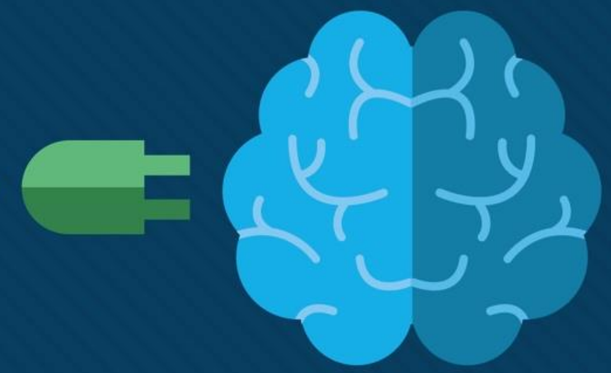


Модуль 13: Конфигурация WLAN

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

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 Настройка беспроводных локальных сетей для удаленных объектов

Video – Configure a Wireless Network

This video will cover the following:

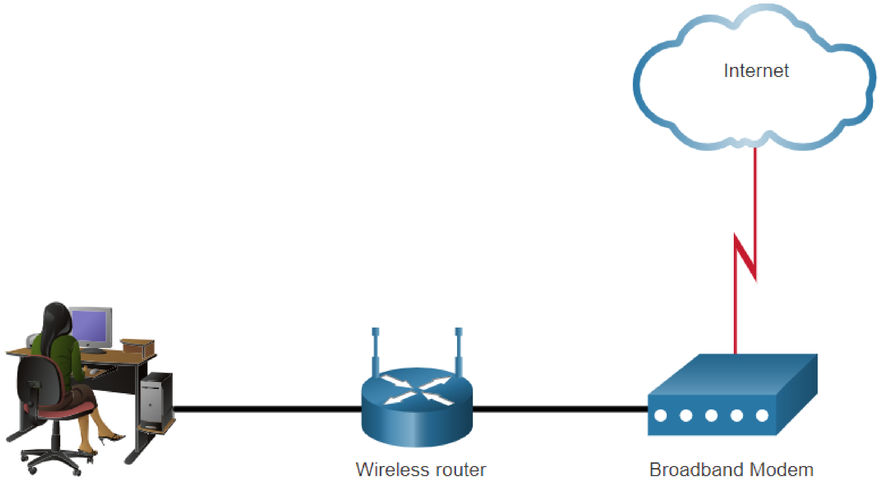
- Use the Wireless Router Web Page
- Change the Password
- Change the WAN and LAN settings
- Connect the Wireless Network

Конфигурация беспроводного маршрутизатора

Удаленные работники, небольшие филиалы и домашние сети часто используют небольшой офис и домашний маршрутизатор.

- Эти маршрутизаторы иногда называют Маршрутизатором с интегрированными сервисами, потому что они обычно включают в себя коммутатор для проводных клиентов, порт для подключения к Интернету (иногда помеченный как “WAN”) и беспроводные компоненты для беспроводного доступа клиентов.
- Эти беспроводные маршрутизаторы обычно обеспечивают безопасность WLAN, службы DHCP, встроенную трансляцию имен (NAT), качество обслуживания (QoS), а также ряд других функций.
- Набор функций зависит от модели маршрутизатора.

Примечание: Конфигурирование кабельного или DSL модема обычно выполняется представителем поставщика услуг либо на месте, либо удаленно через пошаговое руководство с вами по телефону.



Вход в беспроводной маршрутизатор

Большинство из них предварительно настроены для подключения к сети и предоставления услуг.

- Вместе с тем в Интернете легко находятся IP-адреса по умолчанию для беспроводных маршрутизаторов, имена пользователей и пароли.
- Таким образом, первоочередной задачей является изменение этих параметров по умолчанию с целью обеспечения безопасности.

Для доступа к графическому пользовательскому интерфейсу настройки беспроводного маршрутизатора:

- Откройте веб-браузер и в поле Address (Адрес) введите частный IP-адрес по умолчанию для беспроводного маршрутизатора.
- IP-адрес по умолчанию можно найти либо в документации, которая поставляется с беспроводным маршрутизатором, либо в Интернете.
- Слово **admin** обычно используется в качестве имени пользователя и пароля по умолчанию.

Базовая настройка сети

Базовая настройка сети включает в себя следующие шаги:

- Войдите на маршрутизатор через веб-браузер.
- Измените пароль администратора, заданный по умолчанию.
- Войдите с новым административным паролем.
- Измените диапазон адресов DHCP IPv4 по умолчанию.
- Обновите IP-адрес.
- Войдите в маршрутизатор с новым IP-адресом.

Базовая настройка сети

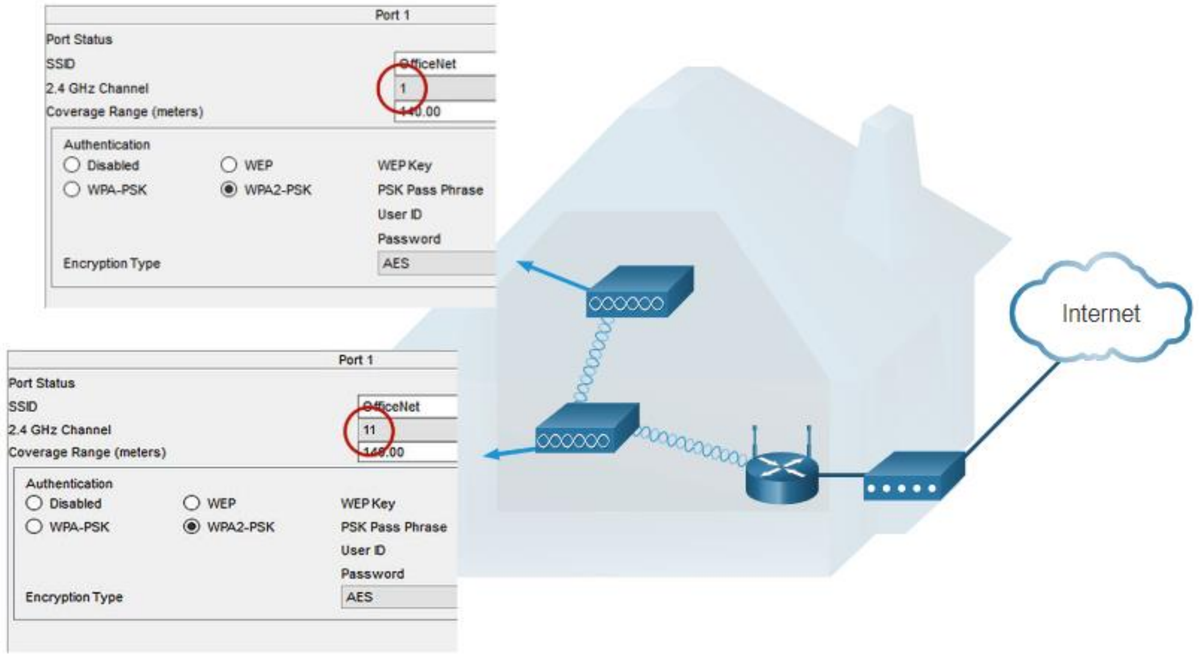
Базовая настройка сети включает в себя следующие шаги:

- Просмотр настроек WLAN по умолчанию.
- Измените сетевой режим, определив, какой стандарт 802.11 должен быть реализован.
- Настройте SSID.
- Настройте канал, убедившись, что используемые каналы не перекрываются.
- Настройте режим безопасности, выбрав Open, WPA, WPA2 Personal, WPA2 Enterprise и т.д.
- Настройте кодовую фразу, как это требуется для выбранного режима безопасности.

Настройка беспроводной ячеистой сети

В небольшом офисе или домашней сети одного беспроводного маршрутизатора может быть достаточно для обеспечения беспроводного доступа ко всем клиентам.

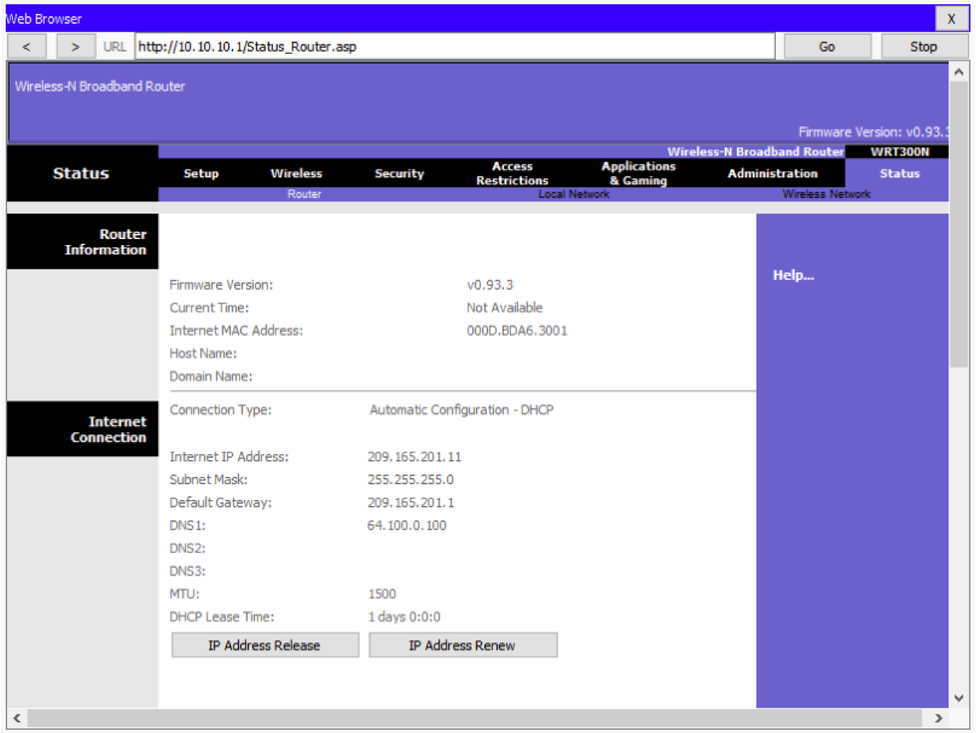
- Однако, если вы хотите расширить радиус действия примерно на 45 метров в помещении и на 90 метров на улице, вы можете добавить точки беспроводного доступа.
- Создайте сетку, добавив точки доступа с одинаковыми настройками, за исключением использования разных каналов для предотвращения помех.
- Расширение сети WLAN в небольшом офисе или дома становится все проще.
- Производители сделали создание беспроводной ячеистой сети (WMN) простым с помощью приложений для смартфонов.



