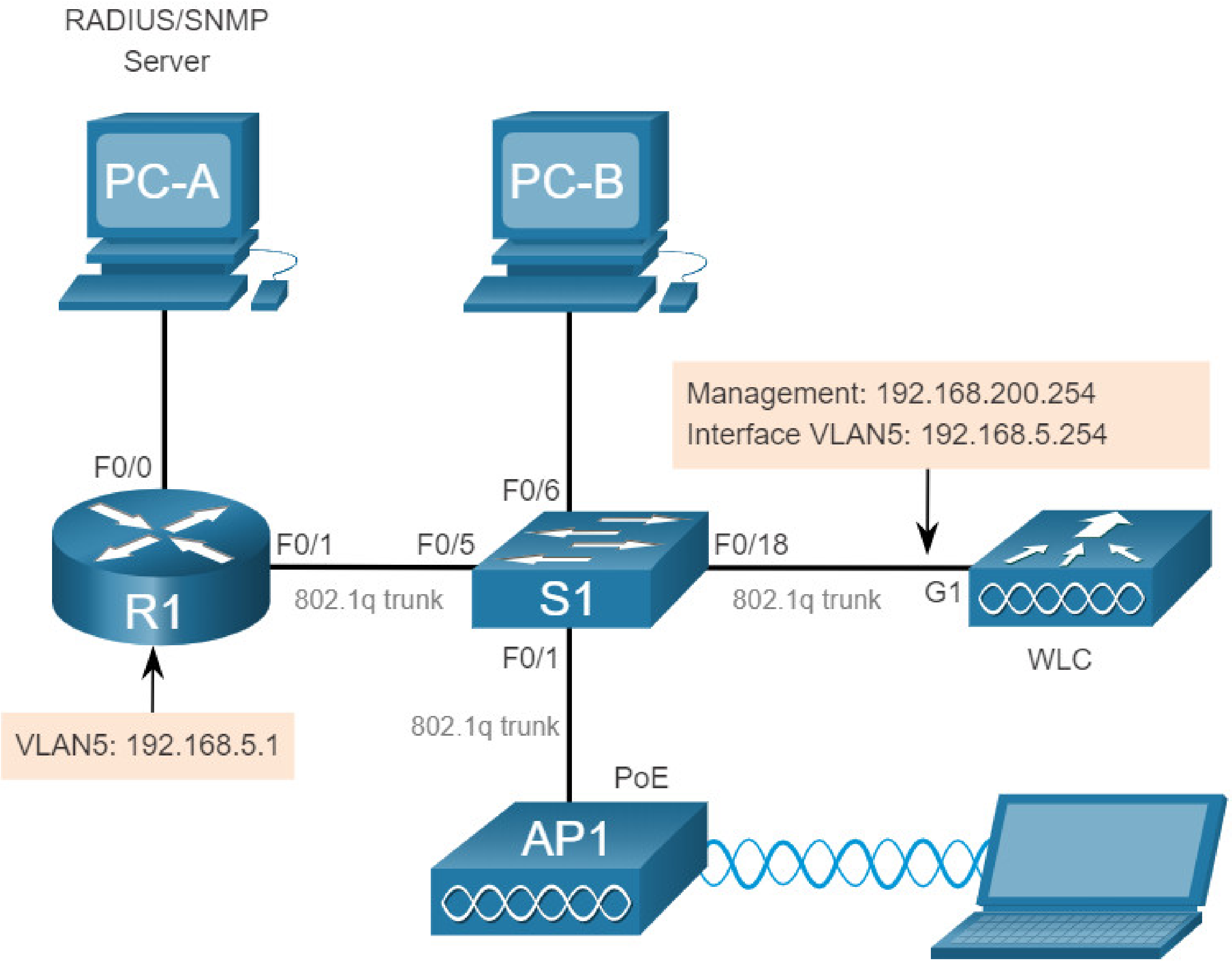
Click Play in the figure to view a demonstration of configuring a VLAN on the WLC.

13.3.6 Topology with VLAN 5 Addressing

Each WLAN configured on the WLC needs its own virtual interface. The WLC has five physical ports for data traffic. Each physical port can be configured to support multiple WLANs, each on its own virtual interface. Physical ports can also be aggregated to create high-bandwidth links.

The network administrator has decided that the new WLAN will use interface VLAN 5 and network 192.168.5.0/24. R1 already has a subinterface configured and active for VLAN 5, as shown in the topology and **show ip interface brief** output.

Topology



```
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#
```

13.3.7 Configure a New Interface

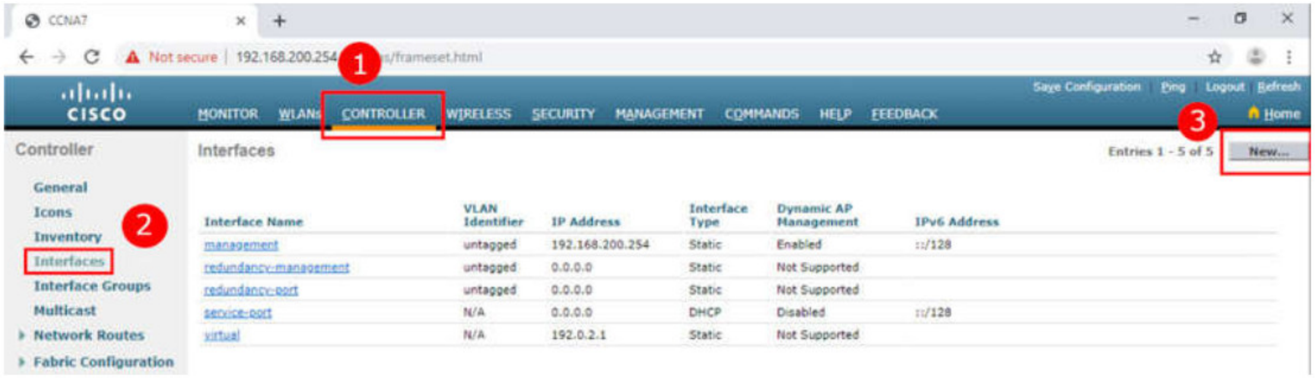
VLAN interface configuration on the WLC includes the following steps:

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.

Click each step for more information and an example GUI.

- 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.

1. Create a new interface.
To add a new interface, click **CONTROLLER** > **Interfaces** > **New...**, as shown in the figure.



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	

1. Click **CONTROLLER**
2. Click **Interfaces**
3. Click **New...**

13.3.8 Video – Configure a DHCP Scope

Click Play in the figure to view a demonstration of configuring DHCP services.

13.3.9 Configure a DHCP Scope

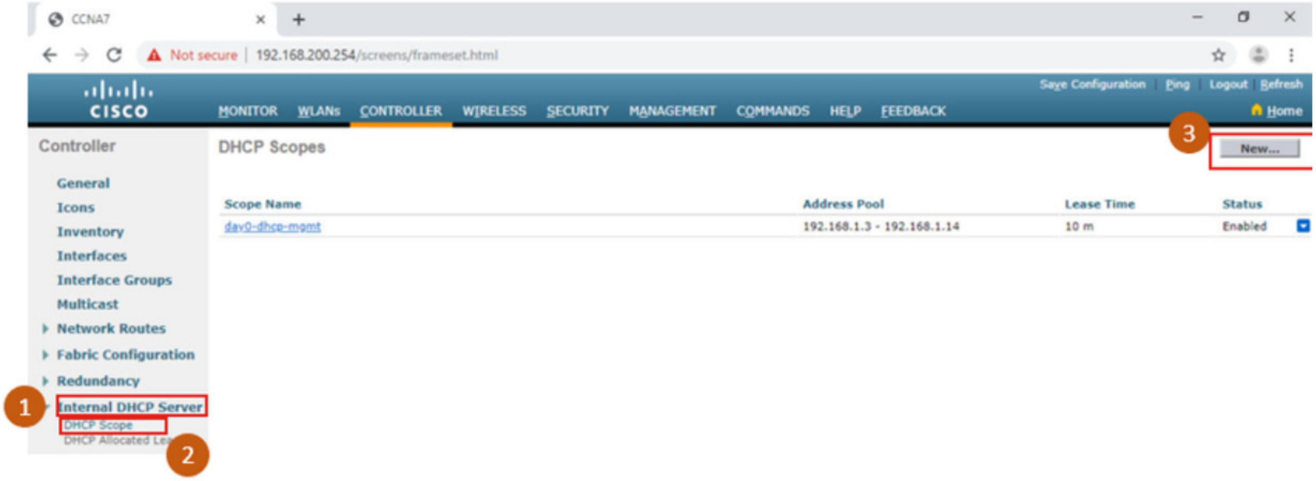
DHCP scope configuration includes the following steps:

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

Click each step for more information and an example GUI.