NAT для IPv4

Как правило, беспроводной маршрутизатор назначает общедоступный маршрутизируемый адрес интернет-провайдером и использует адрес частной сети для адресации в локальной сети.

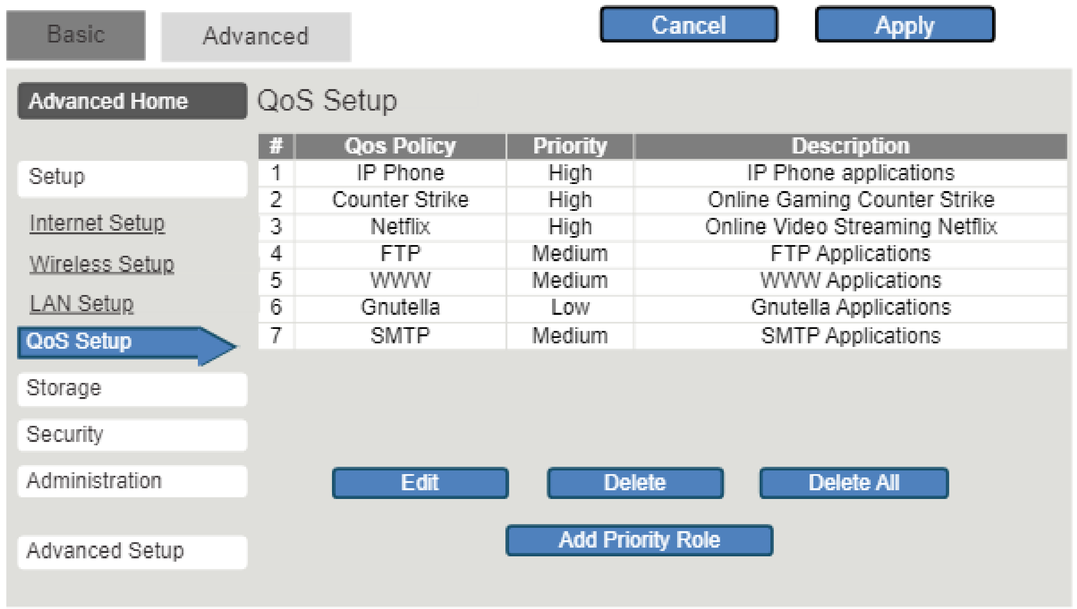
- Чтобы узлы локальной могли обмениваться данными с внешним миром, маршрутизатор будет использовать процесс, называемый преобразованием сетевых адресов (NAT).
- NAT переводит частный (локальный) IPv4-адрес источника в публичный (глобальный) адрес (для входящих пакетов процесс выполняется в обратном порядке).
- NAT делает это возможным, отслеживая номера портов источника для каждого сеанса, установленного устройством.
- Если у вашего интернет-провайдера включен IPv6, вы увидите уникальный IPv6-адрес для каждого устройства.



Настройка качества обслуживания (QoS)

Многие беспроводные маршрутизаторы имеют возможность настройки качества обслуживания Quality of Service (QoS).

- Можно добавить в сеть инструменты обеспечения качества обслуживания (QoS) и предоставить некоторым типам трафика, например голосу и видео, приоритет над трафиком, менее чувствительны к задержкам, таким как электронная почта и просмотр веб-страниц.
- На некоторых беспроводных маршрутизаторах трафик также может быть приоритетным для определенных портов.



Переадресация портов (Port Forwarding)

Беспроводные маршрутизаторы обычно блокируют порты TCP и UDP, чтобы предотвратить несанкционированный доступ в локальную сеть и из нее.

- Однако в некоторых случаях необходимо открыть некоторые порты, чтобы определенные программы и приложения могли связываться с устройствами в других сетях.
- Переадресация (также перенаправление или проброс) портов (Port forwarding) – это способ направления трафика между устройствами в различных сетях на основе правил.
- Включение портов (Port triggering) позволяет маршрутизаторы временно переадресовывать данные через входящие порты определенному устройству.
- Включение портов можно использовать для переадресации данных на компьютер, только если назначенный диапазон портов используется для создания исходящего запроса.

Packet Tracer – Configure a Wireless Network

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

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

Lab – Configure a Wireless Network

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

13.2 Конфигурация Базовой WLAN с контролем беспроводной сети

Video – Configure a Basic WLAN on the WLC

This video will cover the following:

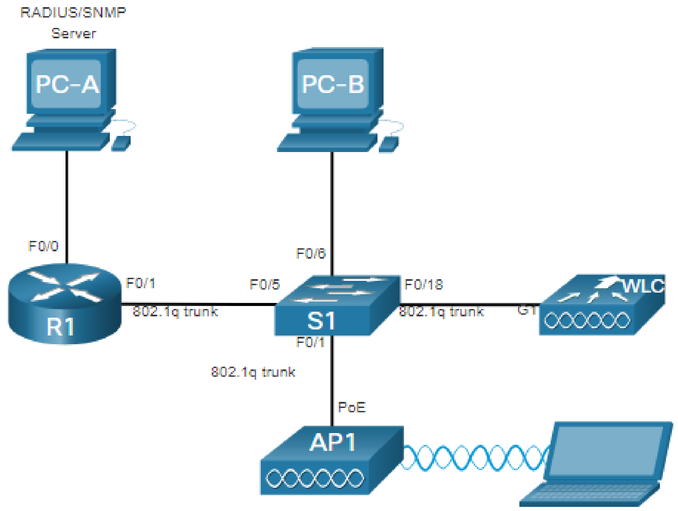
- Review the topology
- Access the GUI for the WLAN controller
- Information about the wireless network on the Network summary screen
- Configure a new WLAN
- Secure the new WLAN

Конфигурация Базовой WLAN с контролем беспроводной сети

WLC топология

Топология и схема адресации, используемые для этой темы, показаны на рисунке и в таблице.

- Точка доступа (AP) является AP на основе контроллера, в отличие от автономной AP, поэтому она не требует начальной настройки и часто называется облегченными AP (LAPs).
- LAPs используют протокол облегченной точки доступа (LWAPP) для связи с контроллером WLAN (WLC), как показано на следующем рисунке.
- Точки доступа, управляемые контроллером, рекомендуется использовать в случаях, когда в сети требуется много точек доступа.
- Поскольку больше AP добавлено, каждый AP автоматически настраивается и управляется WLC.



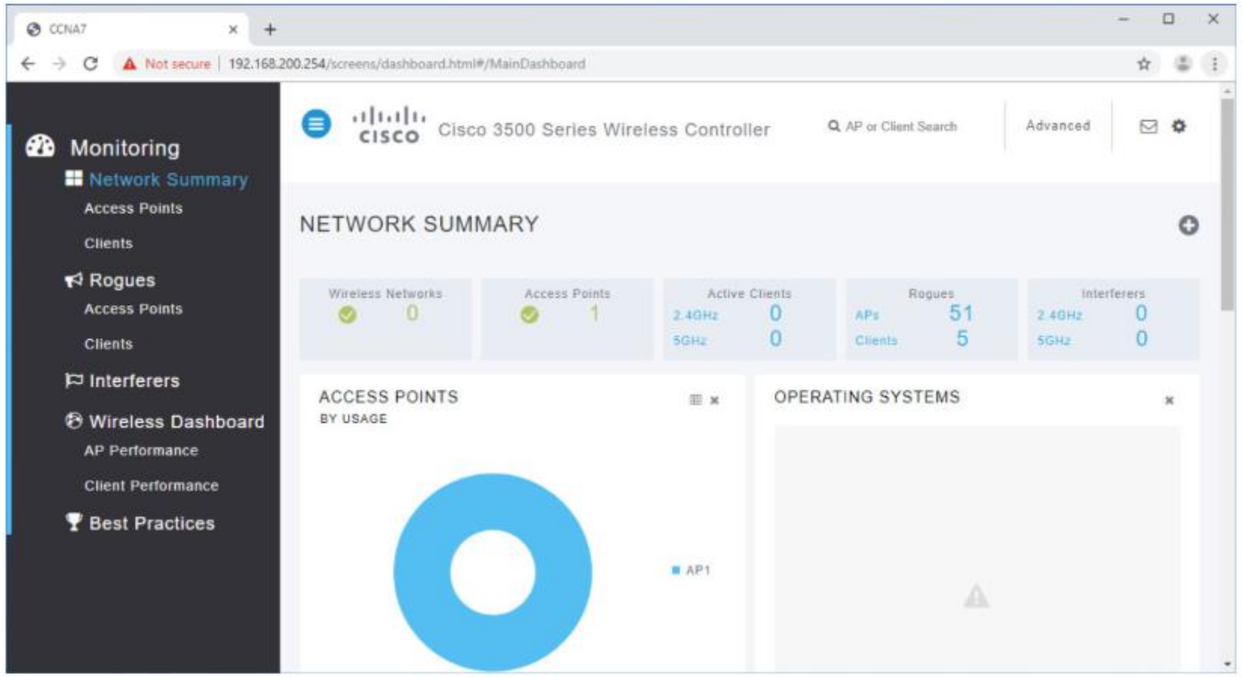
Устройство	Интерфейс	IP-адрес	Маска подсети
R1	F0/0	172.16.1.1	255.255.255.0
R1	F0/1.1	192.168.200.1	255.255.255.0
S1	VLAN 1	DHCP	
WLC	Управление	192.168.200.254	255.255.255.0
AP1	Сетевой адаптер	192.168.200.3	255.255.255.0
ПК-A	NIC	172.16.1.254	255.255.255.0
ПК-B	NIC	DHCP	
Ноутбук	NIC	DHCP	

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.

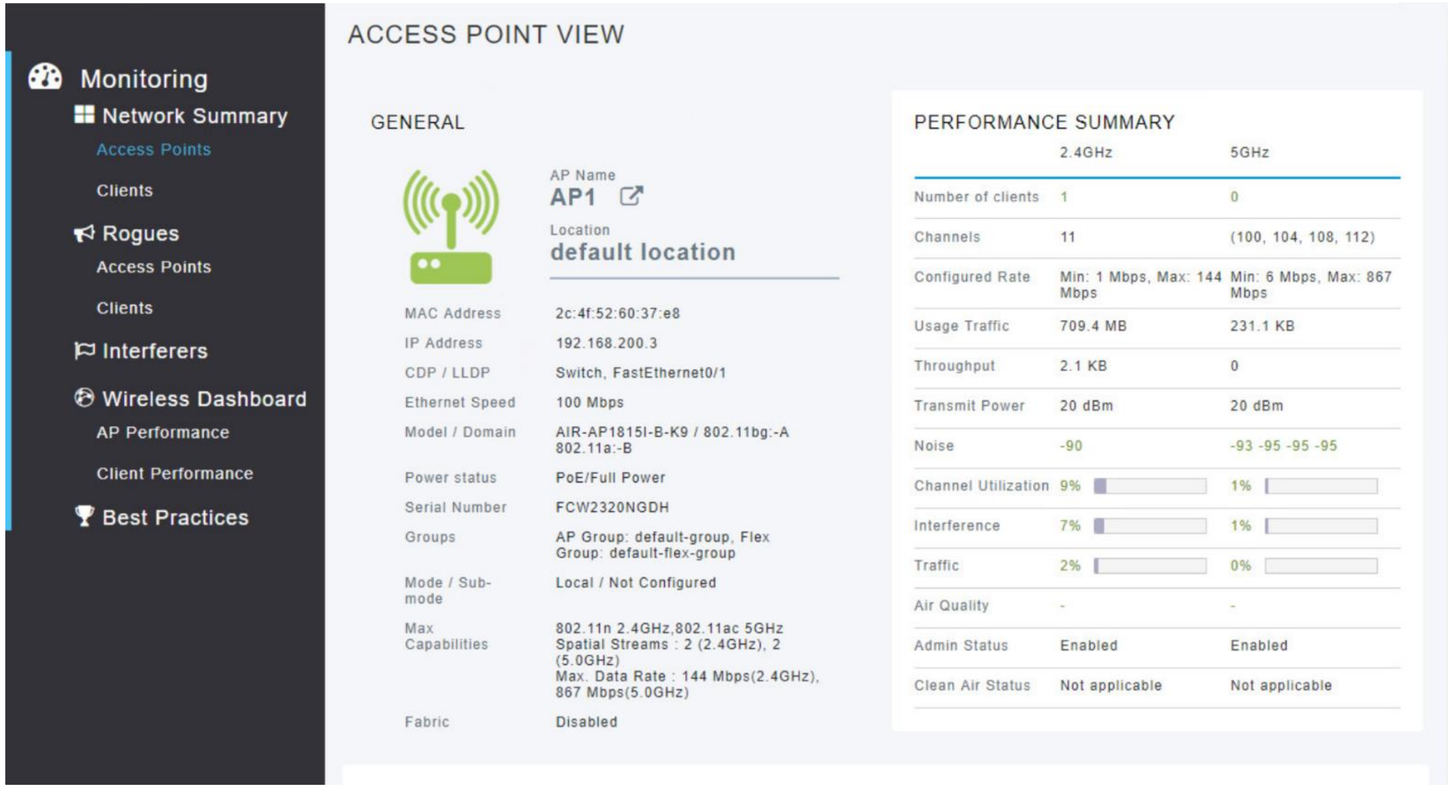
- The **Network Summary** page is a dashboard that provides a quick overview of configured wireless networks, associated access points (APs), and active clients.
- You can also see the number of rogue access points and clients.



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.

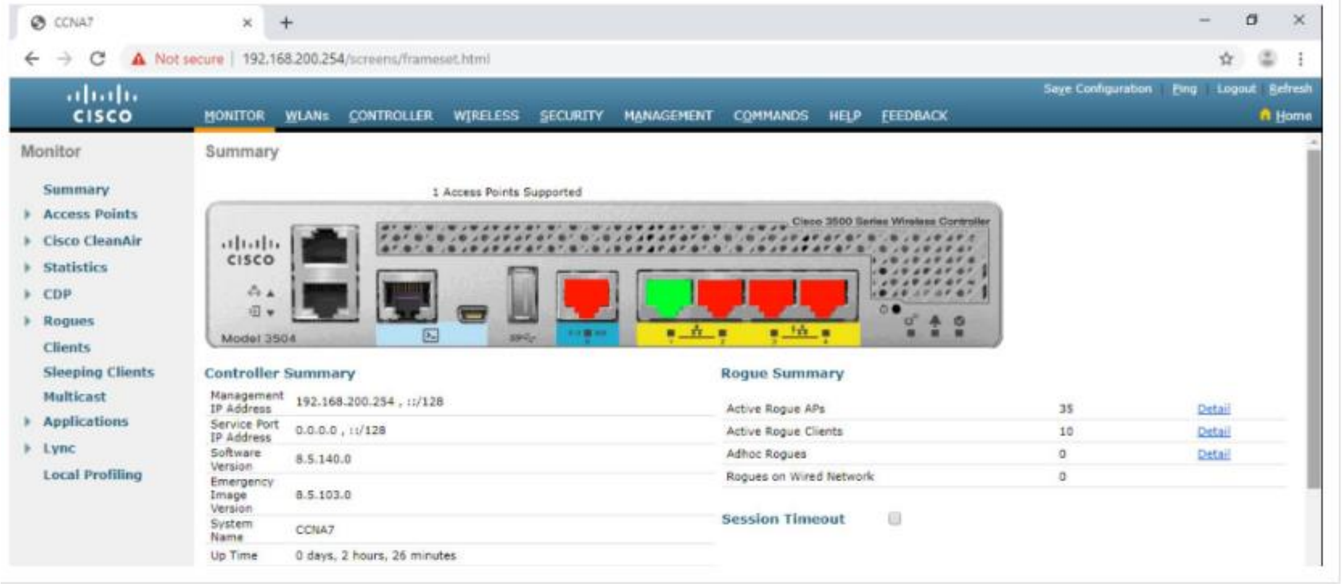


Advanced Settings

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

- However, as a network administrator, you will typically access the advanced settings.

- For the Cisco 3504 Wireless Controller, click **Advanced** in the upper right-hand corner to access the advanced **Summary** page.
- From here, you can access all the features of the WLC.



Configure a WLAN

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

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

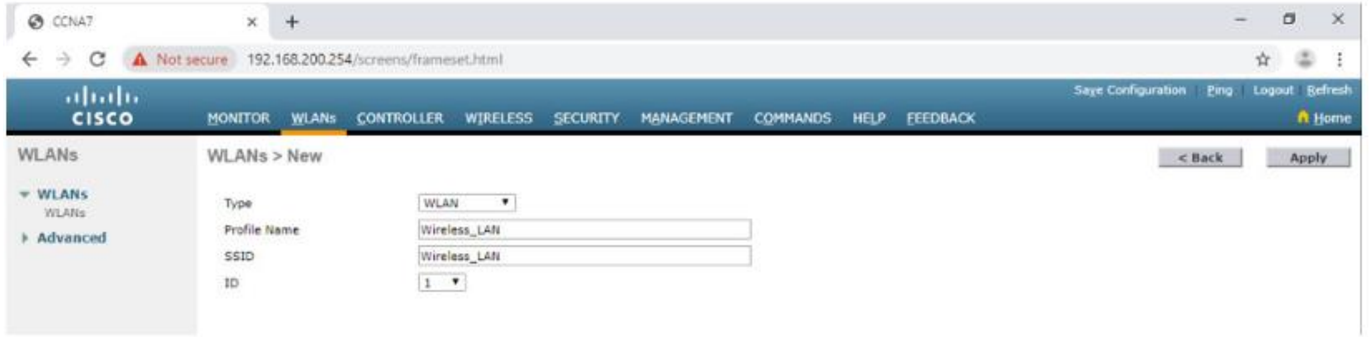
Configure a WLAN (Cont.)