1. Create a new DHCP scope.
A DHCP scope is very similar to a DHCP pool on a router. It can include a variety of information including a pool of addresses to assign to DHCP clients, DNS server information, lease times, and more. To configure a new DHCP scope, click **Internal DHCP Server >**

DHCP Scope > **New...**, as shown in the figure.



DHCP Scopes

Scope Name	Address Pool	Lease Time	Status
day0-dhcp-mgmt	192.168.1.3 - 192.168.1.14	10 m	Enabled

1. Click **Internal DHCP Server**.
2. Click **DHCP Scope**.
3. Click **New...**

13.3.10 Video – Configure a WPA2 Enterprise WLAN

Click Play in the figure to view a demonstration of configuring a new WLAN with WPA2 Enterprise on the WLC.

13.3.11 Configure a WPA2 Enterprise WLAN

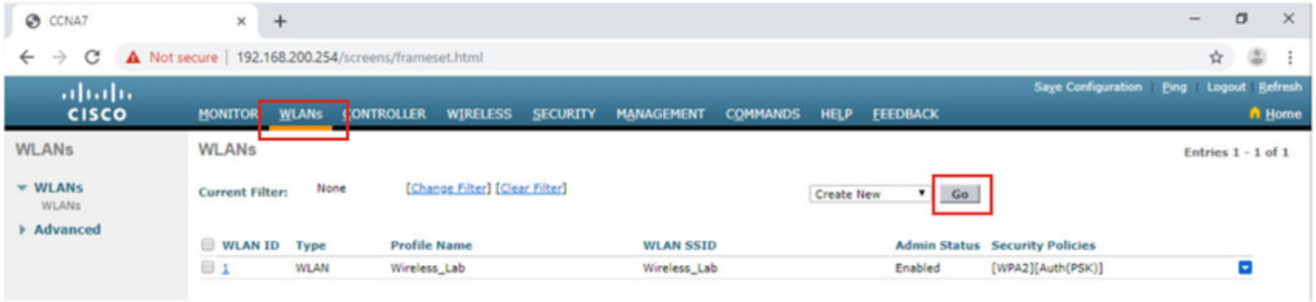
By default, all newly created WLANs on the WLC will use WPA2 with Advanced Encryption System (AES). 802.1X is the default key management protocol used to communicate with the RADIUS server. Because the network administrator already configured the WLC with the IPv4 address of the RADIUS server running on PC-A, the only configuration left to do is to 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.

Click each step for more information and an example GUI.

1. Create a new WLAN.
Click the **WLANs** tab and then **Go** to create a new WLAN, as shown in the figure.



Current Filter: None

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

13.3.12 Packet Tracer – Configure a WPA2 Enterprise WLAN on the WLC

In this 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.

13.3.12 Packet Tracer – Configure a WPA2 Enterprise WLAN on the WLC

13.4 Troubleshoot WLAN Issues

13.4.1 Troubleshooting Approaches

In the previous topics, you learned about WLAN configuration. Here we will discuss troubleshooting WLAN issues.

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.

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.