Basic WLAN configuration on the WLC includes the following steps:

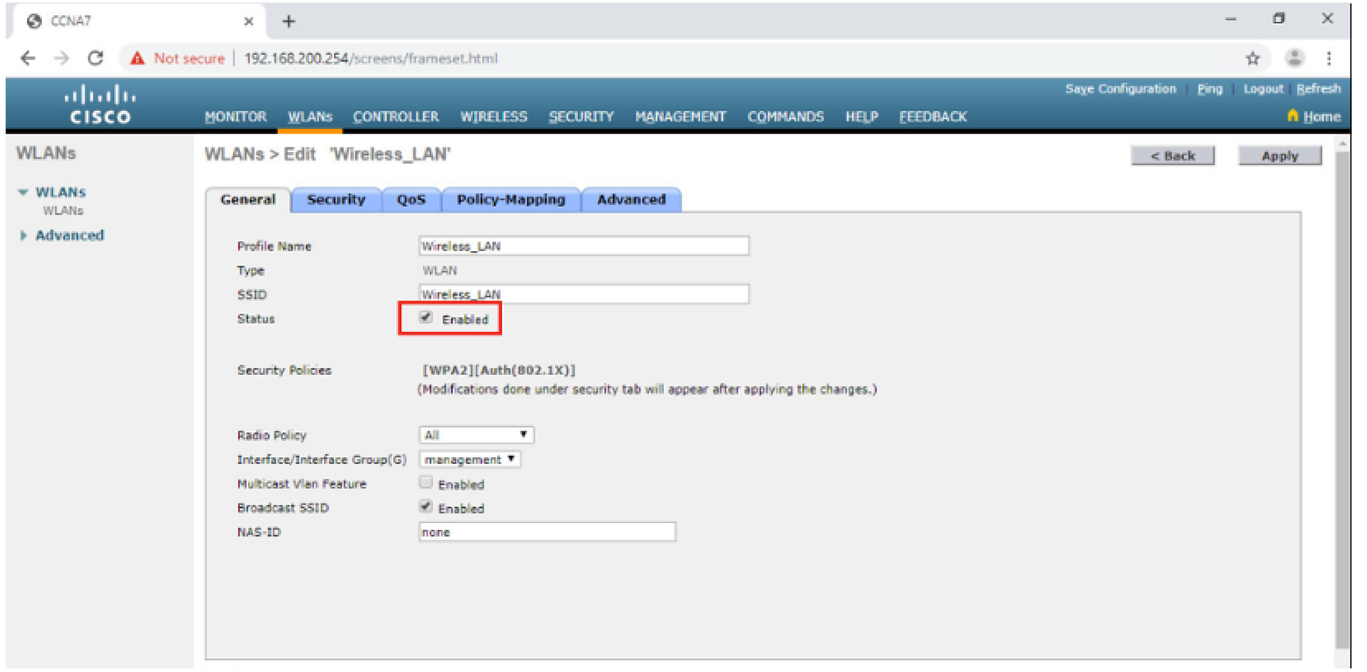
1. Create the WLAN
2. Apply and Enable the WLAN
3. Select the Interface
4. Secure the WLAN
5. Verify the WLAN is Operational
6. Monitor the WLAN
7. View Wireless Client Information

Configure a WLAN (Cont.)

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

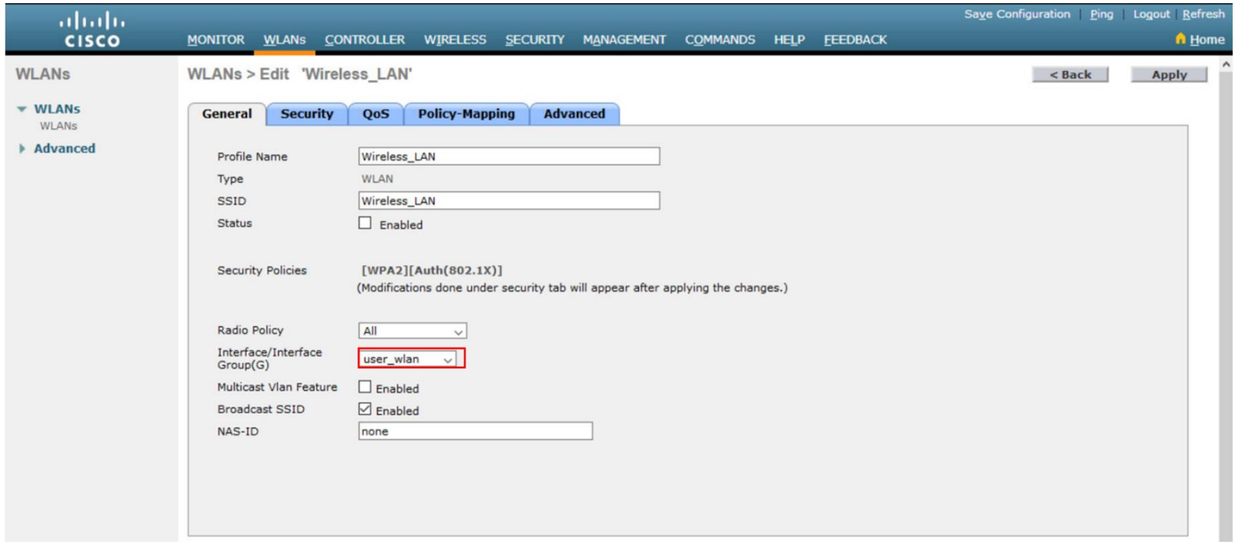


2. **Apply and Enable the WLAN:** Next the WLAN is enabled the WLAN settings are configured.

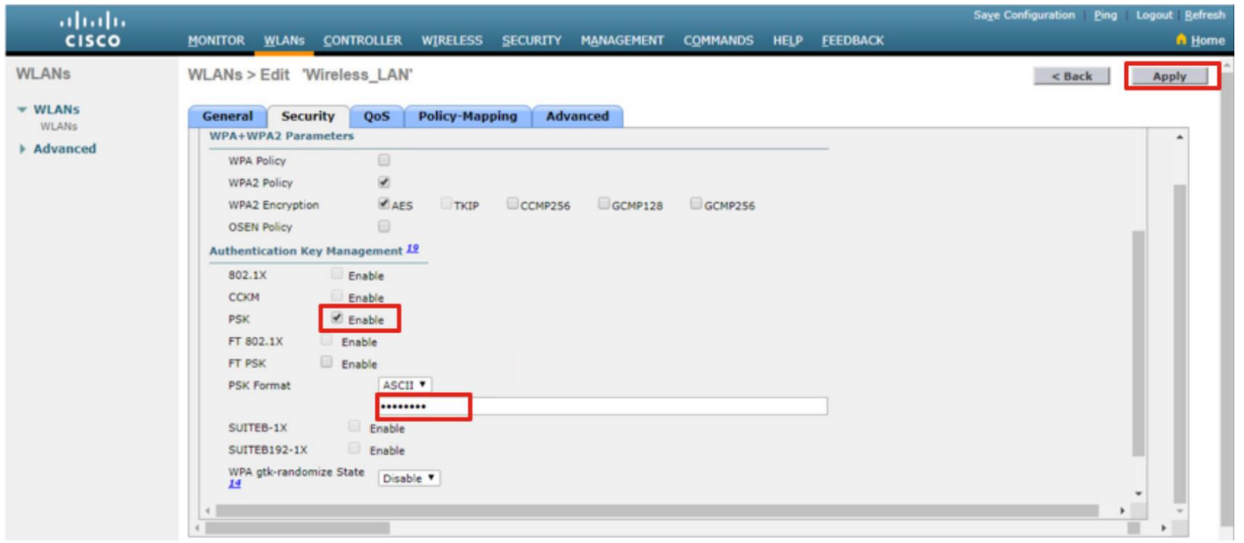


Configure a WLAN (Cont.)

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



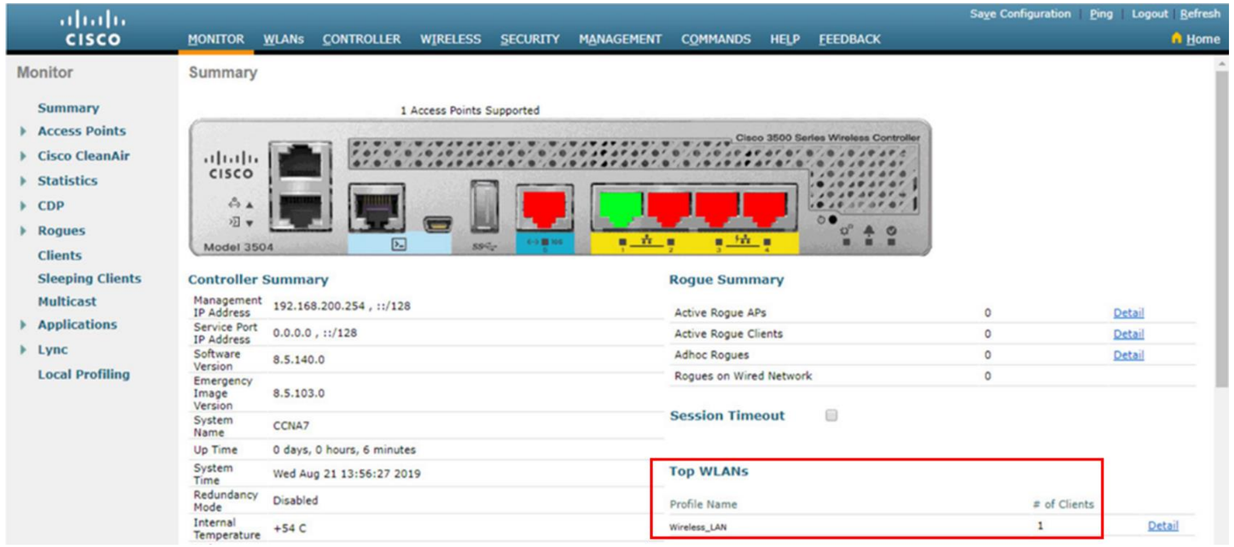
4. **Secure the WLAN**: The Security tab is used to access all the available options for securing the LAN.



Configure a 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.

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



Configure a WLAN (Cont.)

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

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 Конфигурация WPA2 Enterprise WLAN с контроллером беспроводной сети

Video – Define an SNMP and RADIUS Server on the WLC

This video will cover the following:

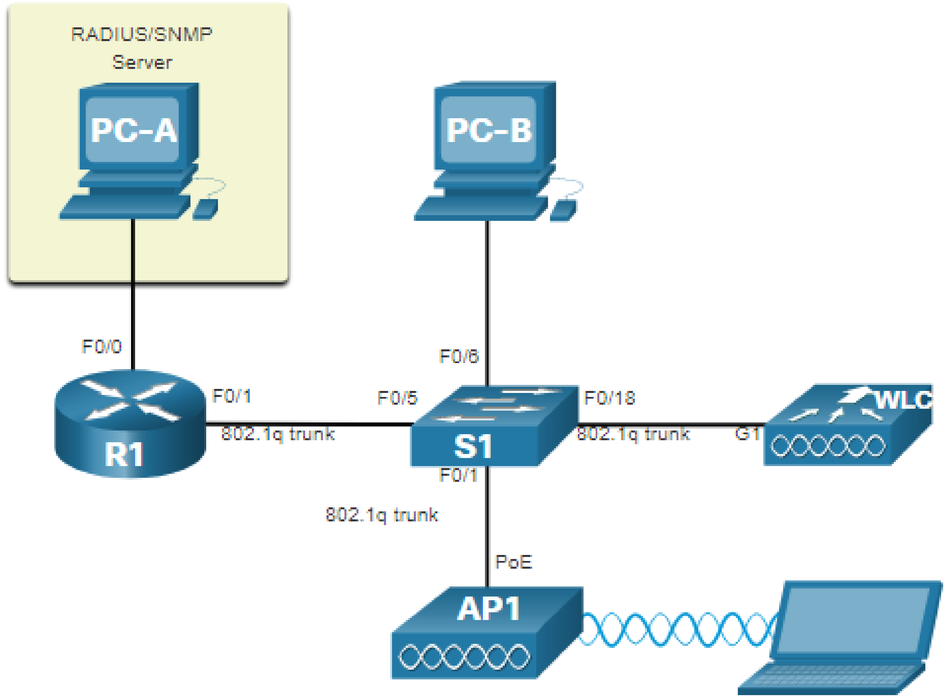
- Configure the WLAN controller to send SNMP traps to an external server
- Configure the WLAN controller to use an external RADIUS server to authenticate WLAN users
- Verify connectivity with the RADIUS server

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.

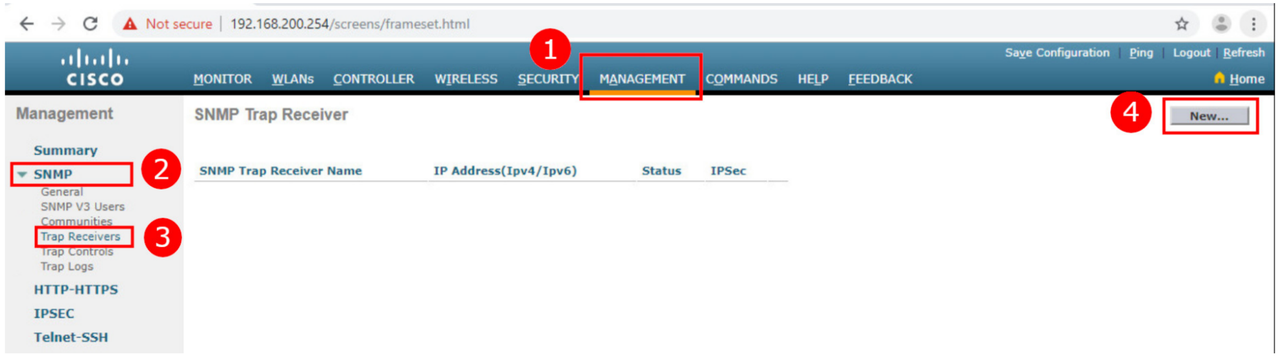
Note: SNMP server and RADIUS server configuration is beyond the scope of this module.



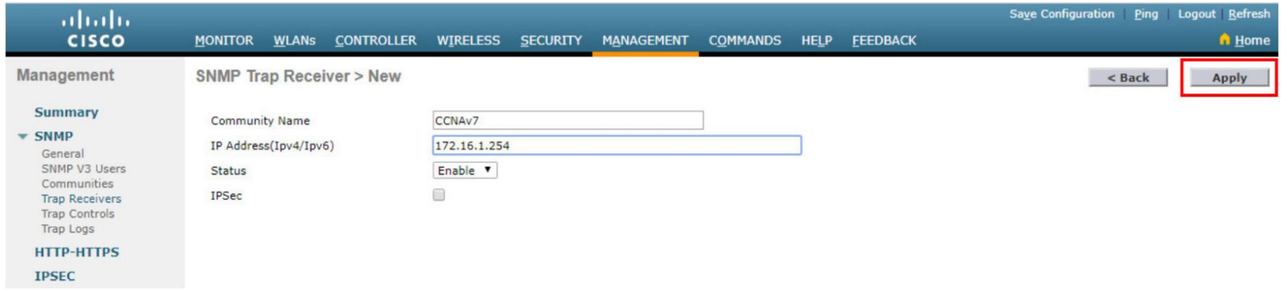
Configure SNMP Server Information

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.

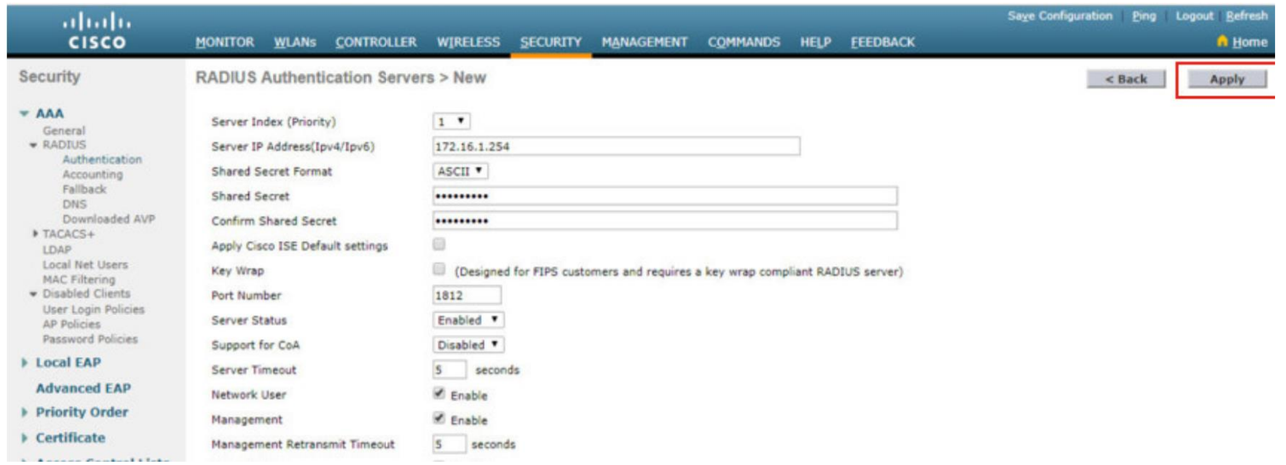


Configure RADIUS Server Information

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.

Video – Configure a VLAN for a New WLAN

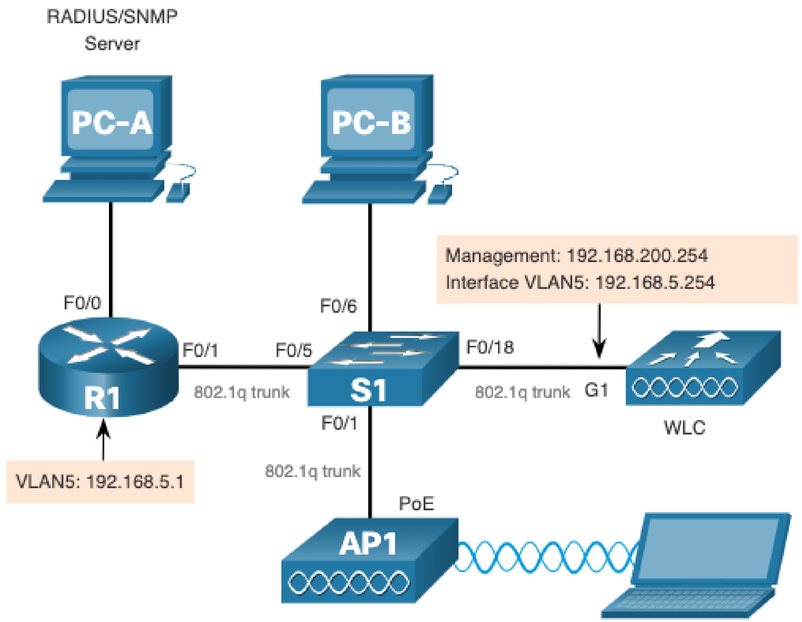
This video will cover the following:

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

Топология с адресацией VLAN 5

Каждой WLAN, настроенной на WLC, нужен собственный виртуальный интерфейс.

- WLC имеет пять физических портов данных, которые можно настроить для поддержки нескольких WLAN и виртуального интерфейса.
- Новая WLAN будет использовать интерфейс VLAN 5 и сеть 192.168.5.0/24, и поэтому R1 был настроен для VLAN 5, как показано в топологии и показывает **show ip interface brief**.




```
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#
```

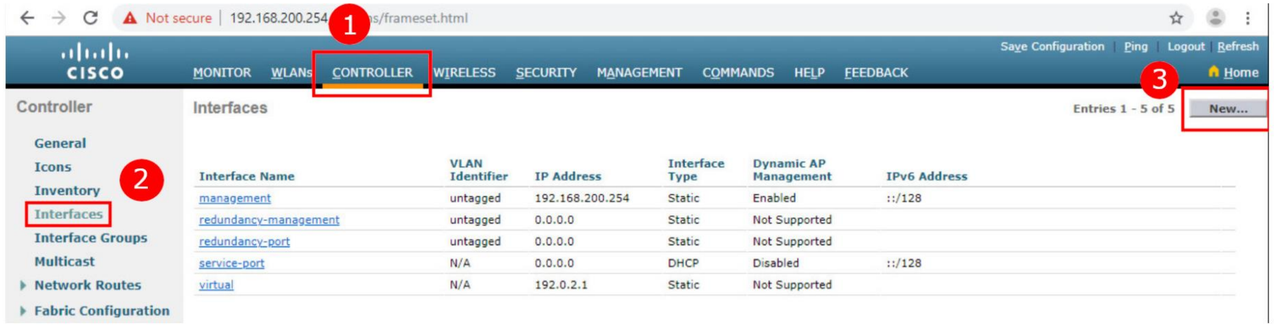
Конфигурация нового интерфейса

Конфигурация интерфейса VLAN на WLC включает следующие шаги:

1. Создать новый интерфейс.
2. Настройте имя и идентификатор VLAN.
3. Настройте порт и адрес интерфейса.
4. Настройте адрес DHCP-сервера.
5. Применить и Подтвердить.
6. Проверка состояния интерфейса.