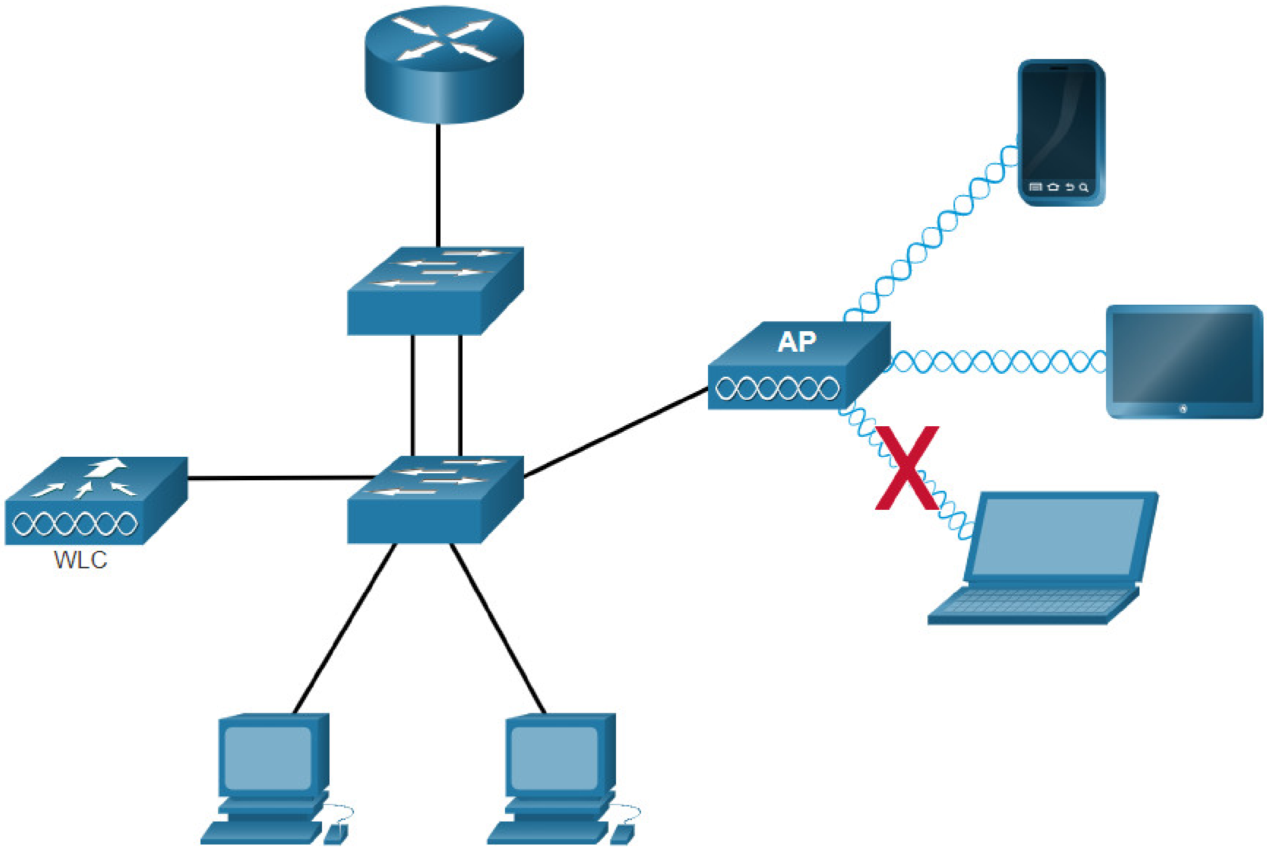
Step	Title	Description
3	Test the Theory to Determine Cause	Based on the probable causes, test your theories to determine which one is the cause of the problem. A technician will often apply a quick procedure to test and see if it solves the problem. If a quick procedure does not correct the problem, 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.

To assess the problem, determine how many devices on the network are experiencing the problem. If there is a problem with one device on the network, start the troubleshooting process at that device. If there is a problem with all devices on the network, start the troubleshooting process at the device where all other devices are connected. You should develop a logical and consistent method for diagnosing network problems by eliminating one problem at a time.

13.4.2 Wireless Client Not Connecting

When troubleshooting a WLAN, a process of elimination is recommended.

In the figure, a wireless client is not connecting to the WLAN.



If there is no connectivity, check the following:

- Confirm the network configuration on the PC using the **ipconfig** command. Verify that the PC has received an IP address via DHCP or is configured with a static IP address.
- Confirm that the device can connect to the wired network. Connect the device to the wired LAN and ping a known IP address.
- If necessary, reload drivers as appropriate for the client. It may be necessary to 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 security settings do not match, the client cannot gain access to the WLAN.

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

- How far is the PC from an AP? Is the PC out of the planned coverage area (BSA)?
- Check the channel settings on the wireless client. The client software should detect the appropriate channel as long as the SSID is correct.
- Check for the presence of other devices in the area that may be interfering with the 2.4 GHz band. Examples of other devices are cordless phones, baby monitors, microwave ovens, wireless security systems, and potentially rogue APs. Data from these devices can cause interference in the WLAN and intermittent connection problems between a wireless client and AP.

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?