Configure a New Interface (Cont.)

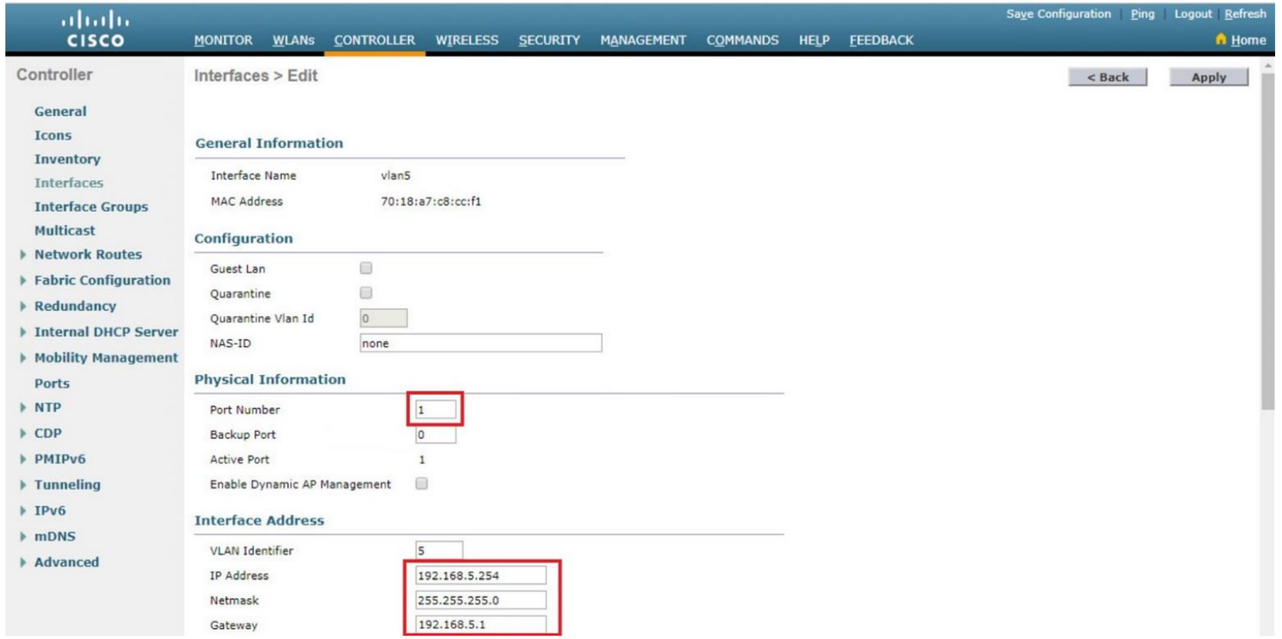
1. **Create a new interface:** Click **CONTROLLER > Interfaces > New...**



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

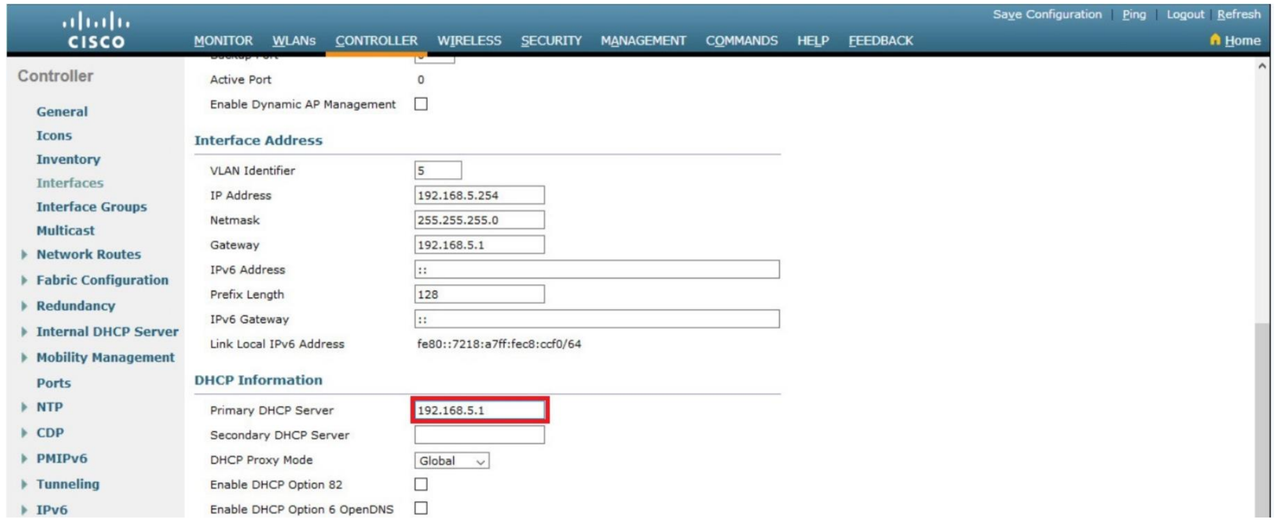
Configure a New Interface (Cont.)

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)

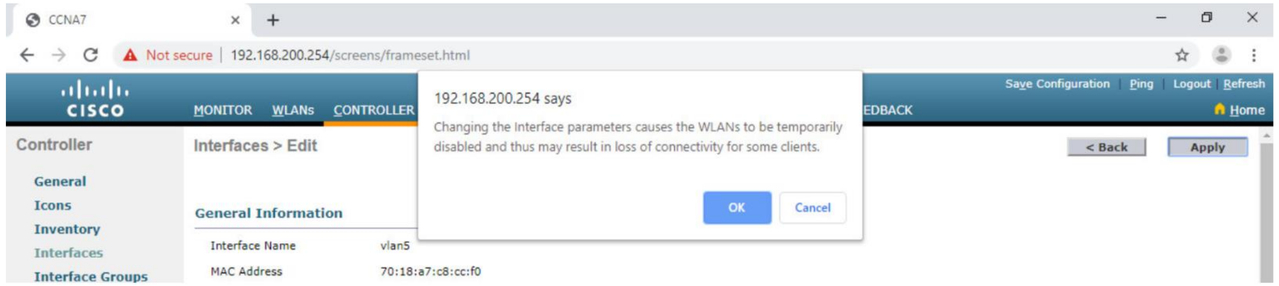


Configure a New Interface (Cont.)

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.

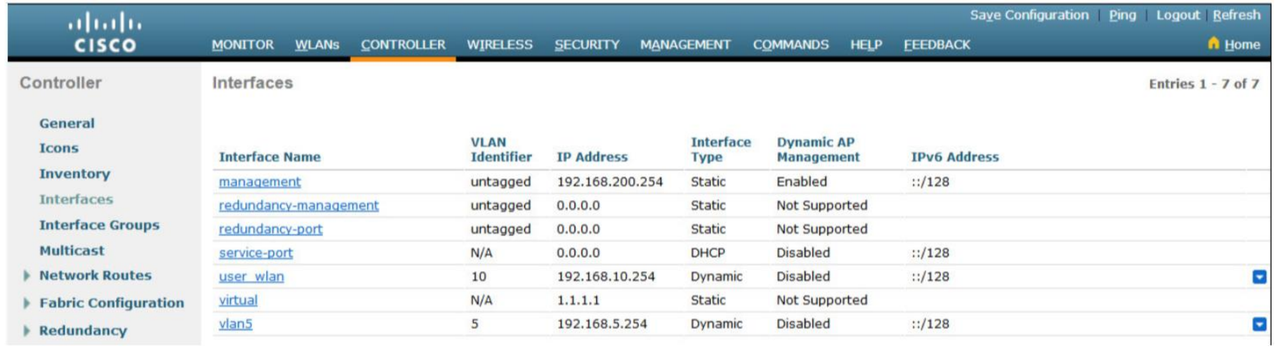


5. **Apply and Confirm:** Scroll to the top and click **Apply** and then click **OK** for the warning message.



Configure a New Interface (Cont.)

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



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

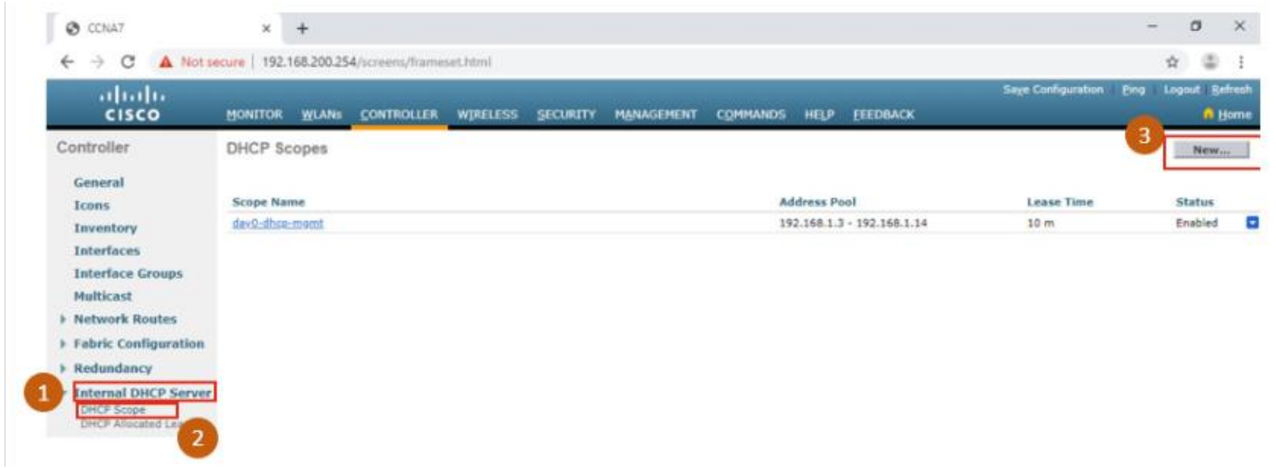
Конфигурация области DHCP

Настройка области DHCP включает следующие шаги:

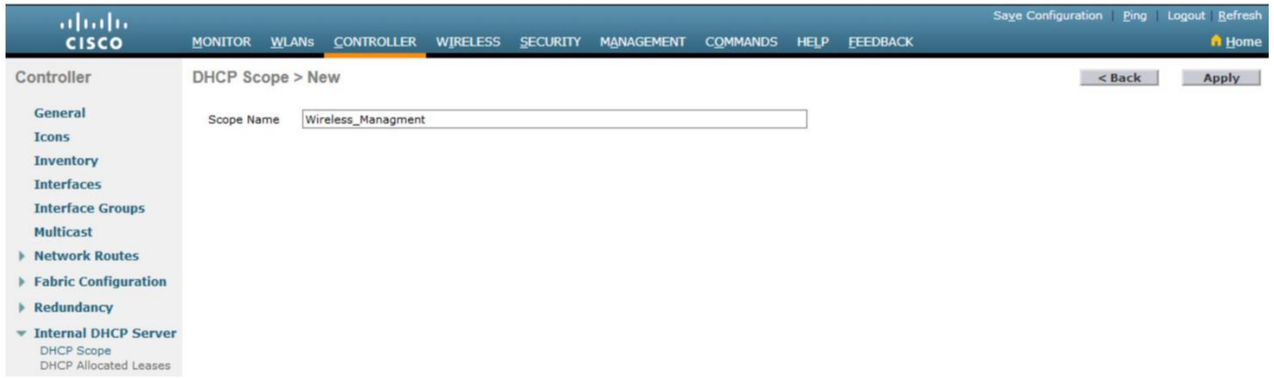
1. Создайте новую область DHCP.
2. Назовите область DHCP.
3. Проверьте новую область DHCP.
4. Настройте и включите новую область DHCP.
5. Проверьте включение области DHCP.

Configure a DHCP Scope (Cont.)

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



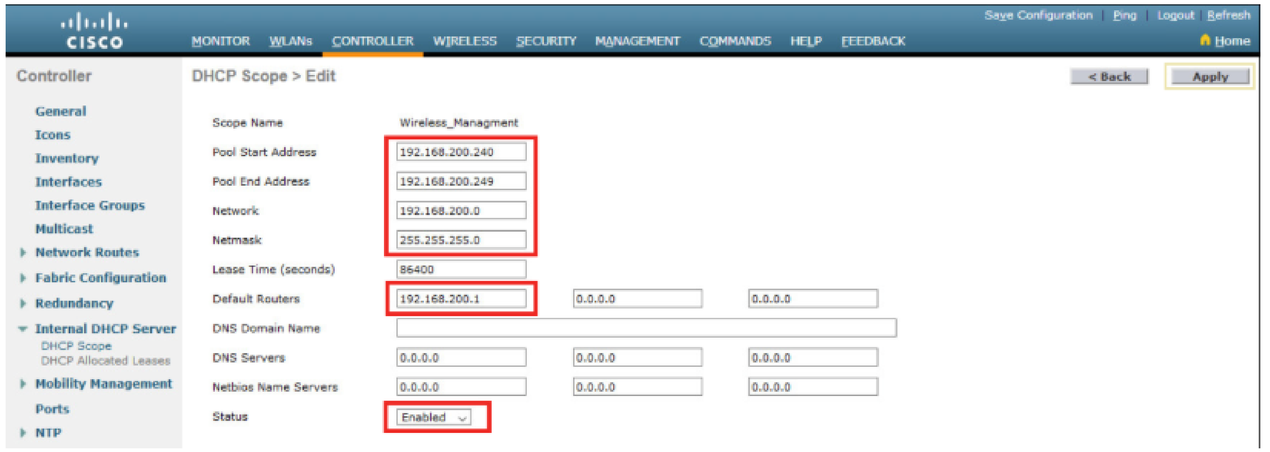
2. **Name the DHCP scope:** The scope is named **Wireless_Management** and then applied.



Configure a DHCP Scope (Cont.)

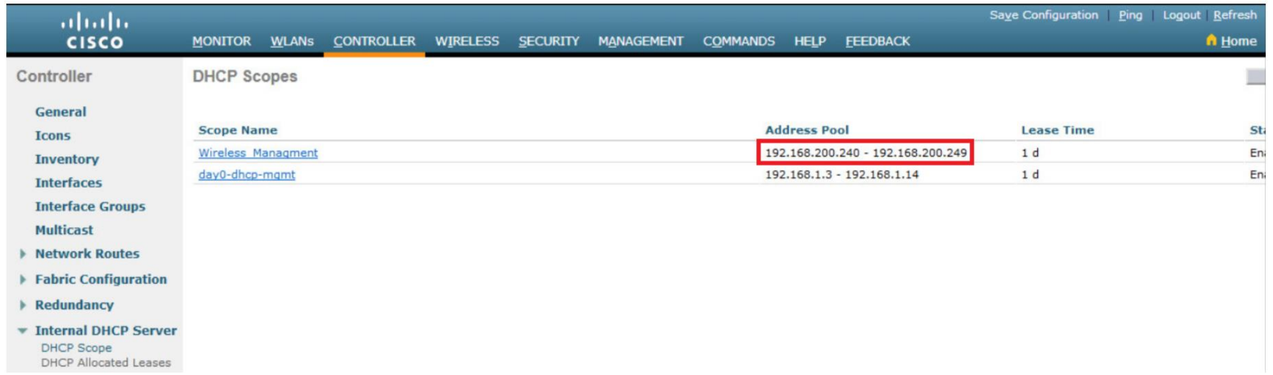
3. **Verify the new DHCP scope:** In the **DHCP Scopes** page click the new Scope Name to configure the DHCP scope.

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**.



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.



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).

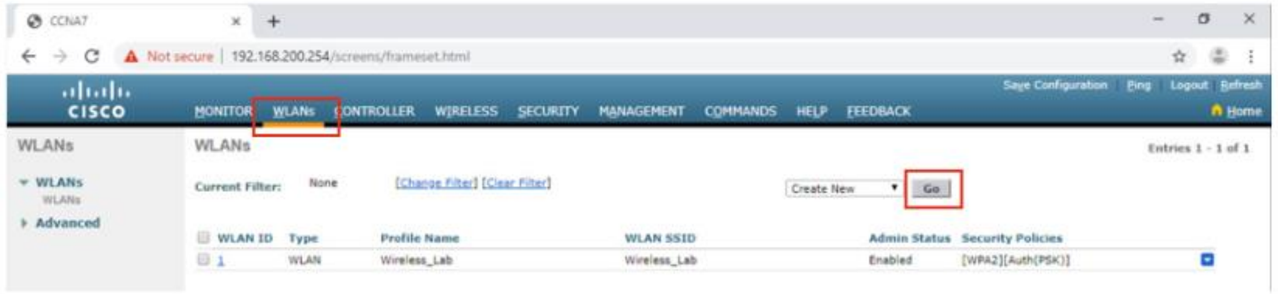
- 802.1X is the default key management protocol used to communicate with the RADIUS server.
- Next, create a new WLAN to use interface **vlan5**.

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

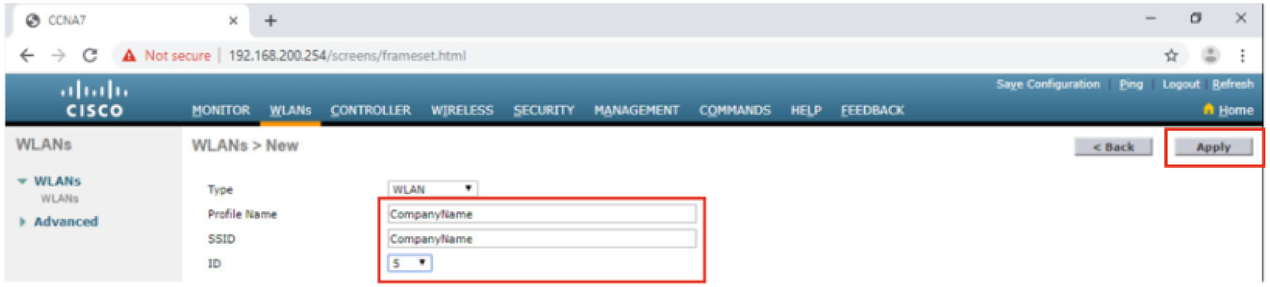
1. Create a new WLAN.
2. Configure the WLAN name and SSID.
3. Enable the WLAN for VLAN 5.
4. Verify AES and 802.1X defaults.
5. Configure WLAN security to use the RADIUS server.
6. Verify the new WLAN is available.

Configure a WPA2 Enterprise WLAN (Cont.)