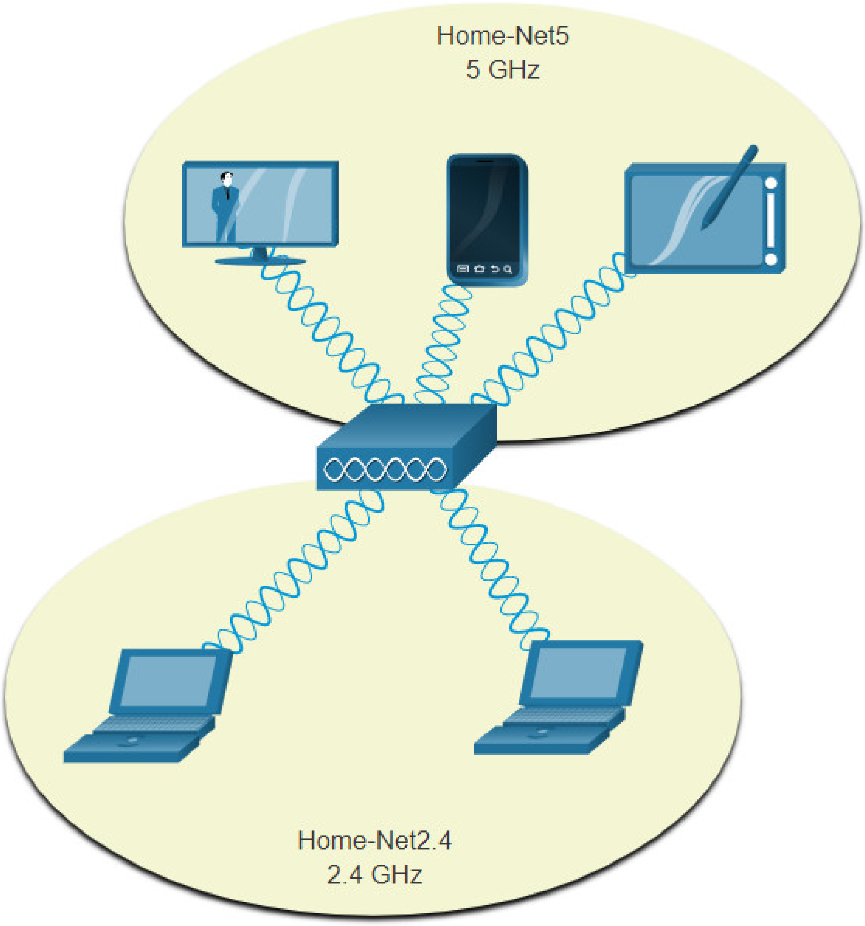
Finally, inspect links between cabled devices looking for bad connectors or damaged or missing cables. If the physical plant is in place, verify the wired LAN by pinging devices, including the AP. If connectivity still fails at this point, perhaps something is wrong with the AP or its configuration.

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.

13.4.3 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. Although 802.11ax was released in 2019, 802.11ac is most likely that highest standard that enterprises can currently enforce.
- **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. For example, use the 2.4 GHz network for basic internet tasks, such as web browsing, email, and downloads, and use the 5 GHz band for streaming multimedia, as shown in the figure.