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

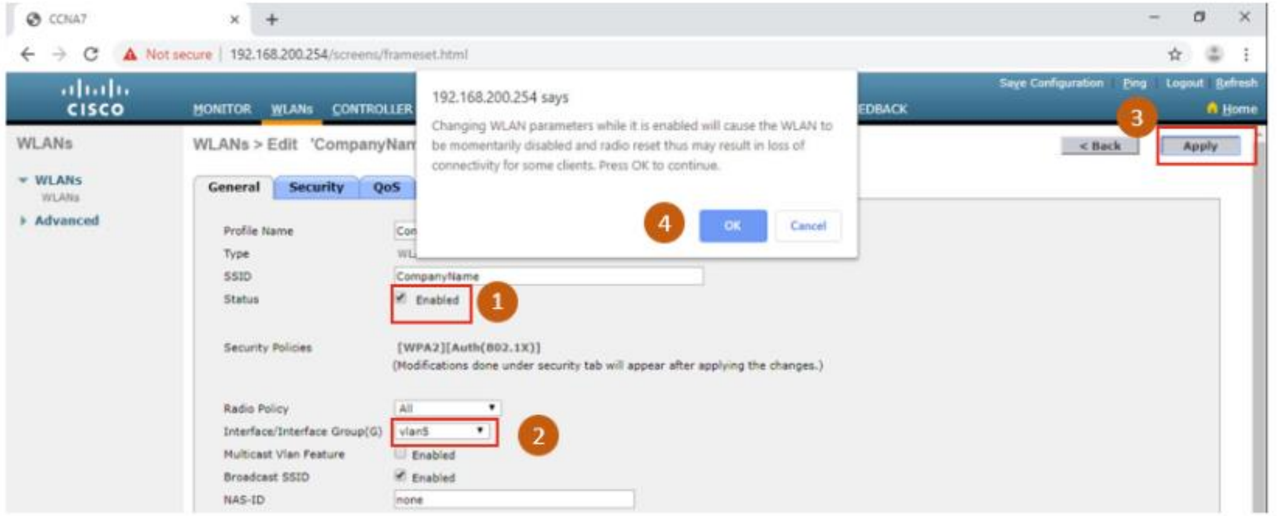


2. **Configure the WLAN name and SSID:** Enter the profile name and SSID, choose an ID of **5**, and then click **Apply** to create the new WLAN.

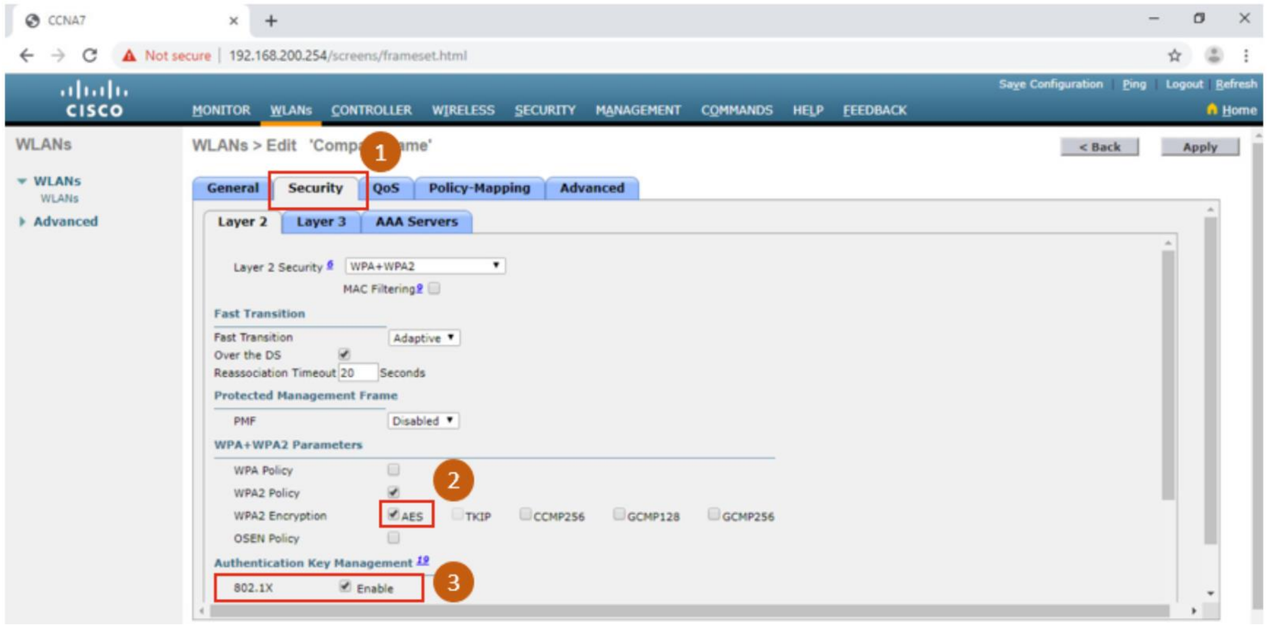


Configure a WPA2 Enterprise WLAN (Cont.)

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.

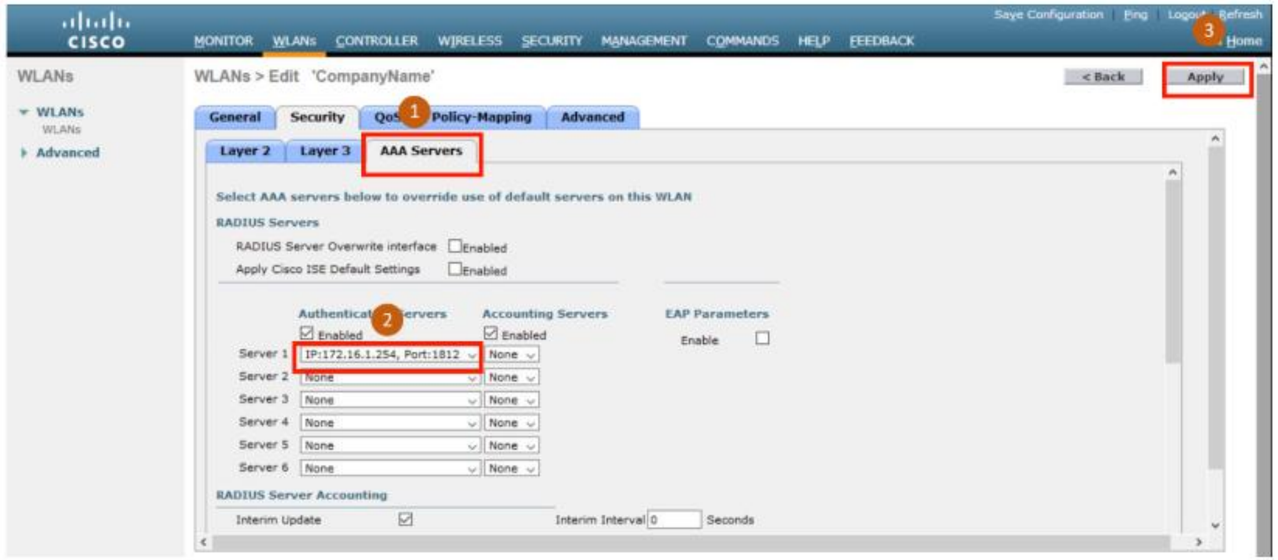


4. **Verify AES and 802.1X defaults:** Click the **Security** tab to view the default security configuration for the new WLAN.



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.



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

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 Поиск и устранение проблем с беспроводными локальными сетями

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.

Подходы к устранению неполадок (Продолжение)

Шаг	Название	Описание
1	Определение проблемы	Первым этапом процедуры поиска и устранения неполадок является определение проблемы. На этом этапе можно использовать различные методы, в том числе, можно расспросить пользователя, что может оказаться очень полезным.
2	Формирование предложений о возможных причинах неполадки	После разговора с пользователем и определения проблемы можно попытаться сформировать предположения о ее возможных причинах. Обычно на этом этапе выявляется несколько возможных причин неполадки.
3	Проверка предположений о причине неполадки	Проверьте свои предположения о вероятных причинах неполадки, чтобы определить истинную причину. Технический специалист может попытаться устранить неполадку, применив быструю процедуру. Если с помощью быстрой процедуры не удается устранить неполадку, следует продолжить поиск точной причины.
4	Разработка плана действий по устранению неполадки и его реализация	Установив точную причину неполадки, разработайте план действий для ее устранения и реализуйте его.
5	Полная проверка функционального состояния системы и принятия профилактических мер	После устранения неполадки выполните полную проверку функционального состояния системы и при необходимости примите профилактические меры.
6	Документирование полученных данных, принятых мер и результатов	На последнем этапе процедуры поиска и устранения неполадок выполняется документирование полученных данных, выполненных действий и результатов. Эта информация очень важна для использования в будущем.

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.

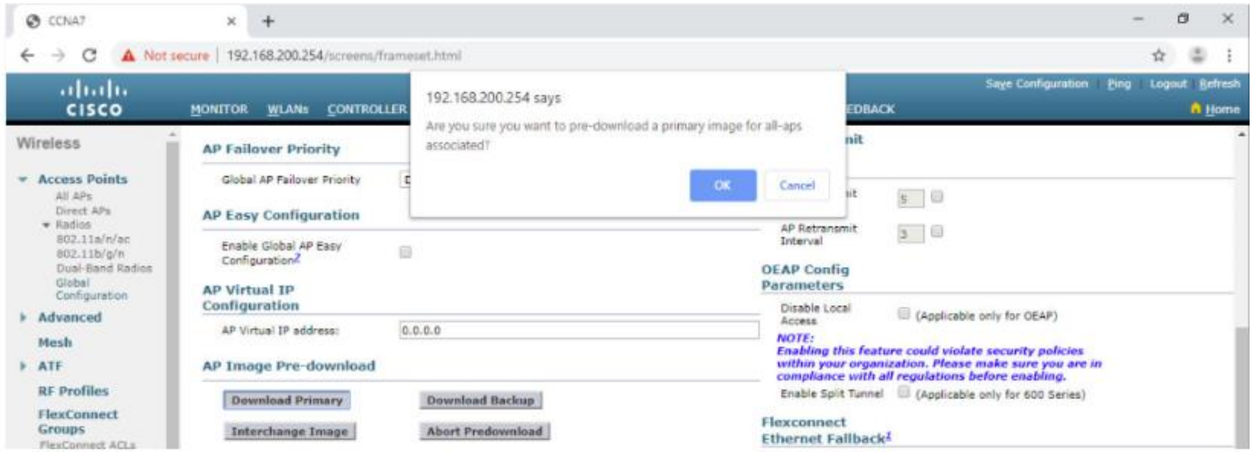
- These block the signal, which shortens the range of the WLAN.
- If this still does not solve the problem, then a Wi-Fi Range Extender or deploying the Powerline wireless technology may be used.

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

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 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.


CISCO