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

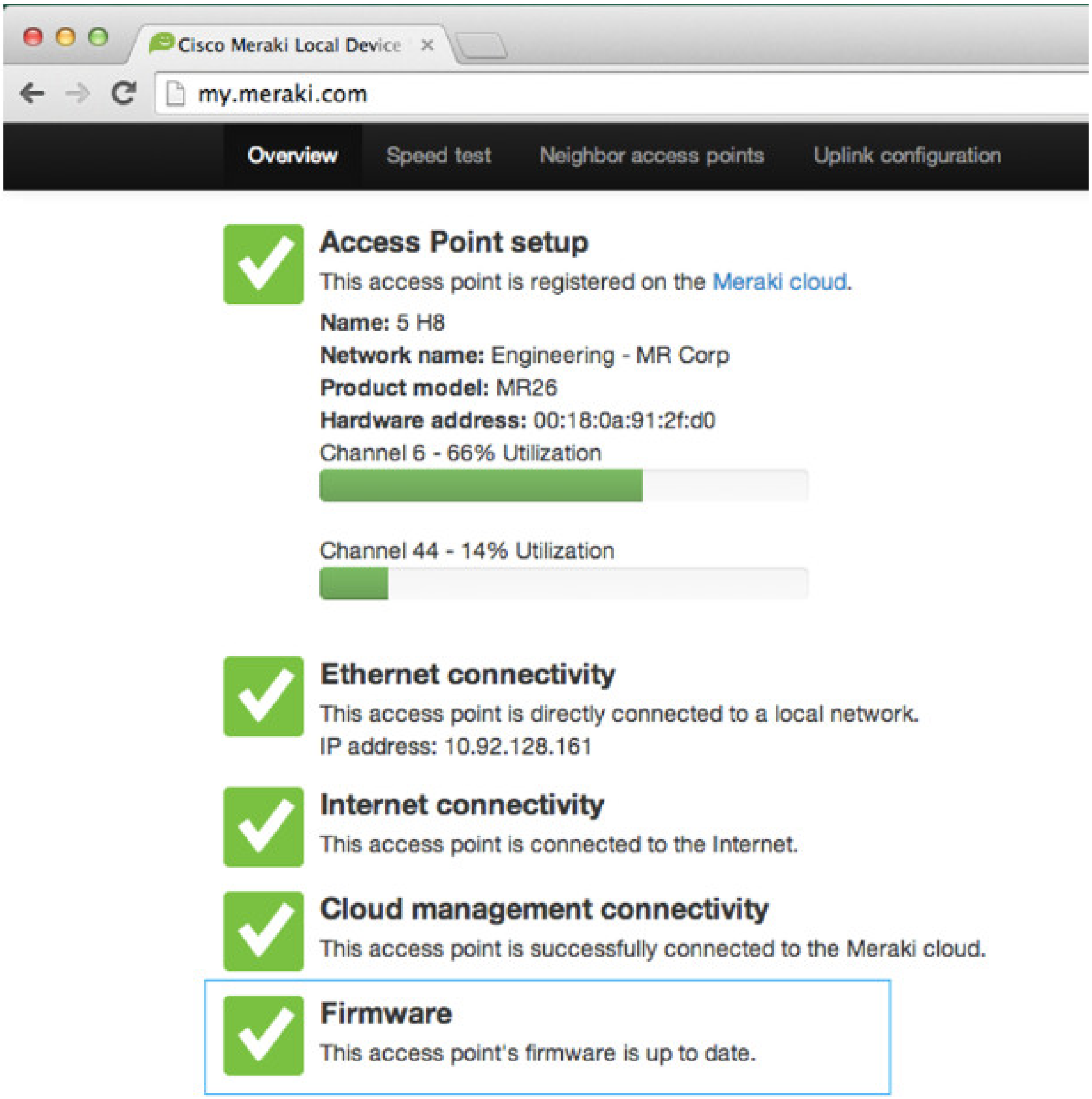
- The 2.4 GHz band may be suitable for basic Internet traffic that is not time-sensitive.
- The bandwidth may still be shared with other nearby WLANs.
- The 5 GHz band is much less crowded than the 2.4 GHz band; ideal for streaming multimedia.
- The 5 GHz band has more channels; therefore, the channel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

By default, dual-band routers and APs use the same network name on both the 2.4 GHz band and the 5 GHz band. The simplest way to segment traffic is to rename one of the wireless networks. With a separate, descriptive name, it is easier to connect to the right network.

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.

13.4.4 Updating Firmware

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. In the figure, the network administrator is verifying that the firmware is up to date on a Cisco Meraki AP.



✓ **Access Point setup**

This access point is registered on the Meraki cloud.

Name: 5 H8
Network name: Engineering - MR Corp
Product model: MR26
Hardware address: 00:18:0a:91:2f:d0
Channel 6 - 66% Utilization

Channel 44 - 14% Utilization

✓ **Ethernet connectivity**

This access point is directly connected to a local network.
IP address: 10.92.128.161

✓ **Internet connectivity**

This access point is connected to the Internet.

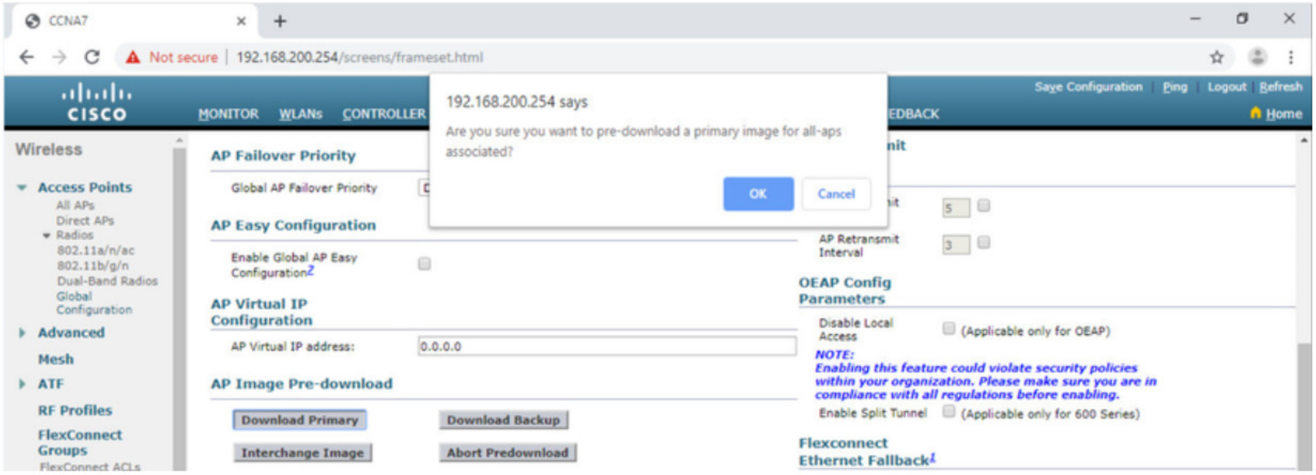
✓ **Cloud management connectivity**

This access point is successfully connected to the Meraki cloud.

✓ **Firmware**

This access point's firmware is up to date.

On a WLC, there will most likely be the ability to upgrade the firmware on all APs that the WLC controls. In the next figure, the network administrator is downloading the firmware image that will be used to upgrade all the APs.



192.168.200.254 says

Are you sure you want to pre-download a primary image for all-aps associated?

Global AP Failover Priority

Enable Global AP Easy Configuration ☐

AP Virtual IP address: 0.0.0.0

AP Retransmit Interval 3 ☐

Disable Local Access ☐ (Applicable only for OEAP)

NOTE:
Enabling this feature could violate security policies within your organization. Please make sure you are in compliance with all regulations before enabling.

Enable Split Tunnel ☐ (Applicable only for 600 Series)

On a Cisco 3504 Wireless Controller, Click the **WIRELESS** tab > **Access Points** from the left menu > **Global Configuration** submenu. Then scroll to the bottom of the page for the AP Image Pre-download section.

Users will be disconnected from the WLAN and the internet until the upgrade finishes. The wireless router may need to reboot several times before normal network operations are restored.

13.4.5 Packet Tracer – Troubleshoot WLAN Issues

Now that you have learned how to configure wireless in home and enterprise networks, you need to learn how to troubleshoot in both wireless environments. Your goal is to enable connectivity between hosts on the networks to the Web Server by both IP address and URL. Connectivity between the home and enterprise networks is not required.

13.4.5 Packet Tracer – Troubleshoot WLAN Issues

13.5 Module Practice and Summary

13.5.1 Packet Tracer – WLAN Configuration

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

13.5.1 Packet Tracer – WLAN Configuration

13.5.2 Packet Tracer – Wireless Technology Exploration

XYZ Corporation is expanding their network capabilities to allow enhanced connectivity at their local offices, as well as connectivity for those wishing to work remotely. In this Packet Tracer Physical Mode (PTPM) activity, you have been asked to assist with this plan by reviewing the current network capabilities and adding wireless functionality as required.

Note: Please be patient. It may take several minutes for this PTPM activity to load.
13.5.2 Packet Tracer – Wireless Technology Exploration – Physical Mode

13.5.3 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. Use your router’s interface to complete basic network and wireless setup. 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). 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 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.

13.5.3 Module Quiz – WLAN Configuration

Download Slide Powerpoint (PPT)

CCNA 2 v7.0 Curriculum: Module 13 - WLAN Configuration.pptx

1 file(s) 10.15 MB

Download

Tags:ccna 2 v7 modules